Einführung von DV-Systemen 06.10.2004

- Probeeinführung
  (Pilotprojekt) Erstmalige Einführung eines neuen Systems / einer neuen Methode, vorerst zu Testzwecken.
  Der Vorteil ist, dass hier das alte System an sich nicht angetastet wird. Diese Art der Einführung hat Testcharakter und dient der Erfahrungssammlung.
  Der Nachteil ist der Zeitaufwand, da hier natürlich zwei Systeme „bedient“ werden müssen, auch wenn das eine nur ein Testsystem ist. Und zum anderen muss hier extreme Vorsicht bei der Übertragbarkeit der Ergebnisse gewahrt werden, denn je mehr Anwender (auch unwissende Anwender) und je mehr Daten über das System fließen je ausfallsicherer und anspruchsvoller muss später die komplette Lösung sein.

- Paralleleinführung
  Realisierung einer EDV-Lösung unter Beibehaltung des alten Systems.
  Der Vorteil ist, dass es Sicherheiten bei evtl. scheitern des neuen Systems bietet. Es bietet auch gute Vergleichbarkeit bei der Verarbeitung der Ergebnisse.
  Dies ist eine sehr Zeit- und Personalaufwendige Lösung.

- Stufeneinführung
  Die Stufeneinführung ist geeignet um komplexe Inhalte / Umbauten zu realisieren. Es gliedert sich in mehrere abgeschlossene Teilstücke. Diese Methode ist gut geeignet um spätere Erweiterungsmaßnahmen schon einmal vorzuimplementieren.
  Der Vorteil ist, dass es die Komplexität der Aufgabe verringert und dadurch evtl. Überforderung entgegenwirkt.
  Die Schwierigkeit hierbei ist, die einzelnen Teilstücke derart modular aufzubauen.
  Die Gesamtfunktionsfähigkeit kann nicht getestet werden.

- Direkteinführung
  Sofortige Einführung relativ einfacher Änderungen zu einem bestimmten Stichtag.
  Der Vorteil liegt in der schnellen Umsetzung der Änderung.
  Der Nachteil ist, dass gerade hier eine umfassende Vorbereitung und Planung stattfinden muss und manche Mitarbeiter mit dem System große Schwierigkeiten haben werden. Sehr hohes Risiko.

Digitale Signatur

Auch elektronische Signatur genannt bezeichnet ein Verschlüsselungssystem von Daten.
Hierbei handelt es sich um PGP-Verschlüsselung (pretty good privacy).
Hierbei gibt es pro Person einen öffentlichen und einen privaten Schlüssel. Der öffentliche Schlüssel kann frei verteilt werden. Hiermit können alle Besitzer eines öffentlichen Schlüssels zwar Daten für die entsprechende Person verschlüsseln, aber nicht wieder entschlüsseln. Für die Entschlüsselung wird der private Schlüssel benötigt. Dieser sollte geheim gehalten werden und sollte niemand anderem in die Hände fallen, da derjenige ansonsten in der Lage ist, evtl. geheime Daten zu entschlüsseln.

PIN

Persönliche Identifikationsnummer

TAN

Transaktionsnummer
Gilt als „Unterschrift“ und verfällt nach einmaligem Gebrauch.

Aufgabe 3

Das neue System soll gegen die Risiken des Internets abgesichert werden.
Elektronische Bestellungen sollen mit einer qualifizierten digitalen Signatur versehen werden.
Erläutere diese Maßnahme.

- Einwählen in das Internet über einen Router – alternativ installieren einer Firewall
- Installieren aller Sicherheitspatches / ServicePacks / sicherheitsrelevanten Softwareupdates (Antivirensignaturen, etc.)
- Installieren eines Antivirenprogrammes
- Aktivieren des Antivirenschutzes beim ISP für die E-Mail-Postfächer
- Aktivieren der Antivirenoption für das interne Mailprogramm

Beim senden der Bestellung wird die Nachricht verschlüsselt. Nur der Empfänger kann nun die Datei wieder entschlüsseln und so wird eine nachträgliche Fälschung der Daten verhindert.

Aufgabe 4

PIN und TAN zusammen ersetzen die rechtsgültige Unterschrift bei Banktransaktionen.

Aufgabe 5

Makroviren: Makros sind auf Basic basierende Befehlszeilen für das Office-Paket (Word / Excel). Diese helfen, dass man die Programme auf die eigenen Bedürfnisse anpassen kann.

Unterschiede:

- **Viren**
  - Programme die vom Benutzer unbemerkt ausgeführt werden
  - diese richten evtl. Schaden auf dem PC an
  - es gibt Bootsektorviren und Word Makroviren

- **Würmer**
  - werden oftmals per Mail versandt und aktivieren sich sobald man die Mail öffnet, bzw. den Anhang der Mail öffnet
  - oft werden z.B. Outlook Programmfehler ausgenutzt
  - somit gelangen die Würmer ins System und können sich weiter versenden, bzw. Schadroutinen, o.ä. nachladen

- **Hoaxes**
  - Diese warnen vor Viren, die gar keine sind. Dies wird z.B. per Anweisung „löschen sie Datei XY.exe“ versucht. Hiermit kann man diverse Programme, oder aber das Betriebssystem selbst beschädigen. Deshalb sollte man versuchen herauszufinden, ob das Programm oder die Datei tatsächlich Malware ist.

Funktionen:

- **Antivirenprogramme**
  - prüft das System im Bezug auf Viren
  - Unterschiede: Echtzeitprüfung / Komplettsystemprüfung / überwachung ein und ausgehender Dateien
  - sobald ein Virus / Wurm / Trojaner / etc. gefunden wird kann er je nach Einstellung warnen, den Schädling direkt löschen, oder das ganze in ein Quarantäneverzeichnis verschieben

- **Firewalls**
  - kontrollieren den Datenverkehr zwischen dem Rechner / Netzwerk und dem Internet
  - sie kann sowohl in einer Hardware als auch in einer Software bestehen
  - es kann genaue Regeln geben, welche Protokolle und Programme „nach Hause telefonieren“ dürfen und welche nicht
  - Ports, die ansonsten beispielsweise Sicherheitslücken darstellen würden sind / können gesperrt werden.

- **Preise (Workstation), Hersteller**
  - Antivirenprogramme:
  - McAfee – Virusscan 44,95
  - H+Bedv – Antivir 69 Euro

- Kaspersky – Anti-Virus Personal 39,95
- Norman – Norman Virus Control 49,00 Euro
- Symantec – Norton Antivirus 2004 39,95 Euro
- eTrust – Antivirus 45,90 Euro

- Firewalls
- Norman – Personal Firewall 39,00 Euro
- Symantec – Norton Personal Firewall 49,95
- McAfee – Firewall 4.0 37,65 Euro
- Kerio – Personal Firewall 37,54
- Tiny Software - Tiny Personal Firewall 46,05 Euro