PC-Viren- Epidemie oder Hirngespinst?

Autor(en): **Plozza, Stefan**

Objekttyp: **Article**

Zeitschrift: **Schweizer Ingenieur und Architekt**

Band (Jahr): **107 (1989)**

Heft 4

PDF erstellt am: **22.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-77035

PC-Viren - Epidemie oder Hirngespinst?

In jüngster Zeit traten auch in der Schweiz gehäuft Fälle von Personal-Computer-Ausfällen auf, hinter denen ein Virus oder ein «Trojanisches Pferd» vermutet wurde. An der HWV in Horw sollen laut einem Artikel im «Vaterland» vor einiger Zeit gleich mehrere PCs «ausgestiegen» sein, nachdem auf diesen Geräten ein Computerspiel gespielt wurde, das innert kürzester Zeit ganz Europa erobert hat: «Leisure Suit Larry». Es wird vermutet, dass auf einer bestimmten Kopie des «Larry» ein Virus installiert wurde, der sich nun mit jeder weiteren Kopie fortpflanzt. In vielen Unternehmen hat der «Larry» Einzug gehalten, und es gibt wohl nicht mehr viele PC-Benützer, die den liebenswürdigen - aber anscheinend gefährlichen - Schwerenöter nicht kennen.

VON STEFAN PLOZZA
BÜLACH

Von verschiedenen «Fachleuten» wurde die Existenz von PC-Viren noch vor kurzem einfach in Abrede gestellt. Die Machbarkeit von Viren ist jedoch unterdessen eindeutig erwiesen; damit ist aber auch das Gefahrenpotential ausserordentlich hoch und dürfte in nächster Zukunft weiter wachsen. Bekanntlich ist die Neugier ja eine der grössten Triebfedern menschlichen Tuns. Banaler ausgedrückt: Wenn Viren machbar sind, findet sich garantiert einer, der sie auch macht.

Reaktionen auf die Zeitungsberichte über PC-Viren sind andererseits auch in den Unternehmungen nicht ausgeblieben: In beinahe schon panisch anmutenden Weisungen werden Kopierverbote ausgesprochen. Verdächtigte PCs dürfen nicht mehr an Datenleitungen angehängt werden, und ihre Datenträger werden nicht etwa nur gelöscht, sondern gleich ausgewechselt. Das Thema «Virus» hat etwas Mystisches - man traut diesen Programmen beinahe überirdische Fähigkeiten zu.

Von beiderlei Reaktionen ist nicht viel zu halten. Die Augen vor dem Problemkreis zu verschliessen ist schlicht und einfach dumm, überrissene Angstreaktionen bringen Arbeitsbehinderungen und bewirken meist nicht einmal den erhofften Schutz. Der PC ist schliesslich ein Arbeitsinstrument, und wenn man die Arbeit damit derart erschwert, kann man geradesogut zu Papier und Bleistift zurückkehren (was, nebenbei gesagt, sowieso nicht immer das Dümmste wäre...). Vielmehr müsste man mit der Virengefahr zu leben versuchen. Dazu jedoch muss der Virus erst einmal auf den Boden der Realität geholt werden. Man kann sich beispielsweise fragen, ob wirklich bereits so viele Computerviren ihr Unwesen treiben, wie einem bisweilen vorgemacht wird. Sämtliche mir bekannten Fälle, bei denen eine Virentätigkeit vermutet wurde, könnten auch auf andere Weise ausgelöst worden sein. Merke:

Es ist nicht immer ein Virus daran schuld, wenn der PC nicht das tut, was man von ihm erwartet.

Was ist ein PC-Virus?

Ein Computervirus - der Name kommt nicht von ungefähr - ist ein Programm, das die Fähigkeit hat, sich in seinem Wirt (dem PC) mehr oder weniger unauffällig zu vermehren. Nach einer bestimmten Zeit wird es virulent und kann dann etwelchen Schaden anrichten, beispielsweise Dateien löschen, Daten verändern oder ganze Datenträger formatieren. Der Virus hat demnach folgende Funktionen:

Vermehrungsfunktion

Viren vermehren sich, indem sie sich selbständig in andere Programme weiterverpflanzen. Jedesmal wenn ein bereits infiziertes Programm gestartet wird, führt der Virus als erstes diese Funktion durch. Er sucht sich dafür vornehmlich Programme aus, die noch nicht infiziert sind.

Normalerweise findet diese Vermehrung immer innerhalb desselben Dateientyps statt: Ein Virus ist meist auf .COM- oder .EXE-Dateien spezialisiert. Primitive Viren überschreiben dabei einfach einmal den Beginn der Datei mit sich selbst. Wird das Programm später einmal aufgerufen, stürzt der Computer ab (nicht ohne dass sich der Virus zuerst noch rasch weiterverpflanzt hat). Geschickter programmierte Viren hängen sich deshalb vorne an das Programm an, so dass dieses vorerst funktionsfähig bleibt.

