Datenschutz und IT-Sicherheit

Die Zehn Gebote des Datenschutzes

1. **Zugangskontrolle**
   Unbefugten den Zugang zu Datenverarbeitungsanlagen,
   mit denen personenbezogene Daten verarbeitet werden, verwehren.

2. **Datenträgerkontrolle**
   verhindern, daß Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können.

3. **Speicherkontrolle**
   die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten verhindern.

4. **Benutzerkontrolle**
   verhindern, daß Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können.

5. **Zugriffskontrolle**
   gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

6. **Übermittlungskontrolle**
   gewährleisten, daß überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können.

7. **Eingabekontrolle**
   gewährleisten, daß nachträglich überprüft und festgestellt werde kann,
   welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind.

8. **Auftragskontrolle**
   gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden,
   nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

9. **Transportkontrolle**
   verhindern, daß bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

10. **Organisationskontrolle**
    die innerbehördliche Organisation so gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird.

IT-Sicherheit

1. Gefahrenquellen

1.1 Datenverlust durch PC-Probleme
- versehentliches Löschen
- Plattencrash
  - lokal
  - Netzlaufwerke

1.2 Viren (ausführbare Dateien, vbs-Dateien)
- als Dateianhänge an eMails
  - durch Download im Internet oder
  - durch Datenträger (Disketten, CD-ROM, DVD etc.)

1.3 unberechtigte Zugriffe auf Daten
- extern (per Internet)
- intern (Passwort)

2. Maßnahmen der EDV-Stelle

2.1 Schutz vor Datenverlust
- Datensicherung
  - alle Serverdaten werden durch SG 1.7 täglich gesichert
  - lokale Daten auf den Arbeitsstationen (Laufwerk C:/)werden nicht gesichert

2.2 Schutz vor Viren auf Datenträgern
- Disketten- und CD-ROM-Laufwerke sind - bis auf Ausnahmen - gesperrt

2.3 Schutz vor Viren per eMail / www
- vbs-Dateien werden an der Firewall abgefangen
  aber:
  Vortäuschen falscher Dateiendungen ist möglich (z.B. loveletter.vbs.htm)!

- ein Download von „exe“-Dateien (gängigste ausführbare Dateien) wird von der Firewall abgewiesen
  aber:
  oft sind solche Dateien gepackt und werden deshalb von der Firewall nicht abgewiesen

- der Virenschutz auf Exchange-Server überprüft alle eingehenden eMails auf Viren
  aber:
  bei hoher Auslastung des Exchange-Servers und damit des Virenschutzes kann eine noch nicht auf Viren gescannte eMail einige Sekunden im Postfach des Empfängers liegen (und vom User geöffnet werden)

daher: Lokaler Virenschutz:

- auf jedem Rechner mit
  - Internetzugang
  - eMail-Postfach und/oder
  - offenen Laufwerken

  ist ein weiterer Virenscanner (auf „C:/ “) installiert

- der lokale Virenschutz startet automatisch beim Anmelden am Netzwerk und scannt alle Dateien, die vom Nutzer bearbeitet werden
  - die Virenscanner werden täglich aktualisiert
  - trotzdem kein absoluter Schutz, da Gegenmaßnahmen zu Viren immer erst nach ihrem ersten Auftreten und damit nach einem Schadensfall erarbeitet werden können

daher:

- auch jeder einzelne User mit
  - Internetzugang
  - eMail-Postfach und/oder
  - offenen Laufwerken

ist gefordert, die Virengefahr weiter zu minimieren

3. Maßnahmen der User

- darauf achten, daß der lokale Virenschutz jedesmal beim Starten des Systems aktiv ist (zwei Symbole neben der Uhr, rechts unten auf der Task-Leiste)

- Datenträger unbekannter Herkunft nicht verwenden

- eMails mit fragwürdigem / unbekanntem Absender
  - ungelesen löschen oder
  - an die EDV-Stelle weiterleiten

- Downloads
  - nur von offiziellen Seiten

4. Datensicherheit bei unbefugten Zugriffen

- Firewall gegen Zugriffe von außen

- das NTFS-Dateiformat ermöglicht die Vergabe von Rechten (durch SG 1.7)

- Anmelden am Netzwerk mit Passwort

- Passwörter niemals weitergeben
  SG 1.7 braucht Passwörter nicht,
  - weil (von SG 1.7) überschreibbar und dann (vom User) neu einzutragen
  - einen „Anruf von SG 1.7 (wg. Passwort)“ kann es also nicht geben

- sichere Aufbewahrung des Passworts
  - bei Vergessen: SG 1.7 kann Passwörter zurücksetzen

Anmelden:
Strg+Alt+Entf (+Passwort)

Arbeitsstation sperren (PC läuft weiter):
Strg+Alt+Entf (+ Arbeitsstation sperren: OK)

Arbeitsstation entsperren (bei laufendem PC):
Strg+Alt+Entf (+Passwort)

(Besprechung der EDV-Beauftragten am 13. Juni 2001)