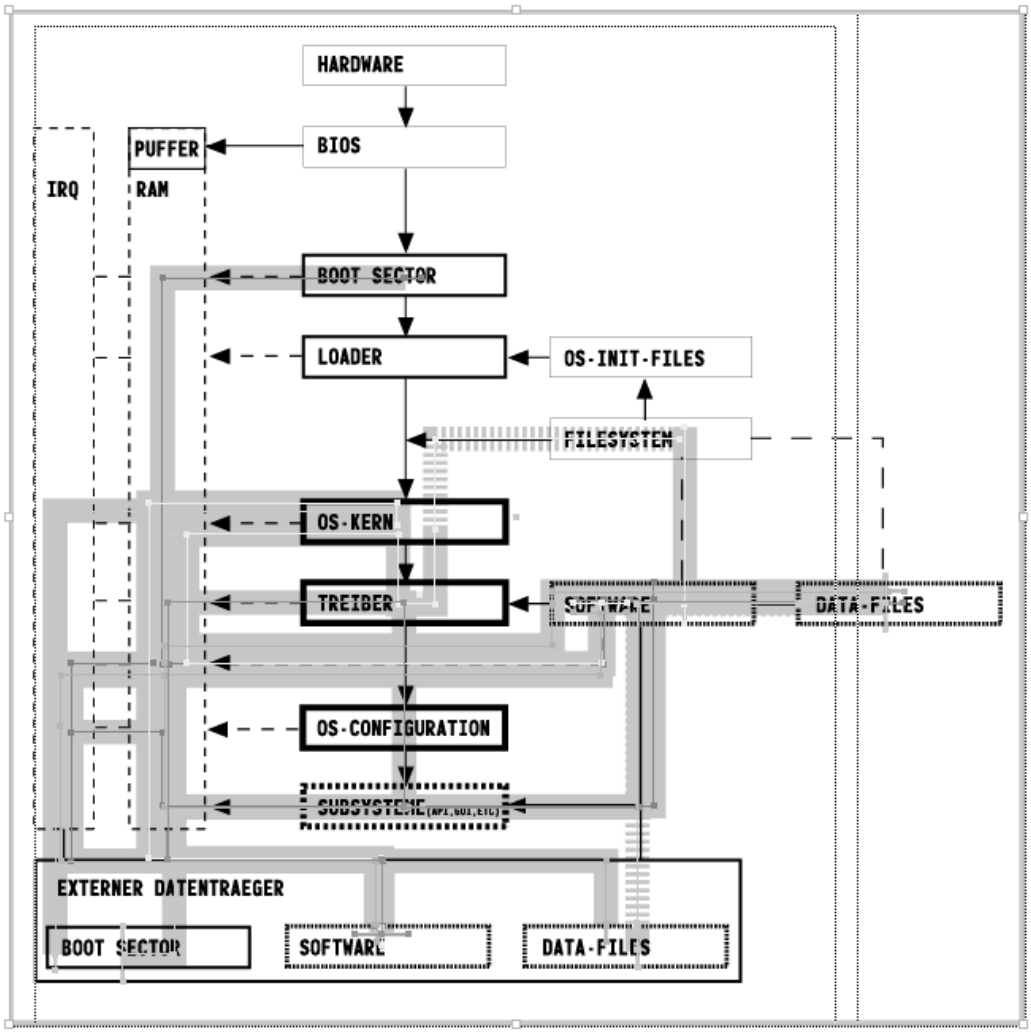
Studienbereich Neue Medien

30/03/02, Zürich

ÄQUIVALENZEN BIOLOGISCHER UND DIGITALER VIREN, DIE ENTWICKLUNG EINER VISUELLEN KLASSIFIZIERUNG DIGITALER VIREN UND THESEN FÜR EIN DIGITALES IMMUNSYSTEM



Äquivalenzen biologischer und digitaler Viren, die Entwicklung einer visuellen Klassifizierung digitaler Viren und Thesen für ein digitales Immunsystem

—— Ist es möglich, dass die Trennung zwischen biologischer und digitaler Welt verschwimmt? Was passiert, wenn sich digitale Viren auf den Menschen übertragen und wenn wir Menschen die Computer mit Grippe infizieren würden? Was können wir für die Entwicklung eines digitalen Abwehrsystems von unserem Immunsystem lernen? Sind biologische und digitale Viren überhaupt vergleichbar? Was sind ihre Ähnlichkeiten und wo liegen ihre Differenzen? Wie werden Viren visualisiert? Sind Viren klassifizierbar? Können sie in Kategorien unterteilt werden? Könnten allenfalls diese Kategorien visualisiert werden? Warum sollten sie und was würde das überhaupt nützen? Gibt es für biologische und digitale Viren womöglich die selben Kategorien?

Inhaltsverzeichnis

1___Einleitung - «Was will ich?»

—— Diese Arbeit baut auf der Annahme, dass sich Computer-Viren (digitale Viren) an ihren biologischen Namensvettern orientieren. Dies vor allem im Bezug auf ihr Vorgehen bei einer Infektion (Ansteckung), deren Ausbreitung und der Vermehrung der Viren selbst. Um diese Annahme zu prüfen, müssen als erstes Äquivalenzen und Analogien zwischen biologischen und digitalen Viren gefunden werden. Während der Analyse dieser Themengebiete habe ich herausgefunden, dass es bis heute keine Methode gibt, um digitale Viren zu visualisieren. Es fehlen sogar fundierte Kategorien, die eine Klassifizierung möglich machen würde. Dies ist wohl auf eine vernachlässigte Forschung zurückzuführen. Hier setze ich ein: Die Entwicklung einer visuellen Klassifizierung von digitalen Viren. Anhand dieser stelle ich Thesen für ein zukünftiges Anti-Viren-System auf, dass sich am Immunsystem des Menschen orientiert.---/

2___Der Begriff «Virus»

—— Der Begriff «Virus» kommt aus dem lateinischen und bedeutet «Gift« oder «giftiger Saft«. Schon der Begriff assoziiert also Gefahr und Schaden, was jedoch nicht immer zutreffen muss. In der biologischen wie auch digitalen Welt gibt es Viren, die keinen eigentlichen Schaden anrichten bzw. apathogen - nicht krankheitserregend sind..

