VTC

UNI HAMBURG

OBERHESSISCHE PRESSE, Mo. 18.11.91

Wenn Virus „Flip“ das komplette Programm auf dem Schirm spiegelt

Hamburger Informatik-Professor sprach über Sicherheitsfragen bei Computern

Marburg. In Wissenschaft und Wirtschaft gibt's ein „großes Maß an Abhängigkeit“ von Informationssystemen.

von Petra Pechacek

Über Sicherheitsprobleme von Rechnern und Computernetzen, über Hackerangriffe und Computerviren sprach am Mittwoch Professor Klaus Brunnstein (Foto) vor 150 Zuhörern im Hörsaalgebäude der Philipps-Universität.

Computerviren, so der Informatik-Professor von der Universität Hamburg, sind vor allem wegen der Abhängigkeit von den Systemen gefährlich. Bei einem Einsatz von über 50 Millionen Computern in der Wirtschaft zum Beispiel müsse der „PC als Instrument der Wertschöpfung eines Unternehmens“ gesehen werden. Ein Ausfall der Systeme könne daher große wirtschaftliche Folgen für ein Unternehmen haben.

Ein Grund für den relativ einfachen Zugriff der sogenannten „Hacker“ auf Dateien sieht Brunnstein darin, daß die meisten Systeme beim Sicherheitsschutz zu niedrig eingestuft werden. Auch für Jugendliche sei es daher schon mit begrenzter Erfahrung möglich, in die Systeme einzubrechen.

Der Informatiker forderte daher eine Erweiterung des Sicherheitsbegriffs für wirtschaftliche und wissenschaftlich genutzte Dateien.

„Die glücklichsten Fälle sind die, bei denen Sie gleich sehen, daß da etwas nicht stimmt“, stellte der Professor anschließend die „normalen“ Computerviren vor: Der „Flip-Virus“ zum Beispiel spiegelt das gesamte Programm auf dem Bildschirm, ein anderer Virus läßt die Buchstaben aus dem Bildfeld purzeln.

Unter den rund 1 200 Viren unserer Datenbanken nannte der Hamburger Wissenschaftler noch die „Trojanischen Pferde“, nicht zu entdeckende Viren und die sogenannten „Würmer“, die durch das Absenden einer Information an verschiedene Adressaten eine Netzüberlastung erzeugen.

Der Gebrauch einfacher Passwörter wie Autokennzeichen, Geburtsdaten oder weiblicher Vornamen erleichtere es mittels eines kombinatorischen Verfahrens, in einen Rechner hineinzukommen. Unter Umständen kann das zu sehr hohen Schäden führen.

Ein Beispiel aus den USA bezifferte Brunnstein auf bis zu 80 Millionen Dollar.

Viele Computerviren werden durch Disketten eingeschleppt. Ein Absehen von der Benutzung geraubter Software reduziere deshalb das Risiko um einiges. Ebenso, riet der Professor, solle man sich nicht auf Antiviren verlassen, denn die hätten oft nicht die Fähigkeit, alle Viren richtig zu erkennen.

Man müsse, warnte der Referent aus Hamburg, immer damit rechnen, daß ein Ausfall oder Unfall passieren kann. Eine Arbeitsorganisation, bei der die Unfallfolgen sehr schnell behoben werden könnten, sei deshalb unbedingt erforderlich.

Brunnstein empfahl ebenso, eine schriftliche Fixierung wissenschaftlicher Ergebnisse nebenherlaufen zu lassen.

Der „Casino-Virus“, der mit dem Computerbenutzer eine Runde Jackpot spielt und nach dessen Niederlage die Dateien löscht, ist nur einer der 50 Viren, die pro Woche neu auftreten. Heute kenne man sogar schon einen Virus, der am 1. Januar 2000 in Aktion treten und die Inhaltsverzeichnisse der Systeme zerstören werde.

Im dramatischen Anstieg der Computerviren und den 15 bis 20 Millionen der in der Wissenschaft eingesetzten Computer, die lahmgelegt werden können, sieht Brunnstein eine „äußerst gravierende Schädigung der wissenschaftlichen Methoden“ begründet. Diese Tatsache erscheine umso bitterer, zumal sie durch üble, sinnlose „Scherze“ einzelner herbeigeführt werde.

