



Passwort-Safes für den PC

Sichere Passwörter haben einen Haken: Kein Mensch kann sie sich merken. PC Professionell testet neun Passwort-Manager, die Ihre Kennwörter speichern und bei Bedarf automatisch hervorkramen. /// Artur Hoffmann, Rüdiger Pein

Ausspionierte PINs und TANs oder ein gehackter E-Mail- oder eBay-Account kosten Anwender viel Geld und Nerven. Dabei sind sie oft selbst schuld daran, denn noch immer wird mit Zugangsdaten zu lax umgegangen: Da werden Passwörter zu einfach gewählt oder es wird der Einfachheit überall dasselbe verwendet, sie liegen als Textdatei auf der Festplatte oder kleben auf gelben Post-its am Monitor.

Allerdings sind solche Verhaltensweisen auch durchaus verständlich, denn richtig gute Passwörter kann sich kaum jemand merken. Laut einer aktuellen Bitkom-Umfrage hat ein PC-Nutzer im Schnitt fünfzehn bis zwanzig verschiedene Zugangsdaten. Und Admins müssen echte Gedächtniskünstler sein, da sie

oft sogar mit über sechzig Kennwörtern jonglieren. Eine Möglichkeit wäre, die Passwörter aufzuschreiben und in einem Safe zu hinterlegen. Das ist jedoch mühsam und in vielen Fällen nicht praxistauglich.

Eine sichere, aber komfortablere Alternative bieten virtuelle Safes in Form von Passwort-Managern. Statt mit Dutzenden Kennwörtern zu hantieren, merken Sie sich nur noch ein einziges. Damit verschaffen Sie sich Zugang zur Programm-Datenbank, die verschlüsselt auf Festplatte gespeichert ist und in der alle Kennwörter abgelegt sind.

Guter Schutz muss dabei keineswegs teuer sein: Die neun Probanden im PCpro-Test kosten zwischen 0 und 36 Euro. Der Test-

INHALT

114 Flexible Sicherheitsverwahrung

Neun Passwort-Safes im Test

116 Passwörter im Browser verwalten

Internet Explorer, Firefox und Opera

120 Sichere Hardware-Lösungen

Smartcard-Chips und Biometrie

122 Ausstattungstabelle

Alle Testergebnisse im Überblick

sieger Acebit Password Depot ist für 30 Euro zu haben, den Budget-Tipp Keepass Password Safe gibt es sogar kostenlos.

Nicht alle Safes sind sicher

Positiv: Seit dem letzten Test in PC Professionell 7/2006 (als PDF-Datei auf Heft-CD) haben viele Hersteller die Kritik beherzigt und den Großteil der Mängel beseitigt. Doch nach wie vor garantieren nicht alle Passwort-Safes uneingeschränkte Sicherheit. So legen Archicrypt Password Safe und Password Manager XP die Zugangsdaten gänzlich unverschlüsselt im Arbeitsspeicher ab. Ein Trojaner könnte dort nach Login-URLs wie <http://signin.ebay.de> suchen und benachbarte Speicherbereiche mit dem Passwort im Klartext an einen Betrüger schicken.

Auch beim Schutz gegen Keylogger müssen vier Testkandidaten passen: Ein Spion kann bei 1 Password Pro sowie den drei Letztplatzierten unbemerkt Tastatureingaben mitzuschreiben oder den Inhalt der Zwischenablage auslesen. Der ungeschützte und umständliche Umweg über die Zwischenablage ist ohnehin nicht empfehlenswert: Ein guter Passwort-Manager trägt die Zugangsdaten entweder automatisch ein oder bietet dafür eine Drag-and-Drop-Funktion.

Um die Sicherheit der Zugangsdaten auf der Festplatte muss sich der Anwender nach aktuellem Wissensstand bei keinem der Programme Sorgen machen. Selbst wenn die Datenbank in falsche Hände gerät, sind Knackversuche zum Scheitern verurteilt – sofern Sie ein sicheres Master-Passwort oder eine Schlüsseldatei verwenden. Alle Tools schützen die Daten zumindest mit AES-Verschlüsselung oder mit der ebenfalls sehr sicheren Twofish-Chiffrierung.

Alternativen zu den Passwort-Safes

Neben den getesteten Software-Safes gibt es eine Reihe Alternativen. Diese können Sie als primäre Kennwort-Verwaltung oder als Ergänzung zu einem der Testkandidaten einsetzen.

Empfehlungen der Redaktion

DIE 5 BESTEN PASSWORT-SAFES

- | | | |
|-----|-----------------------------------------------------------------------|-------------|
| [1] | Password Depot 3.1.4
Acebit | 91,3 |
| [2] | Password Safe and Repository 2006 Professional 4.4.3
Mateso | 90,0 |
| [3] | Password Safe 3.3
Bagusoft | 82,6 |
| [4] | 1 Password Pro 5.65
Heiko Schröder | 82,5 |
| [5] | Keepass Password Safe 1.06
Dominik Reichl | 79,8 |
- Produkt, Hersteller max. 100 Punkte



Acebit Password Depot 3.1.4

Umfassender Schutz, eine intuitive Bedienführung und ausgezeichnete Verwaltungsfunktionen zeichnen Acebit Password Depot aus. Im Test überzeugen auch die Netzwerkfähigkeit und das einfach zu konfigurierende Ausfüll-Feature. Für Privatanwender und Business-Nutzer gleichermaßen geeignet.



Keepass Password Safe 1.06

Auch wenn Keepass nur den fünften Platz erreicht: Das Open-Source-Tool schützt Kennwörter vor fremden Augen und ist einfach zu bedienen. Nur beim Ausfüllen von Webformularen und bei der Netzwerkfähigkeit gibt es Abzüge. Die Budget-Empfehlung ist somit erste Wahl für den Privatanwender.

zen. Kein Passwort-Manager im herkömmlichen Sinn ist zum Beispiel Roboform Pro (www.robiform.de). Das Einsatzgebiet dieser Software ist das automatische Ausfüllen von Webformularen und das Einloggen bei passwortgeschützten Webseiten. In der Praxis funktioniert dies fehlerfrei und ohne die Zwischenablage – Datenspione beißen sich also die Zähne aus. Haben Sie mehrere Konten bei einem Webservice, stellt Ihnen das Tool nach dem Aufruf der Webseite alle Anmeldedaten der programmeigenen Datenbank zur Verfügung. Sie können also gezielt auswählen, unter welchem Benutzernamen Sie sich einloggen wollen. Auch das Auslesen von Webformularen funktioniert einwandfrei. Die Software erkennt, dass Sie Ihre Zugangsdaten in ein Webformular getippt haben, und erkundigt sich, ob diese Angaben in einem als Pass Card bezeichneten Datensatz gespeichert werden sollen.

Roboform Pro unterstützt bis auf Opera alle Browser. Ein Einsatz auf USB-Sticks, U3-kompatiblen Medien sowie Palm- und Windows-Mobile-PDAs ist ebenfalls möglich. Die kostenlose Version speichert zehn Pass Cards, das Vollprodukt kostet 27 Euro.