—— Die Verwendung des Begriffs «Virus» im Zusammenhang mit Computern stammt entweder von Jürgen Kraus oder von Len Adleman. Kraus verfasste 1980 eine Diplomarbeit mit dem Titel «Selbstreproduktion bei Programmen», in welcher zum ersten Mal darauf hingewiesen wurde, dass sich Programme ähnlich wie biologische Viren verhalten können, indem sie sich selbst reproduzieren. Andere Quellen besagen, dass der Begriff «Virus» im Zusammenhang mit Computern erstmalig von Prof. Len Adleman genannt wurde, in einem Gespräch mit seinem Studenten Fred Cohen über selbstkopierende Programme.
—— 1984 veröffentlichte dieser Fred Cohen seine Arbeit mit dem Titel «Computer Viruses - Theory and Experiments« und ging damit erstmals auf die Gefahren ein, die Computer-Viren für Rechner darstellen können. Cohen definierte den Begriff Computer-Virus wie folgt:
«A ‘computer virus’ is a program that can ‘infect’ other programs by modifying them to include a possibly evolved version of itself.»
Diese Definition lässt die Schadensassoziation korrekterweise weg. Fred Cohen gilt als der Erfinder des Computer-Virus.---/

3___Grundlagen biologischer und digitaler Viren Eine Gegenüberstellung

3.1___DEFINITION

Biologisch

——— Biologische Viren sind «körperlos existierende Erbanlagen», können sich also nicht selber Vermehren. Sie bestehen aus nichts als aus einem Nukleinsäurestrang (DNS/RNS), der seine eigene Codierung enthält und den Bauplan der Hülle, in die er verpackt ist. Zu seiner eigenen Reproduktion benötigt das Virus einen Wirt, meistens eine Zelle.

——— Viren haben im Gegensatz zu Bakterien keinen eigenen Stoffwechsel, weshalb auch umstritten ist, ob sie überhaupt als Lebewesen/lebende Organismen bezeichnet werden können.

------- Viren bestehen aus einem Nukleotid, dem eigentlichen Kern mit der Erbinformation (DNS/RNS) des Virus, einer Kapsel, die Capsid genannt wird und einerseits zum Schutz, andererseits für die Anheftung an die Wirtszelle vorhanden ist. Der Nukleotid ist für die eigene Reproduktion innerhalb der Wirtszelle zuständig, während die Capsid den Antigenen Teil des Virus darstellt. Sie repräsentiert die Charakteristik des Virus, ihr Typ ist also virusspezifisch und gegen sie werden somit auch Antikörper gebildet.---/

Digital

——— Ein Computer-Virus ist ein sich selbst reproduzierendes Programm, wobei zur Reproduktion eine ausführbare Wirtsstruktur vorhanden sein muss.

DEFINITION NACH F. COHEN:

——— «Wir definieren ein Computer-Virus als ein Programm, das andere Programme durch Einbinden einer Kopie seiner selbst infizieren kann. Mit diesen Infektionen kann sich ein Virus in einem Computer oder einem Netzwerk unter Zuhilfenahme der üblichen Autorisierungen verbreiten. Jedes infizierte Programm kann sich ebenfalls wie ein Virus verhalten, wodurch sich die Infektion ausbreitet.»

——— Ein Computer-Virus besteht grundlegend aus drei Teilen: Dem Identifizierungsteil, dem Infektionsteil und der schlussendlich auszuführenden Aufgabe.---/

Abb. 3.1:
Beispiel biologischer Viren.

3.2___INFEKTION (ANSTECKUNG), VERMEHRUNG UND AUSBREITUNG VON VIREN

Biologisch

——— Wenn ein Virus eine Zelle infiziert, dann heftet sich dieses an die Wand der Zelle an, durchbohrt sie und entleert durch das entstandene Loch seine Nukelinsäure in die Zelle. Die eingedrungene Nukleinsäure wird daraufhin von der Zelle an die Stelle befördert, wohin Nukleinsäuren in einer ordentlich funktionierenden Zelle gehören: in den Zellkern. Ist die Virusnukleinsäure aber erst einmal dort angelangt, dann legt sie sich einfach an eine der zahlreichen Zellnukleinsäuren an, die hier das Steuerprogramm der Zelle bilden - mit der Folge, dass sich das ganze Zellprogramm schlagartig und folgenschwer ändert.

——— Eine Infektion ist also das Eindringen des Virus' in Zellen des Wirts, um sich dort, ungestört von möglichen Abwehrsystemen, so zu vermehren, dass die Weitergabe des Erbmaterials (DNA) hinreichend gesichert ist.

——— Infizierte Zellen kommen ihrer eigentlichen Aufgabe, z.b. der Produktion von bestimmten Eiweissstoffen, nicht mehr oder nur noch bedingt nach. Sie dienen als Brutkammer des Virus'.

Viren sind wählerisch, d.h. sie infizieren nicht einfach beliebige Zellen, sondern solche ihrer Charakteristik entsprechende: Grippeviren befallen Nase und Hals, während Hepatitis-Viren auf die Leber los gehen und AIDS-Viren sogar die eigentlichen Abwehrzellen angreifen.

——— Wenn viele gleichartige Zellen, die ein Organ bilden, befallen werden und deshalb wichtige Bau-/Nährstoffe nicht mehr ausreichend zur Verfügung gestellt werden, verendet der Wirt (Mensch, Tier etc.) an diesem Mangel.---/

Digital

—— Ein Computer-Virus nistet sich entweder in einer (ausführbaren) Datei ein bzw. kopiert sich in diese hinein oder versteckt sich sonst irgendwo auf der Festplatte (z.B. im Boot-Sektor). Beim Ausführen dieser infizierten Datei bzw. dem Laden des Boot-Sektors vermehrt sich das Virus indem es sich in weiteren Dateien/Sektoren einnistet.

—— Die Infektion ist das virusspezifische, die eigentliche Charakteristik eines Virus, anhand welcher sie auch Klassifiziert werden. Grundlegend lassen sie sich in die Kategorien
- Boot-Sektor-Viren und
- Datei-Viren
unterteilen, wobei sich Datei-Viren wiederum in Programm-Viren und Makro-Viren unterscheiden liessen. Im Grunde geht nur von ausführbaren Dateien (Programmen) eine Gefahr aus, allerdings besteht in der IT-Branche ein Trend, der auch Daten-Dateien immer mehr «Intelligenz» verleihen will, was dazu führt, dass auch in ihnen ein ausführbarer Teil vorhanden sein kann. Die Firma Microsoft erschuf mit der Makro-Technologie diese Möglichkeit: Eigentliche Daten-Dateien wie z.B. MS-Word-Dokumente sind somit beliebte Wirte von Viren.

