Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

Hinweise für die Gestaltung und den Einsatz von Passworten

Für den Benutzer:

1. Ihr Passwort sollte für Sie leicht zu merken, für andere jedoch schwer zu erraten sein. Sie sollten daher keine Trivialpasswörter wie Namen, Geburtstage, Telefonnummern, Urlaubsziele verwenden. Auch gängige Zeichenfolgen (*123456, abcdef, 08/15, 4711, sesam*) bieten keinen wirksamen Schutz. Vermeiden Sie Systematiken (*sesam1, sesam2, sesam3, ...*).
2. nutzen Sie Gestaltungsmöglichkeiten wie Zeichenmischung und Verfremdung (z.B. *zerberus* wird zu *z§rb§r§s* oder *z1rb2r3s*) oder die Mnemotechnik (*Einmal ist keinmal!* wird zu *1x=k1x!*).
3. Notieren oder speichern Sie keine Passworte! Ausnahme: Systemverwalter- oder selten benutzte Passworte. Hinterlegen Sie diese im versiegelten Umschlag an einem sicheren Ort.
4. Geben Sie Passworte grundsätzlich nicht an andere weiter! Soweit dies im Einzelfall unvermeidlich ist, ändern Sie anschließend Ihr Passwort.
5. Ändern Sie Ihr Passwort in angemessenen Zeitabständen, wenn Ihr System Ihnen das nicht automatisch vorgibt. Ändern Sie es nicht zu oft, aber ändern Sie es!
6. Wenn Sie mit mehreren Passworten arbeiten (müssen) versuchen Sie, diese zu synchronisieren. Ein Passwort im Kopf ist günstiger als drei auf Papier.

Für den Systemverwalter:

1. Versehen Sie jede Benutzerkennung mit einem Passwort!
2. Das Passwort sollte mindestens 8 Zeichen lang sein. Sofern nur Ziffern zur Verfügung stehen, sollte die Länge des Passwortes 6 Zeichen nicht unterschreiten. Begrenzen Sie die Zahl erfolgloser Anmeldeversuche und sperren Sie die Benutzerkennung nach Erreichen der zulässigen Anzahl. Sofern für die Passwortvergabe nur Ziffern zur Verfügung stehen, ist die Zahl der zulässigen Fehlversuche auf maximal 3 Fehlversuche zu beschränken.
3. Begrenzen Sie die Gültigkeitsdauer von Passworten; der Zeitraum sollte Abwesenheiten (Urlaub, Krankheit) abdecken, 90 Tage jedoch nicht überschreiten.
4. Passworte sollten verschlüsselt abgelegt werden, und der Zugriff soweit wie möglich beschränkt sein.
5. Nutzen Sie systemseitige Möglichkeiten, die Gestaltung von Passworten zu beeinflussen (Nr. 1 und 2). Soweit möglich, setzen Sie Stopplisten ein, um Trivialpassworte zu verhindern.
6. Richten Sie das System so ein, dass die Benutzer ihr Passwort selbständig ändern können. Von Ihnen sollte lediglich ein Anfangspasswort vergeben werden, das nur für die erstmalige Anmeldung gilt, und anschließend geändert werden muss.

Stand: 01/2017