Passworte...aber richtig

Orientierungshilfe

Landesbeauftragter für den Datenschutz Niedersachsen

So erreichen Sie den Landesbeauftragter für den Datenschutz Niedersachsen:

Schreiben	Postfach 221, 30002 Hannover
Anrufen	0511 / 120-4552
Faxen	0511 / 120-4591
E-Mailen	poststelle@lfd.niedersachsen.de
Surfen	www.lfd.niedersachsen.de
Persönlich	Brühlstraße 9, Hannover

Hinweise zur Paßwort-Gestaltung und Verwendung

Erforderlichkeit

Jede Datenverarbeiterin und jeder Datenverarbeiter sollte ein besonderes Interesse haben, die „eigenen Daten“ vor den neugierigen Augen unberechtigter Dritter zu schützen. § 9 des Bundesdatenschutzgesetzes (BDSG) und § 7 des Niedersächsischen Datenschutzgesetzes (NDSG) verpflichten datenverarbeitende Stellen technische und organisatorische Maßnahmen gegen die unberechtigte Verarbeitung oder Nutzung von personenbezogenen Daten zu treffen.

Das Paßwortverfahren ist gegenwärtig das am meisten verwendete Verfahren, um den unberechtigten Zugriff auf personenbezogene Daten zu verhindern. Benutzer erhalten eine Benutzerkennung und ein persönliches Paßwort, um sich so gegenüber dem IuK-System als Berechtigter ausweisen zu können. Dem nachgewiesenen authentischen Benutzer wird der Zugang zum System, zur Anwendung oder zu Teilen der Anwendung entsprechend den vergebenen Rechten eröffnet.

Mit den folgenden Hinweisen sollen Empfehlungen zur Paßwort-Gestaltung und Tips zur Kontrolle einer datenschutzgerechten Verwendung von Paßworten gegeben werden.

1. Empfehlungen für Benutzer

- Paßwort nirgends notieren und niemanden mitteilen!
  (Ausnahme: z.B. versiegelte Hinterlegung des Systemverwalter-Paßwortes für Notfälle). Die Benutzung des versiegelten Umschlages ist zu begründen.
- Mindestens 6 Zeichen aus Buchstaben, Ziffern und Zeichen gemischt!
- Mindestens 1 Sonderzeichen verwenden!
- Paßwort regelmäßig ändern, aber nicht zu oft!
- Keine Trivialpaßwörter verwenden!

Um sich auch ein kompliziertes Paßwort leicht merken zu können, sollte man aus einem einprägsamen Satz, Lied oder Vers jeden x-ten Buchstaben auswählen und Sonderzeichen einstreuen, so z.B.:

„Eile mit Weile“ = EimiWe?

2. Hinweise für Systemverwalter und interne Datenschutzbeauftragte

Die Paßwortregeln sind nach der Sensibilität der zu verarbeitenden personenbezogenen Daten abgestuft. Die Datenschutzbeauftragten des Bundes und der Länder untergliedern personenbezogene Daten nach dem Grad möglicher Beeinträchtigungen schutzwürdiger Belange in fünf Schutzstufen. Bei der Einordnung in eine der Schutzstufen sind nicht einzelne Datenfelder zu bewerten, vielmehr ist die gesamte Datei, die mögliche Verknüpfbarkeit oder auch das Auswahlkriterium der Speicherung, das nicht selbst gespeichert sein muß, zu berücksichtigen.

3. Checkliste

Zur Beantwortung der Checklisten-Fragen wird es in der Regel ausreichen, jeweils anzukreuzen

- Erfüllt
- Nicht erfüllt
- Trifft nicht zu.

Diese Basisantworten können im Bedarfsfall durch kurze Erläuterungen in dem Feld Bemerkungstext ergänzt werden. Auf diese Weise liegt nach Durcharbeiten der Checkliste eine übersichtliche Aufstellung der noch zu treffenden Maßnahmen vor.

