In Nöten, auch ohne Alzheimer

Hilfe, wo ist mein Passwort geblieben?

Wer viel im Web surft, mehrere Mailkonten besitzt, vielleicht auch noch Newsdienste abonniert hat und Onlinebanking macht, bei dem stapeln sich die Codewörter. So kommt es, dass der User schnell einmal ein Dutzend oder mehr verschiedene Codes auswendig lernen sollte. Nach einer langen Surfnacht oder in der Sommerhitze (ich wünsche allen Lesern einen schönen Sommer!) kann es schon einmal vorkommen, dass man dasteht wie der sprichwörtliche Esel am Berg. Login failed … Acces denied … please repeat your user name and password … In solchen Fällen online zu hirnen oder mögliche Kombinationen durchzuprobieren, ist nicht nur zeitaufwändig, sondern auch oft hoffnungslos. Nach dem dritten oder vierten missglückten Anlauf haut es manch einem den Deckel ab. Um des Dschungels Herr zu werden und als Vorsichtsmassnahme gegen Nervenzusammenbrüche, gibt es aber auch einige Regeln und hilfreiche Programme. Hier meine Tipps.

Thomas Vauthier
th.vauthier@bluewin.ch

Das Problem

Geschlossenen Foren, Abonnemente, Mailinglists, Downloads, Online Einkäufe … Auch der zurückhaltendste Internetbenutzer kommt schnell einmal auf ein Dutzend oder mehr Adressen, die nur mit Passwort oder Code zugänglich sind. Am einfachsten wäre es natürlich, einen universalen Schlüssel zu haben. Gut, damit gäbe es ein Risiko, dass im Fall der Entdeckung ein Unbefugter Zutritt zu all Ihren bestgehüteten Sites hätte. Trotzdem, aus Angst zu vergessen, wählen viele aber zu einfache Passwörter. Dies hat zwei Nachteile: Auf gewissen Websites, bei denen mehrere Millionen von Benutzern angemeldet sind, sind viele Möglichkeiten schon vergeben. Einen Code zu finden, ist oft ganz schön schwierig und ist (selbst erlebt!) auch superstressig, so dass man in der Verzweiflung irgendein Passwort wählt, Hauptsache es wird akzeptiert. Ebendieses hat man aber spätestens beim nächsten Einloggen mit Sicherheit schon wieder vergessen, weil in der Aufregung nirgends notiert.

Zweiter Nachteil: Allzu offensichtliche Passwörter sind leicht zu knacken. Wenn der Code genügend subtil gewählt wäre, z. B. aus einem Mix von Ziffern, Buchstaben und Sonderzeichen (sicher aber nicht Ihr Vorname oder die Telefonnummer der Praxis), wäre das Risiko relativ gering (wesentlich kleiner jedenfalls als bei Bankcodes, die aus höchstens sechs Zahlen zusammengesetzt sein dürfen!). Leider ist die Realität auf dem Net nicht so einfach. Verschiedene Anbieter = verschiedene Vorgaben bei den zulässigen Zeichen. Meistens sind Sonderzeichen nicht erlaubt (z. B. Akzente, #, §, ~ etc.), die schon eine gewisse Schutzwirkung hätten – manchmal nicht einmal einfache Interpunktionszeichen.

Sie haben sich also bei zahlreichen Internetdiensten angemeldet und haben nie das passende Passwort griffbereit. Oder Ihnen ist die Liste mit den zahlreichen Passwörtern, die Sie schon mehrfach geändert haben, in Ihrer Schreibtischschublade einfach zu unsicher. Abhilfe schaffen hier Verwaltungsprogramme, mit denen sie einfach und komfortabel in einer kleinen Datenbankanwendung Ihre Passwörtereingeben verwalten und pflegen (sprich: nach Bedarf ändern) können.

Empfehlenswerte Tools

Idealerweise sollte ein Verwaltungsprogramm für Passwörter folgende Funktionen umfassen:

- Komfortables Eingeben, Verwalten und Pflegen von Passwörtern und Zusatzinfos (integrierter Editor)
- Zugang zu den Daten nur über Masterpasswort
- Masterpasswort veränderbar
- Schneller Zugriff auf Passwörter durch komfortable Such-, Sortierfunktion und Filtermöglichkeit
- Frei definierbarer Passwortgenerator
- Warnfunktion zeigt Passwörter, die innerhalb einer bestimmten Frist ablaufen
- Speichern von formatierten Texten
- Doppelte Sicherheit durch zweifache Verschlüsselung der Passwörter
- Automatischer Log-out (Beenden) nach frei definierbarer Zeit der Nichtbenutzung
- Simples Kopieren der Daten in ein beliebiges Verzeichnis oder auf einen Wechseldatenträger (Back-up)
- Übersicht: als Report ausdruckbar
- TAN-Verwaltung zur Vereinfachung des Onlinebankings
- Alle wichtigen Funktionen per ShortCut aufrufbar

Um Passwörter sicher aufzubewahren, erlauben Tools wie *KeyMaster* (z. B bei www.aborange.de) oder *Password Safe* (www.passwordsafe.de) einen schnellen Zugriff auf die gespeicherten Passwörter, wo immer erforderlich. Nach Typen kategorisiert kann der Anwender mit *KeyMaster* komfortabel nach bestimmten Einträgen suchen und per Zwischenablage die Benutzerkennung und das Passwort eingeben. Zusätzlich lassen sich mit *Password Safe* frei formatierbare Anmerkungen speichern. Neben der Verwaltung von Passwörtern können per Drag-&-Drop-Funktion die entsprechenden Daten in die Eingabefelder einfach übernommen werden. Auch ein Ausdruck aller gespeicherten Daten in einer übersichtlichen Liste ist möglich. Der Anwender muss sich mittels dieser Tools nun nur noch ein Hauptkennwort merken, welches vor unerlaubtem Zugriff schützt. Und das sollte er wirklich im Kopf und nirgendwo sonst behalten!

Norton Password Manager 2004 (www.symantec.de) speichert und verwaltet Kennwörter. Nachdem die Software bereits Teil von Norton System Works war, gibt es sie neu auch als Einzelprodukt.

Zeitsparender Vorteil: Die Passwortverwaltung fügt automatisch das richtige Passwort ein. Der Nutzer muss sich dabei lediglich ein Masterpasswort merken.

Integriert ist auch eine Vervollständigenfunktion, die etwa Daten für Onlinetransaktionen selbstständig eingibt. Der Password Manager selbst schützt die ihm anvertrauten Daten durch mehrere Verschlüsselungsalgorithmen.

Die Software bietet ausserdem die Passwortverwaltung für mehrere Benutzer an. Jeder Anwender kriegt ein eigenes Konto mit eigenen Rechten zugewiesen. Die Software führt auch eine Sicherheitsmessung durch, das heisst, eingegebene Kennwörter werden auf ihre Sicherheit überprüft und bewertet.

Fortsetzung folgt …