Computerviren

Mihajlovic Roland rmihajlo@cosy.sbg.ac.at

Reischmann Stefan sreisch@cosy.sbg.ac.at

Institut fr Computerwissenschaften

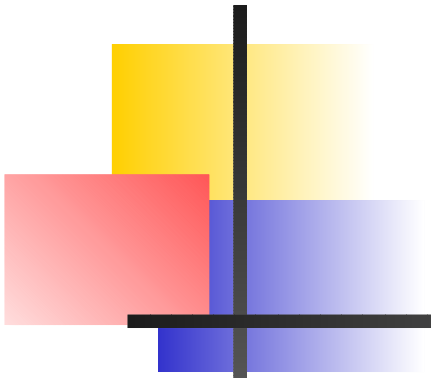
Der I LOVE YOU Virus

Geschichte - Entstehung

- 1.Definition eines Virus von Fred Cohen im Jahre 1984;
- Bedrohung ging vom Personalcomputer aus;
- 1986 das erste mal ein Virus auf einem IBM Computer;
- "Scan"- Codes, Verschlüsselung des "Virus"-Codes;
- Nächste Stufe waren die "Stealth"- oder "Tarnkappen"-Viren;

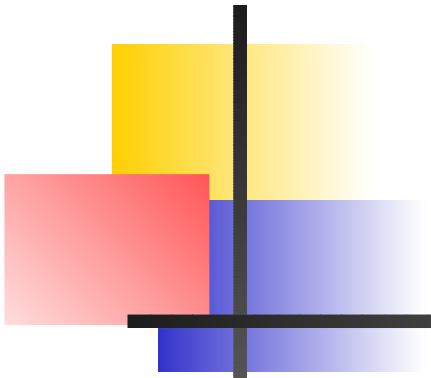
Geschichte - Entstehung

- 1990 Entstehung der polymorphen Computer-Viren;
- Entstehung von "Viren-Baukästen" für Jedermann;



Definition

Ein Computer-Virus ist eine nicht selbstständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt.



Definition

Eine nichtselbständige Programmroutine bedeutet, dass der Virus ein Wirtsprogramm benötigt. Diese Eigenschaft und seine Fähigkeit zur Reproduktion führte in Analogie zum biologischen Vorbild zu der Bezeichnung *Virus*.

Aufbau

- Reproduktionsteil;
- Erkennungsteil;
- Schadensteil;
- Bedingungsteil;
- Tarnungsteil.

Einteilung - Betriebssystem

Computer-Viren sind sehr eng an die jeweilige Computer-Hardware und das jeweilige Betriebssystem gebunden. Sie laufen nicht auf unterschiedlichen Mikroprozessoren,d.h., IBM-kompatible, auf der Basis des Prozessors 8086 der Firma Intel (und kompatible) arbeitende Viren können sich z.B. auf Macintosh-Computern nicht in gleicher Weise ausbreiten.

Einteilung - Betriebssystem

- Windows NT und Derivate;
- MS-DOS, Win95, Win98 und Derivate;
- UNIX, LINUX;
- Apple Macintosh, OS/2 und andere.

Einteilung - Typen

- Bootsektorviren;
- Dateiviren;
- Makroviren;
- Hybridviren;
- Keime;
- Companionviren;
- Polymorphe Viren;
- Tarnkappen Viren;

Einteilung - Typen

- Trojaner;
- Würmer;
- Retroviren.

Schutz - Scanner

- Überprüfen der Dateien auf vorhandene Viren-Bytefolgen;
- Identifikation des Virus oder der Virenart;
- Heuristisches Suchen - Überprüfung auf verdächtigen Programmcode, z.B: Schreiben auf den Bootsektor, Umleitung von Interrupts . . . ;
- Selbsttest des Virenprogrammes.

Schutz - Vergleichsdateien

- Erzeugung einer *einzigartigen* Vergleichsinformationen für jede einzelne Datei;
- Ablegen der Informationen in eigenen Daten-Dateien;
- Erzeugung dieser Informationen durch CRC-Codes (Polynom-Codes);
- Beim Suchen erfolgt der Vergleich der alten und neuen Datei und des Codes und bei Nichtübereinstimmung die Warnung auf Virenbefall(bei einer Veränderung der Datei);

Schutz - Wächter

- Bleiben im Hauptspeicher;
- Suchen Viren beim Dateizugriff;
- Arbeiten im Hintergrund;
- Verbrauchen Systemresourcen.

Schäden durch Computer-Viren

- Datenverlust;
- Zerstörung von Hardwareteilen;
- Inanspruchnahme von Speicherplatz sowohl im Hauptspeicher als auch am Datenträger und Prozessorzeit;
- Verunsicherung der Benutzer;
- Kosten und Zeit.

Quellen der Virenverbreitung

- Originalsoftware;
- Bereits infizierte Datenträger (Disketten, USB-Stick, Festplatten, CD-ROMs, . . .)
- Vernetzung (Internet, eMail, Filesharing-Tools, . . .)

Ende des Jahres 2002 waren an die 70.000 Viren im Umlauf (einschliesslich ihrer Varianten).

Anti-Viren-Programme

Windows

- Testsieger: AntiVirenKit 12 Professional;
- Preistipp: H+BEDV AntiVir Personal Edition.

UNIX bzw. LINUX

- Testsieger: Sophos AntiVirus;
- Preistipp: H+BEDV AntiVir Personal Edition.

Fazit

Einen vollständigen Schutz gegenüber Viren wird es nie geben, alleine schon aus dem Grund, dass helle Köpfe immer neue Methoden der Infizierung entwickeln werden.
Ausserdem wird Software immer noch von Menschen geschrieben und Menschen sind nicht unfehlbar. Deshalb bleiben immer Hintertüren offen, die von Viren genutzt werden können, und später von Anti-Viren-Programmen wieder geschlossen werden.