Richtlinie
zur Wahl und Nutzung von Passwörtern und Passphrases

Stand: 01.06.2012

Alle Personenbezeichnungen in dieser Richtlinie beziehen sich ungeachtet ihrer grammatikalischen Form in gleicher Weise auf Frauen und Männer.

1. Kurzbeschreibung

Der Zugang zu am LRZ betriebenen Diensten und Systemen wird technisch durch Authentifizierungsverfahren abgesichert. Üblicherweise kommen dabei passwortbasierte oder damit verwandte Verfahren zum Einsatz. Der jeweilige Benutzer verwendet in der Regel

- entweder das seiner LRZ-Kennung über das LRZ-Id-Portal zugeordnete Passwort,
- oder er sichert andere zur Authentifizierung genutzte Informationen – beispielsweise die privaten Schlüssel von SSH-Keypairs bzw. (Grid-) User-Zertifikaten – über Passwörter bzw. Passphrases ab.

Die vorliegende Richtlinie regelt die Pflichten aller Benutzer von LRZ-Diensten und -Systemen bei der Wahl und Nutzung von Passwörtern und Passphrases für LRZ-Kennungen, die über Master User vergeben wurden; für LRZ-Kennungen, die über Campus^{LMU}, TUMonline oder Grid-Projekte eingerichtet wurden, gelten separate Regelungen.

2. Begriffsbildung: Passwörter bzw. Passphrases

Jeder über die LRZ-Benutzerverwaltung vergebenen Kennung kann über das LRZ-Id-Portal ein *Passwort* zugewiesen werden. Die Eingabe des Loginnamens der Kennung und des zugehörigen Passworts ist ein klassisches und auch für LRZ-Dienste und -Systeme weit verbreitetes Authentifizierungsverfahren.

Demgegenüber stammt der Begriff *Passphrase* aus dem Umfeld von Public-/Private-Key-basierten Authentifizierungsverfahren, die z.B. mittels SSH-Schlüsselpaaren und (Grid-) User-Zertifikaten für ausgewählte LRZ-Dienste und -Systeme angewendet werden können. Die Authentifizierung erfolgt dabei über einen geheim zu haltenden Private-Key, der i.A. als Datei im Home-Directory des Benutzers abgelegt wird. Diese Datei muss zum Schutz vor unberechtigten Zugriffen verschlüsselt werden. Zu die-

sem Zweck fordern z.B. SSH-Clients und Grid-Middleware-Werkzeuge den Benutzer zur Eingabe einer Passphrase auf – statt eines einzelnen Passworts soll also eine Wortfolge bzw. Phrase mit zu einem Passwort ähnlichen Eigenschaften eingegeben werden.

Im Folgenden wird deshalb primär der Begriff Passwort verwendet; alle Regelungen gelten jedoch sinngemäß auch für Passphrases.

3. Geltungsbereich

Diese Richtlinie gilt für alle LRZ-Benutzer, deren LRZ-Kennung über Master User eingerichtet wurde. Sie bezieht sich auf

- alle IT-Dienste und Systeme, die vom LRZ bereitgestellt, betrieben oder betreut werden;
- alle Kennungen, die auf den o.g. IT-Diensten und Systemen eingerichtet werden, unabhängig davon, ob es sich um in der LRZ-Benutzerverwaltung zentral erfasste Kennungen oder lokal eingerichtete Kennungen handelt;
- alle Authentifizierungsverfahren, die auf Passwörtern basieren bzw. diese unterstützend anwenden können. Neben der Verwendung von Loginname-/Passwort-Authentifizierung umfasst dies insbesondere auch den Einsatz von Passphrases zum Schutz der sog. Private Keys von SSH-Schlüsselpaaren und (Grid-) User-Zertifikaten.

Es obliegt jedem Dienst- und Systembetreiber, darüber hinaus für seine Systeme selbst bedarfsorientiert strengere Regeln als in dieser Richtlinie zu definieren und umzusetzen.

Für LRZ-Mitarbeiter gilt eine separate Dienstanweisung, die ebenfalls strengere Regeln als diese Richtlinie vorgibt.

4. Zielsetzung

Kompromittierte Kennungen, bei denen Angreifer Kenntnis der jeweiligen Passwörter erlangen, gehören bislang zu den häufigsten Ursachen für Sicherheitsvorfälle am LRZ. Die vorliegende Richtlinie zielt auf die Sicherstellung eines notwendigen Sicherheitsniveaus beim Einsatz von Loginname-/Passwort-Verfahren und ähnlichen Authentifizierungsmethoden ab.

Die Richtlinie legt dazu die Pflichten von Benutzern aller Dienste fest, die auf LRZ-Servern erbracht werden. Sie soll einerseits dabei unterstützen, Fehler beim Umgang mit Kennungen und passwortbasierten Authentifizierungsverfahren zu vermeiden. Andererseits soll sie erfolgreichen Angriffsversuchen dadurch vorbeugen, dass von allen Benutzern qualitativ hochwertige Passwörter verwendet werden.

