Merkblatt zur IT-Sicherheit

Die Sicherheit in der Informationstechnik (IT-Sicherheit) ist auch an der Schule ein sehr wichtiges Thema. Insbesondere der Schutz der personenbezogenen Daten vor Verlust, unbefugter Weitergabe und/oder Veränderung ist eine Aufgabe für jeden Beschäftigten.

Die hier genannten Maßnahmen helfen Ihnen dabei, in Ihrer täglichen Arbeit die IT-Sicherheit zu wahren.

Grundlage ist das IT-Sicherheitshandbuch für die Verwaltungen in Berliner Schulen.

1. Benachrichtigen Sie die zentrale Hotline (030 / 90 214 666), falls Sie den Eindruck haben, dass an Ihrem Rechner Manipulationen stattgefunden haben oder wenn seltsame Effekte auftreten.
2. Wenn Sie Ihren Arbeitsplatz verlassen, sperren Sie den Rechner vor fremden Zugriff. Das geht so:
   - **PC in der ZSVU:** Klicken Sie wie beim Abmelden auf Ihren Namen und dort dann auf **Sperren**.
   - **alle anderen PC:**  + ***L*** (Windows- und L-Taste gleichzeitig drücken.) oder Sie drücken gleichzeitig die Tasten ***Strg*** + ***Alt*** + ***Entf*** und wählen ***Computer sperren***.
3. Passwörter sind geheim und dürfen niemals an andere weitergegeben werden.

   Das Passwort sollte:
   - eine Länge von mindestens acht Zeichen haben.
   - regelmäßig (mindestens einmal jährlich) geändert werden.
   - aus einer Kombination von kleinen und großen Buchstaben, Ziffern und Sonderzeichen bestehen.
   - trotz allem gut zu merken sein.
   - in keinem Wörterbuch zu finden sein. Dies gilt auch für Teile des Passwortes.

   Eine Möglichkeit zur Passwortfindung ist die Benutzung eines Satzes, wie zum Beispiel „***Ein Esel hat 2 Ohren und 4 Beine.“***. Für das Kennwort verwendet man nur die Anfangsbuchstaben der Wörter. Statt des Wortes ***und*** wird das Sonderzeichen ***&*** benutzt.
   Das Kennwort würde bei diesem Satz lauten: „**EEh2O&4B.**“.

   Hinweis: Nutzen Sie bitte nie dieses Kennwort. Denken Sie sich einen eigenen Satz aus!

   Wenn Sie ein Passwort notieren, legen Sie es sicher und verschlossen ab. Hinweise dürfen nicht am Monitor oder unter der Tastatur vermerkt sein.
4. Das Herunterladen von ausführbaren Programmen aus dem Internet bzw. das Speichern von ausführbaren Dateien sowie der Besuch von Internetseiten mit aktiven Webinhalten (JavaScript, ActiveX und Java) können besondere Gefahren bergen. Dadurch können Computerviren oder sonstige Schadsoftware Zugang zu Ihrem Rechner bekommen. An Computern, die personenbezogene Daten verarbeiten, dürfen solche Aktionen nicht ausgeführt werden. Im Allgemeinen sind diese Aktionen blockiert.
   Müssen aus dienstlichen Gründen solche Aktionen durchgeführt werden, soll ein PC benutzt werden, der speziell dafür vorgesehen ist und keine personenbezogenen Daten verarbeitet.

5. Benutzen Sie keine Speicherdienste im Internet (sogenannte Clouds). Ihre Daten gehören nur auf den zur Verfügung gestellten Schulserver bzw. auf Ihren Rechner.
6. Das Versenden und Transportieren personenbezogener Daten darf nur verschlüsselt erfolgen.
7. Öffnen Sie keine E-Mail-Anhänge, die Sie nicht erwartet haben, oder die Ihnen zweifelhaft erscheinen.
   Seien Sie besonders vorsichtig bei Anhängen mit den Dateiendungen **.exe, .zip** und **.js**, sowie Office-Dateien mit Makros (Endungen: **.dotm, .xltm**).
8. Leiten Sie nicht leichtfertig E-Mails an eine große Zahl von Empfängern weiter. Kettenmails etc. sind dringend zu vermeiden.
9. Drucken Sie personenbezogene Daten nur auf dem dafür vorgesehenen Drucker.