# Daubes Internet regeln

Details hängen von der tatsächlichen system-konfiguration ab.

- Windows version, Mac OS version.
- Browser (Opera, Netscape, IE, etc)
- E-mail programm (Pegasus, Eudora, Communicator, Outlook[1)] etc)

Das meiste des nachfolgenden ist Windows spezifisch - hier lauern aber auch die grössten gefahren, denn viren-gangster streben natürlich grösste wirkung an.

☐ bedeutet: option nicht gewählt. ☑ bedeutet: option gewählt.

## Grundsätze

❖ Nicht mit der meute heulen: nach möglichkeit alternative programme zu MS 'standard' verwenden: ➔ Opera browser, Pegasus Mail.

❖ Trau-schau-wem: Liebesbriefe aus Moskau? Gratisprogramm ohne dass Sie es angefordert haben? Französische mail von Ihrem italienischen freund? ➔ Zügeln Sie Ihre neugier! Mail sofort in den kübel!

❖ Windows standard-einstellungen sind für dumme. Mindestens im file explorer alle dinge anzeigen lassen (Doppelte file-extensions - ein beliebter trick von viren - müssen sichtbar sein: `harmlos.txt.vbs` .): ➔ **My Computer > View > Options:** ☑ *Show all files;* ☐ *Hide file extensions for known File Types*.

❖ Banne den doppelklick: Wissen Sie wirklich über alle programm-verknüpfungen bescheid? Wissen Sie, was macros und scripte alles machen können? ➔ Jedes programm, in dem aktionen aufgezeichnet und abgespielt werden können, ist potentiell gefährlich!

❖ Programm-verknüpfungen (wirkung des doppelklick) für Word-, Excel-files etc. auf ein *anzeige*programm statt auf ein *bearbeitung*sprogramm legen. Doppelklick auf attachements (dieses typs) wird dann harmlos ➔ *Word View, Quick View Plus*.

1 Als viren-sauger bekannt: internet-world, november '99, s. 82.

## Betriebssystem

❖ Browser *nicht* in den desktop (dateiverwaltung) integrieren! Das kann allerding nur bei der installation von IE bzw neu-aufsetzen von Windows beeinflusst werden. *Divide et impera* war schon Ludwig XI wichtig.

❖ Gemeinsame nutzung von disks verhindern. Windows default-einstellungen geben alle zugriffe frei! ➔ Auf einem einzelplatz macht file-sharing absolut keinen sinn (ausser für hacker).

❖ Spezielles verzeichnis für downloads einrichten (nicht auf drive C: !) ➔ Virenscanner auf dieses verzeichnis ansetzen, nicht immer alles durchsuchen müssen.

❖ Viren-scanner stets à jour halten. ➔ Pro jahr werden mehrere tausend neue viren auf die schläfrige menschheit losgelassen.

❖ Windows Scripting Host abschalten bzw. einschränken[2)]. ➔ Solange Sie das ding nicht programmieren können, wird es nur von maliziösen zeitgenossen ausgenützt.

## Internet-zugang

❖ Ankommende verbindungen nicht abnehmen (eine fax-maschine kommt allemal billiger als ein einziger virenangriff).
➔ **Control Panel > Network > Services > Remote access services > Properties > *modem port* > Configure... > :** ☑ *Dial-out only.*

❖ Verbindung automatisch abbrechen, wenn > 5min inaktiv.
➔ **Control Panel > Internet Options > Connection > (modem) Settings > Advanced:** ☑ *Disconnect if idle for …**5**… minutes.*

❖ Schalten Sie den modem lautsprecher immer ein für eine wahl. So merken Sie, wenn 'irgend ein programm' nach draussen will.
➔ **Control Panel > Internet Options > Connection > (modem) Settings > Properties > Basic > Configure...:** ☐ *Disable Modem Speaker.*

❖ Dial-Up Monitor aktivieren. ➔ Das icon im 'system tray' zeigt an, ob die verbindung aktiv ist.