Passwörter im Web speichern

Online sind Kennwörter auf den ersten Blick besonders schlecht aufgehoben: Selbst wenn Sie dem Anbieter eines Dienstes blind vertrauen, bliebe immer noch die Gefahr, dass die Zugangsdaten durch einen Hackerangriff in falsche Hände geraten. Der Online-Dienst Password Sitter (www.passwordsitter.com) geht daher einen anderen Weg und setzt auf einen Algorithmus des Fraunhofer-Instituts für Sichere Informationstechnologie. Bei der Anmeldung legt der Nutzer ein Master-Passwort fest, das per Einweg-Funktion verschlüs-

selt auf dem Server abgelegt wird. Es dient nur zur Anmeldeüberprüfung, das eigentliche Kennwort kann aus dem verschlüsselten Datensatz nicht rekonstruiert werden. Anhand des Master-Passworts berechnet ein Algorithmus für jedes gewünschte Internetportal ein Kennwort, das standardmäßig zwanzig Zeichen lang ist. Damit ersetzen Sie Ihr bisheriges Kennwort für das jeweilige Internetportal, und zwar über die Zwischenablage.

Der Vorteil: Außer dem verschlüsselten Masterkey liegen keinerlei Anmeldeinfos auf dem Server. Mit einem lokal gespeicherten Profil und einer kostenlosen Java-Anwendung ist Password Sitter zudem für den Offline-Betrieb geeignet. Für künftige Anmeldevorgänge brauchen Sie nur einen PC mit Browser und mindestens Java 1.5. Sie melden sich mit Ihrem Master-Passwort bei Password Sitter an und lassen sich jeweils in Echtzeit wieder die passenden Kennwörter berechnen. Diese Art der Kennwort-Verwaltung hat aber auch Nachteile: Lauert ein Keylogger im System, kann er die Zwischenablage auslesen. Bis zu fünf Zugangsdatensätze speichert Password Sitter kostenlos. Wer mehr will, zahlt für



Clever: Mobilesitter für Handys und PDAs verrät Angreifern nicht, ob das eingegebene Passwort korrekt ist oder nicht.



Statt Passwörter online zu speichern, berechnet sie Password Sitter jedes Mal neu.



Software auf Heft CD/DVD

- | | |
|------------------------------------------------------|-----------|
| 1 Password Pro 5.65 | 1PASS |
| Acebit Password Depot 3.1.5 | ACEBIT |
| Archicrypt Password Safe 4.0.4 | PASSAFE |
| Bagusoft Password Safe 3.3 | BAGUPASS |
| Keepass Password Safe 1.06 | KEEPASS |
| Password Safe and Repository 2006 Professional 4.4.3 | PSR |
| Password Manager XP 2.2.377 | PASSMAN |
| Roboform Pro 6.9.1 | ROBOFORM |
| Subsembly Wallet Desktop 1.4 | WALLET |
| Viskeeper Pro 3.1.0 | VISKEEPER |

bis zu 25 Passwörter eine Jahresgebühr von 10 Euro. Ein unbegrenztes Kontingent erhalten Sie für 15 Euro im Jahr.

Mit einem ähnlichen Verfahren nutzt das Fraunhofer-Institut das Handy als sicheren Datenspeicher. In der Software Mobilesitter, die ab Mai für rund 10 Euro erhältlich sein soll (www.mobilesitter.de), legt der Nutzer ein Master-Passwort fest. Damit werden PINs, TANs und Passwörter verschlüsselt und auf dem Handy abgespeichert. Der Clou: Bei der Eingabe eines falschen Master-Passworts zeigt die Software keine Fehlermeldung, sondern generiert einfach falsche Passwörter. Voraussetzung für den Betrieb ist ein beliebiges Handy oder ein anderes mobiles Endgerät mit Java ME und einer Displaybreite von mindestens 160 Pixeln.

Codes im Kreditkartenformat

Wer seine Passwörter doch lieber aufschreibt, sollte sie zumindest verschlüsselt zu Papier

bringen. Eine solche Möglichkeit bietet die Software Codestar (www.s-a-d.de, 20 Euro), allerdings nicht ganz ohne Sicherheitsrisiken. In Codestar tippen Sie bis zu acht Kennwörter ein und legen ein Master-Passwort fest. Anhand dieses Master-Passworts werden die



»Natürlich kann sich niemand sichere Passwörter merken. Das ist aber keine Ausrede dafür, sich nicht um ein ordentliches Passwort-Management zu kümmern.« /// Rüdiger Pein, Redakteur Security

Zeichen der übrigen Kennwörter durcheinander gewürfelt. Die so generierte Matrix drucken Sie auf die mitgelieferten Laminatbögen im Kreditkartenformat, die Sie immer mit sich führen können.

Das Master-Passwort dient dem Anwender auch als Passwort-Schlüssel. Da die Matrix keine kompletten Zugangsdatensätze spei-

chern kann, eignet sich das Verfahren nur für einfache Passwörter oder PINs.

Das Codestar-Prinzip klingt zwar zunächst einleuchtend, dennoch raten wir ab. Die Software hat drei gravierende Schwachstellen: Das Hauptkennwort ist in seiner

Komplexität sehr eingeschränkt, da es lediglich aus Großbuchstaben bestehen darf und Buchstabendoppler nicht erlaubt sind. Darüber hinaus ist der Zeichensatz offen ersichtlich, was eine Brute-Force-Angriffe enorm erleichtert. Besonders schlimm: Ist ein Passwort bekannt, kann daraus auf die restlichen geschlossen werden. _____ RPE

Flexible Sicherheitsverwahrung Neun Passwort-Safes müssen im Testlabor zeigen, ob sie Kennwörter sicher und komfortabel verwalten.

Passwortverwaltungen haben einen schweren Job: Sie sollen einfach zu bedienen sein und Eingabefelder im Browser automatisch ausfüllen. Nutzer wollen sie auf dem USB-Stick mitnehmen, und im Unternehmenseinsatz müssen sie natürlich netzwerkfähig sein. Dass sie bombensicher vor Datenspionen zu schützen haben, versteht sich von selbst. Den insgesamt besten Schutz bietet neben den Produkten auf den ersten drei Plätzen (Acebit Password Depot, Mateso Password Safe and Repository und Bagusoft Password Safe) der PCpro-Budget-Tipp Keepass Password Safe.

tern, die Datenbanken von sechs Programmen einzusehen. Zwei davon – Archicrypt Password Safe und Password Manager XP – zeigen sogar alle Zugangsdaten im Klartext an. Erschwerend kommt hinzu, dass Benutzernamen und Kennwörter untereinander angeordnet sind, so dass die Zuordnung problemlos möglich ist. PCpro rät vom Einsatz dieser Programme ab.

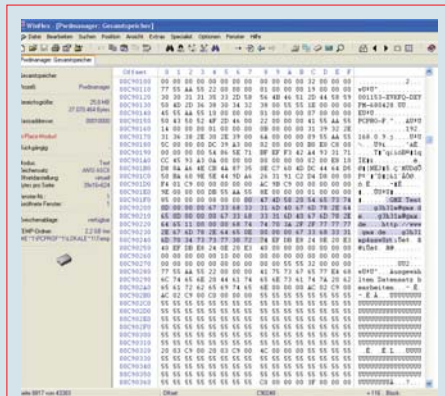
1 Password Pro, Acebit Password Depot, Keepass Password Safe und Mateso Password Safe laden zwar Benutzername, URL und Notizen unverschlüsselt in den Arbeitsspeicher, die Passwörter sind aber zumindest nicht im Klartext zu finden.