—— Infizierte Dateien werden, je nach Art des Virus', entweder vollständig durch das Virus ersetzt und können so ihren eigentlichen Zweck nicht mehr erfüllen, oder das Virus nistet sich so in der Datei ein, dass diese bei einem Aufruf als erstes das Virus ausführt, dann aber der eigentlichen Aufgabe der Datei nachgeht.
Boot-Sektor-Viren schreiben sich, wie der Name sagt, in den Boot-Sektor eines Datenträgers. Dieser Sektor steht am Beginn eines Datenträgers und enthält den Loader, auch Boot-Programm genannt. Dieser dient dazu, dass das Betriebssystem geladen wird und verleiht dem Datenträger somit die Boot-Fähigkeit. Der Grund, weshalb sich ein Virus in den Boot-Sektor schreibt, liegt primär darin, dass es somit beim Booten als erstes in den Arbeitsspeicher (Hauptspeicher) geladen wird und auch dort bleibt. Es wird speicherresident. Dies eröffnet dem Virus ganz neue Möglichkeiten. Da es jetzt andauernd im Hauptspeicher präsent ist, hat es sozusagen die Kontrolle über den Rechner erlangt. Es ist ihm nun möglich zu jeder gewünschten Zeit zu agieren: Es kann weitere Dateien oder Datenträger infizieren und Systemaufrufe abfangen: Es könnte sich z.B. zwischen jeden Zugriff auf einen externen Datenträger schalten und sich gleich auf diesen Mitschreiben.--->

Diese Speicherresidenz kann übrigens auch durch ein Datei-Virus erlangt werden, allerdings ist dies auffälliger als bei einem Boot-Sektor-Virus.

——— Ein digitales Virus kann einen Computer zwar nicht töten, was aber nicht auf eine Unschädlichkeit oder Ungefährlichkeit digitaler Viren, sondern auf den Umstand, dass ein Computer nicht lebt, zurückzuführen ist. Denn, wenn ein digitales Virus elementare Teile eines Betriebssystems befällt oder alle Daten vernichtet, kann das auf abstrakter Ebene sehr wohl in die Nähe des Verenden eines lebenden Organismus gestellt werden. Würde ein digitales Virus die Möglichkeit haben, Teile der HW (z.B. einen Chip) zu infizieren, wären direkte Parallelen ohne weiteres denkbar.---/

4___Visuelle Klassifizierung digitaler Viren

------- Meine Recherche zum Thema «Virus» hat ergeben, dass es bis jetzt kaum eine Visualisierungsmöglichkeit digitaler Viren gibt. Jediglich Ablaufdiagramme oder Ausschnitte aus dem Quellcode bzw. den Binärdaten des Virus sind denkbar. In der Biologie werden Viren zwar abgebildet, jedoch lassen sich daraus keine Funktionsweisen oder Auswirkungen ableiten, erst recht nicht durch Laien.
—— Aus diesem Mangel heraus entwickle ich eine visuelle Klassifizierung digitaler Viren, die als Grundlage für Thesen dienen, wie nach dem biologischen Vorbild ein Immunsystem für den Computer zu entwickeln wäre. Visualisiert werden sollen primär der Verlauf einer Infektion. Die Visualisierung von Schäden oder Auswirkungen, die ein Virus hinterlassen kann, ist sekundär. Der Versuch der Infektion ist für das Immunsystem das Massgebende, da muss es intervenieren. Denn, wird das Virus erkannt, bevor es Wirte befallen hat, ist dessen Bekämpfung durch Anti-Viren-Programme am erfolgreichsten. Dies funktioniert analog zum biologischen Immunsystem: «Beste Wirksamkeit erreichen Antikörper, wenn die Giftstoffe noch frei im Blut schwimmend vernichtet werden. Haben sie sich schon auf den Zellen verankert, können Antikörper diese kaum noch ablösen und unschädlich machen.«

—— Für diese Visualisierung müssen die digitalen Viren als erstes in Kategorien unterteilt werden. Ich wollte mich dazu dem grundlegenden Aufbau eines Computersystems (Abb. 4.1/2/3) bedienen, musste aber bald feststellen, dass dieser den Anforderungen nicht genügt, da z.B. der Boot-Sektor in solch einem Modell nicht vorkommt. Deshalb nahm ich ein Diagramm zur Hilfe, dass den Ablauf eines Boot-Vorgangs aufzeigt (Abb. 4.4), wo z.B. der Boot-Sektor eine grosse Rolle spielt. Nun konnte ich anhand des Modells vom Aufbau eines Computersystems und dem Ablaufdiagramm des Boot-Vorgangs ein neues Schema (Abb. 4.5) erarbeiten, dass es erlaubt, die Infektion durch digitale Viren auf den einzelnen Komponenten eines Computersystems zu visualisieren. Dazu musste ich aus den bestehenden Modellen und Diagrammen (Abb. 4.1/2/3/4) diejenigen Ebenen extrahieren, die für eine Infektion in Frage kommen und miteinander in Relation setzen.---/

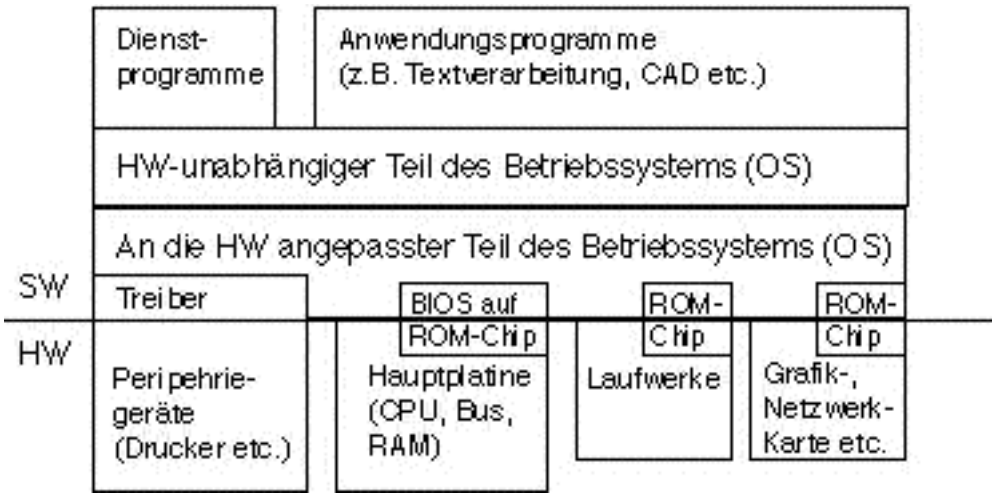


Abb. 4.2:
Detailliertere Aufstellung über das Zusammenwirken der verschiedenen Komponenten. Das Betriebssystem steht zwischen den Anwendungsprogrammen und der Hardware und stellt entsprechende Schnittstellen zwischen diesen Teilen zur Verfügung.