HAMBURGER MORGENPOST
HEUTE MIT TV-BEILAGE
Freitag, 31. Jan. 1992 · 70 Pf · C 1986 A
Nr. 26/5 · Redaktion: (040) 88 303-0 · Anzeigen: (040) 88 303-336

„Michelangelo" – Gefahr für Hamburgs Computer

Firmen fürchten Millionenschäden: Viren sollen am 6. März zuschlagen

„Michelangelo" wartet auf den Befehl zum Angriff – und zwar in den Tiefen der Rechnersysteme. Denn hinter diesem Namen verbirgt sich nicht der berühmte italienische Künstler des 15. Jahrhunderts, sondern ein fieses Stück technischer Intelligenz, das gemeinhin als Computer-Virus bekannt ist. Und das hat die unliebsame Fähigkeit, die Innereien der Elektronik bis zur Unwirksamkeit durcheinanderzubringen. „Michelangelo" gehört dabei zu den gefährlichsten aller Viren – allein in Hamburg drohen Millionen-Schäden. Stichtag: 6. März.

„Dieses Virus breitet sich in einer unglaublichen Geschwindigkeit aus", sagt Computer-Experte Professor Klaus Brunnstein von der Universität Hamburg. „Michelangelo" ist so programmiert, daß er losschlägt, wenn das Systemdatum auf den 6. März umspringt – dem Tag, an dem im Jahre 1475 der echte Michelangelo geboren wurde.

Dann werden blitzschnell und willkürlich von dem Sabotage-Programm die Daten auf der Festplatte – dem Herzstück eines modernen Computers – mit nutzlosen Zeichen überschrieben. Amerikanische Experten fürchten, das weltweit hunderttausende Computer unter der Virus-Attacke durchdrehen. Vor allem solche, die nach dem Betriebssystem MS-DOS funktionieren, also „IBM-kompatibel" sind. Davon existieren in Hamburg Zehntausende.

Vor allem Firmen haben Schlimmes zu befürchten. Wenn einmal eine Festplatte infiziert ist, breitet sich das Virus auf jede Diskette aus, die im System benutzt wird. Möglicher Effekt: Bei Versicherungen werden die Verträge gelöscht, Abrechnungen verschwinden spurlos. Viele Schäden wären mit Geld kaum wett zu machen: Zum Beispiel, wenn der zehn Millionen Mark teure IBM-Rechner des Forschungszentrums DESY durchdreht.

Professor Brunnstein will bis zur zweiten Februar-Hälfte ein Programm von Gegenmaßnahmen vorstellen, daß den „Michelangelo" erkennen und beseitigen kann. Interessierte können es beim Viren-Test-Center der Hamburger Uni kostenlos anfordern. Denn das bloße Umstellen des Datumsanzeigers im Computer hilft nicht unbedingt. Brunnstein: „Es tauchen Viren-Varianten auf, bei denen das Datum der Zerstörung manipuliert wurde."

Auch bei IBM in Hamburg wird an Anti-Viren-Maßnahmen bearbeitet. „Michelangelo ist uns seit April 1991 bekannt. Es gibt schon Anti-Strategien", sagt Sprecher Kuno Brem. Wie wirksam die sind, bleibt geheim. „Das Ganze ist ein sehr heikles Thema." **Heiko Haupt**

2000 Viren-Arten Ende '92

Computerviren sind Programmteile, die sich eigenständig vermehren. Sie breiten sich über Disketten und die Verbindungen zwischen Rechnern aus, zerstören oder verändern Inhalte der Dateien. Oft werden so komplette Computer-Systeme lahmgelegt. Allein in Deutschland sollen sie bis heute Schäden von rund 200 Millionen Mark verursacht haben. 1989 zählte man noch zwölf Viren-Arten, Ende 1992 werden es 2000 sein. Mittlerweile wurden sogar in Anti-Viren-Programme die programmierten Schädlinge eingeschleust.

Computer

Erwachen am 6. März die Todesviren?

Von HANS ILGMOSER

Achtung, Computerbesitzer! Der 6. März könnte der Todestag für alle Programme auf Ihrem PC sein. Dann nämlich wird der gefährliche Computervirus „Michelangelo" (gen. nach dem italienischen Forscher, geb. 6. 3. 1475) aktiv, löscht wichtige Daten. „Kein Scherz", sagt Informatikprofessor Klaus Brunnstein (Uni Hamburg), „dieser Datenkiller-Virus breitet sich mit unheimlicher Geschwindigkeit aus, weil viele PC-Besitzer Programme kopieren."

„Gemeine Programmierer haben die Viren eingebaut, verkaufen die infizierten Disketten als Originalprogramme auf dem grauen Markt", weiß der Hamburger Computer-Experte Andreas Thater. „Tückisch: Die Viren schlafen oft monatelang, bis sie zu einem bestimmten Datum aufgeweckt werden" – am 6. 3.?