Sicherheitslücke Arbeitsspeicher

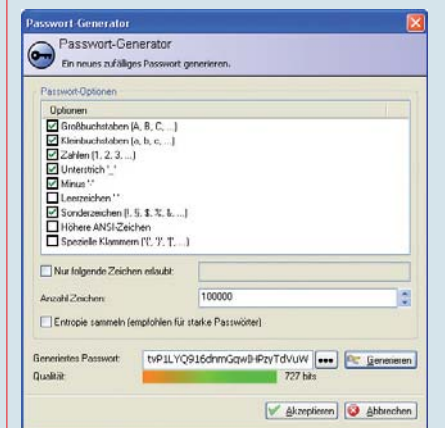
Jede gestartete Windows-Software legt Programmkomponenten im RAM ab. Ausgestattet mit dem passenden Werkzeug, beispielsweise dem Hexeditor Win Hex 13.9 (www.x-ways.net), lässt sich der Inhalt des Arbeitsspeichers auslesen und gezielt nach bestimmten Zeichenketten durchsuchen. Diese Form der Datenspionage spielt in der Praxis aber nur dann eine Rolle, wenn andere Personen Vollzugriff auf den Rechner haben – entweder über eine Backdoor oder aber bei einem PC, der von mehreren Leuten genutzt wird. Unter Laborbedingungen gelingt es den Tes-

Keylogger ins Leere laufen lassen

Die größte Gefahr für die eigenen Passwörter sind Keylogger, die im Hintergrund alle Tastenanschläge protokollieren und die Zwischenablage überwachen. Eine erste Gegenmaßnahme der Passwort-Manager ist eine Bildschirmtastatur zur Eingabe des Master-Passworts. Archicrypt Safe, Bagusoft Password Safe, Acebit Password Depot und Subassembly Wallet besitzen dieses Feature, letzteres Programm allerdings nur für die Eingabe von Zahlen. Bei Keepass Password Safe



Passwort Manager XP legt die Kennwörter unverschlüsselt im Arbeitsspeicher ab. Das ist ein Sicherheitsrisiko.

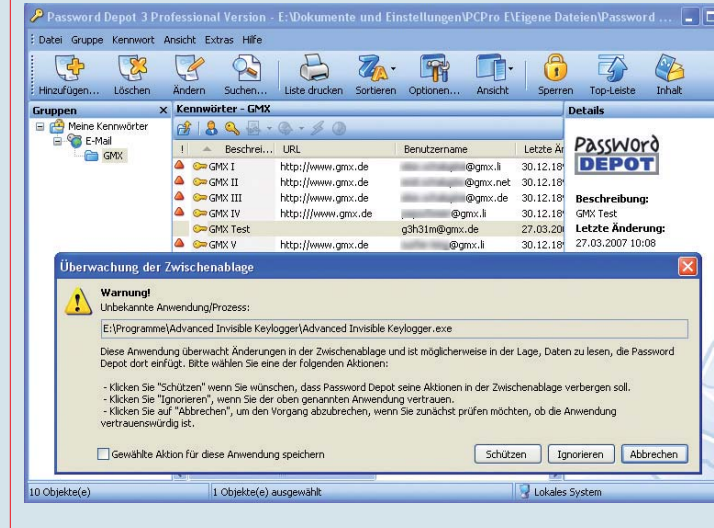


Als einziges Programm beschränkt Keepass Password Safe die Länge der Kennwörter nicht unnötig.

lässt sich die Funktion mit Hilfe eines kostenlosen Plug-ins nachrüsten.

Sicherer ist die Anmeldung mit einer Schlüsseldatei, die auf einem USB-Stick gespeichert wird. Diese Funktion unterstützen Archicrypt Safe, KeePass Password Safe, Acebit Password Depot und Mateso Password Safe and Repository. Viskeeper Pro erlaubt es dem Nutzer, sich per Bild-Passwort am Programm anzumelden. Dazu klickt er die Pixel einer Grafik in einer einmal festgelegten Reihenfolge an – eine ebenfalls sichere Methode. Hardware-basierten Schutz bietet gegen Aufpreis Subsembly Wallet Desktop. Sind Sie im Besitz einer Certgate Card (www.iics.de), können Sie den auf der Mini-SD-/MMC-Karte integrierten Chip zur Anmeldung verwenden. Alternativ dazu nutzen Sie die Programme in Kombination mit der auf Seite 120 vorgestellten Sicherheits-Hardware.

Das Auslesen der Zwischenablage lässt sich einfach vermeiden. Es genügt, die Software mit einer Funktion auszustatten, die testet, ob die Zwischenablage überwacht wird. Eine solche Routine haben die Produkte von BaguSoft, Acebit, CP-Lab, Mateso sowie KeePass Password Safe. Die ersten vier machen den Nutzer auf die Überwachung der Zwischenablage aufmerksam, so dass er prüfen kann, welches Programm dafür verantwortlich ist.



Acebit Password Depot informiert Sie darüber, wenn ein Programm die Zwischenablage überwacht.

KeePass verzichtet auf den Hinweis und legt die Daten stattdessen verschlüsselt in der Zwischenablage ab. Anstelle des Passworts schreibt ein Überwacher also nur Datenmüll mit. Dieses Verfahren, das auch BaguSoft Password Safe nutzt, kommt bei der Eingabe des Master-Passworts ebenfalls zum Einsatz.

Automatisches Einloggen inklusive

Die Anmeldung bei einer Webseite erledigen die Testkandidaten unterschiedlich komfortabel. Am einfachsten gelingt es mit Password

Manager XP: Sie klicken ein Formularfeld mit der rechten Maustaste an und wählen den passenden Datensatz aus. Um diese Auswahl künftig nicht mehr treffen zu müssen, können Sie die Feldverknüpfungen speichern. Doch Vorsicht: Wenn Sie bei einem Webservice wie GMX mehrere Konten eingerichtet haben, melden Sie die Tools immer nur mit dem Standardzugang an.

Gut gelöst haben auch die Hersteller von Acebit Password Depot, Archicrypt Password Safe, BaguSoft Password Safe und Mateso Password Safe die Web-Anmeldung. Deutlich

INTERNET EXPLORER, FIREFOX UND OPERA

Passwörter im Browser verwalten

Moderne Webbrowser bringen bereits ihre eigene Passwortverwaltung mit. Diese ist aber in der Regel weniger flexibel als externe Lösungen.

Internet Explorer, Firefox und Opera – alle gängigen Browser können auf Webseiten eingetippte Passwörter und Formulardaten speichern und sie bei einem erneuten Aufruf der Seite automatisch in die richtigen Felder eintragen. Das funktioniert in der Praxis gut. Deutliche Unterschiede gibt es aber bei Verwaltung und Sicherheit.