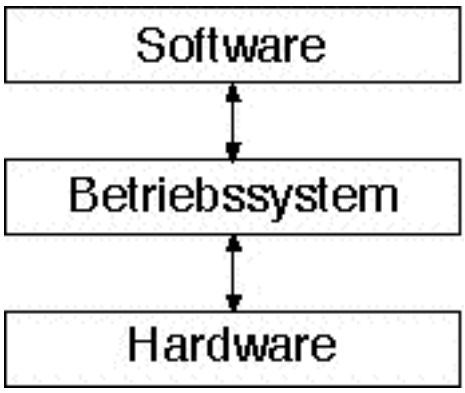


Abb. 4.1:
Grundlegender Aufbau eines Computersystems, der das Zusammenwirken von Hardware, Betriebssystem und Software aufzeigt. Das Betriebssystem bildet die Schnittstelle zwischen Software und Hardware.

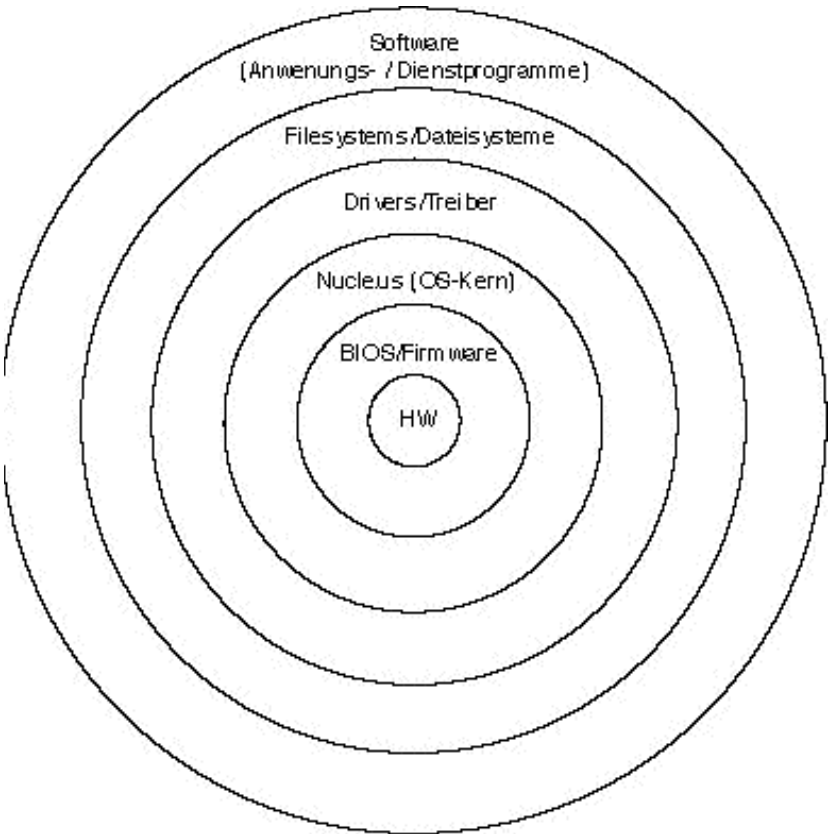


Abb. 4.3:
Schalenmodell eines Computersystems, das dessen Aufbau auf eine andere Art darstellt.Zusätzlich zum vorherigen Modell ist zu erkennen, dass das Betriebssystem auf einem Kernel (Nucleus) beruht und dass Dateisysteme nötig sind, um auf Daten zuzugreifen.

