Passwortrichtlinie der Technischen Universität Darmstadt

IT-Sicherheit der TU Darmstadt
Veröffentlichung: 09. Dezember 2021

TECHNISCHE UNIVERSITÄT DARMSTADT

IT-Sicherhe!t
Informationssicherheit | TU Darmstadt

Kennzeichnung

Titel (Dokumentenkürzel):	Passwortrichtlinie der Technischen Universität Darmstadt (PW-RL)
Ersteller:	Johannes Braun / Review: Jochen Becker
Funktion des Erstellers:	zentraler IT-Sicherheitsbeauftragter / Leiter TUDa-CERT
Versionsnummer:	v02
Letzte Überarbeitung:	10. Dezember 2021
Nächstes geplantes Review:	November 2022
Freigegeben am / durch:	26. November 2021 / Herbert De Gersem, Vizepräsident für Wissenschaftliche Infrastruktur und Digitalisierung
Inkrafttreten:	mit Veröffentlichung, Übergangsfrist bis 30.04.2022
Klassifizierung:	öffentlich
Berechtigte Rollen (Verteilerkreis):	alle Angehörige der TU Darmstadt
Änderungsübersicht:	v01 $\rightarrow$ v02: Erweiterung der erlaubten Sonderzeichen

Zusammenfassung

Das Ziel dieser Richtlinie (Policy) ist die Sicherstellung eines ausreichenden Sicherheitsniveaus für den Einsatz von Benutzername/Passwort-Verfahren. Die dazu notwendigen grundlegenden Regelungen und Handlungsanweisungen sind im Folgenden angeführt. Die Relevanten IT-Grundschutz-Bausteine sind im Literaturverzeichnis am Ende des Dokuments aufgelistet.

Inhaltsverzeichnis

1 Geltungsbereich

Diese Passwortrichtlinie gilt für die von der Technischen Universität (TU) Darmstadt betriebene IT-Infrastruktur, bestehend aus Informationsverarbeitungssystemen, Kommunikationssystemen und weiteren Hilfseinrichtungen sowie die Beauftragung von Subunternehmen im Bereich IT-Infrastruktur.

Diese Passwortrichtlinie gilt für alle Nutzer_innen und Betreiber_innen von IT-Infrastruktur der TU Darmstadt.

2 Passwort Anforderungen

Im Folgenden werden die grundlegenden Gestaltungsrichtlinien für Passwörter festgelegt.

2.1 Allgemeine Passwort Anforderungen

- Das Passwort muss mindestens 12 Zeichen lang sein (maximal 30 Zeichen).
- Erlaubte Zeichensätze:
  - Großbuchstaben: A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z
  - Kleinbuchstaben: a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z
  - Ziffern: 0,1,2,3,4,5,6,7,8,9
  - Sonderzeichen: ! " $ % & ' ( ) * + , - . / ; < = > ? { | } ~] @
- Es dürfen keine persönlichen Daten, Namen oder die Kennung von Nutzenden enthalten sein.
- Es dürfen keine bekannten Wörter aus einem Wörterbuch verwendet werden – auch nicht von Fremdsprachen.

2.2 Passwort Anforderungen für administrative Accounts sowie Proxy- und Gateway-Accounts

- Das Passwort muss mindestens 20 Zeichen lang sein.
- Das Passwort stammt aus einem Random-Passwortgenerator (zum Beispiel „pwgen 20“ oder KeePass).
- Erlaubte Zeichensätze siehe 2.1.

3 Rechte und Pflichten beim Umgang mit Passwörtern

Im Folgenden werden die Rechte und Pflichten der Nutzer_innen von Passwörtern in ihrer jeweiligen Rolle als Anwender_innen oder Administrator_innen beschrieben.

3.1 Initiale Wahl von Passwörtern

- Für jeden Dienst ist ein eigenes Passwort zu verwenden.[1]
- Durch Administrator_innen oder systemseitig gesetzte Passwörter sind beim darauffolgenden Erstzugriff zu ändern.
- Passwörter sollten möglichst zufällig erzeugt werden. Die Verwendung eines Passwortgenerators in Verbindung mit einem Passwortmanager (bspw. KeePass) wird empfohlen.
- Um gut merkbare Passwörter zu erhalten, können Passwort-Sätze verwendet werden.[2]
- Es sollten möglichst viele der in 2.1 aufgeführten erlaubten Zeichensätze verwendet werden.

3.2 Nutzung von Passwörtern

- Bei der Eingabe von Passwörtern ist darauf zu achten, dass die Eingabe nicht beobachtet wird.
- Passwörter die in den Geltungsbereich dieser Richtlinie fallen dürfen nicht an unsicheren (fremden) Systemen eingegeben werden.
- Persönliche Passwörter dürfen nicht an Dritte weitergegeben werden.
- System-Administratorpasswörter dürfen nur den Personen bekannt sein, die sie zur Erledigung der ihnen übertragenen Aufgaben benötigen. Verlässt eine Person den Kreis der berechtigten Personen (beispielsweise durch Verlassen der TU Darmstadt), so sind die betroffenen Passwörter umgehend zu ändern.
- Ein Passwort muss umgehend gewechselt werden, wenn es unautorisierten Personen bekannt geworden ist oder der Verdacht dazu besteht.