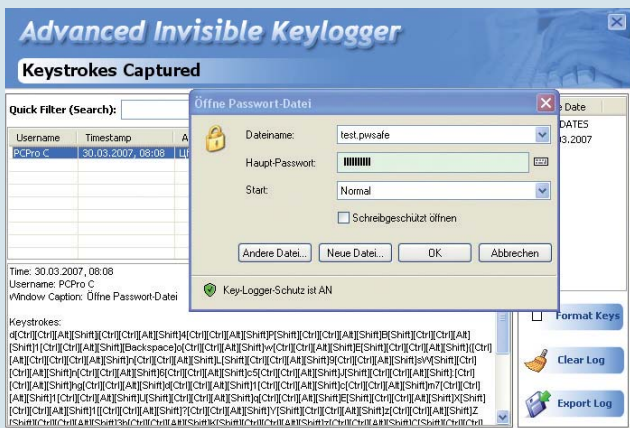
Internet Explorer 6/7 _____ Die Funktion *AutoVervollständigen* merkt sich Eingaben aus Formularen und Login-Dialogen und speichert diese in verschlüsselter Form in der Registry. Dabei kann der Nutzer einstellen, ob sich der Browser nur Web-Adressen, allgemeine Formulardaten oder auch Benutzernamen und Kennwörter merken soll. Eine Ansicht der gespeicherten Daten fehlt komplett, die einzigen Funktionen lauten *Formulare löschen* und *Kennwörter löschen*. Da die Daten nicht durch ein Master-Passwort geschützt werden können, rät

PC Professionell davon ab, *AutoVervollständigen* auf PCs zu verwenden, die von mehreren Personen gemeinsam genutzt werden.

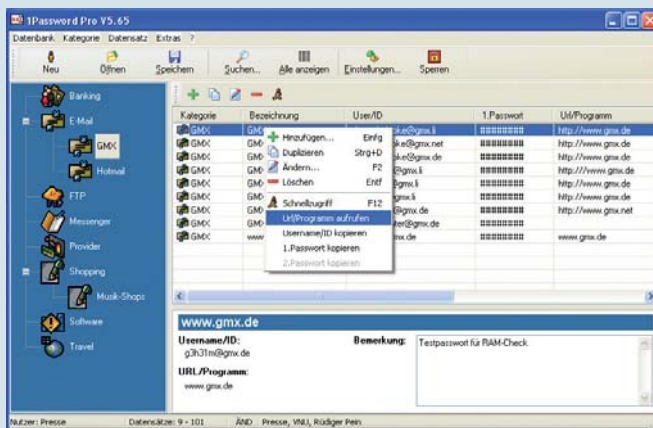
Firefox 2 _____ Im Gegensatz zum Internet Explorer schützt Firefox die gespeicherten Zugangsdaten auf Wunsch mit einem Master-Passwort. Diese Funktion müssen Sie jedoch manuell aktivieren, standardmäßig ist sie ausgeschaltet. Dazu wählen Sie im *Extras*-Menü den Punkt *Einstellungen* und setzen im Register *Sicherheit* ein Häkchen vor die Option *Master-Passwort verwenden*. Praktisch ist, dass Ihnen Firefox die gespeicherten Kennwörter auf Wunsch anzeigt. Dazu klicken Sie im *Sicherheit*-Register auf *Passwörter anzeigen*. Das Abspeichern oder Ausdrucken der unverschlüsselten Kennwörter lässt Firefox hingegen nicht zu. Diese Aufgabe erledigt jedoch das kostenlose Tool Fire Password (<http://nagmatrix.50webs.com>). Auf der gleichen Webseite finden Sie auch

das Programm Fire Master, das mit Wörterbuch- und Brute-Force-Attacken versucht, ein vergessenes Master-Passwort wiederherzustellen.

Opera 9 _____ Auch Opera wartet mit einer Auto-Ausfüll-Routine auf, sie ist jedoch etwas anders zu bedienen als beim Internet Explorer und bei Firefox. Tippen Sie Login-Infos auf einer Webseite ein, speichert Opera diese Daten. Beim nächsten Besuch der Seite sind die Eingabefelder von einem orangefarbenen Rahmen umfasst. Soll Opera die Zugangsdaten automatisch eingetippen, klicken Sie auf das Icon mit dem Zauberstab (englisch *Wand*) oder drücken die Tasten [Strg] + [Eingabe]. Über *Extras/Einstellungen/Wand/Passwörter...* gelangen Sie zu einer Liste der gespeicherten Zugangsdaten. Im Klartext anzeigen lassen sich die Kennwörter zwar nicht, trotzdem gilt wie bei Firefox: Schützen Sie sie unbedingt mit einem Master-Passwort. Dieses geben Sie in den Einstellungen im Abschnitt *Sicherheit* ein und aktivieren die Option *Als Masterpasswort für E-Mail und Wand verwenden*. _____ RPE



Wer das Master-Passwort von Bagusoft Password Safe mit einem Keylogger ausspioniert, erhält nur Datenmüll.



Sinnvolle Komfortfunktionen erleichtern die Arbeit mit 1 Password Pro.

größer ist der Aufwand für User von 1 Password Pro und KeePass Password Safe: Die Ausfüllfunktion wird auf manuellem Weg konfiguriert. Während Ihnen 1 Password Pro zumindest die akzeptierten Befehle in einer Liste anzeigt, müssen Sie das Feature von KeePass Password Safe komplett in Eigenregie anlegen. Ohne Besuche im Support-Forum ist dies kaum zu bewältigen. Subsembly Wallet und Viskeeper Pro verzichten ganz auf die Ausfüllfunktion. Alle anderen Programme arbeiten mit Internet Explorer 7, Firefox 2 und Opera 9 zusammen. Password Manager XP unterstützt nur die beiden Ersteren, klinkt sich dafür aber in deren Kontextmenü ein.

Bis auf Archicrypt und Subsembly erlauben es alle Programme, die in den Datenbanken gespeicherten Zugangsdaten per Drag and Drop in Formularfelder zu ziehen. In diesem Zusammenhang ist es hilfreich, wenn sich das Programm auch in einer kompakten Darstel-

lung betreiben lässt. Dieses Feature bieten 1 Password Pro, Acebit Password Depot, Bagusoft Password Safe sowie Mateso Password Safe. Praktisch: 1 Password Pro erlaubt dem User auch über das Icon in der Systray den Zugriff auf die komplette Kennwort-Datenbank. Archicrypt Password Safe und Bagusoft Password Safe stellen Passwörter ebenfalls über das Systray-Icon bereit, allerdings nur solche, die der Anwender explizit für diese Zugriffsvariante ausgewählt hat.

Felder für die wichtigsten Infos

Für die manuelle Eingabe neuer Kennwörter stellen alle neun Programme die wichtigsten Felder bereit, also URL, Benutzername, Kennwort und eine Bemerkung. Außer bei Archicrypt Password Safe und KeePass kann der Nutzer auch neue Felder definieren. Vorbildlich sind die Routinen von Subsembly Wallet

und Viskeeper Pro. Beide Programme erlauben es, benutzerdefinierte Passwortkarten zu designen. Auf diese Weise lassen sich ohne weiteres Zusatzinfos wie Mail-Server, Kreditkartennummer und Bankleitzahlen zusammen mit den Zugangsdaten speichern – in erster Linie bei der mobilen Nutzung der Passwort-Datenbank ein wichtiges Extra. Und genau darauf zielen die beiden Tools ab, von denen es auch Versionen für Pocket PCs gibt. Doch nicht nur diese beiden Tools arbeiten mit PDAs zusammen. Auch Bagusoft und Mateso bieten spezielle Versionen für Pocket-PC- beziehungsweise Palm-Handhelds an.

