Der Landesbeauftragte für den Datenschutz
Mecklenburg-Vorpommern

Empfehlungen zur Passwortgestaltung und zum Sicherheitsmanagement

Orientierungshilfe

Stand: 2003

Postanschrift
Schloss Schwerin
19053 Schwerin

Hausanschrift
Johannes-Stelling-Str. 21
19053 Schwerin

Kommunikation
Telefon (03 85) 5 94 94-0
Telefax (03 85) 5 94 94-58
E-Mail datenschutz@mvnet.de
Internet http://www.lfd.m-v.de

PGP-Fingerprint
ADB5 030A C111
388C A8FD
92B7 EF40 56E6
71DA 3ABA

- Das Passwort darf nicht leicht zu erraten sein, wie Namen, Kfz-Kennzeichen, Geburtsdaten.

- Innerhalb des Passwortes sollte mindestens ein Zeichen verwendet werden, das kein Buchstabe ist (Sonderzeichen oder Zahl).

- Das Passwort sollte mindestens acht Zeichen lang sein. Es muss getestet werden, wie viele Stellen des Passwortes der Rechner überprüft.

- Voreingestellte Passwörter (z. B. des Herstellers bei Auslieferung von Systemen) sind durch individuelle Passwörter zu ersetzen.

- Für besonders wichtige Funktionen (evtl. Systemverwalter) sollten geteilte Passworte verwendet werden, die von zwei Personen einzugeben sind („Vier-Augen-Prinzip“).

- Passwörter dürfen nicht auf programmierbaren Funktionstasten gespeichert werden.

- Das Passwort darf nur dem Benutzer bekannt sein und ist geheim zu halten.

- Das Passwort sollte regelmäßig gewechselt werden, zum Beispiel alle 90 Tage.

- Das Passwort ist unverzüglich zu wechseln, wenn es unautorisierten Personen bekannt geworden ist.

- Alte Passwörter sollten nach einem Passwortwechsel nicht mehr verwendet werden.

- Die Eingabe des Passwortes sollte unbeobachtet stattfinden.

- Passwörter sollten nur dann schriftlich fixiert werden, wenn für den Vertretungsfall (z. B. bei Urlaub oder Krankheit) keine technischen Maßnahmen wie Stellvertreter-Konten eingesetzt werden können. In diesem Falle sind die Passwörter in einem verschlossenen Umschlag sicher aufzubewahren.

Falls IT-technisch möglich, sollten folgende Randbedingungen eingehalten werden:

- Trivialpasswörter (BBBBBB, 123456) sollten vermieden werden.

- Jeder Benutzer muss sein Passwort jederzeit ändern können.

- Insbesondere für die Erstanmeldung neuer Benutzer sollten Einmalpasswörter vergeben werden, also Passwörter, die nach einmaligem Gebrauch gewechselt werden müssen. In Netzen, in denen Passwörter unverschlüsselt übertragen werden, empfiehlt es sich, Einmalpasswörter dauerhaft zu verwenden.

- Nach dreimaliger fehlerhafter Passworteingabe sollte eine Sperrung erfolgen, die nur der Systemadministrator aufheben kann.

- Bei der Authentisierung in vernetzten Systemen sollten Passwörter nur verschlüsselt übertragen werden.

- Bei der Eingabe sollte das Passwort nicht auf dem Bildschirm angezeigt werden.

- Die Passwörter sollten im System zugriffssicher gespeichert werden, zum Beispiel mittels Einwegverschlüsselung.

- Der Passwortwechsel sollte vom System regelmäßig initiiert werden.

- Die Wiederholung alter Passwörter beim Passwortwechsel sollte vom IT-System verhindert werden (Passwort-Historie).

Bei IT-Systemen, an denen sich die Nutzer mit Benutzernamen und Passwort anmelden, sind darüber hinaus folgende Maßnahmen zu empfehlen:

- Nach längerer Nichtbenutzung (z. B. nach fünf bis fünfzehn Minuten) sollte automatisch eine Bildschirmsperre aktiviert werden. Der Benutzer sollte die Sperre auch manuell starten können. Sie darf nur nach Eingabe eines Passwortes (oder nach anderweitiger Authentifikation) wieder aufgehoben werden.

- Bei längerer Abwesenheit sollte sich der Benutzer abmelden.

- Der Zeitpunkt des letzten erfolgreichen Anmeldens sollte dem Benutzer beim Login angezeigt werden.

- Erfolglose Login-Versuche sollten dem Benutzer ebenfalls beim Login angezeigt werden. Sie sollten protokolliert werden.

- Außerhalb der Arbeitszeit sollte das IT-System keine Anmeldungen von Benutzern annehmen.

- Falls Mitarbeiter nur an einem bestimmten Arbeitsplatz arbeiten, sollten sie sich auch nur dort anmelden können.

- Benutzer sollten sich nicht mehrfach anmelden können.

- Benutzerkennungen sollten nur für den Zeitraum eingerichtet werden, in dem sie tatsächlich benötigt werden. Nicht genutzte Kennungen sind zu löschen oder zu deaktivieren.

Nach: BSI: IT-Grundschutzhandbuch; BSI, Bonn, 2002; Abschnitte M2.11, M4.2, M4.7, M4.15, M4.16