UNIVERSITY OF APPLIED SCIENCES

THM
TECHNISCHE HOCHSCHULE MITTELHESSEN

So behält man auch komplizierte Passwörter

Ein schönes Passwort wäre z. B. dieses:

S5JgekG!

Sie können sich ein solches Passwort nicht merken? Um sich auch ein kompliziertes Passwort leicht merken zu können, sollten Sie aus einem einprägsamen Satz, Lied oder Vers jeden x-ten Buchstaben auswählen und Sonderzeichen einstreuen. Nach dieser Methode wurde das obige Passwort gebildet. In der Langform bedeutet es:

Seit 5 Jahren gab es keine Gehaltserhöhung!

Das ist ein Satz, den Sie so schnell nicht vergessen! Und das Passwort auch nicht! (Das oben genannte Beispiel darf jetzt allerdings nicht mehr verwendet werden!)

Begriffe

Datenschutz umfasst alle Regelungen, die darauf abzielen, das sich aus dem allgemeinen Persönlichkeitsrecht ergebende Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (nach BVerfG als „informationelles Selbstbestimmungsrecht" bezeichnet), sicherzustellen.

Personenbezogene Daten sind Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder (mit Zusatzwissen) bestimmbaren natürlichen Person (wie z.B. Name, Adresse, Geburtstag, Beruf, Titel, Personal-, Matrikel- oder Personalausweisnummer, Telefon- oder Faxnummer, Krankheiten, Beurteilungen).

Datensicherheit ist die technisch-organisatorische Aufgabe, die Sicherheit von Datenbeständen und Datenverarbeitungsabläufen zu gewährleisten. Werden personenbezogene Daten mit automatisierten Verfahren verarbeitet, schreiben die Datenschutzgesetze Maßnahmen zur Datensicherheit vor, vgl. § 10 HDSG.

Kontakte und Informationen

Technische Hochschule Mittelhessen
Wiesenstraße 14, 35390 Gießen

Datenschutzbeauftragter der Hochschule
Hajo Köppen
☎ 0641 309-1030
Fax 0641 309-2907
Gebäude B10, Raum 1.02
Ostanlage 39
hajo.koeppen@verw.thm.de

Homepage des Datenschutzbeauftragten
www.thm.de/datenschutz

Weitere Informationsquellen
www.datenschutz.de
www.datenschutzzentrum.de
www.bfdi.bund.de
www.datenschutz.hessen.de
www.bsi.de
www.datenschutzverein.de
www.foebud.de
www.bigbrotherawards.de
www.bvdnet.de
www.gdd.de
www.zaftda.de
www.zendas.de

Wenn Sie Zweifel oder Fragen haben, wenden Sie sich an den Datenschutzbeauftragten der TH Mittelhessen. Bei Verstößen gegen Datenschutzgrundsätze haben Sie auch das Recht, sich ohne Einhaltung des Dienstweges direkt an den Hessischen Datenschutzbeauftragten zu wenden. Ihre dienstrechtlichen Pflichten bleiben im Übrigen unberührt, § 28 Abs. 2 HDSG.

Stand: 02/12

DATENSCHUTZ-TIPP 2

Hinweise zur Passwortgestaltung und -verwendung

DATENSCHUTZ

Passwörter dienen der Datensicherheit und dem Datenschutz

Sie sagen die PIN zu Ihrer EC-Karte gerne an Freunde, Bekannte und auch Unbekannte weiter? Und dazu verleihen Sie auch gleich noch die EC-Karte? Blöde Frage, werden Sie richtig sagen. Kein klar denkender Mensch gibt eine PIN und seine dazugehörige EC-Karte weiter!
Wie sieht es aber mit dem Passwort aus, das zum Schutz von Daten auf dem Rechner am Arbeitsplatz als Zugriffs-/Benutzerkontrolle eingerichtet wurde? Vor Urlaubsantritt schnell mal das Passwort einer Kollegin oder einem Kollegen mitgeteilt, damit die eingehenden E-Mails bearbeitet werden können? Dem Vorgesetzten wird das Passwort auf sein freundliches Bitten hin selbstverständlich mitgeteilt? Und vorsichtshalber das Passwort auf der Rückseite der Schreibunterlage am Arbeitsplatz notiert? Die Antwort ist so klar wie bei PIN und EC-Karte:

Geben Sie Ihr Passwort niemals an eine andere Person weiter!
Schreiben Sie Ihr Passwort niemals irgendwo auf!