Prüfungsfunktion

Nach Durchführung der Vermehrungsfunktion wird ein Check durchgeführt, ob die Bedingung zum Ausführen der Manipulationsfunktion gegeben ist. Beispielsweise wird auf ein bestimmtes Datum geprüft, es kann aber auch ein Zähler durchlaufen werden, und nach einer bestimmten Anzahl erfolgt der Ausbruch. Solange die Prüfung negativ verläuft, gibt der Virus die Kontrolle an das Programm weiter. Ist das Resultat positiv, kommt es zum Ausführen der

Manipulationsfunktion

Was nun passiert, ist rein von den Fähigkeiten und dem Charakter des Virenprogrammierers abhängig: Am häufigsten dürfte dabei wohl das Formatieren sämtlicher angeschlossener Datenspeicher sein, allenfalls begleitet von einem mehr oder weniger intelligenten Spruch auf dem Bildschirm.

Bereits gibt es eine Gruppe von europäischen Viren-Fachleuten. Einer von ihnen, Ralf Burger, hat «Das grosse Computer-Viren Buch» geschrieben. Burgers Kontakte reichen vom Chaos-Computer-Club Hamburg bis zu Regierungsstellen in der BRD. Er befasst sich primär auf wissenschaftlicher Basis mit Computerviren. Die erste Hälfte seines Buches behandelt definitorische Fragen, die Geschichte der Viren und die Rechtslage. Im zweiten Teil ist dann für den PC-Freak mehr «Fleisch am Knochen»: Zum Beweis, dass PC-Viren machbar sind, hat doch Burger selber solche entwickelt. Es finden sich Listings harmloser Viren in verschiedenen Sprachen, Burger geht auf die verschiedenen Formen der Vermehrung und der Manipulation ein und kommt endlich auf Schutzstrategien zu sprechen. Um diese soll es im weiteren auch hier gehen.

Schutz gegen Viren

Voraus sei klar festgehalten:

Einen hundertprozentigen Schutz gegen Viren kann man nur mit Hardware erreichen, und zwar unter arbeitserschwerenden Bedingungen.

Jeder Software-Schutz dagegen kann, sofern er dem Virenprogrammierer bekannt ist, umgangen werden - eine Tatsache, derer sich die Software-Häuser unterdessen auf einem anderen Gebiet

bewusst geworden sind: Da jeder auf Software basierende Kopierschutz jeweils in kurzer Zeit «geknackt» wurde, verzichten viele Hersteller heute auf diesen und machen die Originalversionen ihrer Programme auf andere Art attraktiv. Trotzdem sind wir den Viren nicht wehrlos ausgeliefert. So klein er auch sein mag, jeder Virus hat eine bestimmte Grösse und hinterlässt Spuren. Auch muss er sich weiterverpflanzen. In diesem Augenblick der Aktivität kann man ihn «erwischen». Nicht alle Viren sind gleich geschickt programmiert, und man darf davon ausgehen, dass man mit einfachen Schutzmassnahmen einen grossen Teil der umlaufenden Viren abwehren kann.

Tips zu Diagnose und Schutz

Programme kontrollieren

Viren gehen in aller Regel auf Programme (Files des Typs .COM oder .EXE) los. Man kann deshalb regelmässig prüfen, ob sich diese verändert haben. Dies geschieht in einer ersten Stufe durch einen simplen Vergleich der File-Grösse und des Modifikationsdatums.

In einer zweiten, schon recht sicheren Stufe sollte man hie und da die Files mit denen auf der Originaldiskette auf den Inhalt hin vergleichen. Diese Diagnose ist recht sicher, aber zeitaufwendig. Vielleicht kauft man sich deshalb eine pfannenfertige

Viren-Diagnose-Software

Eine davon ist der «ARCUS Virus Detektor». [1] Ein «Labor-Exemplar» davon wurde an der SwissData vorgestellt, unterdessen ist das Programm im Handel. Dieses Programm legt eine Log-Datei mit den wesentlichen Parametern der .EXE- und .COM-Dateien an und vergleicht deren Einträge bei jedem Einschalten des PCs mit den aktuellen Werten. Bei Differenzen wird der Benutzer gewarnt. [2] Ein weiteres Programm ähnlicher Funktion ist «C-4» von Inter-Path. Es wird beim Starten des PCs geladen und verbleibt aktiv im Memory. Sobald aus einem Programm ein Zugriff auf ein .EXE- oder .COM-File oder auf den Boot-Sektor versucht wird, erscheint eine Warnung an den Benutzer, und C-4 stoppt die Aktion des «verdächtigen» Programms, bis der Benutzer sein Einverständnis zu ihrer Durchführung gibt. Beide Programme kosten zwischen Fr. 100.– und Fr. 200.– und sind reine Viren-Diagnosen. Was man bei Eintreten eines Virenbefalls tut, bleibt dem Benutzer überlassen.