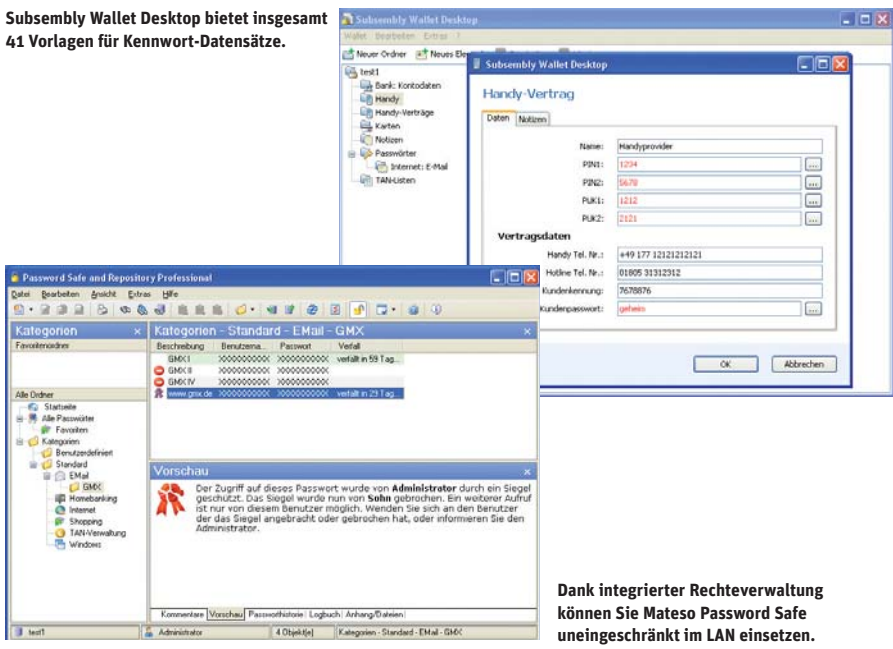
Der mobile Einsatz setzt aber nicht zwingend einen PDA voraus. Alle Passwort-Manager laufen auch von einem USB-Stick, lediglich Mateso verlangt dabei Geld für eine Zusatzlizenz. Teils gibt es auch speziell angepasste Versionen für U3-Sticks (siehe Tabelle auf Seite 122). Subsembly Wallet Desktop unterstützt sogar ausschließlich Wechselmedien, die diese Spezifikationen erfüllen.

Meist komfortable Bedienung

Je mehr Passwörter ein User verwalten muss, desto wichtiger das Kennwort-Management. An oberster Stelle steht dabei die Übersicht. Der Usability zugute kommt die Option aller Kandidaten, Passwörter in verschiedene Rubriken und Untergruppen einzuteilen. So legt der User übersichtlich gestaffelte Hierarchien wie *Internet/E-Mail-Accounts/GMX* an.

Dabei vertrauen alle Programme auf das Dateimanager-Bedienprinzip: In der linken Spalte stehen die diversen Rubriken, das Hauptfenster ist für die Anzeige der einzelnen Passwort-Datensätze reserviert. Unterschiede gibt es jedoch bei der Darstellung der Datensätze. Archicrypt Password Safe und Viskeeper Pro verzichten auf eine Listendarstellung und zeigen die Daten ausschließlich als Karteikarten an. Der Nachteil daran: Es ist nicht möglich, einzelne Datensätze per Drag and

Subsembly Wallet Desktop bietet insgesamt 41 Vorlagen für Kennwort-Datensätze.



Dank integrierter Rechteverwaltung können Sie Mateso Password Safe uneingeschränkt im LAN einsetzen.

Drop aus einer Rubrik in eine andere zu verschieben. Zudem kann man nicht mehrere Einträge gleichzeitig markieren, etwa um sie zu löschen. Aber auch Bagusoft Password Safe und Mateso Password Safe – zwei Tools, die auf die Listendarstellung setzen – verzichten auf diese grundlegende Windows-Funktion.

Sichere Passwörter erzeugen

Die Passwortgenerierung per Entropie, also auf Basis zufällig erzeugter Tastenanschläge beziehungsweise Mausbewegungen, ist mit Keepass Password Safe, Bagusoft Password Safe, Password Depot und Mateso Password Safe möglich. Auch Archicrypt Password Safe bietet eine derartige Funktion, allerdings nur beim Generieren der Schlüsseldatei. Die Stärke eines Passworts gegenüber Brute-Force-Angriffen zeigen bis auf Password Manager XP und Viskeeper Pro alle Programme an, wobei sich 1 Password Pro auf das Master-Kennwort beschränkt.

Auch gute Kennwörter sollten Sie regelmäßig aktualisieren. Keine Hilfe sind dabei 1 Password Pro, Subsembly Wallet Desktop und Viskeeper Pro. Archicrypt Password Safe erlaubt zumindest die Vorgabe eines Ablaufdatums für die Schlüsseldatei. Bei den übrigen Programmen können Sie auch die Passwörter mit einem Verfallsdatum versehen.

Passwort-Datenbank im Netzwerk

Alle neun Programme im Testfeld erlauben es, die Datenbank auf einem Netzwerk-Share abzulegen. Dies allein garantiert aber nicht die Nutzung innerhalb eines LANs. Vielmehr definiert sich die Netzwerkfähigkeit über drei andere Faktoren: simultaner Zugriff, automatischer Abgleich der Datenbank und integrierte Rechteverwaltung. Diese Features bieten nur Testsieger Acebit Password Depot,

Password Manager XP und Mateso Password Safe. Somit sind diese Tools ideal für die Nutzung in Business-Umgebungen. Die beiden letztgenannten Programme sind bereits in der Grundausrüstung für den Netzwerkeinsatz vorbereitet. Um Acebit Password Depot im LAN verwenden zu können, installieren Sie auf dem Server das separat zu ladende Depot-Server-Modul. Drei Clients können ohne zusätzliche Lizenz auf den Server zugreifen.

Die beiden Programme Acebit Password Depot und Password Manager XP setzen auf eine klassische Client-Server-Architektur. Die Passwort-Datenbanken werden zentral auf dem System abgelegt, auf dem das Server-Modul läuft. Den Zugriff auf die Passwörter erledigen die User wie gewohnt mit dem jeweiligen Client. Mateso Password Safe verfolgt einen anderen Ansatz: Die Passwort-Datenbank liegt auf einem Netzwerk-Share, so dass kein spezielles Servermodul notwendig ist. Dafür ist die Performance aber nicht so hoch, da der jeweils von einem Nutzer gelesene Teil der Datenbank über das Netzwerk übertragen werden muss. Laut Mateso wird die kommende Version von Password Safe daher ebenfalls auf das Client-Server-Prinzip setzen.

Auf die Datenbanken von 1 Password, Keeppass Password Safe und Viskeeper Pro haben ebenfalls mehrere Nutzer simultan Zugriff. Spezielle Funktionen für das Rechte-management sind allerdings nicht implementiert, was den Praxisnutzen deutlich schmälert. Im Privatbereich ist der Verzicht auf eine Benutzerverwaltung zu verschmerzen. Teilen sich mehrere Personen einen Rechner, genügt es, verschiedene Passwort-Datenbanken anzulegen. Dies ist mit allen neun Programmen möglich. Das Ablegen der Kennwort-Datenbank auf einem FTP- oder HTTP-Server unterstützt hingegen nur der Testsieger Acebit Password Depot. *_____RPE*

Vier Programme – 1 Password Pro, Bagusoft Password Safe, Acebit Password Depot und Mateso Password Safe – bieten auch einen verkleinerten Mini-Modus.