Automatisierte Verfahren öffentlicher Stellen, also auch die der Technischen Hochschule Mittelhessen, sind gem. § 10 Abs. 2 Hessisches Datenschutzgesetz (HDSG) so zu gestalten, dass eine unbefugte Speicherung sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten verhindert wird. Außerdem ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems berechtigten Personen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können. Deshalb ist es erforderlich die Person zu authentisieren, die das Datenverarbeitungssystem zu benutzen beabsichtigt. In der Regel wird zu diesem Zweck programmgesteuert zunächst eine Benutzerkennung (Name, Dienststellennummer o. ä.) abgefragt. Da diese Kennung nicht geheim ist, muss sich jeder Benutzer zusätzlich ein nur ihm bekanntes Passwort (Kennwort) ausdenken und im System ablegen. Das Passwort wird bei jeder Nutzung des Datenverarbeitungssystems abgefragt. Stimmt es mit dem gespeicherten Wert überein und kann man davon ausgehen, dass das Passwort nur derjenigen Person bekannt ist, die sich mit der betreffenden Benutzerkennung anmelden darf, sind die Anforderungen des § 10 Abs. 2 HDSG erfüllt und dem betreffenden Benutzer können die entsprechenden Programme, Verfahren und Datenbestände zur Verfügung gestellt werden. Gleichzeitig wird ihm die Verantwortung für alle folgenden Aktivitäten unter seiner Kennung zugerechnet.

Nur geheime Passwörter sind gute Passwörter

Von einer effektiven Geheimhaltung eines Passwortes hängt also ein wesentlicher Teil der System- und Datensicherheit ab. Nicht nur der/die Mitarbeiter/in darf es niemandem verraten, auch aus dem System darf es von Unbefugten nicht ausgelesen werden können. Die Passwörter werden in den IT-Systemen daher nicht im Klartext, sondern so verschlüsselt gespeichert, dass ein effizientes Entschlüsseln praktisch nicht möglich ist. Seit einiger Zeit sind aber Programme auf dem Markt (im Internet), die durch Probieren (z. B. durch Abgleiche mit einem speziellen elektronischen Wörterbuch) und Verwendung verschiedener mathematischer Methoden die verschlüsselten Passwörter ermitteln können. Dies ist umso schwieriger, je länger das Passwort und je vielfältiger die Zeichenfolge ist. Für das Ermitteln eines einfachen Passwortes sind nur wenige Sekunden erforderlich. Selbst bei der Verwendung von alphanumerischen vier- bis fünfstelligen Passworten liegt die „Ratezeit" noch im Minutenbereich. Tests mit echten Passwortbeständen haben gezeigt, dass mit derartigen Programmen im Verlauf weniger Stunden mehr als die Hälfte aller verwendeten Passworte ermittelt werden konnten.

Was bei Passwörtern beachtet werden muss

Es wird daher für die Gestaltung und Nutzung von Passwörtern die Beachtung folgender Mindestanforderungen dringend empfohlen:

- Das Passwort muss unbedingt geheim gehalten werden und darf nur dem Benutzer bekannt sein (Ausnahme: z.B. versiegelte Hinterlegung des Systemverwalter-Passwortes für Notfälle im Tresor. Die Benutzung des versiegelten Umschlages ist zu dokumentieren).
- Das Passwort darf nicht leicht zu erraten sein wie Name, Kfz-Kennzeichen, Geburtsdatum etc. Es dürfen keine Trivialpasswörter („123456") und Zeichenfolgen („BBBBBB") verwendet werden. Es soll kein Wort benutzt werden, das im Wörterbuch zu finden ist.
- Das Passwort sollte eine Mindestlänge von mindestens acht Zeichen haben, besser sind zwölf.
- Innerhalb des Passwortes sollte mindestens ein Zeichen verwendet werden, das kein Buchstabe ist (Sonderzeichen oder Zahl).
- Ein Passwortwechsel ist durchzuführen, wenn das Passwort unautorisierten Personen bekannt ist.
- Das Passwort muss regelmäßig geändert werden, z. B. alle 90 Tage. Alte Passwörter dürfen nach einem Passwortwechsel nicht mehr genutzt werden.
- Passwörter dürfen nicht auf programmierbaren Funktionstasten oder an anderer Stelle gespeichert sein, wodurch eine automatisierte Eingabe ermöglicht wird, z.B. in Startdateien der Systeme.