Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg

Hinweise zum Umgang mit Passwörtern

Stand: 1. Mai 2017

Werden personenbezogene Daten mit Hilfe von Computern verarbeitet, so ist sicherzustellen, dass nur berechtigte Personen darauf zugreifen können und dies auch nur im dienstlich notwendigen Umfang[1]. Notwendig ist daher, dass sich derjenige, der auf personenbezogene Daten zugreifen will, zunächst gegenüber dem Computersystem identifiziert und seine Zugriffsberechtigung nachweist. Dies kann mit Hilfe persönlicher Chipkarten, durch Prüfung biometrischer Eigenschaften (z. B. Fingerabdruck) oder durch Eingabe einer Benutzerkennung und eines Passwortes erfolgen. Kartengestützte und biometrische Anmeldeverfahren gewinnen zwar immer mehr Bedeutung; in der Praxis dominiert jedoch bislang die Anmeldung mit Benutzerkennung und Passwort. Dieses Merkblatt stellt dar, wie sich ein möglichst sicherer Passwortschutz realisieren lässt.

Grundprinzip des datenschutzgerechten Passwortschutzes

Erfährt jemand die Benutzerkennung und das Passwort einer anderen Person, so kann er sich damit unter fremdem Namen anmelden und auf Daten und Programme zugreifen, die nicht für ihn bestimmt sind. Da Benutzerkennungen vielfach nicht geheim sind, kommt der Geheimhaltung der persönlichen Passwörter die entscheidende Rolle zu, wenn es darum geht, den Zugriff unberechtigter Personen auf personenbezogene Daten zu verhindern. Folgendes ist generell zu beachten:

Der berechtigte Benutzer muss sich sein Passwort leicht merken können. Für alle anderen muss es dagegen möglichst schwer sein, das Passwort herauszufinden.

---

[1] Dies ergibt sich unter anderem aus § 9 Abs. 3 Nr. 4 des Landesdatenschutzgesetzes (LDSG) sowie aus der Anlage zu § 9 Satz 1 des Bundesdatenschutzgesetzes (BDSG).

Leider wird dem Passwortschutz in der Praxis nicht immer die notwendige Aufmerksamkeit geschenkt. Die festgestellten Mängel reichen von am Arbeitsplatz notierten Passwörtern über die Benutzung des eigenen Vor- oder Nachnamens als Passwort bis hin zu schlecht konfigurierten Computersystemen, die es Angreifern ermöglichen, die Passwortdatei zu kopieren und Passwörter mit Hilfe spezieller Entschlüsselungsprogramme herauszufinden.

Folgende Regeln sollten daher beachtet werden, um die Sicherheit der Passwörter zu wahren:

- **Es sind individuelle Kennungen und Passwörter zu verwenden (R1).**
  Jeder Benutzer erhält ein eigenes Passwort, das nur von ihm benutzt werden darf. Passwörter, die von mehreren Personen benutzt werden (Gruppenpasswörter) sind zu vermeiden, denn sie lassen sich nicht in gleicher Weise geheim halten wie individuelle Passwörter. Ferner lässt eine Gruppenkennung, die beispielsweise in Protokollen sicherheitsrelevanter Ereignisse erscheint, keinen eindeutigen Rückschluss auf den Verursacher zu.

- **Ein Passwort muss geheim gehalten werden. Es darf nirgendwo aufgeschrieben und keiner anderen Person - auch nicht dem Systemverwalter oder dem dienstlichen Stellvertreter - mitgeteilt werden (R2).**
  Ansonsten könnten Systemverwalter oder Stellvertreter beispielsweise unter fremder Kennung Daten verändern, wobei das Protokoll der Datenänderung den Inhaber der persönlichen Kennung als Urheber der Änderung ausweist. Ebenso könnten unter fremdem Namen E-Mails versandt werden, die beim Empfänger den Eindruck hinterlassen, sie seien von dem Inhaber der persönlichen Kennung versandt worden.
  Eine Ausnahme gilt lediglich für betriebswichtige Passwörter wie Administrator-Passwörter; diese können in einem verschlossenen Umschlag in einem Tresor aufbewahrt werden.

- **Triviale Passwörter sind zu vermeiden (R3).**
  Dazu zählen etwa Namen oder Vornamen, die Benutzerkennung, das Geburtsdatum, das Kfz-Kennzeichen, die Telefonnummer oder andere Angaben aus dem persönlichen Umfeld des Benutzers, die auch anderen Personen bekannt sein können. Solche Passwörter sind leicht zu erraten.

- **Ein Passwort muss aus mindestens zehn Zeichen bestehen (R4).**
  Innerhalb des Passworts sollte mindestens ein Sonderzeichen (wie z.B. ?, #, !) enthalten sein. Es sollte sowohl Groß- als auch Kleinbuchstaben sowie Ziffern enthalten (R5).
  Dadurch wird es erschwert, Passwörter durch Ausprobieren herauszufinden.
  Um sich ein solches Passwort trotzdem merken zu können, kann es beispielsweise von einem Merksatz abgeleitet werden. So kann man sich etwa anhand des Satzes "**S**iche-re **P**asswörter **s**ollten **m**indestens **a**us **10 Z**eichen **b**estehen**!“** das Passwort **SPsma10Zb!** merken.
  Wir empfehlen, keine Umlaute zu verwenden.

