Passwortsicherheit

Das Passwort

Das Passwort ermöglicht die Authentifizierung der Benutzer an verschiedenen Servern im URZ und in der Verwaltung der FSU.
Es wird in verschlüsselter Form gespeichert; nicht einmal der Systemverwalter kann es lesen.
Sie besitzen also möglicherweise mehrere verschiedene Passwörter:

- ein Passwort für Ihre E-Mail
- ein Passwort für tägliche Programm-Anwendungen
- ein Passwort für Web-Anwendungen usw.

In diesen Erläuterungen soll nur auf den Zugang zum Universitätsnetz eingegangen werden.
Das Passwort ist Ihrer Benutzerkennung fix zugeordnet.
Das Passwort darf nur dem Besitzer der Benutzerkennung bekannt sein, um Missbrauch der Benutzerdaten zu vermeiden.
Eine Weitergabe an Dritte verstößt gegen die Benutzungsregelungen.
Wer ein berechtigtes Interesse am Zugang zum Netz der Verwaltung der Universität Jena hat, kann jederzeit einen eigenen Zugang erhalten.

Wie soll ein Passwort aussehen?

Vermeiden Sie:

- *Namen oder typischen Daten:* Namen berühmter Menschen oder Charaktere aus Kino und Fernsehen, Namen von Orten, Kinofilmen, Fernsehshows und -serien, Titel von Liedern, Geburtsdaten, Studienrichtung etc.
- *Beispiel-Passwörter aus Hilfetexten oder Formularen*
- *Einträge aus Wörterbüchern oder Wörter aus irgendeiner Sprache:* diese können mit modernen Passwort-Suchprogrammen erkannt werden und erleichtern auch das Erraten der Passwörter.

Verwenden Sie:

- *mindestens acht Zeichen mit mindestens zwei Buchstaben und einer Zahl oder einem Sonderzeichen*, sonst besteht die Gefahr, dass es kombinatorisch geknackt werden könnte
- *folgende erlaubte Sonderzeichen*:
  & ! ? * \ ' $ % : + , - < = # " @ ; > /) (_ [.] { ~ }
  Die Verwendung von Steuerzeichen (z.B. CONTROL-Sequenzen) und Umlauten wird nicht empfohlen, da dies zu unerwünschten Effekten führen kann.

Wie sieht ein gutes Passwort aus?

- eine Buchstaben-Zahlen-Sonderzeichen-Kombination, die als gebräuchlicher Ausdruck nicht vorkommt, die aber über bestimmte Assoziationen **leicht zu merken** ist
- eine ungewöhnliche Groß- und Kleinschreibung und bewusstes "Falschschreiben": siehe Beispiel unten
- das Passwort soll schnell und sicher einzugeben sein, um Mitlesen durch andere personen bei der Eingabe zu vermeiden
- Passwörter sollten niemals auf aufgeschrieben (Negativbeispiel: Post-It am Monitor) oder im Rechner gespeichert werden. Falls Sie das Passwort zur Sicherheit doch aufschreiben möchten, behandeln Sie den Zettel mit dem aufgeschriebenen Passwort wie z.B. einen Bankautomatcode, der anderen Personen nicht zugänglich sein soll.

Beispiele (nächste Seite):

Beispiel 1:
Nehmen Sie ein Lied, das Sie besonders mögen oder auch eine längere Gedichtzeile, die Sie ohne Probleme auswendig aufsagen können. Folgende Liedzeile nehmen, kennt bestimmt fast jeder:
Im Frühtau zu Berge wir zieh`n fallera...
Nun nehmen wir die Anfangsbuchstaben (oder die Endbuchstaben) der Worte und nehmen statt des Wortes **wir** die Zahl **vier**, die ähnlich klingt (bewusstes Verfälschen); dabei kommt heraus:
I F z B 4 z f
das sind aber nur 7 Zeichen: IFzB4zf
Lassen Sie sich noch etwas einfallen, z.B.:
Als sie das letzte mal wanderten,
schien die Sonne ***** (Sonderzeichen) Passwort: **IFzB4zf***
oder der Himmel war bedeckt **)** Klammer zu (Himmel zugezogen) Passwort: **IFzB4zf)**

Beispiel 2:
Sie haben im letzten Urlaub in **Südtirol,** Stadt **Meran, Hotel "Alpenglühen", Zimmer 265** gewohnt:
--> Passwort nach ähnlichem Schema:
SM,H"A"265

Beispiel 3 (einfaches Schema):
DZMRkF2mal
Auflösung: **D** aumen **Z** eigefinger **M** ittelfinger **R** ingfinger **k** leiner **F** inger **2** mal **(oder 2x)**
Der Fantasie sind keine Grenzen gesetzt.

Trotz aller Vorsichtsmaßnahmen wird ein regelmäßiger Wechsel des Passwortes, mindestens einmal monatlich, empfohlen. Alle Passwörter, die Ihnen vom Systemadministrator zugewiesen werden, müssen sofort geändert werden!