Handlungsempfehlung der Goethe-Universität Frankfurt zum Umgang mit Passwörtern

Diese Handlungsempfehlung gilt für alle Angehörigen der Goethe-Universität Frankfurt. Sie regelt den sicheren Umgang mit Passwörtern. Ordnungen und Satzungen der Goethe-Universität, insbesondere die IT-Sicherheitsordnung, IT-Sicherheitsrichtlinie und die IuK-Nutzungsordnung[1], werden durch diese Handlungsempfehlung nicht berührt.

Die Daten in einem System müssen geschützt sein und nur berechtigte Personen dürfen darauf zugreifen. Dies kann mithilfe persönlicher Chipkarten, durch Prüfung biometrischer Eigenschaften (z. B. Fingerabdruck) oder durch Eingabe einer Benutzerkennung und eines Passwortes erfolgen. Kartengestützte und biometrische Anmeldeverfahren gewinnen zwar immer mehr an Bedeutung; in der Praxis dominiert jedoch bislang die Anmeldung mit Benutzerkennung und Passwort. Dieses Merkblatt stellt dar, wie sich ein möglichst sicherer Passwortschutz realisieren lässt.

Erfährt jemand Ihre Benutzerkennung und Ihr Passwort, so kann er sich damit unter Ihrem Namen anmelden und auf Ihre Daten und Programme zugreifen, die nicht für ihn bestimmt sind. Da Benutzerkennungen vielfach nicht geheim sind, kommt der Geheimhaltung der persönlichen Passwörter die entscheidende Rolle zu.

Das Sicherheits-Management-Team (SMT) der Goethe-Universität empfiehlt folgende Regeln für die Wahl von Passwörtern:

1) Es wird eine Passwortlänge von **16 Zeichen** empfohlen, mindestens 10 Zeichen sollten es aber auf jeden Fall sein.

2) Das Passwort sollte Groß-/Kleinbuchstaben, Zahlen und möglichst **Sonderzeichen** enthalten.

3) Um ein Passwort der nötigen Länge zu finden, das man sich auch leicht merken kann, können beispielsweise zwei oder mehr ***zusammenhangslose (!)*** Wörter aneinandergehängt werden, wenn zufällige Zeichen zwischen sie gestreut werden.

4) Sofern technisch nur kürzere Passwörter möglich sind, sollte auf eine große „**Zufälligkeit**“ der Zeichen geachtet werden. Dies kann man erreichen, indem man sich einen Satz merkt, die Anfangsbuchstaben der Worte nimmt und an passender Stelle noch Sonderzeichen einstreut.

[1] Allgemeine Nutzungsordnung für die Informationsverarbeitungs- und Kommunikationsinfrastruktur der Goethe-Universität Frankfurt

5) Das Passwort darf nicht leicht zu erraten sein, wie zum Beispiel Benutzername, Vor- oder Nachname, Kfz-Kennzeichen, Geburtsdatum.

6) Das Passwort muss **geheim** gehalten und sollte regelmäßig geändert werden. **Dienstliche Passwörter** dürfen **nicht** bei externen Diensten verwendet werden.

7) Ein Passwort sollte immer nur an einer Stelle benutzt werden. Leicht merken kann man sich diese Passwörter dennoch, wenn man z. B. einige wechselnde Zeichen vor eine häufiger genutzte Zeichenkette stellt, also beispielsweise „`GUHier2Mond%Kachel`“, „`1aHier2Mond%Kachel`“ ...

8) **Mail-Zugänge** müssen besonders gut geschützt werden, da darüber alle anderen Passwörter geändert werden können. Hier dürfen also keinesfalls Passwörter verwendet werden, die auch an anderer Stelle genutzt werden.

9) **Beispiele** für Passwörter sind (verwenden Sie diese Beispiele auf keinen Fall als Passwort, diese kann man nämlich jetzt einfach ausprobieren …):

   ```
   Hier2Mond%Kachel
   6uybi+sY
   msJ$DR8Ttx
   …
   ```

10) „**Passwort-Manage**r”, also Programme, die Passwörter speichern, helfen, viele verschiedene Passwörter zu nutzen. Die Passwort-Manager der Webbrowser sollten nur genutzt werden, wenn diese mit einem eigenen Passwort geschützt werden können. Externe Programme sind eher zu empfehlen.

11) Ein **Passwortwechsel** ist sofort durchzuführen, wenn der Verdacht besteht, dass das Passwort unautorisierten Personen bekannt geworden ist oder wenn der Verdacht auf eine **System-Kompromittierung** besteht. In diesem Fall wenden Sie sich unverzüglich an den zuständigen Administrator bzw. IT-Sicherheitsbeauftragten. Das **HRZ-Passwort** können Sie unter diesem Link ändern: https://kartenservice.uni-frankfurt.de/mitarbeitercard/password

12) Bei Fragen können Sie sich an Ihren zuständigen IT-Support bzw. an Ihre/n IT-Sicherheitsbeauftragte/n wenden.

Informationsquellen

- Bundesamt für Sicherheit in der Informationstechnik (BSI)
  https://www.bsi-fuer-buerger.de

- DFN Computer Emergency Response Team (DFN-CERT)
  https://www.dfn-cert.de

- IT-Sicherheitsmanagement-Team (SMT) der Goethe-Universität
  https://www.uni-frankfurt.de/smt

- Goethe-Universität Computer Emergency Response Team (GU-CERT)
  https://www.rz.uni-frankfurt.de/gu-cert

- Hochschulrechenzentrum (HRZ) der Goethe-Universität
  https://www.uni-frankfurt.de/hrz/it-sicherheit