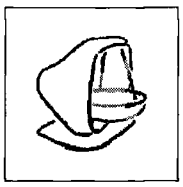
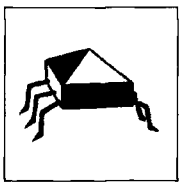




Weitere Beeinträchtigungen durch Netzwerk-Verbund

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

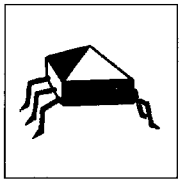
Die Informationstechnik (IT) ist inzwischen eine Schlüsseltechnologie für die wirtschaftliche und gesellschaftliche Entwicklung unseres Landes geworden; sie ist auch unverzichtbar für die Funktionsfähigkeit des Sozialstaates. Umso wichtiger ist es heute, sich der Risiken und Gefahren beim – und durch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

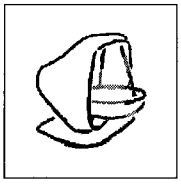
"IT-Sicherheit"

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





zu erhalten. Durch Gesetz wurde 1990 das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bonn begründet, dessen 300 Mitarbeiter seitdem "die Förderung der Sicherheit in der Informationstechnik" betreiben, nämlich untersuchen, beraten und Hilfe leisten. Typisch ist das Angebot eines leistungsfähigen Virensuchprogrammes, für das jetzt das 6. Update ausgeliefert wurde.

BSI und BDSG

Das BSI kann aber nur Empfehlungen geben: Niemand *muß* sie umsetzen, niemand *muß* das Virensuchprogramm einsetzen. Forderungen zur IT-Sicherheit stellt jedoch auch das *Bundesdatenschutzgesetz* (BDSG). Regelungsziel des BDSG – und Grundgedanke des Datenschutzes – ist es, den einzelnen davor zu schützen, daß er durch den Umgang mit seinen Daten in seinem *Persönlichkeitsrecht* beeinträchtigt wird. Nach den Vorschriften des BDSG sind bei der Verarbeitung und Nutzung personenbezogener Daten zwei *Grundsätze* zu berücksichtigen:

- Personenbezogene Daten dürfen nur soweit erhoben, verarbeitet und genutzt werden, wie dies gesetzlich erlaubt und im Einzelnen erforderlich ist – es sei denn, der Betroffene hat eingewilligt.
- Dabei sind angemessene technische und organisatorische Maßnahmen zur *Datensicherung* zu treffen.

Wenn personenbezogene Daten verarbeitet werden, besteht also eine *gesetzliche Verpflichtung*, Datensicherungsmaßnahmen zu treffen. Diese müssen *auch* die IT-Sicherheit gewährleisten, darüberhinaus jedoch einer Reihe weiterer Erfordernisse entsprechen. So ist z.B. das *Auskunftsrecht* der Betroffenen – die speichernde Stelle hat ihnen auf Anfrage die zu ihrer Person gespeicherten Daten aktuell und vollständig mitzuteilen – technisch und organisatorisch zu gewährleisten; z.B. für ein Unternehmen mit zahlreichen Niederlassungen im gesamten Bundesgebiet durchaus keine Trivialaufgabe. Welche Maßnahmen zur Datensicherung zu treffen sind, regeln die Vorschriften des § 9 BDSG sowie der Anlage hierzu. Diese enthält die *"Zehn Gebote der Datensicherung"* für den IT-Einsatz zur Verarbeitung personenbezogener Daten:

Wie können persönliche Daten geschützt werden?

"Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind,

- Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (*Zugangskontrolle*),
- zu verhindern, daß Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (*Datenträgerkontrolle*),
- Die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (*Speicherkontrolle*),
- zu verhindern, daß Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (*Benutzerkontrolle*),
- zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (*Zugriffskontrolle*),
- zu gewährleisten, daß überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können (*Übermittlungskontrolle*),
- zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogene Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (*Eingabekontrolle*),
- zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (*Auftragskontrolle*),
- zu verhindern, daß bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (*Transportkontrolle*),
- die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (*Organisationskontrolle*)."