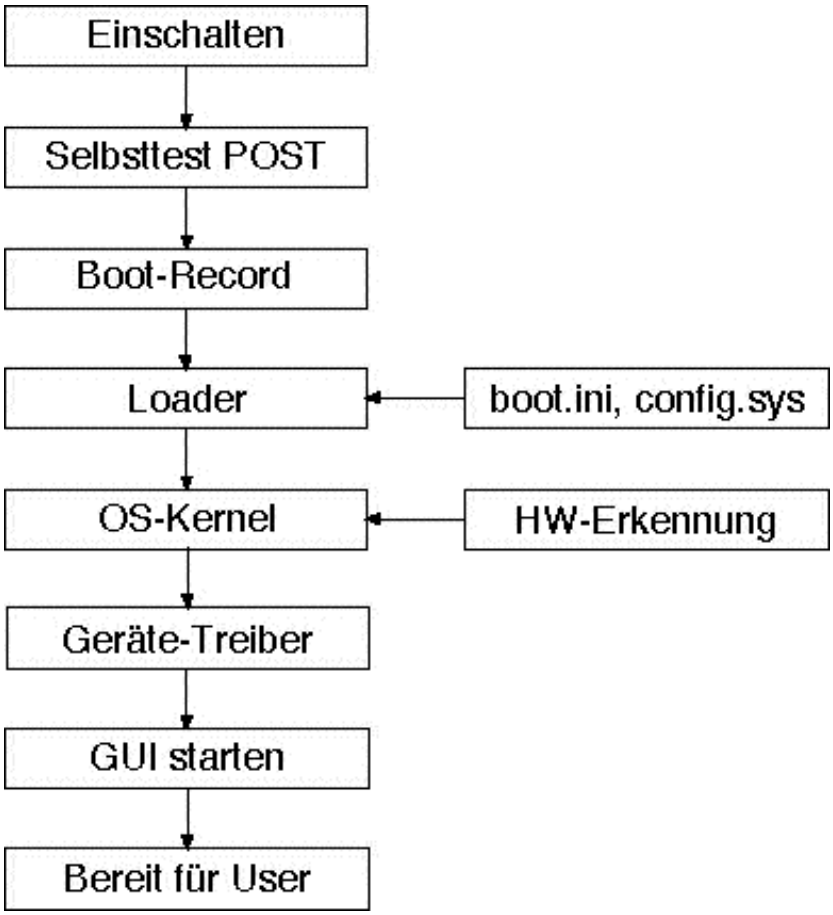


Abb. 4.4:
Der Boot-Prozess (Aufstarten des Computers):
1. Selbsttest (Power-On Self Test) testet die Hardware und zählt den Arbeitsspeicher.
2. Boot-Record wird durch BIOS-Funktionen aufgerufen. Falls vorhanden, wird der Loader ins RAM geladen.
3. Der Loader lädt Initialisierungs-Files, aufgrund derer z.B. das Dateisystem geladen wird. Nun kann der Kernel geladen werden.
4. Der Kernel stellt den Kern des Betriebssystems (OS) dar. Die HW-Erkennung identifiziert die installierten Geräte.
5. Nach dem Laden der Geräte-Treiber ist das OS in seinen Grundfunktionen bereit.
6. Aufgrund weiterer Konfigurations-Files können Subsysteme wie z.B. das GUI geladen werden.

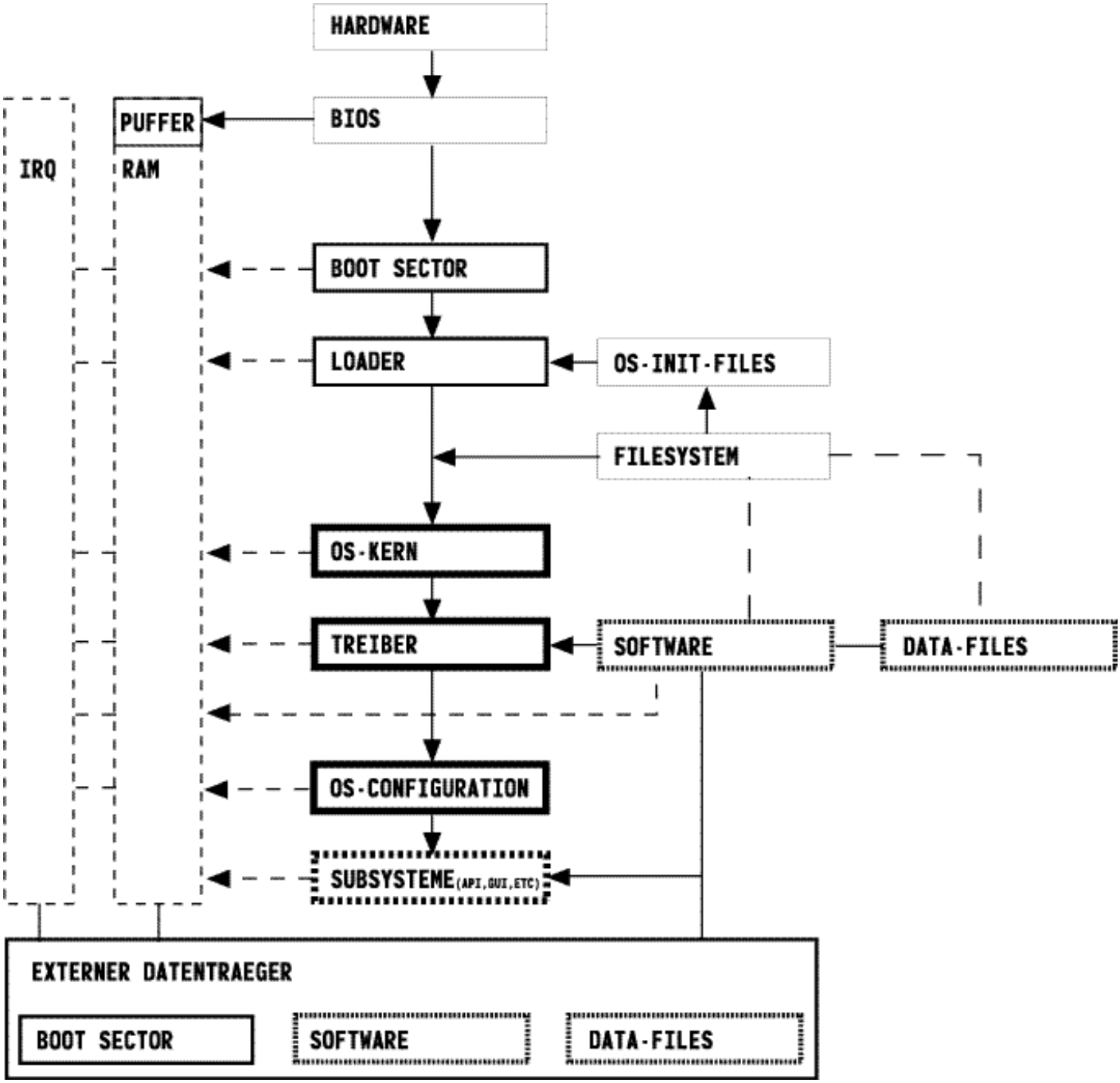


Abb. 4.5:
Schema zur visuellen Klassifizierung digitaler Viren

LEGENDE ZU ABBILDUNG 4.5

- RAM:
Arbeitsspeicher, in das sich der Virus neben dem Betriebssystem und anderer Software laden kann.

- RAM-Puffer:
Batteriegepufferter Speicher, in welchem Grundeinstellungen abgelegt werden, die auch beim Ausschalten des Computers nicht verloren gehen.

- IRQ:
Interrupt-Requests sind Signale, die von Hardware und Software-Komponenten benützt werden, um sich beim Prozessor zu melden und bestimmte Service-Routinen aufzurufen. Konkret heisst das, dass es ein speicherresidentes Virus z.B. jeden Zugriff auf die Floppy-Diskette oder jegliche Eingabe der Tastatur abfangen und beeinflussen kann.

- Hardware:
Die Hardware (Chips etc.) kann durch Viren-Programme nicht befallen werden, es wäre aber theoretisch möglich, dass in die Logik eines Chips auch gleich ein Virus miteingeschrieben würde. Dies setzt aber eine physische Manipulation am Computer-Gerät voraus.

