UMGANG MIT PASSWÖRTERN

Ratgeber zum Datenschutz 3

Herausgeber:
Berliner Beauftragter für Datenschutz und Informationsfreiheit

Verantwortlich:
Volker Brozio
Redaktion:
Laima Nicolaus

An der Urania 4-10, 10787 Berlin
Tel.: (030) 1 38 89 0
Fax.: (030) 2 15 50 50
Internet: www.datenschutz-berlin.de
Email: mailbox@datenschutz-berlin.de

Grafik Design: www.studiohiggins.com

EINLEITUNG

Voraussetzung dafür, dass

- die Vertraulichkeit, Integrität und Authentizität personenbezogener Daten gewährleistet werden kann,
- die zu überwachenden Datenverarbeitungsprozesse auch tatsächlich nachvollzogen werden können,
- die Kontrollanforderungen des Bundesdatenschutzgesetzes (Anlage zu § 9 BDSG) erfüllt werden können,

ist die Identifizierung mit einer persönlichen Kennung und die dazugehörige Authentifizierung mit einem geheimen Passwort. Dieses Verfahren ist in lokaler Umgebung für den mittleren Schutzbedarf hinreichend.

Der Benutzer weist sich mit Kennung und dazugehörigem Passwort dem System gegenüber als berechtigt aus. Das System prüft, ob die Kennung existiert und ob das Passwort zu der Kennung gehört. Es lässt danach eine Benutzung zu oder weist sie ab.

Damit mit einem solchen Verfahren die gewünschten Sicherheitsziele erreicht werden können, müssen Mindestanforderungen an die

- technischen Mechanismen,
- organisatorischen Regelungen und Bedingungen und
- persönlichen Verhaltensweisen der Benutzer und Systemverwalter

erfüllt werden.

1. ANFORDERUNGEN AN DIE TECHNIK

- Die Passwörter sind im System verschlüsselt und gegen unbefugte Schreibzugriffe und möglichst auch gegen unbefugte Lesezugriffe zu schützen.

- In Protokollen oder Dateien dürfen Passwörter nie in Klarschrift erscheinen.

- Mehrmalige Falscheingaben von Passwörtern müssen vom System unterbunden und mit Restriktionen beantwortet werden.

Das System sperrt die Kennung nach dreimaliger Falscheingabe; nur der Systemadministrator bzw. der Benutzerverwalter kann die Nutzerkennung später wieder freigeben.

Die Freigabe kann nur erfolgen, wenn der Benutzer seine Authentizität und die Berechtigung nachweisen kann.

- Die Eingabe des Passwortes hat verdeckt zu erfolgen.

Das Passwort wird am Monitor nicht abgebildet, möglichst auch nicht durch Sonderzeichen (*, @, # o.Ä.), da sich sonst die Passwortlänge erkennen lässt.

- Bei der Passworteinrichtung oder -änderung muss die Möglichkeit der Bestätigung gegeben sein, damit eine unbewusste Falscheingabe sofort auffällt und nicht erst beim nächsten - dann natürlich vergeblichen - Anmeldeversuch.

- Das System sollte die regelgerechte Bildung von Passwörtern überprüfen und bei Abweichung abweisen können.

- Die Mindestlänge von Passwörtern sollte acht Zeichen, mindestens aber sechs betragen.

- Durch die Verlängerung des Passwortes lassen sich die Kombinationsmöglichkeiten bei der Zeichenauswahl erhöhen und so die Erfolgsaussichten von „Hackern“ senken.

- Das Passwort sollte aus einem alphanumerischen Zeichenmix mit mindestens einem Sonderzeichen gebildet werden.

- Es sollte ein zwangsweiser zyklischer Wechsel (alle 90 Tage) des Passwortes erfolgen.

Vorsicht: Zu kurze Wechselrhythmen fördern u.U. nicht die Sicherheit, da zu häufiges Wechseln zum Notieren von Passwörtern führen kann.

- Die Wiederverwendung eines bereits benutzten Passwortes sollte erst nach mehreren Wechseln (mindestens 5) möglich sein.

- Die Benutzung von Trivialpasswörtern ist zu verhindern.

Sollte dies systemseitig nicht implementiert sein, so ist zumindest in einer organisatorischen Regelung beispielhaft auf unzulässige Passwörter hinzuweisen: Namen, Geburtsdaten, Kfz-Kennzeichen, Arbeitsgebiet, Zeichenketten ohne Zeichenwechsel ...

- Vom System automatisch generierte Passwörter sollten nicht verwendet werden, da diese zum Aufschreiben (z. B. im Terminkalender) verführen.

