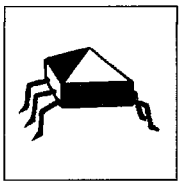
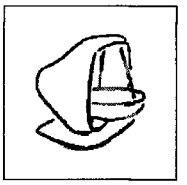




Arbeitskreis Viren

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

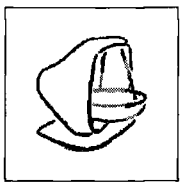
Sicherheitsanforderungen wurden nicht berücksichtigt.

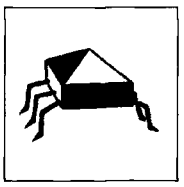
Heute verbreitet eingesetzte Informations- und Kommunikationstechniken sind *nicht* unter dem Gesichtspunkt eines sicheren Betriebes konzipiert worden. Insbesondere wurden *"Personal Computer"* unter Microsoft-Betriebssystemen (MS-DOS, Windows) für "persönliche Zwecke" (ursprünglich als "Home Computer") 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.





Weitere Beeinträchtigungen durch Netzwerk-Verbund

Das an sich schon *"un-sichere" Arbeiten mit einzelnstehenden Geräten und Systemen* wird weiter beeinträchtigt, wenn solche Geräte über Netzwerke verbunden werden. Auch in jüngeren Netzwerkkonzepten wurden nämlich *elementare Sicherheitsanforderungen vernachlässigt.* Nicht bloß die technischen Träger der Netzverbindung – lokal durch Koaxialkabel oder überregional über die Leitungen der Telekom oder anderer Dienstanbieter – bergen Risiken, etwa der *Abhörbarkeit oder Störbarkeit.* Erhebliche Risiken importieren die Softwareschichten, angefangen bei Übertragungsprotokollen (wobei das UNIX-nahe Internet-*Protokoll TCP/IP* in vielerlei Hinsicht als *Muster eines unsicheren Protokolls* gelten darf) bis zu manchen Aspekten der Hardware, Software und Organisation der Netzsysteme. Die Mängel an sicherheitstechnischen Verfahren *machen "Angriffe" – ob in böswilliger Absicht oder als Nebeneffekt von Neugier und Spieltrieb – oft allzu einfach.* So kann *"bösartige Netz-Software" wie Computer-"Würmer", Kettenbriefe sowie Hacker-Angriffe einschließlich Verfahren der Adreßfälschung oder Abhörung von Netzen zu erheblichen Risiken* beitragen.

Die aktuelle Viren-Gefahr

Vor diesem generellen Hintergrund stellt der Vortrag den *aktuellen Stand der Bedrohung durch "Computer-Viren"* dar. Ausgerichtet auf PCs werden wichtige Arten von Viren, insbesondere *System-* (Boot- und MBR-) sowie *Programm-* (File-) *Infektoren* vorgestellt. Im Sommer 1995 sind erstmals auch *Viren über Dokumente* (insbesondere Word) verbreitet worden, wodurch eine neue Form der Bedrohung (*"Makro-Viren"*) entstand. Neben den *Verfahren der Verbreitung* ("Infektion") wird auch auf Selbstschutz-Verfahren eingegangen (etwa durch Selbstverschlüsselung, "vielgestaltige" (oligo/polymorphische) Mutation, Tarnkappenverfahren (stealth) u. a. m., mit denen Viren gegen Entdeckung "getarnt" werden. *Wirkungen von Viren* (*"payloads"*) können die programmierbaren Aktionen sein, von der Anzeige eines Textes über das Abspielen einer Melodie bis zum Überschreiben von Daten und Formatieren ganzer Datenträger. Solche Wirkungen können von Bedingungen ("Trigger"), etwa einem speziellen Datum oder dem Eintreten eines Ereignisses abhängen. Die Wirkung einiger ausgewählter Viren wird demonstriert.

Anti-Virus-Programm vs. über 8.000 PC-Viren

Angesichts der *über 8.000 bekannten PC-Viren* ist für deren *Erkennung und Beseitigung* ein gutes Standard-Verfahren, *"Anti-Virus-Programm"* genannt, erforderlich. Die *Arbeitsweise* solcher Programme, etwa Viren-Scanner, heuristische Prüfverfahren, Integritäts- oder Checksummenverfahren sowie die *Grenzen dieser Verfahren* werden vorgestellt, und es wird über *Testergebnisse des Virus Test Centers der Universität Hamburg* berichtet. Es werden Maßnahmen vorgestellt, bei deren Beachtung die Virengefahr zwar nicht völlig ausgeschlossen werden kann (weil Viren ja auch von sonst vertrauenswürdigen Herstellern übermittelt werden können), aber die Risiken doch deutlich minimiert werden können. Es werden auch *Hinweise auf das Verhalten im Notfall* vorgestellt.

Rechtliche Verfolgung der Viren-Autoren

Abschließend wird an Fallbeispielen dargestellt, welche Probleme *bei der rechtlichen Verfolgung von Virenautoren und Virenverbreitung* sich ergeben. Als Beispiel wird die Verurteilung des Virenautors "Black Baron" nach dem englischen "Computer Misuse Act" (1995: 18 Monate Haft) dargestellt. Ausgehend vom Beispiel des *Schweizer AntiViren-Gesetzes* wird gezeigt, warum die allgemeine *Strafbestimmung "Computersabotage"* (§ 303b StGB) für die *Beurteilung von Virenkriminalität wenig geeignet* ist.

Datensicherung als Folgerung des Bundesdatenschutzgesetzes

Horst Alke

IT = Schlüsseltechnologie

Die Informationstechnik (IT) ist inzwischen eine Schlüsseltechnologie für die wirtschaftliche und gesellschaftliche Entwicklung unseres Landes geworden; sie ist auch unverzichtbar für die Funktionsfähigkeit des Sozialstaates. Umso wichtiger ist es heute, sich der Risiken und Gefahren beim – und durch den – Einsatz der IT bewußt zu sein und ihnen entgegenzuwirken.

"IT-Sicherheit"

Da gilt es zunächst, für *"IT-Sicherheit"* zu sorgen, also Systeme und Daten selbst zu sichern, d. h. ihre

- Verfügbarkeit,
- Integrität und
- Vertraulichkeit

Dipl.-Ing. Horst Alke ist Referatsleiter beim Bundesbeauftragten für den Datenschutz