- BIOS:
Das Basic Input Output System ist auf einem ROM-Chip gespeichert. Es wird zum Booten des Computers benötigt und bildet, wie der Name sagt, eine Schnittstelle zur Ein- und Ausgabe von Daten. Das BIOS kann nicht durch Viren infiziert werden (ausser HW-Viren, siehe «HW«).

- Boot Sector:
Erster Sektor auf einer Festplatte oder einem anderen boot-fähigen Datenträger, der auch als erstes ins RAM geladen wird. Enthält Adress-Informationen über den Speicherort der ersten Betriebssystem-Komponente und ev. auch Informationen über das Dateisystem. Der Boot-Sektor ist ein sehr beliebtes Ziel von Viren. Er lädt den Loader ins RAM.

- Loader:
Der Loader (auch Urlader oder Boot-Programm genannt) ist der erste Teil eines Betriebssystems und enthält bereits ausführbare Instruktionen. Er ist in der Lage, Initialisierungs-Dateien zu laden. Diese Dateien werden interpretiert und aufgrund dieser Informationen z.B. das Dateisystem/Filesystem geladen. Seine Aufgabe besteht --->

darin, weitere Komponenten des Betriebssystems auf dem Datenträger zu suchen, diese ins RAM zu laden und ihnen die Kontrolle zu übergeben. Falls ein Virus den Boot-Sektor infiziert, lädt es zuerst sich selbst und verweist erst dann auf den Loader.

- OS-Init-Files:
Vom Loader geladene Initialisierungs-Dateien, aufgrund derer z.B. das Dateisystem geladen wird.

- Filesystem:
Das Dateisystem definiert auf den Datenträgern (Speichermedien) Bereiche und Verwaltunsstrukturen, führt Dateinamen ein und Verzeichnisstrukturen ein. Das Dateisystem ist betriebssystemspezifisch. Unter DOS wird z.B. die FAT (File Allocation Table) am Beginn des Speichermediums abgelegt. Dabei handelt es sich um eine Art Inhaltsverzeichnis des Datenträgers. Es wird also für jeden Zugriff auf eine Datei benötigt.

- OS-Kern:
Kernel und weitere Kernkomponenten des Betriebssystems (OS), die nach dem Loader ins RAM geladen werden und für den Start des Computers notwendig sind. Da es sich beim Kernel und weiteren Systemkern-Komponenten oft um ausführbare Programme handelt, können sie natürlich unabsichtlich oder willentlich durch Viren befallen werden oder Ziel von Manipulationen werden.

- Treiber:
Die Geräte-Treiber sind für die Kommunikation zu Geräten (z.B. Peripherie wie Drucker etc.) zuständig und notwendig. Eine Infizierung kann Sinn machen, da die Treiber oft ständig im RAM resident sind und sie ev. auch zur Weiterverbreitung des Virus auf weitere Datenträger verwendet werden können. Dies würde aber eine ziemlich Treiber-spezifische Programmierung voraussetzen; eine Infizierung des entsprechenden Interrupts wäre da einfacher.

- OS-Configuration:
Weitere Konfigurations-Dateien, aufgrund derer die restlichen Subsysteme des Betriebssystems (OS) geladen werden: z.B. das GUI, die BenutzerInnen-Verwaltung oder Teile des API.

- Subsysteme (GUI, API etc.):
Restliche Subsysteme des Betriebssysteme (OS), die aufgrund der OS-Config-Files geladen werden: z.B. das GUI (Graphical User Interface bzw. grafische BenutzerInnen-Schnittstelle), die BenutzerInnen-Verwaltung oder Teile des API (Application Programers Interface; --->

eine Schnittstelle, die der SW und deren EntwicklerInnen Funktionen zur Verwendung des Systems zur Verfügung stellt). Eine Infizierung wäre auch hier schon alleine deshalb denkbar, weil es sich oft um ausführbare Komponenten handelt bzw. diese ins RAM geladen werden.

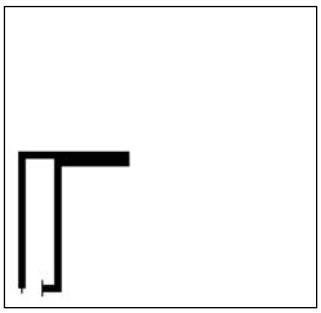
- Software:
Jegliche Anwendungs- und Dienstprogramme, die oft Ziel von Datei-Viren werden. Diese Software-Komponenten werden jedoch erst bei ihrem Aufruf durch den User ausgeführt bzw. ins RAM geladen.
All diese Dateien sind natürlich im Filesystem organisiert/abgelegt.

- Data-Files:
Dateien, die keinen ausführbaren Teil, sondern nur Daten enthalten, weshalb eine Infizierung zwar möglich, aber sinnlos ist. Ein Ausnahme bilden da Dateien mit Makros, welche durch die öffnende SW ausgeführt werden können.
All diese Dateien sind natürlich im Filesystem organisiert/abgelegt.

- Externer Datenträger:
Alle externen (beschreibbaren) Datenträger wie Floppy-Disk, ZIP etc. sind potentiell infizierbar und sehr oft Überträger von Viren. Gleich wie bei der Festplatte können Boot-Sektor, SW-Programm- und Daten-Files als Wirte dienen.

---/

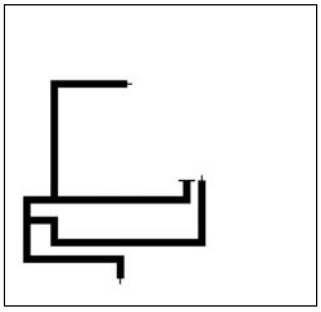
——— Es ist unleicht zu erkennen, dass das Schema aus Komponenten der vorhergehenden Modelle und Diagramme besteht. Der Boot-Prozess wurde durch den detaillierteren Aufbau eines Betriebssystems ergänzt. Was für das Aufzeigen einer Virus-Infektion sehr wichtig ist, bis jetzt aber in keiner der Abbildungen vorgekommen ist, ist der Arbeitsspeicher/das RAM, in welcher sich ein Virus oft lädt, um von dort aus Kontrolle über das ganze Betriebssystem ausüben zu können. Wie schon kurz angetönt, macht es diese Speicherresidenz dem Virus z.B. möglich, Systemaufrufe - sogenannte Interrupts - abzufangen und sich so u.a. zwischen jede Kommunikation mit Floppy-Diskette zu schalten. Deshalb muss das RAM auf dem Schema allgegenwärtig vorhanden sein und da die Interrupts ebenfalls zur Weiterverbreitung benützt werden können, müssen sie auch auf dem Modell vorhanden sind. ---/



