Passwortrichtlinie

Christian-Albrechts-Universität zu Kiel
Rechenzentrum

Stand Juli 2017

Präambel

Viele Systeme und Datenbestände an der Christian-Albrechts-Universität zu Kiel (CAU) sind mit Benutzername/Passwort-Kombinationen geschützt. Sinn der Passworte ist es, sowohl zum Schutz dienstlicher Daten als auch in Ihrem eigenen Interesse eine Einsicht oder Änderung Ihrer Daten durch Unbefugte zu verhindern. Um diese Vertraulichkeit zu gewährleisten, legt das Rechenzentrum im Folgenden Mindestanforderungen an Passworte fest. Diese Richtlinie richtet sich an alle Personen innerhalb der CAU, die IT-Dienste nutzen, und ergänzt die für alle verbindliche Benutzungsrahmenordnung (Satzung) für die Kommunikations- und Datenverarbeitungsinfrastruktur der CAU.

Zielsetzung

Die unten vorgegebenen Regeln haben das Ziel, eine Sicherheit gegen automatisches Durchprobieren von Passwörtern zu erreichen. Für die angestrebte Schutzstärke gegen Durchprobieren ist ein Mindestmaß an Strukturlosigkeit / Zufälligkeit / Komplexität von Passwörtern erforderlich. Bedenken Sie aber auch, dass keine technische Richtlinie schützen kann, wenn Passwörter bewusst oder unbewusst, etwa durch so genannte „Phishing-Attacken“ an Dritte weitergegeben werden. Gehen Sie daher stets sorgsam mit Ihren Passwörtern um.

Die folgenden Regeln sind Mindestanforderungen für den allgemeinen Betrieb; wenn Sie mit vertraulichen, personenbezogenen oder sonstigen besonders schutzbedürftigen Informationen arbeiten, sollten Sie Ihr Passwort im Zweifelsfall länger wählen.

Aufbau von Passwörtern

Ein Passwort darf sich aus Zeichen der folgenden vier Gruppen zusammensetzen:

- Kleinbuchstaben: `abcdefghijklmnopqrstuvwxyz`
- Großbuchstaben: `ABCDEFGHIJKLMNOPQRSTUVWXYZ`
- Ziffern: `1234567890`
- Sonderzeichen: `!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~`

Bitte beachten Sie, dass diese Liste aus technischen Gründen insbesondere nicht Umlaute, ß, Leerzeichen sowie einige auf der Tastatur verfügbare Sonderzeichen wie § und ° umfasst.

Die erforderliche Mindestlänge des Passwortes hängt davon ab, wie viele der oben genannten Zeichengruppen verwendet werden und beträgt

- **14 Zeichen**, falls das Passwort nur aus Groß- oder nur aus Kleinbuchstaben besteht. Ein Passwort, das nur aus Ziffern oder nur aus Sonderzeichen besteht, ist nicht zulässig.
- **12 Zeichen**, falls zusätzlich zur Gruppe Großbuchstaben oder zur Gruppe Kleinbuchstaben eine weitere Zeichengruppe benutzt wird, also z.B. Kleinbuchstaben und Ziffern oder Groß- und Kleinbuchstaben.

- **10 Zeichen**, falls drei der oben genannten Zeichengruppen benutzt werden, also z.B. Großbuchstaben, Ziffern und Sonderzeichen.
- **9 Zeichen**, falls alle vier der oben genannten Zeichengruppen benutzt werden.

Die hier genannten Längen sind Mindestlängen, um das angestrebte Sicherheitsniveau mit einem „zufällig gewürfelten" Passwort (z.B. „NR27fHUpfG") zu erreichen. Ein Passwort, das „sinnvolle" Worte enthält, sollte mindestens 50% länger sein als oben empfohlen. Zusätzlich behält das Rechenzentrum sich vor, eine Sperrliste mit zu einfach zu erratenden Passwortbestandteilen (z.B. „passwort" oder „1234") zu führen, die in Ihrem Passwort dann nicht vorkommen dürfen.

Leider sind nicht alle eingesetzten Systeme in der Lage, diese Richtlinien vollständig umzusetzen (z.B. wegen einer Längenbeschränkung der Passwörter auf 6 Zeichen). In diesen Fällen ist die Richtlinie so gut wie möglich umzusetzen, etwa durch Ausschöpfung der erlaubten Passwortlänge und zufällige Wahl aus allen erlaubten Zeichengruppen.

Änderung der Passwörter

Angesichts der relativ hohen Zufälligkeit des Passwortes halten wir einen turnusmäßigen Änderungszwang im Regelfall nicht für notwendig. Sie sollten allerdings in folgenden Fällen unbedingt Ihr Passwort ändern:

- Sie haben Befürchtung, dass Ihr Passwort nicht mehr geheim ist, etwa,
  - weil Sie es auf einem Rechner eingegeben haben, der sich nachträglich als nicht vertrauenswürdig herausgestellt hat (Viren- oder Malwareinfektion, etc.),
  - weil Sie dem Link in einer unerwarteten Mail gefolgt sind, die Sie zu einer Passwortänderung aufgefordert hat,
  - weil Sie eine alte Festplatte oder ein Mobiltelefon mit noch gespeicherten Zugangsdaten verloren haben oder diese nicht regelgerecht entsorgt wurden. Auch ein Gerätedefekt bedeutet im Regelfall nicht, dass die gespeicherten Daten nicht mehr auslesbar sind!
- Ihr Passwort wurde für Sie neu gesetzt.

Sicherer Umgang mit Passwörtern

Auch ein gegen automatisierte Angriffe geschütztes Passwort ist nicht gegen physischen oder digitalen Diebstahl geschützt.

- Geben Sie Ihr Passwort nicht auf Rechnern ein, denen Sie nicht vertrauen!
- Speichern Sie Ihr Passwort nicht unverschlüsselt auf Ihrem Rechner oder Mobilgerät!
- Setzen Sie in Anwendungssystemen wenn möglich Masterpasswörter.
- Geben Sie Ihr Passwort nicht Dritten bekannt! RZ-Mitarbeiter werden Sie nie nach Ihrem Passwort fragen! Folgen Sie keinen Links in Mails, die Sie unerwartet zur Änderung des Passwortes oder zur Bestätigung Ihres Accounts auffordern!

- Falls Sie Ihr Passwort in schriftlicher Form aufbewahren, tun Sie dies in geeignet gesicherter Form, etwa in einem verschlossenen/versiegelten Umschlag im abgeschlossenen Aktenschrank oder Safe!
- Wenn Sie ein neues Passwort erhalten haben, ändern Sie dieses umgehend, um sicherzustellen, dass das gültige Passwort nur Ihnen bekannt ist.
- Verwenden Sie das gleiche Passwort nicht für mehrere Benutzerkonten oder bei mehreren Dienstanbietern! Es existiert eine große Zahl (auch kostenfreier) Passwortmanager-Software, die Sie bei der Verwaltung mehrerer Passwörter unterstützt. Weitere Informationen finden Sie auf den Web-Seiten des Rechenzentrums.

Rechenzentrum der CAU, 06.07.2017