5. Regelungen zur Wahl und Nutzung von Passwörtern und Passphrases

§1) Passwortqualität: Um ein Erraten von Passwörtern, z.B. durch wörterbuchbasierte Angriffe oder ein systematisches Ausprobieren aller möglichen Zeichenkombinationen, zu erschweren, gelten folgende Pflichten bei der Wahl von Passwörtern:

1. Das Passwort muss aus mindestens acht Zeichen bestehen. Insbesondere bei Kennungen mit besonderen Berechtigungen (z.B. Systemadministration) sind bis zu 20 Zeichen lange Passworte zu wählen.
2. Das Passwort soll so komplex wie möglich aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen zusammengesetzt werden. Es muss mindestens zwei Buchstaben und mindestens eine Ziffer oder ein Sonderzeichen enthalten.
3. Bei Passwortänderungen muss sich das neue Passwort in mindestens drei Stellen vom alten unterscheiden. Es darf zudem den Loginnamen der Kennung nicht enthalten, auch nicht in Form einer Permutation.
4. Passwörter, die leicht zu erraten sind, dürfen nicht verwendet werden. Zu vermeiden sind dabei insbesondere
    a. Zeichenwiederholungen,
    b. Zahlen und Daten aus dem Lebensbereich des Benutzers,
    c. einfache Ziffern- und Buchstabenkombinationen,
    d. Zeichenketten wie 1qay2wsx, die durch nebeneinander liegende Tasten eingegeben werden,
    e. Zeichenkombinationen, die Suchbegriffen in Wörterbüchern oder Lexika entsprechen.
5. Passwörter für LRZ-Kennungen müssen sich von Passwörtern für Dienste, die außerhalb des Münchner Wissenschaftsnetzes erbracht werden, unterscheiden.

§2) Passwortablauf: Passwörter müssen von Benutzern nach einer dem Schutzbedarf angemessenen Frist, spätestens jedoch nach zwölf Monaten gewechselt werden.

§3) Passwortnutzung: Bezüglich der Nutzung von Passwörtern von *persönlichen LRZ-Kennungen* gelten die folgenden Regelungen:

1. Passwörter sind geheim zu halten. Sie dürfen nicht an andere Personen weitergegeben oder diesen zugänglich gemacht werden; insbesondere werden LRZ-Mitarbeiter nie per E-Mail, telefonisch oder persönlich nach Passwörtern fragen (siehe auch LRZ-Benutzungsrichtlinien §4 (3)).
2. Passwörter sind von anderen unbeobachtet einzugeben.
3. Passwörter dürfen nicht unverschlüsselt auf Rechnern gespeichert werden.
4. Initialpasswörter und zurückgesetzte Passwörter sind vor der Nutzung der Dienste durch eigene Passwörter zu ersetzen.

5. Nicht mehr benötigte oder für einen längeren Zeitraum nicht genutzte Kennungen sind zu sperren.
6. Auf zum Zugriff auf LRZ-Dienste und -Systeme genutzten Endgeräten sind nach Möglichkeit passwortgeschützte Bildschirmschoner bzw. damit funktional äquivalente Software zu verwenden, die beim Verlassen des Arbeitsplatzes bzw. nach einer angemessenen Zeit den Zugriff auf das angemeldete Endgerät verhindern.

Verbindliche Anmerkungen:

1. Der in §2 vorgegebene Passwortablauf wird durch eine rechtzeitige Aufforderung des Benutzers zur Passwortänderung und durch eine Sperre der Kennung nach Verstreichen der Ablauffrist unterstützt. Dadurch gesperrte Kennungen können über das LRZ-Id-Portal wieder entsperrt werden. Ausgenommen von automatischen Sperren sind LRZ-Kennungen, die über Campus^{LMU}, TUMonline oder Grid-Projekte vergeben wurden, da für diese separate Vereinbarungen und Sicherheitsmaßnahmen getroffen wurden.
2. §3 Regelung 3 gilt sinngemäß auch für andere Authentifizierungsinformationen, insbesondere Private-Keys, die für persönliche Kennungen im Rahmen von SSH-Schlüsselpaaren und (Grid-) User-Zertifikaten eingesetzt werden. Diese Private-Keys müssen mit einer Passphrase geschützt werden, die den Vorgaben von §1 - §3 entspricht.
3. Für die so genannten *LRZ-Funktionskennungen*, die beispielsweise im Rahmen von am LRZ gehosteten Webdiensten eingesetzt werden, gelten diese Regeln sinngemäß mit der Ausnahme, dass die beschränkte Weitergabe der Passwörter und deren unverschlüsselte Speicherung z.B. in Skripten für Web-Anwendungen gemäß den LRZ-Benutzerverwaltungsprozessen zulässig sind (siehe http://www.lrz.de/wir/kennung/). Hierbei ist darauf zu achten, dass das unerlaubte Auslesen der Passwörter, beispielsweise durch strikte Zugriffsbeschränkung im Dateisystem, verhindert wird.
4. Das LRZ-Id-Portal überprüft bei Passwortänderungen die Qualitätskriterien §1 1.-3. (Länge, Komplexität und Unterschied zum vorherigen Passwort).

6. Inkrafttreten und Durchsetzung

Diese Richtlinie wurde von der Leitung des LRZ verabschiedet und tritt zum 01.06.2012 in Kraft. Ansprechpartner zu Fragen rund um die Verwendung von Passwörtern durch Benutzer sind die jeweiligen Master User.

7. Anhang

7.1. Weitere relevante Dokumente

Die folgenden LRZ-Dokumente haben einen unmittelbaren Bezug zu dieser Richtlinie:

- LRZ-Benutzungsrichtlinien, siehe http://www.lrz.de/wir/regelwerk/benutzungsrichtlinien.pdf
- LRZ-Artikel zum sicheren Umgang mit Kennungen und Passwörtern, siehe http://www.lrz.de/services/security/passwords/

7.2. Literatur

Die folgende Literatur ist im Rahmen dieser Richtlinie relevant:

- ISO/IEC 27001, normativer Anhang A.11 Zugangskontrolle, insb. *A.11.3.1 Passwortverwendung*
- BSI IT-Grundschutz-Kataloge, Maßnahmenkataloge, insb. *M 2.11 Regelung des Passwortgebrauchs*