Eine beantwortete Checkliste deckt möglicherweise vorhandene Sicherheitslücken des Systems auf. Daher ist die ausgefüllte Checkliste bis zur vollständigen Beseitigung dieser Mängel entsprechend vertraulich zu behandeln!

Checkliste – Paßwort-Gestaltung und -Verwendung

Klassifizierung der Schutzstufe Begründung der Einstufung (Extrablatt)				
Stufe A	Stufe B	Stufe C	Stufe D	Stufe E

Erläuterung:
Die einzelnen Anforderungen sind nach dem Schutzstufenkonzept (siehe Anlage 1) gestaffelt aufgeführt. Die Grundschutzforderungen unter der Schutzstufe A – B sind immer anzuwenden. Die unter den Schutzstufen C, D oder E aufgeführten Anforderungen kommen aufgrund der höheren Datenschutzsicherungsanforderung jeweils ergänzend hinzu.

1	**Paßwortgestaltung (Identifikation/ Authentifikation)**		**Erfüllt**	**Nicht erfüllt**	**Trifft nicht zu**	**Bemerkungstext**
Daten der Schutzstufe A - B:						
1.1	Vor dem Zugriff auf Daten oder Programme des Systems wird die Anmeldung mittels Benutzerkennung und Paßwort erzwungen **(Paßwortschutz).**					
1.2	Jeder Benutzer hat bei der Anmeldung ein nur ihm bekanntes Paßwort einzugeben **(persönliches Paßwort).**					
	für das Booten: für das Bios: für das Netzwerk: für die Applikation:	☐ ☐ ☐ ☐				
1.3	Das Paßwort wird nicht auf dem Bildschirm wiedergegeben **(Dunkelsteuerung).**					
1.4	Trivialpaßwörtern (z.B. Vornamen, Geburtsdaten, Dienstnummern) dürfen nicht verwendet werden (**keine Trivialpaßwörter).**					
1.5	Die Paßwörter müssen spätestens nach 6 Moanten geändert werden **(Paßwortalterung).**					
1.6	Die Paßwort-Mindestlänge beträgt sechs Zeichen **(Paßwort-Mindestlänge).**					

1	Paßwortgestaltung (Identifikation/ Authentifikation)	Erfüllt	Nicht erfüllt	Trifft nicht zu	Bemerkungstext
1.7	Paßwörter werden verschlüsselt gespeichert **(Verschlüsselung).**				
1.8	Die Paßwort-Regeln und Hinweise für Benutzer sind in einer schriftlichen, allen Benutzern bekannten Anweisung festgelegt. Die Einhaltung wird regelmäßig überwacht **(Verfahrensanweisung).**				
Daten der Schutzstufe C:					
1.9	Das System ist so einzurichten, daß eine Umgehung des Paßwortschutzes auch mit zusätzlichen Mitteln (z.b. bootfähige Diskette) praktisch nicht möglich ist **(Systemabsicherung).**				
1.10	Der Zeitraum, in dem eine Anmeldung möglich ist, werden auf das organisatorisch vertretbare Minimum begrenzt **(Sperrung).**				
1.11	Die Anzahl der Fehlversuche hintereinander wird begrenzt (max. fünf), danach wird die Benutzerkennung gesperrt **(Begrenzung der Fehlversuche).**				
1.12	Nach spätestens sechs Monaten wird ein Paßwortwechsel technisch erzwungen. Nach neun Monaten erfolgt eine Benutzersperre **(Paßwortalterung).**				
1.13	Bei der Erstanmeldung eines Benutzers muß die Paßwortänderung technisch erzwungen werden **(Paßwortübergabe an Benutzer).**				
1.14	Beim Verlassen des Raumes muß sich der Benutzer abmelden oder den APC durch eine Pausenfunktion sperren. Spätestens jedoch nach 20-minütiger Nichtbenutzung der Tastatur oder Maus wird der APC automatisch gesperrt. Nur durch Eingabe des Paßwortes kann die Arbeit fortgesetzt werden **(gesicherte Pausenfunktion).**				
1.15	Eine Zeichenmischung ist vorgeschrieben. Für das Paßwort sollten verwendbar sein: Große und kleine Buchstaben, Zahlen, Sonderzeichen **(Zeichenmischung/alphanumerische Zei-**				