Archicrypt Password Safe arbeitet mit allen gängigen Browsern zusammen.

WERTUNGEN

GESAMTWERTUNG 100%

Acebit Password Depot	★★★★★	91,3
Mateso Password Safe	★★★★★	90,0
Bagusoft Password Safe	★★★★★	82,6
1 Password Pro	★★★★★	82,5
Keeppass Password Safe	★★★★★	79,8
Password Manager XP	★★★★★	78,4
Archicrypt Password Safe	★★★★★	77,3
Viskeeper Professional	★★★★★	67,7
Subsembly Wallet Desktop	★★★★★	63,2

LEISTUNG 40%

Acebit Password Depot	★★★★★	89,9
Mateso Password Safe	★★★★★	87,7
Keeppass Password Safe	★★★★★	82,6
Bagusoft Password Safe	★★★★★	81,0
Password Manager XP	★★★★★	79,5
1 Password Pro	★★★★★	75,0
Archicrypt Password Safe	★★★★★	70,3
Viskeeper Professional	★★★★★	69,9
Subsembly Wallet Desktop	★★★★★	69,6

AUSSTATTUNG 25%

Acebit Password Depot	★★★★★	90,0
Mateso Password Safe	★★★★★	88,4
Archicrypt Password Safe	★★★★★	87,8
Bagusoft Password Safe	★★★★★	87,1
1 Password Pro	★★★★★	85,1
Password Manager XP	★★★★★	79,6
Keeppass Password Safe	★★★★★	78,9
Subsembly Wallet Desktop	★★★★★	65,1
Viskeeper Professional	★★★★★	60,0

BEDIENUNG 25%

1 Password Pro	★★★★★	93,5
Mateso Password Safe	★★★★★	93,5
Acebit Password Depot	★★★★★	92,0
Bagusoft Password Safe	★★★★★	86,0
Password Manager XP	★★★★★	84,0
Keeppass Password Safe	★★★★★	78,0
Viskeeper Professional	★★★★★	73,0
Archicrypt Password Safe	★★★★★	72,5
Subsembly Wallet Desktop	★★★★★	56,5

SERVICE 10%

Acebit Password Depot	★★★★★	98,0
Mateso Password Safe	★★★★★	94,0
Archicrypt Password Safe	★★★★★	91,0
1 Password Pro	★★★★★	78,0
Keeppass Password Safe	★★★★★	75,0
Bagusoft Password Safe	★★★★★	69,0
Viskeeper Professional	★★★★★	65,0
Password Manager XP	★★★★★	57,0
Subsembly Wallet Desktop	★★★★★	50,0

Leistung (40%) Security-Funktionen, Passwort-Erzeugung, Passwort-Verwaltung, USB-Stick-Support, Netzwerkfähigkeit, Auto-Fill-Funktion, TAN/iTAN-Modul
Ausstattung (25%) Verschiedene Nutzeridentitäten, verschiedene Logins auf einer Seite pro Nutzer, Browser-Support, Biometrie-Support
Bedienung (25%) Einfachheit der Installation, Benutzerführung, Qualität der Wizards
Service (10%) Qualität des Handbuchs, Hilfe, FAQ, Erreichbarkeit und Kosten der Hotline, Mail-Support

★★★★★	sehr gut	90,0–100 Punkte
★★★★	gut	80,0–89,9 Punkte
★★★	befriedigend	65,0–79,9 Punkte
★★	ausreichend	50,0–64,9 Punkte
★	mangelhaft	0,00–49,9 Punkte

Passwort-Safes mit Sicherheits-Hardware

Spezielle USB-Module machen die Verwaltung von Passwörtern noch sicherer: Sie nutzen für die Anmeldung Smartcard-Chips und Fingerabdruck-Scanner.

Alle Passwort-Safes im Test laufen auch direkt von einem USB-Stick. Neben der Standardware gibt es Sticks und andere USB-Geräte mit integrierten Sicherheitsfunktionen, die die Kennwortdatenbank besonders schützen.

Der bis zu 2 GByte große Codemeter-Stick von WIBU (www.wibu.de) ist mit seinem eingebauten Smartcard-Chip ursprünglich für den Einsatz als Kopierschutz-Dongle konzipiert. Dank des kostenlosen CM Password Manager 3.20 nutzen Sie den USB-Stick auch als sichere Kennwortverwaltung mit Auto-Ausfüllfunktion für Firefox und den Internet Explorer. Die sensiblen Zugangsdaten liegen dabei verschlüsselt in einem geschützten Speicherbereich des USB-Mediums. Mit den mitgelieferten Applikationen Securi Key Lite und Steganos Safe Lite können Sie den USB-Stick auch zur Windows-Anmeldung einsetzen und weitere Bereiche des Speichermediums verschlüsseln. Die Preise liegen zwischen 50 Euro für 128 MByte und 100 Euro für den 2-GByte-Stick (www.codemeter.de).

Ebenfalls auf die Kombination aus Smartcard-Chip und USB-Medium setzt Kobil mit dem M-Identity-Stick (www.kobil.de). Der in Größen zwischen 64 und 1024 MByte erhältliche Sicherheits-Datenspeicher merkt sich Zugangsdaten, füllt Webformulare und Windows-Dialogfelder automatisch aus und sichert Daten verschlüsselt. Optional kann er auch das Windows-Login schützen. Der Zugang zum Stick ist durch eine maximal 30 Zeichen lange PIN abgesichert. Die ebenfalls bei der erstmaligen Inbetriebnahme eingegebene PUK dient als Rettungsanker und erlaubt es, eine gesperrte Karte wieder zu

aktivieren. Je nach Ausführung und Größe des Security-Sticks müssen Sie für M-Identity zwischen 70 und 300 Euro bezahlen.

Anmeldung per Fingerabdruck

Als besonders sicher gelten biometrische Authentifizierungsverfahren, etwa mit einem Fingerabdruck. Wird zusätzlich noch ein Passwort abgefragt (2-Faktor-Authentifizierung), trägt Biometrie in jedem Fall zu erhöhter Sicherheit bei. Neben einem fest im Notebook verbauten Fingerabdruck-Scanner bie-

dem Internet Explorer. Rufen Sie eine bereits in der Datenbank gespeicherte Seite im Browser auf, fordert Sie die Software auf, sich mit Ihrem Fingerabdruck auszuweisen.

