universität wien

Zentraler Informatikdienst

Policy

Passwörter

Genehmigt durch Ulf Busch

Gültig ab 05.08.2014

Version 1.01

universität wien
Zentraler Informatikdienst

Umgang mit Passwörtern

Zweck

Eine sichere IT-Infrastruktur erfordert es, dass BenutzerInnen nur die Services und Daten zur Verfügung haben, zu deren Nutzung sie berechtigt sind (Autorisierung). Dreh- und Angelpunkt dabei ist die sichere Verwendung von BenutzerInnenkennungen und Passwörtern. Die Policy legt daher einen Mindeststandard für Passwörter an der Universität Wien fest.

1. Anwendungsbereich

Diese Policy bezieht sich auf BenutzerInnenberechtigungen, die vom Zentralen Informatikdienst (ZID) der Universität Wien im Rahmen allgemeiner Services vergeben und verwaltet werden (u:account-UserIDs etc.). Die zugehörigen Passwörter werden im Folgenden als ZID-Passwörter bezeichnet.

2. Policy

2.1. Wahl eines sicheren Passworts

Passwörter müssen so gestaltet sein, dass sie ausreichenden Schutz gegen zu erwartende Angriffe bieten. Ein sicheres Passwort im Sinne dieser Policy

- ist mindestens acht Zeichen lang,
- ist nicht identisch mit einer bestehenden BenutzerInnenkennung und
- enthält mindestens einen Buchstaben (a–z, A–Z) und ein anderes Zeichen (Ziffer und/oder Sonderzeichen).

Weitere Merkmale können bei Bedarf vom ZID im Hinblick auf aktuelle Bedrohungsszenarien festgelegt und bekanntgemacht werden.

Policykonforme Passwörter sind beispielsweise: „m.E.isdaeiguPw“, „Hier-werd-ich-gscheit!“, „Dw1B&k1.“, nicht konforme und unsichere Passwörter sind Zeichenfolgen wie: „12345678“, „qwertzuiop“.

2.2. Weitergabe von Passwörtern

Persönliche Passwörter sind in keinem Fall weiterzugeben, auch nicht an Dienstvorgesetzte, Vertretungen etc. Sie sind weiters auch nicht zur Verwendung „im Notfall" für Dritte zu hinterlegen (z. B. im Institutstresor).

Passwörter zu nicht personenbezogenen BenutzerInnenkennungen (z. B. Service-Mail-Adressen) dürfen nur an Berechtigte weitergegeben werden.

InhaberInnen von BenutzerInnenkonten tragen, sofern sie ihr Passwort z. B. in einem Passwortsafe hinterlegen, die Verantwortung dafür, dass ihr Passwort weder Dritten noch, im Fall von nicht personenbezogenen Kennungen, nicht mehr Berechtigten zugänglich werden kann.

2.3. Zulässige Verwendung von Passwörtern

ZID-Passwörter müssen stets so gewählt werden, dass sie sich von anderen Passwörtern (z. B. für soziale Netzwerke, Webshops etc.) signifikant unterscheiden.

ZID-Passwörter sind nur in Eingabemasken von Systemen einzugeben, die vom ZID betrieben werden (webbasierte Services wie UNIVISonline, Webmail etc.) oder dem lokalen Zugang (z. B. Anmeldung am Arbeitsplatz-PC) dienen.

2.4. Betreiber

Services, die von anderen Einrichtungen der Universität oder externen Dienstleistern betrieben werden, dürfen ZID-Passwörter nicht abfragen oder verarbeiten. Stattdessen ist das Single-Sign-On-System des ZID zu verwenden (die genauen Bedingungen sind am ZID zu erfragen) oder eine separate Accountverwaltung einzurichten, die auch deutlich als solche erkennbar sein muss.

2.5. Änderung und Sperren von Passwörtern

Wenn Grund zur Annahme besteht, dass ein ZID-Passwort Dritten bekanntgeworden sein könnte, ist unverzüglich ein neues zu wählen. Bei Gefahr im Verzug ist der ZID berechtigt, BenutzerInnenkonten, Passwörter, IP-Adressen etc. temporär oder dauerhaft zu sperren. Um diese Sperren wieder aufzuheben, ist der Helpdesk des ZID zu kontaktieren.

Die/Der InhaberIn einer BenutzerInnenkennung hat jedenfalls ein neues, nicht zuvor benutztes Passwort zu wählen

- bei Verlust eines Gerätes, auf dem ZID-Passwörter eingegeben wurden,

- bei Kompromittierung eines solchen Geräts (z. B. durch einen Virus),
- bei Weitergabe des Passworts (z. B. Antwort auf Phishing-Angriff) oder
- nach Ablauf von zwei Jahren seit der letzten Passwortänderung.

Im Fall von nicht personenbezogenen Kennungen ist auch ein neues Passwort zu wählen, sobald einE BerechtigteR die Berechtigung verliert.

BenutzerInnen sind dazu aufgefordert den ZID zu unterstützen, indem sie bei Bedarf an der Aufklärung allfälliger Zwischenfälle mitwirken.

3. In Kraft treten

Bestehende Services oder Prozesse, die noch nicht dieser Policy entsprechen, sind sobald wie möglich zu aktualisieren. Darüber ist das Einvernehmen mit der Stabsstelle IT Security herzustellen.

Bei Zweifels- oder Auslegungsfällen präzisiert die Stabsstelle IT Security in erster, der CIO in zweiter und letzter Instanz die gegenwärtige Richtlinie.