- **Ein Passwort darf bei der Eingabe nicht am Bildschirm angezeigt werden (R6).**
  Es könnte sonst leicht jemandem bekannt werden, der den Bildschirm einsehen kann.

- **Die Passwörter sind im Computer verschlüsselt zu speichern (R7).**
  Dies verhindert, dass Systemverwalter und andere Personen, die zumindest lesend auf die Passwortdatei zugreifen können, die darin gespeicherten Passwörter im Klartext zur Kenntnis nehmen und sich unter fremder Benutzerkennung anmelden können.

- **Die Passwortdatei ist gegen unberechtigtes Kopieren zu sichern (R8).**
  Dies verhindert, dass jemand die Passwortdatei auf seinen Computer kopiert und anschließend unbehelligt versuchen kann, die Passwörter durch automatisiertes Ausprobieren mit Hilfe von Passwort-Knackprogrammen herauszufinden.

- **Hat ein Systemverwalter einem Benutzer ein neues Passwort eingerichtet, so muss der Benutzer dieses Start-Passwort bei seiner ersten Anmeldung ändern (R9).**
  Um möglichst schnell zu erreichen, dass das mit der Benutzerkennung verbundene Passwort nur dem Benutzer bekannt ist, sollte diese erste Anmeldung umgehend nach Einrichtung des Start-Passworts erfolgen.

- **Ein Passwort ist regelmäßig zu ändern (R10).**
  Das neue Passwort sollte sich von den früher verwendeten unterscheiden (R11).
  Dies verhindert, dass derjenige, dem ein fremdes Passwort bekannt wurde, dieses zu späteren Zeitpunkten wiederholt für unberechtigte Zugriffe nutzen kann. Um sicherzustellen, dass die Änderung tatsächlich erfolgt, ist ein automatischer Verfall der Passwörter zu realisieren. Als Änderungsintervall sind Zeiträume von 90 bis 180 Tagen empfehlenswert. Um den Ausschluss früher verwendeter Passwörter zu gewährleisten,

sollte der Computer zumindest jeweils die letzten fünf früheren Passwörter in einer sog. Passwort-Historie speichern und deren Wiederverwendung ablehnen.

- **Ein Passwort muss umgehend geändert werden, wenn der Verdacht besteht, dass es einer anderen Person bekannt wurde (R12).**

- **Passwort-Änderungen müssen von den jeweiligen Benutzern selbst durchgeführt werden können (R13).**
  Ansonsten würde das Passwort neben dem Benutzer noch anderen Personen bekannt.

- **Nach mehreren fehlerhaften Anmeldeversuchen unter derselben Benutzerkennung muss die Kennung für die weitere Benutzung gesperrt werden (R14).**
  Diese Sperre ist erforderlich, um ein systematisches Durchprobieren aller möglichen Passwörter zu verhindern (sog. Brute-Force-Attacken). Die Sperre sollte nach drei bis fünf Fehlversuchen greifen und so lange bestehen bleiben, bis sie von einem Systemverwalter aufgehoben wird. Mitunter lässt sich zudem einstellen, nach welcher Zeitspanne ein Fehlversuch nicht mehr in die Zählung der Fehlversuche einbezogen wird. In Betracht kommen hier Werte ab 30 Minuten. Nicht erfolgreiche Anmeldeversuche sind zu protokollieren.

- **Anmeldefehlversuche sind zu protokollieren (R15).**
  Erfolglose Anmeldeversuche können auf einen Eindringversuch hinweisen. Die entsprechenden Protokolle sind regelmäßig auf sicherheitsrelvante Vorkommnisse hin zu überprüfen. Nach Möglichkeit sollten mehrfach hintereinander auftretende Anmeldefehlversuche unter einer Benutzerkennung einen Alarm beim Systembetreuer auslösen (z. B in Form einer E-Mail).

- **Alle Passwörter von System- oder Anwendungssoftware, die vom Hersteller voreingestellt wurden, sind nach der Installation des Systems umgehend zu ändern (R16).**
  Da die Hersteller oft die gleichen Passwörter bei der Auslieferung ihrer Produkte voreinstellen, sind diese einem großen Personenkreis bekannt. Zudem sind die entsprechenden Kennungen vielfach mit umfassenden Berechtigungen verbunden. Deshalb sind die Passwörter umgehend zu ändern.

