(Entwurf)

Handbuch zum Passwort-Speicher "MyPasswords"

Mit diesem Programm können Sie Ihre Passwörter, aber natürlich auch jeden anderen beliebigen Text zuverlässig vor dem Ausspähen Dritter schützen.

"MyPasswords" bedient sich dabei mehrerer Techniken, um die Sicherheit Ihrer Daten zu gewährleisten. So benötigen Sie zum Ver- oder Entschlüsseln

1. Eine Schlüssel-Datei
2. Ein Passwort
3. Eine "PIN-Nummer"

Das Programm liegt in einer Windows und in einer Linux-Version vor. Falls Ihre Linux-Version nicht sogleich startet, dann denken Sie bitte daran, das Programm "MyPasswords" "ausführbar" zu machen!!!

Sie haben die Möglichkeit, beliebig viele verschlüsselte Dateien zu verwalten. Zur Veranschaulichung bezeichne ich diese verschiedenen Dateien als "Tresorfächer" innerhalb eines Tresors. Beim Programmstart, bzw. um im Bild zu bleiben: Nach dem Betreten des Tresorraums können Sie Ihre Tresorfächer anwählen oder auch in beliebiger Anzahl neu erzeugen. Die verschiedenen Dateien werden im Ordner "/Tresor" gespeichert. Sicherungsdateien liegen grundsätzlich im Ordner "/DaSi". Alle diese Ordner liegen im Programmverzeichnis. "Installieren" müssen Sie "MyPasswords" nicht! Erzeugen Sie einfach einen neuen Ordner mit einem beliebigen Namen, kopieren Sie das Programm zusammen mit diesem Handbuch in diesen Ordner und starten dann das Programm "MyPasswords".

Beim ersten Programmstart legen Sie Schlüssel-Datei, Passwort und "PIN-Nummer" fest. Das Programm führt Sie durch diesen Prozess.

Zunächst erzeugt "MyPasswords" eine "Schlüssel-Datei". Die technischen Datails erkläre ich gleich, aber zunächst möchte ich Ihnen eine kurze "Step-by-Step"-Anleitung geben:

Klicken Sie auf den Button "Neues Tresorfach erzeugen". es erscheint sogleich ein grünes Eingabefeld, in das Sie einen beliebigen Namen des Tresorfachs eingeben, das Sie generieren wollen. Bei der Eingabe von z.B. "Fach01" wird später das File "Fach01.Tresor" im Ordner "/Tresor" erzeugt.In dieser Datei finden sich verschlüsselt Ihre später eingegebenen Daten.

Wie schon erwähnt, braucht "MyPasswords" eine sogenannte "Schlüsseldatei". Diese ist zunächst ja nicht vorhanden und wird beim ersten Programmstart erst einmal angelegt. Dazu müssen Sie ein Passwort eingeben. Diese Schlüsseldatei muss pro Tresorfach nur ein einziges mal erzeugt werden; Sie brauchen dieses Passwort also (theoretisch) ebenfalls nur ein einziges mal. Dieses "Schlüssel-File-Passwort" sollte sich von dem dann sogleich angeforderten Passwort aus Sicherheitsgründen unterscheiden.

Als weiteren Schritt geben Sie ein Passwort ein, wie Sie dies von vielen anderen Programmen her gewohnt sind.

Anschließend wird eine sogenannte "PIN-Nummer" festgelegt. Diese "PIN-Nummer" besteht nur aus Zahlen und kann (und sollte) über die Maus eingegeben werden. Dadurch haben auch sogenannte "Keylogger" keine Chance mehr, diese PIN-Nummer auszuspähen. Auch die

Bildschirmpositionen, an welchen die Zahlen während der Eingabe auf dem Bildschirm erscheinen, ändern sich mit jeder Eingabe, so dass z.B. Rückschlüsse auf "gleiche Zahlen" nicht möglich sind.

