Inhalt

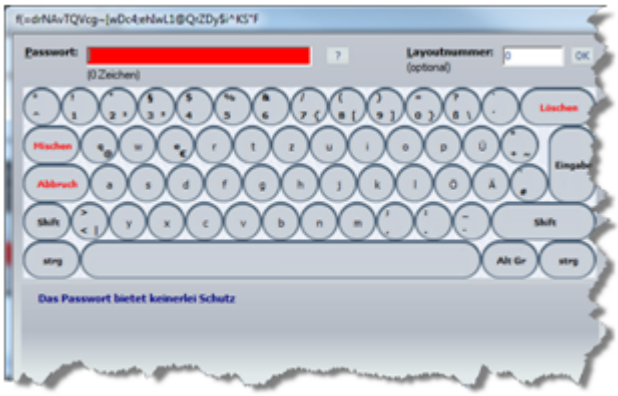
Art der Passworteingabe *

Frage: In ArchiCrypt Passwort Safe kann man wählen, wie man das Passwort für den Passwort Safe eingeben möchte. Welche Variante empfehlen Sie, welches Verfahren ist die beste Wahl?

Antwort: Wenn Sie als Absicherung ein Passwort gewählt haben, können Sie dieses Passwort ganz klassisch über Tastatur eingeben oder über eine virtuelle Tastatur.

1. **Eingaben über die Tastatur** können belauscht werden. So genannte **KeyLogger** protokollieren jeden einzelnen Tastendruck und sind so unter Umständen in der Lage, aus dem Zeichenstrom Passwörter zu extrahieren. Gegen die meisten dieser Schadprogramme bringt ArchiCrypt Passwort Safe bereits einen wirksamen Schutz mit. Das **Anti-KeyLogger Modul**, welches Sie in den Einstellungen finden, schützt dabei auch andere Anwendungen gegen bestimmte Taktiken beim Ausspähen von Tastatureingaben.

2. Die **<u>Eingabe über die virtuelle Tastatur</u>** verhindert generell das Mitschneiden von Tastatureingaben. Sie wählen die Zeichen Ihres Passwortes mit Hilfe der Maus, folglich gibt es keine Tastatureingabe, die man ausspähen könnte. Ein Angreifer müsste hier die komplette Eingabe abfilmen. Im Vergleich zu der eher kleinen Datei beim Protokollieren der Tastatureingaben, die zum Rechner eines Angreifers übertragen werden müsste, würden hier große Datenmengen anfallen. Ein solcher Angriff fällt viel schneller auf und ist extrem aufwendig.



Neben dem klassischen Passwort bietet ArchiCrypt Passwort Safe die Möglichkeit, die Daten mit einer s.g. **<u>Schlüsseldatei</u>** abzusichern. Eine Schlüsseldatei enthält einen 100 Zeichen langen, aus Zufallsdaten aufgebauten Schlüssel, mit dem dann die Daten im Passwort Safe verschlüsselt werden. Eine Schlüsseldatei gibt es in zwei Versionen.

1. **Unverschlüsselte Schlüsseldatei**Sie enthält direkt den Schlüssel, mit dem die Daten im Passwort Safe verschlüsselt werden. Die Schlüsseldatei sollte auf einem Wechselmedium (*zum Beispiel USB-Stick*) abgelegt werden. Das Wechselmedium entfernt man nach dem Öffnen des Passwort Safes. Ein Datendieb müsste hier die Schlüsseldatei in dem kurzen Moment der Verwendung stehlen.
2. Eine **verschlüsselte Schlüsseldatei** kann nicht unmittelbar genutzt werden. Erst die Eingabe eines Passwortes entschlüsselt die Zeichenkette dieser speziellen Schlüsseldatei. Erst diese entschlüsselte Zeichenkette ist dann in der Lage den Passwort Safe zu öffnen.

In allen Fällen muss ein Angreifer neben dem Passwort auch Ihren Passwort Safe stehlen.

Schutz durch Wissen *

Variante 1 (*Passworteingabe via Tastatur*) und 2 (*virtuelle Tastatur*) schützen die Daten durch Wissen. Wer das Passwort weiß, kommt an die Daten. Das ist zum Beispiel vergleichbar mit Ihrer PIN für das Telefon-Banking. Wer die PIN kennt, hat Zugriff.

Schutz durch Besitz *

Variante 3 (*unverschlüsselte Schlüsseldatei*) schützt durch Besitz. Wer die Schlüsseldatei besitzt, der kann Ihren Passwort Safe öffnen. Das ist vergleichbar mit Ihrem Haustürschlüssel. Wer den besitzt, kommt in Ihre Wohnung.

Schutz durch Besitz und Wissen *

Variante 4 (verschlüsselte Schlüsseldatei) kombiniert die beiden Varianten. Sie müssen das Passwort für die Schüsseldatei wissen und Sie müssen die Schlüsseldatei selbst besitzen. Dieses Prinzip ist vergleichbar mit einer EC-Karte. Man muss die Karte besitzen und die PIN kennen, um Geld abzuheben.

Wie sieht es jetzt mit der Sicherheit der Verfahren aus, welche Variante ist die sicherste? *

Man sieht relativ leicht, dass Version 4 (*verschlüsselte Schlüsseldatei*) die sicherste Wahl ist. Hier muss der Angreifer erheblichen Aufwand betreiben. Er muss die Passwort Safe Datei entwenden, die Passworteingabe, die selbst eventuell wieder abgesichert ist, mitschneiden und die Schlüsseldatei, die idealerweise auf einem nur kurz angeschlossenen Wechselmedium abgelegt ist, stehlen.

An die zweite Stelle würde ich, vom Aufwand für den Angreifer aus betrachtet, die Version 2 (*virtuelle Tastatur*) setzen. Hier fallen beim Ausspähen zu viele Daten an, um sie unbemerkt aus dem Rechner zu schleusen.

Sofern Sie die Anti-KeyLogger Funktion nutzen, kann man die Eingabe über Tastatur und die unverschlüsselte Schlüsseldatei gleichauf an Position 3 setzen. Wenn Sie die Anti-KeyLogger Funktion nicht nutzen können, dann findet sich die klassische Passworteingabe via Tastatur auf dem 4. Platz wieder.

Warum werden dann überhaupt verschiedene Varianten angeboten? *

Die Wahl ist immer ein Kompromiss. Lege ich mehr Wert auf Komfort oder mehr auf Sicherheit. Die verschlüsselte Schlüsseldatei auf Wechselmedium verlangt dem Anwender Geduld und Konsequenz ab. Die Eingabe über Tastatur ist hingegen bei einem 12 Zeichen Passwort immer noch schnell erledigt, könnte jedoch leichter belauscht werden. Wenn Sie, alles andere wäre grob fahrlässig, eine aktuelle Schutzsoftware (*Antiviren-Software und Firewall*) auf Ihrem Rechner haben, sind jedoch alle Varianten ausreichend sicher.

Aber, wie immer, wenn es in der digitalen oder realen Welt um Sicherheit geht, gilt der Spruch:

> **Eine hundertprozentige Sicherheit gibt es nicht!**