- Das so genannte „Durchreichen“ des Passwortes von der Benutzeroberfläche in die eigentlichen Anwendungen (Programme) ist möglichst zu unterstützen, um das dann zu erwartende Notieren von mehreren unterschiedlichen Passwörtern zu verhindern.

- Die letzte Systemnutzung sollte dem Benutzer automatisiert bei der aktuellen Anmeldung angezeigt werden.

Auf diese Weise kann der Anwender sehen, wann die letzte Anmeldung mit seiner Nutzerkennung erfolgte, und so u. U. einen Missbrauchsversuch feststellen.

- Der letzte nicht erfolgreiche Versuch einer Anmeldung sollte dem Benutzer automatisiert angezeigt werden.

- Nicht erfolgreiche Logins sollten auf jeden Fall protokolliert werden.

2. ANFORDERUNGEN AN ORGANISATORISCHE REGELN UND BEDINGUNGEN

- Jeder Benutzer hat eine eigene Nutzerkennung mit Passwort.
- Passwörter werden benutzerabhängig vergeben.

Der Benutzer hat ausschließlich Zugriff auf die Programme und Daten, die er für die Erfüllung seiner Aufgaben benötigt; es sollte möglichst kein so genanntes „Generalpasswort" geben, mit dem der Besitzer Zugriff auf „ALLES" hat.

- Die Vergabe von Nutzerkennzeichen und Passwörtern ist in einem Konzept zur Benutzerverwaltung zu regeln. Diese Regelung sollte Bestandteil eines umfassenden Datenschutz- und Sicherheitskonzeptes sein.

- Richtet der Systemverwalter so genannte „Einstiegs-Passwörter" ein, so sind diese bei der Erstanmeldung der jeweiligen Benutzer zwangsweise (wenn nicht implementiert, unverzüglich) durch selbstgewählte (s.u.) Passwörter zu ersetzen.

- Die Vergabe von Gruppenpasswörtern ist zu vermeiden. Die Einrichtung von Gruppen bzw. Gruppenrechten sollte dazu dienen, die Benutzer (mit ihrer persönlichen Kennung) den jeweiligen Gruppen mit gleichen Zugriffsrechten zuzuordnen.

- Ist die berechtigte Nutzung mehrerer ADV-Anwendungen an eine Passworteingabe gebunden und ein automatisches Durchreichen des Passwortes nicht möglich, kann ein Passwort für diese Anwendungen benutzt werden, wenn es die Sensibilität der zu verarbeitenden Daten zulässt.

Das Passwort des Systemadministrators ist gesichert zu hinterlegen. Der Gebrauch durch Dritte ist zu protokollieren (Datum, Uhrzeit, Grund ...). Anschließend ist das Passwort unverzüglich zu ändern und wieder zu hinterlegen.

- Bei Verdacht einer Ausspähung des Passwortes ist dieses unverzüglich zu wechseln.

- Bei systemimmanenten Benutzerkennungen (root, admin ...) sind die Passwörter bei der Erstanmeldung zu ändern. Zeitweise nicht benutzte Kennungen sind zu sperren bzw. zu deaktivieren.

- Es müssen Vertretungsregelungen für Abwesenheitszeiten (Urlaub, Krankheit ...) festgelegt werden. Kennungen sind zu sperren, wenn eine längere Abwesenheit vorhersehbar ist. Der Vertreter sollte möglichst über eine eigene Kennung mit Passwort verfügen.

- Kennungen von ausgeschiedenen Mitarbeitern sind unverzüglich zu löschen bzw. zu sperren.

- Nach vorübergehender Vertretung in Ausnahmesituationen sind die damit u.U. verbundenen Rechtezuweisungen zu deaktivieren.

- Passwörter dürfen nicht auf programmierbaren Funktionstasten gespeichert werden.

3. ANFORDERUNGEN AN DIE PERSÖNLICHE VERHALTENSWEISE VON BENUTZERN UND SYSTEMVERWALTERN

- Das Passwort darf grundsätzlich nicht weitergegeben werden, es muss geheim gehalten werden.

- Wird ein Passwort unautorisierten Personen bekannt, so ist dieses unverzüglich zu wechseln.

- Die Eingabe des Passwortes sollte unbeobachtet stattfinden.

Der Monitor & die Tastatur sind so aufzustellen, dass ein Beobachten der Zeicheneingabe ausgeschlossen wird.

Herausgeber:
Berliner Beauftragter für Datenschutz und Informationsfreiheit

Verantwortlich:
Volker Brozio
Redaktion:
Laima Nicolaus

An der Urania 4-10, 10787 Berlin
Tel.: (030) 1 38 89 0
Fax.: (030) 2 15 50 50
Internet: www.datenschutz-berlin.de
Email: mailbox@datenschutz-berlin.de

Grafik Design: www.studiohiggins.com

Stand: Juli 2008