Datenschutz-Tipps

Nr. 2 / Januar 2014

Datenschutz ist ein Thema, das in den Medien zunehmendes Interesse genießt. Dazu trägt sicher auch die aktuelle Diskussion zu den Abhöraktivitäten diverser Nachrichtendienste bei. Bei vielen Bürgern wächst die Sensibilität hinsichtlich der Frage, wo personenbezogene Daten gespeichert werden sollten. Wir als öffentliche Hochschule haben hier gesetzliche Pflichten zu erfüllen, die sich insbesondere aus dem Berliner Datenschutzgesetz (BlnDSG) ergeben. Die „Datenschutz-Tipps“ sollen einen praktischen Beitrag dazu leisten, dass den Angehörigen der Hochschule ein datenschutzkonformer Umfang mit personenbezogenen Daten an der Hochschule erleichtert wird. Deshalb werden wir als behördliche Datenschutzbeauftragte in unregelmäßigen Abständen diesen Infobrief zur Verfügung stellen.

Prof. Dr. Hartmut Aden und Prof. Dr. Rainer Rumpel
Behördliche Datenschutzbeauftragte
E-Mail: Datenschutz@hwr-berlin.de

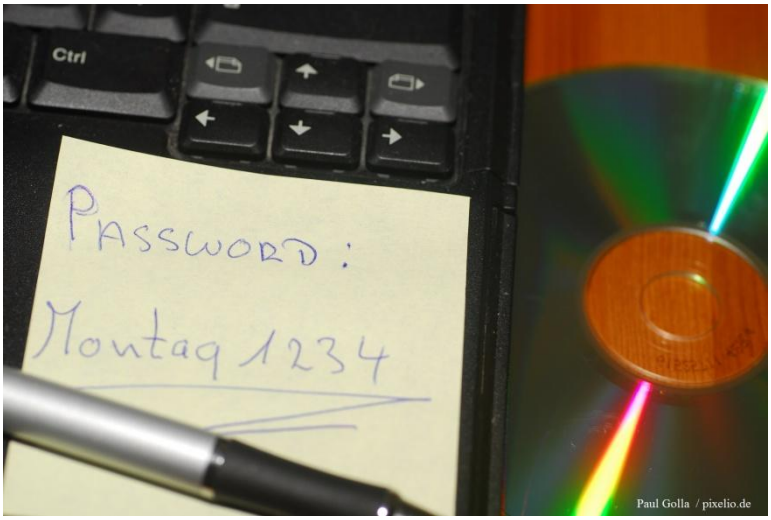
Das heutige Thema

- Umgang mit Kennwörtern

Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Kennwortauswahl und –verwendung

Sie geben die PIN zu ihrer Maestro-Karte an Freunde, Bekannte oder Unbekannte weiter? Und dazu verleihen Sie auch gleich noch diese Karte? Dumme Fragen, werden Sie richtig sagen. Kein vernünftiger Mensch gibt eine PIN und seine dazugehörige Bankkarte weiter!
Wie sieht es aber mit dem Kennwort aus, das zum Schutz von Daten auf dem Computer am Arbeitsplatz als Zugangsschutz eingerichtet wurde? Teilen Sie vor dem Urlaubsbeginn schnell mal das Kennwort einer Kollegin oder einem Kollegen oder dem Vorgesetzten mit, damit die eingehenden E-Mails bearbeitet werden können? Oder haben Sie vielleicht für alle Fälle das Kennwort auf der Rückseite der Schreibunterlage am Arbeitsplatz notiert? Die Antwort ist so klar wie bei PIN und EC-Karte:
Kein verantwortlich handelnder Mitarbeiter gibt sein Kennwort weiter oder schreibt es an zugänglicher Stelle auf!
Aber es gibt noch einige weitere Aspekte, die bei der Verwendung von Kennwörtern beachtet werden sollten:



- Das Kennwort darf nicht leicht zu erraten sein. Namen, Kfz-Kennzeichen, Geburtsdatum etc. sind ungeeignet. Es dürfen keine Trivialkennwörter („1234567“ oder „ABCEDF“ u.ä.) verwendet werden. Verwenden Sie bitte kein Wort, das im Wörterbuch zu finden ist.
- Das Kennwort sollte eine Länge von mindestens acht Zeichen haben, besser sind zehn oder mehr.
- Innerhalb des Kennwortes sollte mindestens ein Zeichen verwendet werden, das kein Buchstabe ist (Zahl oder Sonderzeichen).
- Das Kennwort sollte regelmäßig geändert werden, z. B. alle 90 Tage.
- Ein gutes Kennwort wäre z. B. dieses: *Ibs12Jha!* Kann man sich ein solches Kennwort merken? Das geht, wenn Sie aus einem einprägsamen Satz, Lied oder Vers jeden x-ten Buchstaben auswählen und beachten, dass auch Sonderzeichen oder Zahlen vorkommen. So wurde das obige Kennwort gebildet. In der Langform bedeutet es: *Ich bin seit 12 Jahren hier angestellt!* Das dürfte ein Satz sein, den Sie nicht so schnell vergessen. Und somit das Kennwort auch nicht. Schade, ein Kennwort mehr, das ungeeignet ist, denn es ist ja nun bekannt!
- Wenn Sie glauben, ihr Kennwort aufschreiben zu müssen, dann sollten Sie das nur tun, wenn es in verschlüsselter Form geschieht (zum Beispiel in einem Tresor oder einer kennwortgeschützten Word-Datei). Letzteres macht natürlich nur dann Sinn, wenn Sie sich das Kennwort für die Kennwortdatei NICHT aufschreiben und dieses hinreichend sicher ist.