Datenschutz – RUA: Passwortrichtlinie

Dokumentation für die Freie Christengemeinde KdöR, Sonnefeld

Richtlinie zur Vergabe von Passwörtern

1. Allgemeines

a) Rechtliches

Alle Programme und Online-Dienste sind mindestens mit Passwort oder PIN zu schützen, wenn personenbezogene Daten oder personenbezogene Daten besonderer Kategorien dadurch verarbeitet werden. Dies trägt zur Umsetzung der BFP-DSO und zur allgemeinen IT-Sicherheit bei.

b) Alternativen

Falls vorhanden sind bessere Authentifizierungsmethoden wie z.B. die 2-Faktor-Authentifizierung oder die Public-Key-Infrastructure dem Passwort vorzuziehen.

Ist Programmseitig kein Passwortschutz vorgesehen, so sind die entsprechenden Datendateien (z.B. durch Passwort geschützte ZIP-Files), oder der verarbeitende Rechner durch Passwort zu schützen.

2. Anforderungen an das Passwort

a) Allgemein

Ein Passwort sollte auf keinen Fall eines der folgenden Kriterien enthalten:

- Benutzername
- Klarnamen
- Adresse
- Telefonnummer
- Geburtsdatum
- mit einer Jahreszahl enden

b) Komplexität

Ein Passwort sollte folgende Kriterien erfüllen:

- mindestens 1 Kleinbuchstabe
- mindestens 1 Großbuchstabe
- mindestens 1 Zahl
- mindestens 1 Zeichen
- mindestens 8 Zeichen lang

Empfohlen werden 20 Zeichen lange Passwörter, die durch einen Generator erzeugt wurden.

3. Gültigkeit

a) Häufung

Ein Passwort sollte immer nur für einen einziges Programm bzw. einen einzigen Online-Dienst gelten.

b) Regelmäßiger Wechsel

Ein regelmäßiger Wechsel der Passwörter ist zu empfehlen. Mindestens jedoch alle 3 Jahre sollten alle Passwörter einmal ausgetauscht werden. Die Verwendung alter Passwörter sollte vermieden werden.

4. Aufbewahrung

a) Elektronische Aufbewahrung

Zur Aufbewahrung geeignet sind Passwort-Safe-Programme wie z.B. KeePassXC.

b) Manuell geführte Passwortlisten

Bei manuell geführten Passwortlisten sind diese vor Zugriff durch fremde zu schützen.