2 Viele viren (zb I-LOVE-YOU) arbeiten mit Visual Basic!

- Nur das netzwerk-protokoll TCP/IP aktivieren.[3)]
- Lieber etwas zahlen als risiken eingehen. ➔ Der MS-dienst *hotmail* ist ein beliebtes ziel von attacken.

## Browser

- Verwenden Sie nach möglichkeit den Internet Explorer nur für die anzeige der neuen HTML Helps. Fürs surfen sind Netscape 6.1 oder Opera 5.12 wesentlich sicherer.
- Lassen Sie den browser nicht automatisch ins netz gehen. Die "homepage" daher nicht auf dem default stehen (zb `www.microsoft.com/...`), sondern definieren Sie entweder eine leere seite oder eine eigene.
  ➔ In IE: **Tools > Internet Options > General: Use Blank** (oder zb `file:///E:/Web_local/_kld_homF.html`)
- Sicherheitseinstellungen mindestens auf medium einstellen (in IE: **Tools > Internet Options > Security > Custom level: reset to: *medium***)
- Cookies am ende der session löschen.
  ➔ In IE: **Tools > Internet Options > Security > Custom Level... > Cookies:**
  *Disable*: Allow cookies stat are stored on your computer
  *Enable*: Allow per-session cookies (not stored)
- Identität verschleiern (zumindest die e-mail adresse).
- Direktes starten von applikationen auf ein minimum setzen. Keinesfalls macro-fähige anwendungen direkt starten lassen. In IE werden die system-definitionen verwendet. In Netscape und Opera kann für jeden datentyp individull definiert werden, welche aktion ausgeführt werden soll (programm x starten, file speichern, ...)
- Active-X- controls verbieten. Es kann dann allerdings vorkommen, dass neuere online-hilfen nicht mehr funktionieren!
  ➔ in IE: **Tools > Internet Options > Security > Custom Level... > Cookies:**
  *Disable*: Initialize and script ActiveX controls not marked as safe.
  *Enable*: Run ActiveX controls an plug-ins.
  *Enable*: Script ActiveX controls marked safe for scripting.

3 TA-Computerbund 2000-04-10: *Schlupflöcher für Viren im DFÜ Netwerk stopfen*).

## E-mail

- Meldungen als normalen text erstellen und keine HTML mail erlauben[4)]. Wenn Sie wirklich etwas schön gestaltetes versenden wollen, verwenden Sie ein PDF attachment.
- Zusätzliche daten als attachement (anhang), *nicht* als enclousure (einschluss) senden. Nur so kann der empfänger die anhänge separat abspeichern.
- Anhänge (attachements) immer im betreff ankündigen:

```
Info zu map ID file (1 PDF attached)
Aufgabenliste KLD (1 excel attached)
```

- Statt attachements sofort auszuführen, speichern Sie das file in Ihrem download-bereich, den Sie mit einem virenscanner überwachen lassen. Sehen Sie sich das file an (browse, view). ➔ In den seltensten fällen müssen Sie das file mit der 'original-sofware' bearbeiten.Eigenen e-mail client im browser definieren. Zb in IE: **Tools > Internet Options > Programs:**
- Filter zum abfangen unerwünschter mail einrichten. Die prozedur ist natürlich je nach e-mail client verschieden.
  ➔ In Pegasus: **Tools > Mail filtering rules > Create/Edit general rule set**.
- Provider suchen, der nicht als mail-relais eingesezt werden kann. Im mail client muss dann meist eingestellt werden, dass zuerst 'post abgeholt wird' und dann erst gesendet.
  ➔ In Pegasus: **Tools > Internet Options > Sending (SMPTP):** ☑ *Authenticate by doing a prior POP3 mail check*.
- Vom provider anti-spam massnahmen bestätigen lassen. Der provider kann mail aus bestimmten quellen abblocken.
- Für heikle sachen verschlüsselung vorsehen. Das muss aber mit dem empfäner abgesprochen sein (er muss ja einen schlüssel haben).

4 Neueste viren verstecken sich in HTML mail, wo ja scripts drin sein können. Die viren führen sich aus, sobald das HTML angezeigt wird - also ohne Ihr zutun!