KeePass2

Passwortmanager

Umgang mit Passwörtern

Ob Zugang zum Dienstrechner oder zu SAP, Anmeldung am Webmailer oder am VoIP-Telefon – nicht nur privat, sondern auch beruflich sammeln sich immer mehr Passwörter an. Häufig führt dies dazu, dass viele Nutzer ein Passwort für alle Dienste nutzen oder unsichere Passwörter wie „geheim12“ oder „Hallo“ verwenden. Ausreichend lange und komplexe Passwörter werden aus Gründen der schlechteren Merkbarkeit eher vermieden.

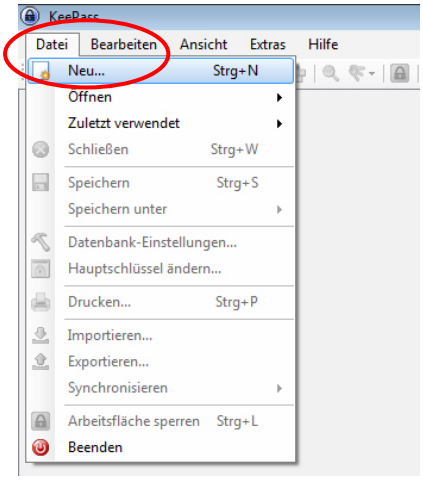
Die Folgen des Gebrauchs unsicherer Passwörter sind fatal. Kriminelle machen sich diese zu eigen und können damit unter falschem Namen E-Mails versenden, auf Forschungsdaten zugreifen oder das Bankkonto plündern. Um sich vor solchen Angriffe zu schützen, ist es unumgänglich sich sichere Passwörter zu überlegen. Unterstützt wird man dabei von sogenannten Passwort-Managern.

An der Universität Bielefeld ist das Open-Source-Produkt **KeePass2** im Einsatz. Mit diesem Tool ist es sowohl möglich neue Passwörter zu generieren als auch bereits vorhandene Passwörter zu verwalten sprich nach Kategorien geordnet abzulegen. Die Passwörter werden sicher in einer verschlüsselten Datenbank (AES 256-bit-Schlüssel) gespeichert. Um an diese zu gelangen, muss man sich nur noch ein Passwort, den sogenannten Hauptschlüssel, merken.

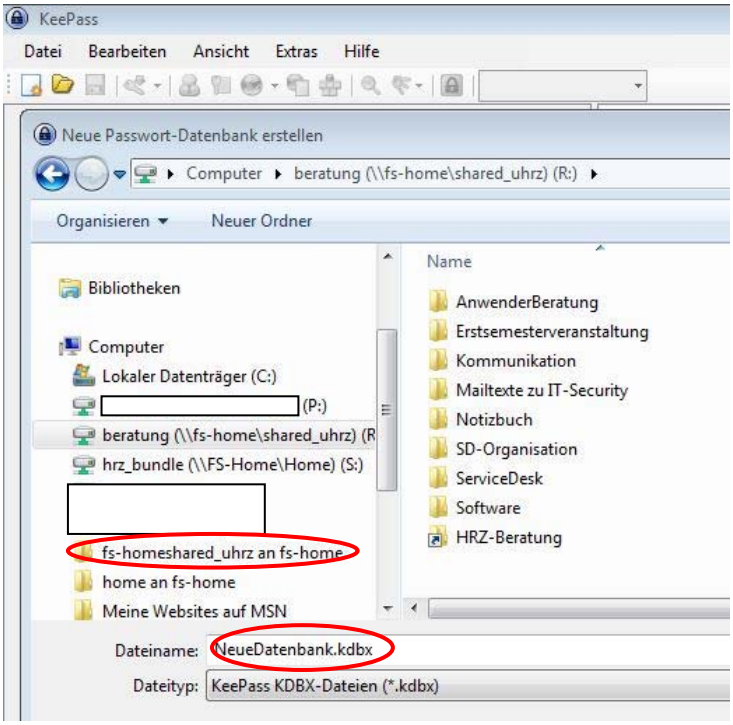
Auf allen Rechnern der Verwaltung steht KeePass2 automatisch zur Verfügung. Ansonsten kann man sich die Software hier herunterladen: http://keepass.info/download.html

Das Programm wird standardmäßig in Englisch installiert. Es lassen sich aber Sprachpakete hinzufügen: http://keepass.info/translations.html

1) Starten Sie KeePass2 und erstellen Sie mit **Datei>Neu** eine neue KeePass-Datenbank.



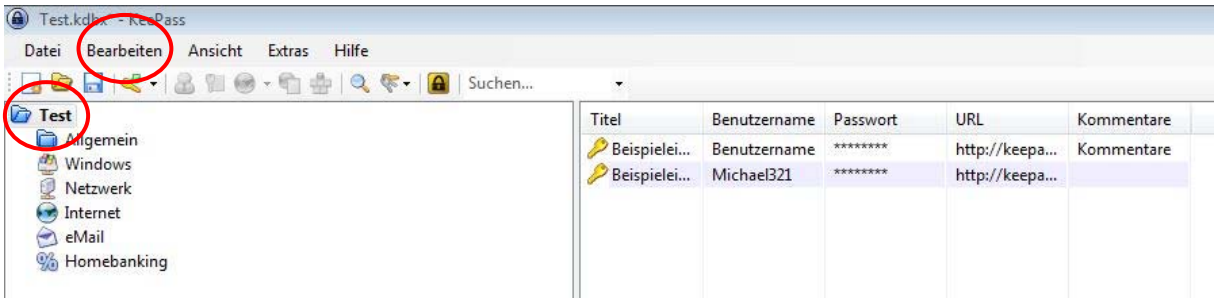
2) Wählen Sie Speicherort und Dateiname der Datenbank. Wir empfehlen ausdrücklich als Speicherort das **universitäre Netzlaufwerk** (entweder das persönliche Laufwerk oder das Gruppenlaufwerk).



