INFORMATIONSSICHERHEIT

20.06.2016

Merkblatt: Gute Passwörter

Ein gutes Passwort ...

- schöpft die volle Möglichkeit von acht (besser 10 oder deutlich mehr) Zeichen aus
- enthält mindestens zwei Buchstaben unter Verwendung von Groß- als auch Kleinbuchstaben
- enthält mindestens zwei Ziffern oder Sonderzeichen, diese stehen nach Möglichkeit nicht nur am Anfang und/oder Ende
- kann man sich leicht merken
- kann man schnell eintippen (das Passwort ist durch „Über-die-Schulter-Schauen“ nicht leicht erkennbar)
- enthält keine (erkennbare) Systematik, d.h. erscheint wie eine zufällig erzeugte Zeichenfolge
- ist kein Wort einer bekannten Sprache
- ist nur dem Inhaber der Kennung bekannt

Mehrere Kennungen

Allgemein gilt: für verschiedene Kennungen sollte man verschiedene Passwörter wählen. Besitzen Sie mehrere Kennungen und sind dadurch gezwungen, sich viele verschiedene Passwörter zu merken, empfiehlt es sich, systematisch Passwort-Familien zu erzeugen. Sie bilden ein 6-7 Zeichen langes Passwort. Dieses kann dann durch 1-2 Zeichen ergänzt werden, die Ihnen die Unterscheidung der verschiedenen Kennungen ermöglichen (Rechnernamen oder Zweck der geschützten Anwendung). Eine weitere Möglichkeit zur Verwaltung mehrerer Passwörter sind sog. „Passwort-Safes“. Dies sind Programme, in denen in einer stark verschlüsselten Datenbank Passwörter gespeichert werden. Diese ist dann mit einem besonders starken Passwort zu schützen.

Bildungsregeln

Es existieren mehrere Möglichkeiten, ein Passwort zu bilden. Grundsätzlich gilt immer: Nicht das Passwort wird gemerkt, sondern die Methode, mit der es gebildet wird!

Eine Übersicht gängiger Passwortbildungsregeln finden Sie auf den Seiten des RRZ unter https://uhh.de/rrz-passwortregeln

Sollten Sie Fragen zum Thema oder Anregungen haben, wenden Sie sich bitte an die ServiceLine des RRZ unter +49 40 42838-7790 oder rrz.serviceline@uni-hamburg.de