Hamburger Abendblatt Fr 31. 1. 1992

Warnung vor Michelangelo

Computer-Experte rechnet mit Virus

Eigentlich könnte es ein Freudentag sein: Am 6. März jährt sich der Geburtstag des berühmten italienischen Bildhauers, Malers und Architekten Michelangelo zum 517. Male. Doch die Besitzer der bundesweit 4,3 Millionen IBM-kompatiblen Personal-Computern werden an diesem Tag um ihre Daten bangen müssen: Der Hamburger Informatik-Professor Klaus Brunnstein warnt vor dem Virus-Programm „Michelangelo", das bei infizierten Computern am 6. März alle Daten löscht.

Mit dem Austausch von Programmen oder Daten über Disketten, andere Datenträger oder telefonische Datenleitungen verbreiten sich versteckte Virus-Programme, die von böswilligen Computer-Freaks entwickelt werden. „Michelangelo" versteckt sich in den Speichern der infizierten Computer und schlägt erst zu, wenn die interne Uhr des Rechners als Datum den 6. März angibt. „Dann löscht er den kompletten Datenträger und schreibt ihn mit Nullen voll", sagt Virus-Experte Brunnstein.

Einmal infizierte Computer kopieren das Virus auf jede Diskette, die mit ihnen verwendet wird und sorgen so für schnelle Ausbreitung. „Michelangelo" trat zum erstenmal im Februar vergangenen Jahres auf; er hat sich besonders schnell verbreitet. „Einige, auch namhafte Geräte- und Software-Hersteller haben das Virus unbeabsichtigt mit ihren Produkten an die Kunden weitergegeben", erklärt Professor Brunnstein, Leiter des Hamburger Viren-Test-Zentrums.

Normalerweise achten die Hersteller peinlich genau auf die Virenfreiheit ihrer Erzeugnisse. Rund 90 Prozent aller Viren, so Brunnstein, werden von ihren Erfindern in illegale Kopien von Programmen oder kostenlose „Public-Domain"-Software eingeschleust – besonders oft in Spiele.

Von den auf dem Markt erhältlichen Anti-Virus-Programmen können laut Professor Brunnstein zum Beispiel die Programme „Salomon" oder „Skulasson" das „Michelangelo"-Virus zuverlässig erkennen und vernichten. Das Hamburger Viren-Test-Zentrum bietet eine telefonische „Seelsorge" für die Virenbekämpfung unter der Nummer 54 71 54 05 an. Ein einfaches Kopieren der Daten auf Diskette kann zwar am 6. März vor dem Datenverlust schützen, doch das Virus wird mitkopiert.

Brunnstein warnt auch vor dem oft gegebenen Rat, den Computer am 6. März einfach nicht anzuschalten, damit das Virus nicht aktiv werden kann: „Für böswillige Computer-Kundige ist es ein Kinderspiel, das Virus vor der Weitergabe auf ein anderes Datum zu ändern – zum Beispiel auf den 5. oder 7. März."

THOMAS BORCHERT

...nautenges ▲ ...ock und Kragen aus ...plissierter ...erlone – auch von Paco Rabanne.

Schön und aggressiv: ein Kettenhemd. Damit's ▲ nicht drückt, sind die Plättchen aus federleichtem Plastik – eine Idee von Paco Rabanne.

BILD Freitag 31.1.92

Computer: Erwachen am 6. März die Todesviren?

Von HANS ILGMOSER

Achtung, Computerbesitzer! Der 6. März könnte der Todestag für alle Programme auf Ihrem PC sein. Dann nämlich wird der gefährliche Computervirus „Michelangelo" (gen. nach dem italienischen Forscher, geb. 6. 3. 1475) aktiv, löscht wichtige Daten. „Kein Scherz", sagt Informatikprofessor Klaus Brunnstein (Uni Hamburg), „dieser Datenkiller-Virus breitet sich mit unheimlicher Geschwindigkeit aus, weil viele PC-Besitzer gegenseitig Programme kopieren."

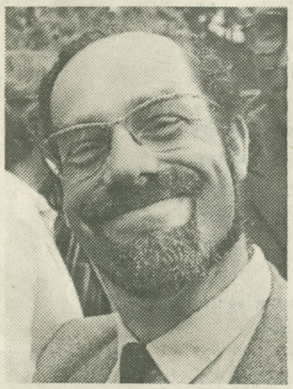
„Gemeine Programmierer haben die Viren eingebaut, verkaufen die infizierten Disketten als Originalprogramme auf dem grauen Markt", weiß der Hamburger Computer-Experte Andreas Thater. „Das Tückische daran: die Viren schlafen oft monatelang, bis sie zu einem bestimmten Datum aufgeweckt werden" – am 6. 3.?

Die Viren kommen

Immer mehr Miniprogramme befallen Computer und zerstören Daten

Am Sonntag sollte man nicht arbeiten - dieser Ansicht sind auch Computerviren. Wer sonntags seinen Rechner einschaltet, muß darauf gefaßt sein, daß auch der „Sunday"-Computervirus aktiv wird. „Warum arbeitest du am Sonntag?" flackert es dann spitzbübisch auf dem Bildschirm, ehe er dunkel wird.

