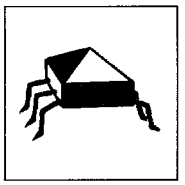

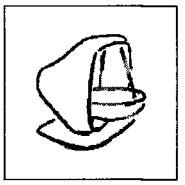

Arbeitskreis Viren

Wolfgang Tauchert

Überblick

Zielsetzung des Arbeitskreises ist die Aufklärung bezüglich der Wirkungsweise, des Gefahrenpotentials und der Abwehrmöglichkeiten von Viren (Vortrag Brunnstein) sowie – auch im Hinblick darauf – die gesetzlichen Vorschriften zur Datensicherheit (Vortrag Alke).
Vortrag 1: *Professor Dr Brunnstein* (Universität Hamburg): "Viren".
Dabei sollen folgende Punkte angesprochen werden:

- Was sind Viren?
  Erklärung, Unterschied zu anderen Störungen am Rechner, erste Hinweise für einen Befall und Möglichkeiten der Diagnose, Art der Auswirkungen (Unterbrechung, Absturz, Manipulation und Verlust von Daten ...)
- Wahrscheinlichkeit des Befalls, kritische Anwendungen (DFÜ) und Betriebsweisen
- Auswirkungen auf das Einzelgerät, das Gesamtsystem
- Maßnahmen zur Verminderung der Befallswahrscheinlichkeit (technisch, organisatorisch)
- Maßnahmen zur Eindämmung der Auswirkung nach Befall (technisch, organisatorisch)
- Handhaben von Virenscannern und -entfernern
- Fehlermöglichkeiten beim Umgang damit, Beispiele

Vortrag **2:** *H. Alke*, Regierungsdirektor beim Bundesbeauftragten für Datenschutz: Datensicherung als Forderung des Datenschutzgesetzes (Allgemeine Vorschriften bzw. Empfehlungen zur Datensicherheit).

"Computer-Viren: Stand der Bedrohung, Erkennung, Gegenmaßnahmen, Rechtsprobleme"

Klaus Brunnstein

Sicherheitsanforderungen wurden nicht berücksichtigt.

Heute verbreitet eingesetzte Informations- und Kommunikationstechniken sind *nicht* unter dem Gesichtspunkt eines sicheren Betriebes konzipiert worden. Insbesondere wurden *"Personal Computer"* unter Microsoft-Betriebssystemen (MS-DOS, Windows) für "persönliche Zwecke" (ursprünglich als "Home Computer") geplant, wobei *Sicherheitsanforderungen – etwa Gewährleistung der Identität und Authentizität von Benutzern, Kontrolle der Zugangs- und Benutzungsberechtigungen, Gewährleistung der geforderten Funktionen, bis hin zur Aufzeichnung eventueller Schutzverletzungen* – nicht berücksichtigt wurden. Bei *UNIX-Systemen*, heute in Client-Server-Systemen vielfach eingesetzt, wurden sogar die umfangreichen *Sicherheitsmechanismen* der MULTICS-Systeme *bewußt ausgebaut*, um *Anwendungen im technisch-wissenschaftlichen Labor* schneller und effizienter (wenn auch weniger sicher) durchführen zu können. Erst bei einigen Weiterentwicklungen (OS/2, Windows NT, Secure UNIX) wurden einige Sicherheitsaspekte nachträglich berücksichtigt.

Schäden und Fehlfunktionen unvermeidbar

Weil PCs und UNIX-Systeme trotz ihrer *erheblichen Mängel* sich in wichtigen Anwendungen in Wirtschaft, Staat und Gesellschaft epidemisch ausgebreitet haben, sind *schädliche Folgen unvermeidbar*. Aber nicht bloß technische Mängel der Hardware und Software, der schlechte Ausbildungs- und Kompetenzstandard vieler Benutzer und das mangelhafte Sicherheitsbewußtsein von Entscheidern führen zu spürbaren Konsequenzen wie Fehlfunktionen von Programmen, Systemen und Geräten bis hin zum Datenverlust. Auch unerkannt enthaltene Fehlfunktionen, etwa Programmfehlern wie *"Wanzen" (bugs)* oder *"bösartiger Software" wie Trojanische Pferde und Computer-"Viren"* beeinträchtigen die Beherrschbarkeit und Sicherheit heutiger Informationstechniken.

Dr. Klaus Brunnstein ist Professor für Anwendungen der Informatik an der Universität Hamburg.