Passwortsicherheit

Und jetzt ab in den Safe!

Spätestens bei drei Passwörtern oder PIN-Nummern ist es erfahrungsgemäß so weit. Um sich alles merken zu können, neigt der Anwender dazu, sich seine Zugangscodes zu notieren. Dies führt alle Bemühungen des DSB um Datensicherheit ab absurdum. Eine Alternative bietet das Programm Password Safe. Damit können Sie Passwörter und PIN-Nummern in einen virtuellen Safe sperren.

Bruce Schneier – ein bekannter und anerkannter IT-Sicherheitsexperte – schuf den virtuellen Safe für Passwörter. Mittlerweile ist das Produkt zu einem Open-Source-Projekt geworden, das eifrig weiterentwickelt wird (http://passwordsafe.sourceforge.net/, www.fpx.de/fp/Software/ Gorilla/).

Das Programm speichert Passwörter und generiert solche auch selbst

Das Programm speichert alle Ihre Benutzernamen und Passwörter in verschlüsselter Form. So stehen Ihnen Ihre Zugangscodes gesammelt an einem sicheren Ort zur Verfügung. Der Schutz der gesammelten Passwörter steht und fällt jedoch mit dem Master-Passwort, mit dem Sie den Safe öffnen. Ist es zu schlicht gewählt, lässt sich der Safe knacken, indem das Passwort geraten wird. Vergessen Sie es, bleibt der Safe für immer zu.

Sie können mit dem Programm auch Passwörter selbst generieren. Die Regeln zur Passwortgenerierung lassen sich individuell anpassen. Die so generierten Passwörter sind von sehr guter Qualität.

Die Speicherung bietet zusätzliche Features, die das Leben erleichtern

Zu jedem Passworteintrag gibt es ein Notizfeld, das sich mit Text füllen lässt. Wird in das Notizfeld eine URL, die mit http://, https:// oder ftp:// beginnt, eingegeben, so schaltet sich automatisch der Eintrag „Browse to URL“ im Kontext-Menü frei. So müssen Sie z.B. die Webadresse fürs Internet-Banking nicht mehr „irgendwo“ aufschreiben. Password Safe speichert sie geschützt vor neugierigen Blicken.

Mit der Autotype-Funktion können Sie das unsichere Kopieren und Einfügen von Daten umgehen. Die Autotype-Funktion trägt Benutzername und Passwort automatisch in ein Online-Formular ein. Das Kopieren hat nämlich den entscheidenden Nachteil, dass die Zwischenablage – und damit die Zugangsdaten – allen Programmen zum Lesen offen steht.

Wichtige Sicherheitseinstellungen

Unter „Optionen“ lassen sich Sicherheitseinstellungen vornehmen. Die minimalen Einstellungen, die Sie mit einem Häkchen versehen sollten, sind:

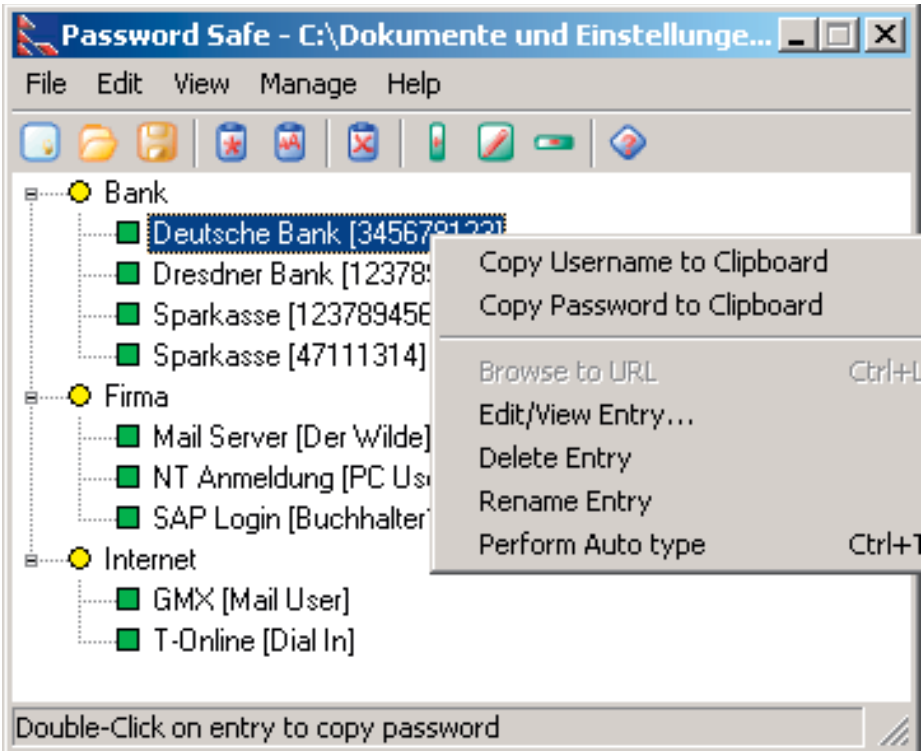
- Löschen der Zwischenablage beim Minimieren bzw. Verlassen (Clear clipboard upon minimize or exit)
- Abmelden von der Datenbank beim Start des Bildschirmschoners (Lock password database on workstation lock) und nach Zeitablauf (Lock password database after ...). Die voreingestellten fünf Minuten sollten Sie nicht verlängern.

Wählen Sie das Masterpasswort sehr sorgfältig. Einerseits darf man es nicht vergessen, andererseits darf es nicht leicht zu raten sein. Acht bis zehn Zeichen stellen die minimale Länge dar. Es sollte Sonderzeichen, Ziffern, große und kleine Buchstaben enthalten.

Sicherer Safe statt unsicheres Papier

Password Safe ist ein mächtiges Programm zur sicheren Aufbewahrung von Passwörtern, PINs und dergleichen. Vor allem ist es eine hervorragende Alternative zu Merkzetteln, die vergessliche Mitarbeiter mehr oder weniger offen herumliegen lassen.

Prof. Dr. Rainer W. Gerling



Die Einträge im Password Safe lassen sich gut in Kategorien strukturieren. Über das Kontext-Menü können Sie Username und Passwort übernehmen.