Direkt auf einem USB-Stick integriert ist der Fingerabdrucksensor beim Stealth MXP (www.mxsecurity.com). Der Vorteil: Die sensiblen Daten sind auf dem USB-Medium gespeichert, das je nach Ausführung zwischen 0,5 und 4 GByte groß ist. Die zur Administration benötigte Software liegt auf einer speziellen Read-only-Partition. Zusätzlich zum allgemein zugänglichen Bereich steht jedem



Der APC Biometric Password Manager gibt die Zugangsdaten erst nach einer Anmeldung per Fingerabdruck frei.

ten sich je nach Zweck auch ein USB-Stick mit integriertem Sensor an oder ein Standgerät, das über USB an den PC angeschlossen wird. Zur letzten Kategorie gehört der APC Biometric Password Manager (www.apc.com). Im Lieferumfang der rund 70 Euro teuren Hardware, die bis zu 20 verschiedene Fingerabdrücke verwalten kann, ist der Passwort-Manager OmniPass enthalten. Die Software kann in Webseiten eingetippte Passwörter in die Datenbank übernehmen, so dass Sie die Zugangsdaten fortan nicht mehr eingeben müssen. Allerdings funktioniert das nur mit






der maximal fünf Benutzer eine eigene verschlüsselte Partition auf dem Stick zur Verfügung. Als Kryptoalgorithmus kommt dabei 256-Bit-AES zum Einsatz.






Die Anmeldung ist mit dem Master-Passwort, Fingerabdruck oder beiden kombiniert möglich. Eine spezielle Passwortverwaltung ist nicht integriert. Sie können jedoch jeden Kennwort-Manager verwenden, der sich auf einem USB-Stick installieren lässt. Diese Variante gehört zu den sichersten, mit einem Preis zwischen 140 und 250 Euro jedoch auch zu den teuersten. _____ RPE

Der Codemeter-Stick sichert die Passwörter in einer eigenen, verschlüsselten Partition.

Die USB-Sticks der Stealth-MXP-Reihe speichern die komplette Admin-Software in einer Read-only-Partition.

Mit USB-Sticks aus der Serie Kobil M-Identity können Sie auch das Windows-Login absichern.

122	AKTUELL SPECIAL TEST IT IM UNTERNEHMEN PRAXIS	PASSWORT-MANAGER	6 2007	PC Professionell
	 			
PRODUKT	PASSWORD DEPOT 3.1.4.0	PASSWORD SAFE AND REPOSITORY 2006 PROFESSIONAL 4.4.3	PASSWORD SAFE 3.3.001	1 PASSWORD PRO 5.65
HERSTELLER	ACEBIT	MATESO	BAGUSOFT	HEIKO SCHRÖDER
Internet	www.password-depot.de	www.passwordsafe.de	www.bagusoft.de	www.1pw.de
Preis	29 Euro	25/36 Euro (privat/kommerziell)	24 Euro	10/15 Euro (privat/kommerziell)
Gesamturteil (Note/Punkte)	sehr gut 91,3	sehr gut 90,0	gut 82,6	gut 82,5
Leistung (40%)	gut 89,9	gut 87,7	gut 81,0	befriedigend 75,0
Ausstattung (25%)	sehr gut 90,0	gut 88,4	gut 87,1	gut 85,1
Bedienung (25%)	sehr gut 92,0	sehr gut 93,5	86,0	sehr gut 93,5
Service (10%)	sehr gut 98,0	sehr gut 94,0	befriedigend 69,0	gut 78,0
FAZIT	<p>Vorbildlich in Sachen Ausstattung und Bedienung. Überragende Verwaltungs-Features, gutes Zusammenspiel mit Browsern. Gute Schutzfunktionen.</p> <p>Verpasst den Testsieg wegen kleiner Mankos: gibt keine Kennwort-Richtlinien vor, verzichtet auf eine Bildschirmtastatur zum Eintippen des Master-Passworts.</p> <p>Hat Schwächen im Detail, etwa bei der Listendarstellung, die sich nicht nach beliebigen Kriterien sortieren lässt und keine Mehrfachauswahl unterstützt.</p> <p>Sehr einfach zu bedienendes, gut ausgestattetes Programm mit Schwächen bei der Sicherheit. Hauptkritikpunkt: keine Warnung vor Keyloggern.</p>			
PASSWORT-GENERATOR				
Integrierter Passwort-Generator	ja, maximal 256 Zeichen	ja, maximal 99 Zeichen	ja, maximal 256 Zeichen	ja, maximal 999 Zeichen
Zeigt Passwort-Sicherheit	ja	ja	ja	nein, nur bei Master-Passwort
Vorgabe von Kennwortrichtlinien	ja	nein	nein	nein
Verfallsdatum für Passwörter	ja	ja	ja	nein
PASSWORTVERWALTUNG				
Anlegen benutzerdefinierter Felder	ja	ja	ja	ja
Doppelte Eingabe des Passworts erforderlich	ja	nein	nein	ja
Importformate für Passwort-Dateien	CSV, XML	CSV	CSV, XML, TXT	CSV, TXT
Exportformate für Passwort-Dateien	CSV, TXT, HTML, XML	CSV, TXT, HTML, XML u. a.	TXT, HTML	CSV, TXT, HTML, XML
Verschiedene Passwort-Datenbanken für mehrere User	ja	ja	ja	ja
Integrierte Benutzerverwaltung mit Rechtevergabe	ja, Servermodul nötig	ja	nein	nein
Zugriffsschutz	Master-Passwort, Schlüsseldatei	Master-Passwort, Schlüsseldatei	Master-Passwort	Master-Passwort
Bildschirmtastatur	ja	nein	ja	nein
Unterstützte Verschlüsselungsalgorithmen	AES (256 Bit)	Blowfish (448 Bit), Twofish (256 Bit), Gost (256 Bit)	AES (256 Bit), Blowfish (448 Bit), Twofish (256 Bit)	AES (256 Bit), Blowfish (448 Bit), Twofish (256 Bit) u. a.
Keylogger-Schutz	ja	ja	ja	nein
Passwörter nur verschlüsselt im RAM	ja	ja	ja	ja
Zwischenablage löschen	ja, zeitgesteuert	ja, beim Beenden u. zeitgesteuert	ja, zeitgesteuert	ja, beim Beenden u. zeitgesteuert
Automatische Programmsperre	ja, bei Inaktivität, im Ruhezustand, zeitgesteuert und manuell	ja, zeitgesteuert	ja, zeitgesteuert und manuell	ja, zeitgesteuert und manuell
Sonstiges	Speicherung der Passwörter auf Web- und FTP-Server	Passwörter lassen sich versiegeln und sperren	Zusammenführen mehrerer Passwort-Datenbanken	
KOMFORTFUNKTIONEN				
Zusammenspiel mit beliebigen Anwendungen	ja	ja	ja	ja
Unterstützte beim Ausfüllen von Eingabefeldern	ja, automatisch	ja, automatisch	ja, automatisch	ja, per Shortcut
Integration ins Kontextmenü von IE 7/Firefox 2/Opera 9	nein/nein/nein	nein/nein/nein	nein/nein/nein	nein/nein/nein
Unterstützung von IE 7/Firefox 2/Opera 9	ja/ja/ja	ja/ja/ja	ja/ja/ja	ja/ja/ja (jeweils nur ein Browser)
Übernahme auf Webseiten eingetippter Zugangsdaten	ja, über Assistenten	ja, über Auslesen des Formulars	nein	nein
Passworteingabe per Drag and Drop/Mini-Modus	ja/ja	ja/ja	ja/ja	ja/ja, aber nur einzelne Einträge
Schnellzugriff auf Passwörter via Systray-Icon	nein	nein	ja, aber nur auf »Schnellzugriff«	ja
Druck-Funktion	ja	ja	ja	ja
Netzwerk-Nutzung der Datenbank möglich	ja, Servermodul nötig	ja	nein	ja
Synchronisation mit PDAs	nein	ja, Palm	ja, mit Pocket PC	nein
USB-Stick-Support	ja	nein, Zusatzlizenz erforderlich	ja	ja
U3-Version des Programms	nein	nein, Zusatzlizenz erforderlich	nein	ja, separater Download
TAN- und iTAN-Modul/Importformate für TAN-Listen	ja/CSV, TXT, XML	ja/TXT	ja/keine	ja/CSV, TXT
SUPPORT				
E-Mail-/Web-Support	ja/ja	ja/ja	ja/nein	ja/ja
Hotline	(061 62) 800 20	(090 05) 22 55 62 34	(02 21) 424 96 99	(03 41) 879 85 86