«Steril» arbeiten

Die beste Prävention ist es natürlich, wenn der PC nur von einer Person benützt wird, die immer darauf achtet, nur virenfreie Software zu übernehmen. Dies gestaltet sich jedoch schon heute recht schwierig. Bei neuer Software, direkt aus der Originalverpakkung installiert, darf man zwar davon ausgehen, dass sie unverseucht ist. Absolute Sicherheit hat man aber auch dabei nicht, und – Hand aufs Herz! – welcher fröhliche PC-Benützer lässt es sich nehmen, hie und da ein interessantes Programm von einem Kollegen auszuprobieren?

Programme umbenennen

Ein gewisser Schutz kann dadurch erreicht werden, dass man die Extensionen der Files ändert, z.B. aus .EXE ein .XXX und aus .COM ein .CCC macht. Ein Virus, der sich nach der Extension richtet, findet dann keine Dateien, die er infizieren kann. Eine Gefahr ist damit allerdings verbunden: Manche Viren treten dann in das virulente Stadium ein, wenn sie sich nicht weiter verbreiten können: Ein solcher Virus begänne sein Zerstörungswerk deshalb sofort. Diese Lösung ist auch ein wenig unhandlich: Jedesmal, wenn ein Programm ausgeführt werden soll, muss seine Extension erst in die korrekte umgewandelt werden. Man kann sich dies natürlich mit Batch-Files automatisieren.

Schreibschutz verwenden

Ein beinahe selbstverständlicher Schutz: Alle Datenträger mit einem Schreibschutz versehen, bei Originalen – sofern es überhaupt eine Schreibkerbe gibt – noch vor dem ersten Einlesen.

Daten regelmässig sichern

Um einigermassen sicherzugehen, sollte man den gesamten Bestand des PC des öfteren auf andere Datenträger kopieren. Mit den heute üblichen «raschen» Sicherungsprogrammen und bei den gegenwärtigen Preisen für Disketten bedeutet es keinen grossen Aufwand, sich mehrere Sätze von Sicherungen anzulegen. Zwei Sätze von Disketten – abwechselnd eingesetzt – genügen. Daneben zahlt es sich unter Umständen aus, in grösseren Abständen auch eine bleibende Sicherung vorzunehmen, auf die im Notfall zurückgegriffen werden kann.

Tips für die Therapie

Was, wenn ein Virus einmal ausfindig gemacht wird oder gar in Aktion «erwischt» wird? Die folgenden zwölf Schritte sind dem Buch Burgers [3] entnommen:

☐ PC ausschalten (vom Netz trennen). Dies verhindert erst mal jede weitere virale Aktion.

☐ Allfällige Datenübertragungsleitungen abtrennen. Wir wollen ja nicht auch noch andere Benützer eines Netzes (mit)infizieren.

☐ Alle Datenträger mit Schreibschutz versehen.

☐ Das System mit eingelegter Originaldiskette des Betriebssystems aufstarten.

☐ Sämtliche Daten und Programme auf neue Datenträger kopieren und versiegeln.

☐ Alle alten Datenträger neu formatieren (wenn möglich mit einem Werkzeug, das auch das Formatieren des Boot-Sektors und der FAT-Area erlaubt).

☐ Nun kann das Betriebssystem und sämtliche Software von den Originaldisketten wieder installiert werden.

☐ Die gesicherten Daten (NUR Daten, keine Programme!) auf ihre Ordnungsmässigkeit überprüfen.

☐ Wenn Daten in Ordnung sind, können sie wieder auf den PC übertragen werden. Von ihnen geht keine Gefahr aus.

☐ Sollten sie nicht in Ordnung sein, eine ältere Sicherung zum Restaurieren verwenden.

☐ Einsenden der versiegelten Kopien an eine Forschungseinrichtung, die sich des Virenverdachts annehmen kann. (Burger selbst betreibt eine solche Stelle in Deutschland: Die Erste Viren-Sammelstelle Deutschlands EVISAD).

☐ Ab sofort nur noch mit einer Diagnose-Software arbeiten und das System genau kontrollieren.

Literatur

[1] «ARCUS Virus Detektor» von Satellite Logic, Von May-Str. 37, 3604 Thun

[2] «C-4» von InterPath erhältlich bei: Mega Shop BE und ZH

[3] *Ralf Burger:* Das grosse Computer-Viren Buch, Data Becker, 1988 Schutzprogramme

Adresse des Verfassers: *S. Plozza*, Hohfuristr. 18, 8180 Bülach.