5___Beispiele digitaler Viren und deren Visualisierung

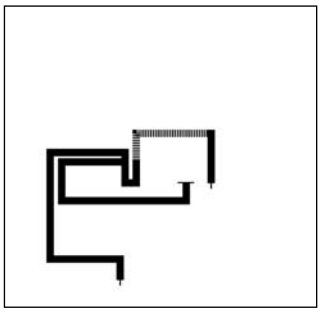
3APA3A:

Es handelt sich um ein speicherresidentes Virus. Es infiziert den Boot-Sektor der Floppy-Disk und das File io.sys auf dem Laufwerk C:\, womit es sich während dem Booten ins RAM lädt. Um die Floppy-Disk zu infizieren, wird der Interrupt 13H umgeleitet.



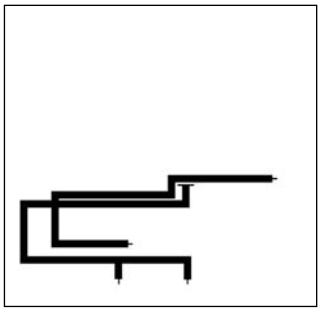
Arya.461:

Dies ist ebenfalls ein speicherresidentes Virus. Es infiziert den Master-Boot-Record der Festplatte, .com und .exe Programm-Dateien. Beim Ausführen einer infizierten Datei, wird der MBR infiziert und die Interrupts 13H und 21H umgeleitet, um beim Zugriff auf Floppy-Disks und durch das Abfangen von Dateisystem-Funktionen (Verzeichnis wechseln und Dateien löschen) weitere Programm-Dateien zu infizieren.



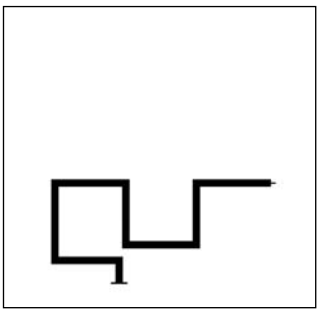
DirII:

Ein speicherresidentes Virus, dass z.B. beim Schreiben/Lesen von und Suchen nach Dateien weitere .com und .exe Programm-Dateien des aktuellen Verzeichnis' infiziert. Das Virus schreibt sich in den letzten Cluster der Festplatte und manipuliert die Programm-Dateien nur so, dass sie als erstes auf diesen Cluster springen und so das Virus ausführen.
Während der Initialisierung dringt das Virus in den DOS-Kernel ein und manipuliert die Adresse des System-Disk-Treibers, um jegliche DOS Aufrufe umzuleiten.



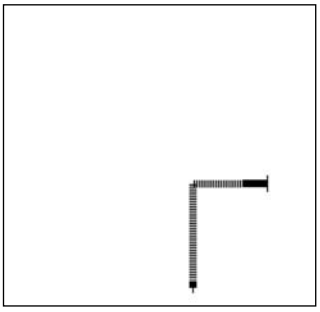
Frodo:

Ein speicherresidentes Virus, dass Dateien beim Ausführen oder Schliessen infiziert. Es ist auch möglich, dass Daten-Dateien infiziert werden. Das Virus fängt die Interrupts 13H und 21H ab und infiziert die Datei command.com.



Win95.Darkmil:

Beim Ausführen einer infizierten Datei prüft das Virus, ob das RAM schon infiziert ist. Falls nicht, kopiert es sich in einen Treiber und fängt gewisse Ein-/Ausgabe API-Funktionen ab, um sich jeweils auf weitere Dateien auszubreiten. Es werden .exe und .src, also Programm- und Quellcode-Dateien infiziert.



Macro.Word.Blash:

Es handelt sich hier um ein kleines Makro-Virus, dass sich beim Öffnen von anderen Word-Dateien weiterverbreitet.

——— Mit der Einführung dieser Zeichen für die Darstellung von Viren biete ich ein neues Vocabular zur Klassifizierung und Ordnung von Computerviren an. Ihre visuellen Charakteren werden von der Funktionsweise und Ausbreitungsstrategie eines Virus' innerhalb eines Computer-Systems abgeleitet. Mit dieser neuen Formgebung und Visualisierungsmethode ist eine schnelle Zuordnung, Neutralisierung und Isolation gewährleistet. Im Gegensatz zur Darstellung biologischer Viren, welche nur von einem/r Mediziner/in korrekt gelesen und gedeutet werden kann, macht das Modell als Schlüssel die Zeichen für jede Person sofort erfass- und lesbar.

——— Anbei finden Sie ein Test-Set, das Ihnen beim Erlernen des Vocabulars zur Klassifizierung und Einordnung von Viren behilflich ist.
——— Schnell sind durch visuelle Analogien Unterschiede auszumachen und Vergleiche zu ziehen. Jede Folie repräsentiert ein Virus.
——— Durch das Übereinanderlegen von Folie und Modell, sprich Virus und Computer erkennen Sie die verschiedenen Typen, Charakteren, Eigenschaften und Ausbreitungsstrategien digitaler Viren.

6___Thesen für ein digitales Immunsystem

—— Vor allem durch die Viren-Beispiele und deren Visualisierung wird ganz klar ersichtlich, dass digitale Viren praktisch auf allen Ebenen eines Computer-Systems und zu jeder Zeit zuschlagen können. Die HW-Komponenten sind durch die Schwierigkeit eines, für eine allfällige Infizierung notwendigen, physischen Zugangs am sichersten. Deshalb ist es auch logisch, dass HerstellerInnen von Anti-Viren-Systemen, Konzepte für ein auf Hardware basierender Schutz entwickeln, dessen Software nicht durch Viren angegriffen werden kann.