PC	6 2007	PASSWORT-MANAGER		AKTUELL SPECIAL TEST IT IM UNTERNEHMEN PRAXIS		123
    						
PRODUKT	KEEPASS PASSWORD SAFE 1.06	PASSWORT MANAGER XP PROFESSIONAL 2.2.375	ARCHICRYPT PASSWORD SAFE 4.0.4.2160	VISKEEPER PROFESSIONAL 3.1.0	WALLET DESKTOP 2.0	
HERSTELLER	DOMINIK REICHL	CP-LAB	PATRIC REMUS	SFR	SUBSEMBLY	
Internet	www.KEEPASS.info	www.cp-lab.com	www.archicrypt.com	www.sfr-software.de	www.subsembly.com	
Preis	kostenlos (Open Source)	25 Euro	25 Euro	30 Euro	15 Euro	
Gesamt (Note/Punkte)	befriedigend 79,8	befriedigend 78,4	befriedigend 77,3	befriedigend 67,7	ausreichend 63,2	
Leistung (40%)	gut 82,6	befriedigend 79,5	befriedigend 70,3	befriedigend 69,9	befriedigend 69,6	
Ausstattung (25%)	befriedigend 78,9	befriedigend 79,6	gut 87,8	ausreichend 60,0	befriedigend 65,1	
Bedienung (25%)	befriedigend 78,0	gut 84,0	befriedigend 72,5	befriedigend 73,0	ausreichend 56,5	
Service (10%)	befriedigend 75,0	ausreichend 57,0	sehr gut 91,0	befriedigend 65,0	ausreichend 50,0	
FAZIT	Weist ein paar Schwächen bei Bedienung und Ausstattung auf, zum Beispiel die wenig komfortable Konfiguration der Ausfüllhilfe.		Schlecht: Die Datenbank liegt gänzlich unverschlüsselt im Arbeitsspeicher. Die Bedienung überzeugt in vielen Details.	Auch hier liegt die Datenbank schutzlos im Speicher. Unnötig komplizierte Verwaltung, keine Importfunktion.	Große Lücken bei Komfort und Ausstattung: Eine Ausfüllfunktion fehlt komplett, die Verwaltungsfunktionen lassen zu wünschen übrig.	
PASSWORT-GENERATOR						
Integr. Passwort-Generator	ja, beliebige Länge	ja, maximal 999 Zeichen	ja, maximal 100 Zeichen	ja, maximal 32 Zeichen	ja, maximal 48 Zeichen	
Zeigt Passwort-Sicherheit	ja	nein	ja	nein	ja	
Kennwortrichtlinien	nein	nein	nein	nein	nein	
Verfallsdatum Passwörter	ja	ja	nur für Schlüsseldateien	nein	nein	
PASSWORTVERWALTUNG						
Benutzerdefinierte Felder	nein	ja	nein	ja	ja	
Doppelte Eingabe des Passworts erforderlich	ja	nein	ja	nein	nein	
Importformate für Passwort-Dateien	CSV, TXT, weitere Formate über Plug-Ins	CSV, TXT	keine	CSV, TXT	CSV	
Exportformate	CSV, TXT, HTML, XML	CSV, TXT	CSV, TXT, HTML, DOC u.a.	TXT	CSV, HTML	
Verschiedene Datenbanken für mehrere User	ja	ja	ja	ja	ja	
Integrierte Benutzerverwaltung mit Rechtevergabe	nein	ja	nein	nein	nein	
Zugriffsschutz	Master-Passwort, Schlüsseldatei	Master-Passwort	Master-Passwort, Schlüsseldatei	Master-Passwort, Bild-Passwort	Master-Passwort, Certgate-Card (kostenpflichtig)	
Bildschirmatastatur	ja, Plug-in nötig	nein	ja	nein	ja, aber nur Zahlen	
Unterstützte Verschlüsselungsalgorithmen	AES (256 Bit), Twofish (256 Bit)	AES (256 Bit), Blowfish (384 Bit) u. a.	AES (256 Bit)	Twofish (128 Bit)	AES (256 Bit)	
Keylogger-Schutz	ja, teilweise	ja	nein	nein	nein	
Passw. verschlüsselt im RAM	ja	nein	nein	ja	ja	
Zwischenablage löschen	ja, zeitgesteuert	ja, manuell	ja, manuell	nein	nein	
Automatische Programmsperre	ja, bei Minimierung, Benutzerwechsel, zeitgesteuert	ja, bei Inaktivität, Minimierung und manuell	ja, zeitgesteuert	ja, zeitgesteuert	ja, zeitgesteuert	
Sonstiges	diverse Importfilter als Plug-Ins erhältlich	Synchronisation von Passwort-Datenbanken	Zusammenführen v. Datenbanken, Ausfüllfunktion für komplette Webformulare			
KOMFORTFUNKTIONEN						
Zusammenspiel mit beliebigen Anwendungen	ja	nein	ja	nein	nein	
Unterstützung beim Ausfüllen von Eingabefeldern	ja, per Shortcut	ja, über rechte Maustaste	ja, per Shortcut	nein	nein	
Integration ins Kontextmenü von IE/Firefox/Opera	nein/nein/nein	ja/ja/nein	nein/nein/nein	nein/nein/nein	nein/nein/nein	
Unterstützung von IE 7/Firefox 2/Opera 9	ja/ja/ja	ja/ja/nein	ja/ja/ja	nein/nein/nein	nein/nein/nein	
Übernahme auf Webseiten eingetippter Zugangsdaten	nein	ja, per Shortcut	nein	nein	nein	
Passwordeingabe per Drag & Drop/Mini-Modus	ja/nein	ja/nein	nein/nein	ja/nein	nein/nein	
Schnellzugriff auf Passwörter via Systray-Icon	nein	nein	ja, aber nur auf Favoriten	nein	nein	
Druck-Funktion	ja	ja	nein	nein	nein	
Netzwerk-Nutzung der Datenbank möglich	ja	ja	nein	ja	nein	
Synchronisation mit PDAs	nein	nein	nein	ja, mit Pocket PC	ja, mit Pocket PC	
USB-Stick-Support	ja	ja	ja	ja	ja	
U3-Version des Programms	ja, separater Download	nein	ja	nein	ja, separater Download	
TAN- und iTAN-Modul/Importformate für TAN-Listen	ja/keine	nein/keine	ja/CSV, TXT	ja/keine	ja/TXT, XML	
SUPPORT						
E-Mail-/Web-Support	nein/ja	ja, Englisch/nein	ja/nein	ja/ja	ja/nein	
Hotline	keine	keine	(089) 66 00 08 93	keine	keine	