Vortrag:
Hardenberg Institut für Kulturwissenschaften

Zur Einleitung: Präambel der CCC-Satzung

Gegenstand: Stand heutiger Computer- oder allgemeine IuK-Technologien, Gefährdung der Informationsgesellschaft durch Angriffe auf Computertechnik, Angriffsmotive und Angriffsformen.

Zum Stand der heutigen Computertechnik

Die elektronische Datenverarbeitung hat in den letzten Jahren Einzug in praktisch alle Bereiche unseres Lebens gehalten - zum Teil sogar unbemerkt. Schon lange nicht mehr beschränkt sich der Computereinsatz auf seinen Ursprungsort, das Militär. Neben Universitäten, Industrieunternehmen und öffentlicher Verwaltung finden sich auch im privaten Bereich mehr und mehr Computeranwendungen. Vor allem im Industriebereich zeigt sich zunehmend, daß eine nicht mehr reduzierbare Abhängigkeit zwischen Computereinsatz und Arbeitsablaufgeschehen, die im Notfall sogar nicht mehr von Menschen substituiert werden kann. Lagerhaltung, Produktionssteuerung, Lohnbuchhaltung, Bank- und Geschäftsverbindungen werden in größeren Betrieben ausschließlich von Computern übernommen.
Und die öffentliche Verwaltung zieht nach. Unter dem Schlagwort "Das Papierlose Büro"

wird die computerunterstützte Erfassung und Verarbeitung von Verwaltungsdaten propagiert.

Je mehr Rechner → Vernetzung sinnvoll.

heute vorhandene Datennetze:

Telefonnetz, Datex-P VDA (X.25)
EARN, ARPA, Rechnernetze von Computerherstellern DECNET,
Telex, Telefax, Btx

geplante Netze:

ISDN, Landesverwaltungsnetz, BLIX

Vernetzung macht Computer verletzlich:

früher: abgeschlossene Rechenzentren, in die nur authorisierte Personen Zugang haben

heute: Netze prinzipiell offen, mit entsprechendem Gerät von jeder Person zu nutzen.

→ Neue Sicherungskonzepte nötig

Anmelden am Comp: Userid (Account)
Passwort

Im Rechner drin: nur erlaubte Programme und Daten aufrufen und manipulieren. Abgeschottete Benutzerbereiche. In einer speziellen Datei sind die Zugriffsrechte der jeweiligen Userid auf andere Datensätze geregelt. Im allgemeinen werden auch alle Aktionen eines Benutzers im Rechner mitprotokolliert.

Angriffsmotive:

x - Arbeitsstreß
x - Unüberwindliche Datenbarrieren
x - Betriebliche Auseinandersetzungen
- - Wirtschaftliche Gesichtspunkte
- - Spionage
x - Entlassung
x - finanzielle Vorteile, EC-Kartenbetrug
x - billige Waren
x - Datendiebstahl
x - Softwarediebstahl
x - Teilediebstahl
x - Erpressung
x - Unzufriedenheit mit der Datenverarbeitung
x - Neugier (Hackermotive)
x - politische Überzeugung
- -

Angriffe auf DV-Anlagen

konventionell:
- Bomben- und Brandanschläge
- Überflutung
- Kappen der Stromzuführung (Strommasten)
- Klimaanlagen zerstören
- Diebstahl von Daten oder Programmen

Zukünftig: Die Angriffsmethoden dürften zunehmen, da auch Computer irgendwo eingesetzt werden.

Die Hardware wird in Zukunft kaum geschützt werden gegen diese Art der Angriffsformen. Als Angriffstäter kommen dann nur noch Personen mit hohes Kenntnis von DV-Vorgängen und sehr gute Kenntnis der Verwendeten Rechner und Betriebssysteme.

Daher werden die Angriffsformen der Zukunft eher programmtechnischer Natur sein. Mit diesen Angriffsformen will ich mich abschließend befassen:

Einigen unter Ihnen wird es jetzt vielleicht so vorkommen, als hätte ich das Thema gewechselt. Da gibt es jetzt ein Sammelsurium von Würmern, Viren, Bakterien, ~~usw.~~ Pferden usw. ~~Doch~~ Obwohl alle Begriffe aus der Zoologie kommen, ~~gehöre~~ bleibe ich beim Thema Computersicherheit. Was steckt also hinter diesen Bezeichnungen?

trojanisches Pferd: Ein TP ist eine Programmsequenz, die in vorhandene Anwendungsprogramme versteckt eingefügt worden ist. Man unterscheidet noch genauer nach Funktion:

logische Bombe:
ein Programm, das zu einer bestimmten Zeit oder auf ein Stichwort hin, Programmabläufe auslöst, die Computerfehlfunktionen oder sogar Zerstörung von Programmen und Daten zur Folge hat.

Datenleck:
Übertragung von Daten oder Programmkopien in dem Angreifer zugängliche Bereiche.

Impersonation:
Sammeln von Zugangspasswörtern durch Simulation des Anmeldeprozedur.

Bakterien: B. sind selbstständige Programme, die sich automatisch über Datennetze von einem Rechner in einen anderen verbreiten, und so in die Lage, eine Netzüberlastung hervorzurufen und/oder in jeweiligen Rechner Manipulationen vorzunehmen.

Würmer sind ebenfalls Lebewesen, die in Datennetzen leben. Wie biologische Würmer bestehen sie aus Segmenten. Jedes Segment ist ein Programm auf einem anderen Netzrechner. Der Zusammenhalt des Wurms wird über Datenaustausch auf dem Netz kontrolliert. Fällt diese Kommunikation aus oder wird sie gestört (Durchschneiden eines Wurms), so kann jedes Segment den ganzen Wurm aus sich selbst heraus generieren. Würmer können im Netz wandern indem einzelne Seg. sich neue Wirtsrechner suchen. Würmer können jede von Programmen durchführbare Manipulation in Rechner bewirken.

Beim Virus wird die biologische Analogie perfekt. Ein Virus infiziert/befällt ein Wirtsprogramm (Zelle) im Rechner und manipuliert es so, daß dieses Programm, ~~läuft~~ wird es gestartet, selbst Viren im Computer freisetzt, die noch nicht

infizierte Programme befallen können.
Damit sind nach und nach der gesamte
Prgm-~~Daten~~bestand eines Rechners vom Virus in-
fiziert. Der Virus kann sich verbreiten ohne
aufzufallen. Nach einer bestimmten Zeit
(Inkubationszeit) bricht dann die eigentliche
Krankheit aus: Programmlöschung, Daten-
manipulation, Computerfehlfunktion. Ein
so befallenes Rechenzentrum (Körper) ist
in der Regel nicht mehr zu retten, denn
auch die Backups der Datenbestände
(Blutkonserven) sind nach einiger Zeit
infiziert. Auch eine Ansteckung anderer
Rechenzentren über Datennetze ist möglich.

Wie funktioniert ein Virus?