3.3 Aufbewahrung von Passwörtern

- Eine unverschlüsselte Speicherung von Passwörtern auf IT-Systemen ist unzulässig.
- Eine verschlüsselte Speicherung in einem Passwortmanager (bspw. KeePass) ist zulässig.
- Das Notieren von Passwörtern ist zu vermeiden. Ist ein Notieren auf Papier unumgänglich, sind die Unterlagen an einem sicheren, zugangsgeschützten Ort aufzubewahren.
- Die Notfallhinterlegung von Passwörtern in einem Tresor ist zulässig.

[1] Bei Verwendung des TUDa-SSO (Single Sign-On) ist dieser als ein Dienst zu betrachten.

[2] Denken Sie sich einen Satz aus und benutzen Sie von jedem Wort nur den 1. Buchstaben (oder nur den 2. oder letzten etc.). Anschließend verwandeln Sie bestimmte Buchstaben in Zahlen oder Sonderzeichen. Ein Beispiel: „Morgens stehe ich früh auf und putze meine Zähne drei Minuten lang.“ Nur die ersten Buchstaben: „MsifaupmZdMl“. „i“ sieht aus wie „1“, „&“ ersetzt das „und“: „Ms1fa&pmZdMl“.

4 Rechte und Pflichten für Systembetreiber

Betreiber_innen von Authentisierungssystemen haben für ihre Systeme einige grundlegende Regelungen einzuhalten und können darüber hinaus auch weitere Schutzmechanismen etablieren. Systembetreiber_innen können über diese Richtlinie hinausgehende Anforderungen an Passwörter definieren. Diese müssen mindestens das Sicherheitsniveau der vorliegenden Richtlinie erfüllen. Die Einhaltung der Passwortrichtlinie ist soweit technisch möglich systemseitig sicherzustellen. Hierbei ist mindestens die Passwortlänge zu prüfen.

4.1 Speicherung und Zugriffsschutz

- Der Zugriff auf den Passwortspeicher ist kryptografisch gemäß dem Stand der Technik gegen unerlaubten Zugriff zu schützen.
- Passwörter dürfen grundsätzlich nur verschlüsselt über unsichere Netze übertragen werden.

4.2 Intrudersperre und Angriffsschutz

- Es ist ein Verfahren zum Zurücksetzen von Passwörtern zu definieren.
- Eine automatische Accountsperre muss nach 5 Fehleingaben des Passwortes in Kraft treten.
- Sperrfrist des Accounts bei einer automatischen Sperrung beträgt mindestens 5 Minuten.
- Die automatisch erteilte Accountsperre darf (ggf. automatisiert) frühestens nach der Sperrfrist wieder aufgehoben werden.

4.3 Qualitätssicherung der Passwörter

- Die/der Betreiber_in kann direkt beim Setzen eines Passwortes technische Maßnahmen zum Überprüfen der geltenden Policy einsetzen. Hierbei ist unter anderem ein Plausibilitätstest, der trivial oder leicht zu erratende Passwörter verhindern soll, möglich.
- Die/der Betreiber_in kann automatisierte Testprogramme über seinen Nutzerstamm laufen lassen. Diese müssen so gestaltet sein, dass die/der Betreiber_in kann zu keinem Zeitpunkt Kenntnis der konkreten Passwörter seiner Nutzer_innen erhält. Sollten hierbei ungültige oder unsichere Passwörter detektiert werden, so darf der dazugehörige Account direkt gesperrt werden. Die/der entsprechende Nutzer_in muss zur Änderung des Passwortes aufgefordert werden.

Literatur

[1] BSI. „ORP.4.A8 Regelung des Passwortgebrauchs [Benutzer, IT-Betrieb] (B)“. In: *IT-Grundschutz-Kompendium*. Bd. Edition 2021. Bundesamt für Sicherheit in der Infromationstechnik. 2021.

[2] BSI. „ORP.4.A22 Regelung zur Passwortqualität [IT-Betrieb] (B)“. In: *IT-Grundschutz-Kompendium*. Bd. Edition 2021. Bundesamt für Sicherheit in der Infromationstechnik. 2021.

[3] BSI. „ORP.4.A23 Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme [IT-Betrieb] (B)“. In: *IT-Grundschutz-Kompendium*. Bd. Edition 2021. Bundesamt für Sicherheit in der Infromationstechnik. 2021.

[4] BSI. „ORP.4.A11 Zurücksetzen von Passwörtern [IT-Betrieb] (S)“. In: *IT-Grundschutz-Kompendium*. Bd. Edition 2021. Bundesamt für Sicherheit in der Infromationstechnik. 2021.

[5] BSI. „ORP.4.A12 Entwicklung eines Authentisierungskonzeptes für IT-Systeme und Anwendungen [IT-Betrieb] (S)“. In: *IT-Grundschutz-Kompendium*. Bd. Edition 2021. Bundesamt für Sicherheit in der Infromationstechnik. 2021.