Beim nächsten Programmstart wird – bei vorhandener Schlüssel-Datei – nur noch Ihr Passwort und die "PIN-Nummer" abgefragt. Sie müssen dann auch diese Passwörter natürlich nicht mehr zweimal eingeben; bei Falscheingaben beendet sich ganz einfach das Programm "MyPasswords".

Jederzeit haben Sie die Möglichkeit, Ihre Schlüsseldatei, Ihr Passwort oder Ihre PIN-Nummer zu verändern. "MyPasswords" führt Sie dabei durch das Programm.

Wenn Sie dies alles in dieser Reihenfolge gemacht haben, dann sehen Sie ein Text-Eingabefeld, dem Sie Ihre Passwörter sehr beruhigt anvertrauen können – aber natürlich auch beliebige andere Texte.

Beenden Sie nun "MyPasswords". Ihre Daten werden dabei "automatisch" verschlüsselt und auf Ihre Festplatte geschrieben.

Wenn Sie nun das Programm starten, werden Sie feststellen, dass nun nur noch Ihr Passwort und die Zahlen-PIN abgefragt werden. Das Schlüsselpasswort benötigen Sie jetztnicht mehr, die Schlüsseldatei befindet sich ja bereits auf Ihrer Festplatte und "MyPasswords" erstellt daraus einen der drei "Teilschlüssel". (sh. unten)

Viel Spaß!

A. Geigenberger

<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Nun zu einigen "technischen" Einzelheiten:

Ihre Passwörter bzw. Ihr Text wird mit dem welweit anerkannten Programm GPG verschlüsselt.

"MyPasswords" generiert intern zu der Schlüsseldatei, zu Ihrem Passwort und zu Ihrer PIN einen separaten Schlüssel und erzeugt dann erneut aus diesen drei "Teilschlüsseln" einen "Gesamtschlüssel". Dieser "Gesamtschlüssel" existiert im System jeweils nur wenige Millisekuden und nur dann, wenn er Ver- oder Entschlüsseln Ihrer Datei gebraucht wird.

Die Salt-Datei wird normalerweise nur einmal beim "Erzeugen" eines neuen Tresorfachs erzeugt und trägt den gleichen Namen wie Ihre Daten.Datei, jedoch mit einer anderen Dateierweiterung.
Beispiel:
Ihre verschlüsselte Datendatei hat den Namen: Fach1.Tresor
Dann hat die zugehörige Salt-Datei den Namen Fach1.Salt
Beide Dateien finden Sie im Verzeichnis "/Tresor", das beim allerersten Programmstart von "MyPassworts" automatisch erstellt wird. (Näheres sh. FAQ)

Eine weitere sicherheitsmaßnahme von "MyPasswords" ist die Tatsache, dass dieses Programm das erzeugte GPG-File nachträglich(!) willkürlich verändert: Es werden Buchstaben innerhalb des verschlüsselten Textes vertauscht; WIE dieses Vertauschen Stattfindet hängt wiederum von den eingegebenen schlüsseln ab und ist nachträglich in keinster Weise dem "Buchstabensalat" des

verschlüsselten Textes anzusehen. Ihre verschlüsslte datei kann also mit dem "GPG-Programm" nicht mehr entschlüsselt werden, da bereits ein einziger falscher Buchstabe in diesem GPG-File ein Entschlüsseln unmöglich machen würde.
Diese Vorsicht ist wahrscheinlich übertrieben, schadet aber auch niemadem. Vielleicht macht die Mathematik und die Primzahlforschung ja plötzlich weitere und unerwartete Fortschritte oder Quantencomputer finden in wenigen Jahrzehnten jedes Passwort in Bruchteilen von Sekunden:
Mit "MyPasswords" sind Sie darauf vorbereitet ;-)