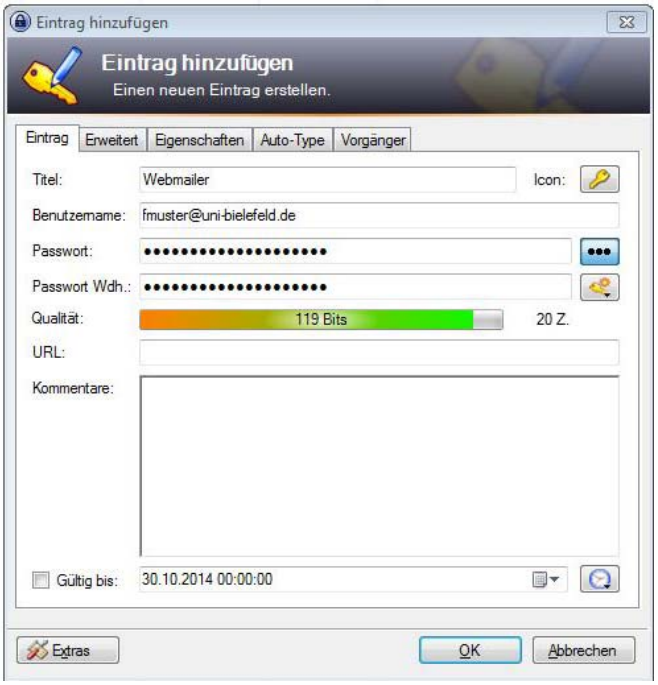
3) Klicken Sie auf **Speichern** und im geöffneten Dialog-Fenster legen Sie das Master- bzw. Hauptpasswort fest.

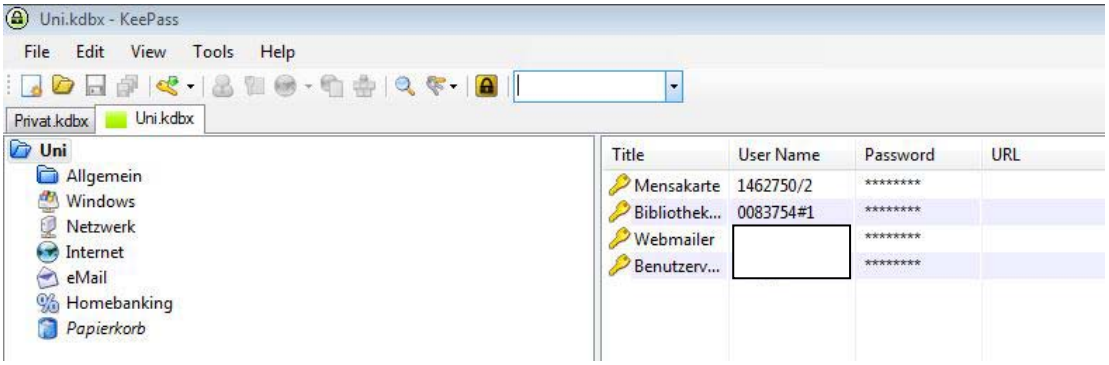
Geben Sie das Hauptpasswort ein. Je länger und komplexer das Hauptpasswort ist, umso sicherer ist die Datenbank vor unberechtigten Zugriffen. Der farbige Balken hinter **Geschätzte Qualität** zeigt an, wie sicher das Passwort einzustufen ist. Bestätigen Sie mit **OK**. Danach öffnet sich ein weiteres Fenster. Hier nehmen Sie bitte keine Änderungen in den Einstellungen vor. Bestätigen Sie mit **OK.**

4) Passworte in Datenbank ablegen



Nach dem Abspeichern erscheint der Name der Datenbank oben links neben dem Symbol eines kleinen geöffneten Ordners. Darunter sind Vorschläge für Kategorien. Im rechten Bereich sind zwei Beispiele für Einträge hinterlegt. Um einen neuen Eintrag zu generieren bitte auf **Bearbeiten>Eintrag hinzufügen** klicken. Es öffnet sich ein neues Dialogfenster. Dort bitte den Titel des Eintrags, den Benutzernamen und das entsprechende Passwort eingeben. Danach mit **OK** bestätigen. Der Eintrag erscheint nun in der Datenbank.





Um die Einträge den verschiedenen Kategorien zuzuordnen, müssen diese einfach mit der linken Maustaste markiert und dann in die entsprechende Kategorie gezogen werden. Sie können einen Eintrag aber auch direkt in der jeweiligen Kategorie vornehmen.

Sobald Sie KeePass verlassen, werden Sie gefragt, ob Sie die geöffnete Datenbank sichern möchten. Dies bestätigen Sie mit **OK.**

Wie gelange ich an meine Passwort Datenbank?
Wenn Sie nun Zugriff auf Ihre in der Datenbank hinterlegten Passwörter haben möchten, können Sie die Datenbank entweder direkt öffnen oder Sie starten erst KeePass und öffnen dann die entsprechende Datenbank über **Datei>Öffnen>Datei öffnen**. In beiden Fälle können Sie die Datenbank erst dann öffnen, wenn Sie das Masterpasswort eingegeben haben.

Achtung: Sollten Sie das Hauptpasswort/den Hauptschlüssel vergessen haben, haben Sie keinen Zugriff mehr auf die Datenbank. Gleiches gilt, beim Verlust der Datei mit der Datenbank. Es besteht nicht die Möglichkeit sich ein neues Passwort bzw. Schlüssel zu setzen! Sollten Sie das Hauptpasswort notieren, hinterlegen Sie es an einem sicheren Ort den ausschließlich Sie kennen.