Hinweise zur Umsetzung der Regeln

Verantwortlich für die Einhaltung dieser Regeln sind die Daten verarbeitenden Stellen. Je nach Art der Regeln ist ein unterschiedliches Vorgehen erforderlich:

- Einige Regeln lassen sich ausschließlich durch eine entsprechende technische Gestaltung der eingesetzten Software sicherstellen. Sie sind bereits bei der Beschaffung zu berücksichtigen. Dies gilt beispielsweise für das Anliegen, Passwörter nicht im Klartext zu speichern oder am Bildschirm anzuzeigen.
- Zur Umsetzung einiger weiterer Regeln, wie etwa die Forderung nach regelmäßigem Wechsel der Passwörter, könnte auf den ersten Blick neben technischen Maßnahmen auch eine organisatorische Maßnahme, z. B. eine entsprechende Dienstanweisung, in Frage kommen. Bei der Wahl organisatorischer Maßnahmen ist jedoch die konsequente Umsetzung der Regeln nicht so zuverlässig gewährleistet wie dies bei technischen Maßnahmen der Fall ist. Daher ist die Einhaltung aller Regeln, bei denen dies möglich ist, durch technische Maßnahmen sicherzustellen. Dies gilt beispielsweise für die regelmäßige Passwort-Änderung ebenso wie für die Mindestlänge, die Zeichenmischung oder die Notwendigkeit, ein Start-Passwort bei der ersten Anmeldung zu ändern. Um dies leisten zu können, ist bei der Beschaffung von Software darauf zu achten, dass diese die erforderlichen Funktionen bietet. Da aber nicht in jeder Software, die beispielsweise eine Passwortmindestlänge garantiert, die erforderliche Mindestzahl der Zeichen mit "10" oder einem höheren Wert voreingestellt sind, ist es erforderlich, die entsprechenden Einstellungen ggf. manuell anzupassen.
- Die Einhaltung einiger Regeln lässt sich nicht technisch sicherstellen. Sie müssen daher von den einzelnen Benutzern selbst beachtet werden. Dies gilt beispielsweise für die Forderung, Passwörter sofort zu ändern, wenn sie einem Dritten bekannt geworden sein können. Um diese Regeln umzusetzen, muss die Daten verarbeitende Stelle ihre Mitarbeiterinnen und Mitarbeiter in einer Dienstanweisung über die entsprechenden Passwortregeln unterrichten und sie zu deren Einhaltung verpflichten. Um unnötige Fehlermeldungen bei der Eingabe von Passwörtern zu vermeiden, sind die Mitarbeiterinnen und Mitarbeiter ferner darüber zu informieren, welchen technisch sichergestellten Eigenschaften die Passwörter entsprechen müssen.

Grenzen gängiger Passwortverfahren

Passwortschutz-Mechanismen können mitunter auch dann, wenn sie den genannten Regeln entsprechen, noch Sicherheitsdefizite aufweisen. Zwei Problembereiche sind dabei besonders relevant:

- Bei der Nutzung gängiger Client-Server-Systeme benötigt ein Benutzer heutzutage mitunter drei oder mehr Passwörter. Je mehr Passwörter sich ein Benutzer merken

muss, desto schwerer fällt es, die genannten Regeln zum Umgang mit Passwörtern einzuhalten und desto niedriger ist die damit letztlich erreichbare Sicherheit. Um dem entgegenzuwirken ist bei der Nutzung vorhandener und vor allem bei der Planung neuer IT-Verfahren verstärkt darauf hinzuarbeiten, die Zahl der Passwörter, die sich jeder einzelne Benutzer merken muss, möglichst gering zu halten. Besonders wirkungsvoll lässt sich dies durch Verwendung sog. **Single-Sign-On**-Verfahren realisieren, bei denen sich ein Benutzer nicht an jedem Computer und Verfahren im Netz, sondern nur einmal an einer zentralen Stelle anmelden muss. Dort werden alle Berechtigungen zur Nutzung dezentraler Systeme und Verfahren verwaltet und kontrolliert.

- Probleme können sich bei der Nutzung gängiger Passwortverfahren ferner dann ergeben, wenn die für die Anmeldung benötigten Daten über ungesicherte Netze oder unzulängliche Protokolle (http statt https) übertragen werden. Sofern dabei nicht ausgeschlossen werden kann, dass die übertragenen Benutzerkennungen und Passwörter von Unberechtigten abgehört werden, besteht das Risiko, dass diese sich durch späteres Wiedereinspielen der Daten unberechtigten Zugriff auf die durch die Passwörter geschützten Daten und Programme verschaffen. Dieses Risiko besteht übrigens nicht nur, wenn die Passwörter unverschlüsselt übertragen werden, sondern auch dann, wenn die Passwörter vor ihrer Übertragung stets auf gleiche Weise verschlüsselt werden. Ist dieses Risiko unter Berücksichtigung der Sensibilität der durch die Passwörter geschützten Daten nicht tragbar, so ist es durch den Einsatz von **Einmal-Passwörtern, Zwei-Faktor-Authentifizierung** oder **kryptografischen Authentifikationsverfahren** (z. B. Challenge-Response-Verfahren) auszuräumen.