1	Paßwortgestaltung (Identifikation/ Authentifikation)	Erfüllt	Nicht erfüllt	Trifft nicht zu	Bemerkungstext
	chen).				
Daten der Schutzstufe D:					
1.16	Über mindestens fünf Generationen wird automatisch verhindert, dass das alte Paßwort als neues Paßwort verwendet werden kann. Es muss an mindestens drei Stellen unterschiedlich sein **(keine Paßwortwiederholung).**				
1.17	Trivialpaßwörter (z.B. Vornamen, Geburtsdaten, Telefonnummern) werden technisch ausgeschlossen **(keine Trivialpaßwörter).**				
1.18	Eine Mischung von Zeichen wird technisch erzwungen **(erzwungene Zeichenmischung).**				
1.19	Ist ein Benutzer über einen längeren Zeitraum (3 Monate) abwesend, ist der Benutzer zu sperren **(Benutzersperrung).**				
Daten der Schutzstufe E:					
1.20	Das Systemverwalter-Paßwort besteht aus zwei Teilen, die jeweils unterschiedliche Personen bekannt sind **(Vier-Augen-Prinzip).**				

Anlage 1 - Schutzstufenkonzept

Klassifizierung schutzwürdiger Belange

Personenbezogene Daten werden nach dem Grad möglicher Beeinträchtigung schutzwürdiger Belange bei Missbrauch dieser Daten in 5 Schutzstufen untergliedert. Bei der Klassifizierung sind Datenfelder niemals einzeln zu bewerten. Die Betrachtung ist vielmehr auf die gesamte Datei, ggf. auf die gesamte DV-Anlage auszudehnen. Werden personenbezogene Daten unter einem Auswahlkriterium in eine Datei aufgenommen, das in der Datei nicht enthalten ist, so ist dieses Auswahlkriterium bei der Klassifizierung mit zu bewerten. Enthalten Dateien umfassende Angaben zu einer Person (Dossiers), so sind sie in eine höhere Schutzstufe einzuordnen, als dies nach den Einzeldaten erforderlich wäre.
Es werden folgende Schutzstufen unterschieden:

Stufe A: Frei zugängliche Daten, in die Einsicht gewährt wird, ohne dass der Einsichtnehmende ein berechtigtes Interesse geltend machen muss, z.B. Adressbücher, Mitgliederverzeichnisse, Benutzerkataloge in Bibliotheken.

Stufe B: Personenbezogene Daten, deren Missbrauch zwar keine besondere Beeinträchtigung erwarten lässt, deren Kenntnisnahme jedoch an ein berechtigtes Interesse des Einsichtnehmenden gebunden ist, z.B. beschränkt zugängliche öffentliche Dateien, Verteiler für Unterlagen.

Stufe C: Personenbezogene Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann ("Ansehen"), z.B. Einkommen, Sozialleistungen, Grundsteuer, Ordnungswidrigkeiten.

Stufe D: Personenbezogene Daten, deren Missbrauch die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann ("Existenz"), z.B. Unterbringung in Anstalten, Straffälligkeit, Ordnungswidrigkeiten schwerwiegender Art, dienstliche Beurteilungen, psychologisch-medizinische Untersuchungsergebnisse, Schulden, Pfändungen, Konkurse.

Stufe E: Daten, deren Missbrauch Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen kann, z.B. Daten über Personen, die mögliche Opfer einer strafbaren Handlung sein können.

Falls die Sensitivität nicht bekannt ist, ist von der höchsten Sensitivitätsstufe auszugehen. Denkbar ist auch, dass der Schutz empfindlicher Firmendaten ohne Personenbezug die Einstufung bestimmt.