—— Für mich ist das nur der Beginn eines Ansatzes, der zu einem ernsthaften Schutz führen könnte. Was gebraucht wird, ist ein digitales Immunsystem!
—— Bei den jetzigen Anti-Viren-Programmen handelt es sich mehr oder weniger um Symptom-Bekämpfung, obwohl natürlich Teile davon weiterbenützt werden müssen. Das biologische bzw. menschliche Immunsystem als Vorbild; dies war schon die Idee verschiedener, schlussendlich eher erfolglosen Projekte. Meiner Meinung nach, weil sie zu technisch an das Problem herangegangen sind: es bringt kaum etwas, das biologische Immunsystem eins zu eins auf den Computer mappen zu wollen. Zuerst muss die dahinter stehende Idee analysiert werden, bevor Parallelen abgeleitet werden, die sich in ihrer Umsetzung vertechnisieren. Ein Beispiel dazu ist das Konzept der Anti-Körper: eine Software-Firma ist auf die Idee gekommen, viele kleine Prográmmchen auf einem Computer laufen zu lassen, die Ausschau nach einem Virus halten und diese dann irgendwie eliminieren. Naja, leider beschäftigten diese vielen Prozesse den Computer so sehr, dass er zu sonst nichts mehr zu gebrauchen war, was während einer Infektion ja noch verständlich wäre, aber sonst kaum.

—— Es braucht ein System, dass auf allen Ebenen agiert und sich an das grundlegende Konzept des biologischen Immunsystems anlehnt: die Unterscheidung zwischen «selbst» und «nicht-selbst». Zudem muss das Immunsystem integraler Bestandteil des Computer-Systems sein und nicht als Zusatzstück vertrieben werden. Es gehört vielmehr in den Aufbau eines Betriebssystem hinein, wenn nicht sogar zum Computer überhaupt. Denkbar wäre, dass ein Betriebssystem so aufgebaut wird, dass es ebenfalls zwischen «selbst» und «nicht-selbst» unterscheidet. Angedacht wird dies schon mit dem Berechtigungskonzept, wo die verschiedenen User unterschiedliche Rechte besitzen. Ich stelle mir das aber etwas konsequenter vor: auf erster Ebene muss natürlich schon bei der Installation bzw. beim Kopieren von Software eine --->

Sicherheitsüberprüfung stattfinden, aber viel wichtiger ist für mich die zweite Ebene; das Benützen von Ressourcen des Systems, vorwiegend von Prozessen. Jede Ausführung, sei sie noch so unscheinbar, benötigt den Prozessor - das Herz des Computers, weshalb es mir logisch erscheint, auch auf dieser Ebene aufzusetzen. Hier könnte ich mir den Einsatz von Antikörpern wiederum vorstellen: z.B. ein Chip, der mit Software zusammenarbeitet, um «fremde» Einheiten/Operationen zu erkennen. Es wäre auch möglich, dass sich jeder Prozess authentifizieren muss, wobei ich dies schon wieder als potentiell manipulierbar einstufen würde.

——— Die einzelnen Komponenten, Prozesse und Operationen müssten eine Art Erbmaterial in sich tragen, dass eine Codierung als «selbst» erlaubt. Diese Codierung muss vom Immunsystem bzw. von den einzelnen Objekten gegenseitig erkannt werden können. Eindringende Viren verfügen nicht über solch eine Codierung, da diese gerätespezifisch ist, können also als «fremd» erkannt und somit neutralisiert werden.
Die Frage läuft wie bei der Evolution darauf hinaus, wie das Innere schon infizierter Wirte kontrolliert und, wenn nötig zerstört wird. Die Evolution hat das so gelöst, dass der allgemeine Sensor auf der Zelloberfläche von Amöben (die Ur-Urahnen des menschlichen Immunsystems) sich immer spezifischer entwickeln musste, um nicht mehr nur das eine oder andere Virus als Solches zu erkennen, sondern um bestimmte fraktale Strukturen, also wenige molekulare Merkmale identifizieren zu können, die mit grosser Sicherheit auf ein Ganzes, eben auf das eine bestimmte, in der Zelle versteckte Virus schliessen lassen. Das Erkennungssignal «selbst» muss im Falle einer infizierten Zelle dem Signal «nicht-selbst», ausgelöst durch den spezifischen Sensor, der bestimmte fraktale Strukturen eines Virus auf der Zelloberfläche erkennt, untergeordnet werden. Durch diese Unterordnung des «selbst» gegenüber dem «nicht-selbst», wird die infizierte Zelle trotz ihrer «selbst»-Codierung gefressen. Allerdings findet dies zielorientiert statt, d.h. zugunsten des Überlebens einer nicht-virusinfizierten Art.
——— Dieses grundlegende Konzept ist es, dass ein digitales Immunsystem ermöglicht! Es braucht ein evolutionärer Schritt in der Entwicklung der Computer-Architektur, um dies zu vollziehen. Die Frage ist, ob den Menschen die Bedrohung durch Computer-Viren genügend gross erscheint, um diesen zu vollziehen, oder ob sie durch ein Umdenken auf den Schluss kommen, anders zu Handeln und ihr Verhältnis gegenüber dem Computer von Grund auf neu zu definieren.---/

Anhang

1___QUELLEN UND HILFSMATERIAL

Unterrichtsunterlagen «Informatik Grundlagen» der TBZ (technische Berufsschule Zürich)

Unterrichtsunterlagen «Computer-Viren/Datensicherheit» des SIB (Schweizerisches Institut für Betriebsökonomie)

«Das grosse Computer Lexikon 98», Data Becker

«Betriebssysteme. Grundlagen und Konzepte» von R. Brause

«Das Immunsystem des Menschen. Bindeglied zwischen Körper und Seele» von K. Zänker
---
Pschyrembel. Klinisches Wörterbuch

«Innere Medizin» von Mischo-Kelling und Zeidler

AVP Virus Encycloedia: www.avpp.ch/avpve/

Computer Virus Classification: www.avp.ch/avpve/classes/classes.stm
---
«Trickreiche Killer oder Hilfe mein Rechner ist krank! (Virus im Computer)» von R. Rick: www.rotary-es-filder.de/vortrag/word/980715VI.doc
---
BSI (Bundesamt für Sicherheit in der Informationstechnik) zu Viren: www.hu-berlin.de/bsi/viren/

Computerviren: www.ssaxer.ch/viren.html

Mr. Virus: www.mr-virus.cc

«Ein Immunsystem für den PC»: www.hrz.uni-dortmund.de/computerPostille/Maerz11996/einimmun.htm---/