<u>**FAQ (Häufige Fragen)**</u>

<u>Kann man beliebige Salt-Dateien verwenden?</u>

Prinzipiell schon, ich bin mir aber nicht sicher, ob dies den Schutz Ihrer Daten tatsächlich weiter erhöht. Sie können eine beliebige Bilddatei z.B.: (xy.jpg) oder ein MP3-File ebenfalls als "Salt-Datei verwenden. Dazu müssen Sie diese Datei zunächst umbenennen. Wenn Ihr zukünfiges Tresorfach den Namen "Fach33" haben soll, dann lautet die Datendatei "Fach333.Tresor". Wenn Sie nun VOR der Generierung dieser Datendatei ihre gewünschte Salt-Datei umbenennen in "Fach33.Salt" und dieses File in den Ordner "Tresor" kopieren, dann wird Ihre gewünschte "Salt-Datei" bei der Erzeugung Ihrer Datendatei "Fach33.Tresor" als gültige "Salt-Datei" anerkannt. Ein nachteil dieser Vorgehensweise könnte sein, dass sie diese "individuelle Salt-Datei" nie mehr erzeugen können, wenn diese Datei verloren geht. Wenn Sie eine Salt-Datei verwenden, die vom Programm "MyPasswords" erzeugt wird, dann können Sie diese Salt-Datei erneut erzeugen, wenn Sie das Passwort noch wissen, das diese Salt-Datei erzeugt hat.

<u>Kann ich nur Passswörter verschlüsseln?</u>

Natürlich nicht! Jeder beliebige Text kann mit "MyPasswords" extrem sicher verschlüsselt werden.

<u>Gibt es eine Möglichkeit, die Anzeige der Passwörter alphabetisch zu sortieren?</u>

Programmtechnisch wäre dies sehr leicht realisierbar. Es gibt aber Probleme, wenn Sie beliebige Texte mit "MyPasswords" speichern und verschlüsseln, denn auch dann werden die Zeilen innerhalb dieses Textes alphabetisch sortiert, was zu Unlesbarkeit Ihres Textes führen würde. Außerdem machen Sie ja möglicherweise Anmerkungen zu einzelnen Passwörtern in einer neuen Zeile. auch derartige Anmerkungen wären dann nicht mehr ihrer ursprünglichen Textzeile zuordenbar.

<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Das Programm "GPG" ist in vielen Linux-Distributionen bereits vorhanden und wird deshalb in der einen Linux-Download-Datei nicht "mitgeliefert".
In der Windows-Download-Datei ist das Programm "gpg.exe" enthalten.
Sollte in Ihrer Linux Distribution nicht installiert sein, so installieren Sie diese Programme bitte noch gesondert nach. Ihre Linux-Distribution bietet Ihnen die entsprechenden Möglichkeiten.

"MyGPGNoSpy" nutzt das Programm "GPG", das wohl bedeutsamste und anerkannteste Verschlüsselungsprogramm als eigenständiges "externes" Programm in unveränderter Form. Sowohl in "MyMemoryDB" als auch in "MyGPGNoSpy" und auch in "MyPasswords" ist KEIN Programmcode von "GPG enthalten. "GPG" wird lediglich als externes "Fremdprogramm" von "MyPasswords" aufgerufen.

Die Lizenzbedingungen für "GPG" finden Sie hier:
http://www.gnu.de/documents/gpl.de.html - http://www.gnupg.de/index.de.html
Diese werden in der Windows-Version beim Download mitgeliefert.

Das Programm "MyGPGNoSpy", "MyMemoryDB" und "MyPasswords" ist kostenlos und in seiner Nutzungsdauer undim Nutzungsumfang in keiner Weise eingeschränkt.

Sehr gerne dürfen Sie diese Programme auch weiterempfehlen und auch weiterverbreiten. Jedoch dürfen diese Programme nicht verändert werden, insbesondere nicht dieser Text und der Name des Autors.

Die Nutzung des Programmsgeschieht auf eigene Gefahr und Verantwortung. Weder Programmautor noch eine Person, die dieses Programm anbietet und verbreitet, kann für Nutzungsschäden haftbar gemacht werden.