Viren hängen sich an Nutzprogramme wie Textverarbeitungen und nötigen, plötzlich aus ihrem Versteck in fremden Programmen hervorspringend, den Computer zu selbstzerstörerischem Verhalten. Jüngstes Beispiel: der „Michelangelo"-Virus, der am 6. März, dem Geburtstag des Meisters, die Festplatte des Infizierten löscht. Die in den Computer eingebaute Uhr zeigt ihm, wann seine Stunde schlägt.



Den Viren auf der Spur: Prof. Klaus Brunnstein
Foto: Argus

Andere Viren zünden im Advent Kerzen auf dem Schirm an oder spielen gar zu Weihnachten Lieder. Doch die Dinger sind nicht so lustig, wie sie scheinen: in den meisten Fällen droht ein schmerzlicher Datenverlust.

Den Virus holt man sich unbemerkt. Beim Übertragen von Programm auf andere Rechner kommt er einfach mit. Hat man sie einmal, vermehren sie sich: Viren kopieren sich selbst immer wieder. Die Viecher verstecken sich mit Vorliebe in Programmen, also in Dateien mit den Namensendungen .EXE, .COM und .SYS. Wer nur Texte auf Disketten tauscht, braucht keine Ansteckungsgefahr zu fürchten - zwischen den Buchstaben wären die kleinen Killerprogramme leicht zu entdecken.

Virenepidemie

Gab es 1987 noch weniger als zehn Virenkarten, so sind heute über 1000 bekannt, die den gebräuchlichsten Computertyp, das MS-DOS-System, angreifen. Um ihre Funktionsweise zu erforschen und wirksame Suchprogramme zu entwickeln, die Viren bekämpfen können, gründete der Rechnersicherheitsexperte Klaus Brunnstein 1988 das Hamburger Viren-Testzentrum. Bis heute gibt es in Deutschland nur noch an den Unis in Karlsruhe und Rostock vergleichbare Einrichtungen. Die Privatwirtschaft hinkt der „Computerkrankheit" hinterher.

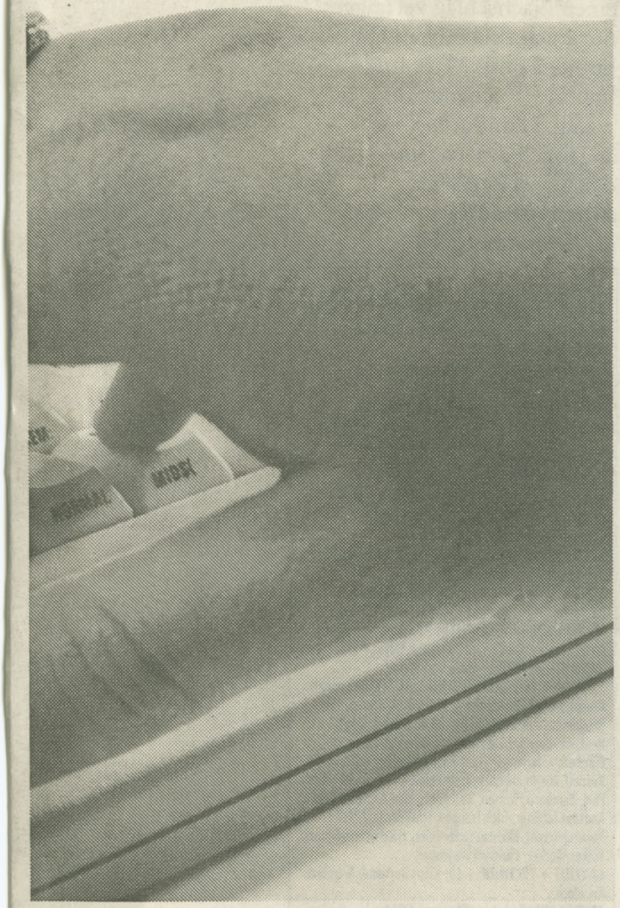
Ist der Rechner erst mal befallen, gibt das Viren-Testzentrum der Hamburger Uni kurzfristig Tips zur ersten Hilfe. Doch Vorsorge ist auch bei Computern besser: Brunnstein entwickelt Ideen für einen virensicheren Computerbau. In den trostloskahlen Räumen in Stellingen kommen jeden Dienstag 20 Informatikstudenten mit rauchenden Köpfen zusammen, die beim „Viren-Projekt" als Freiwillige vorgesprochen hatten. Während der gemeine Nutzer heimlich teure Textverarbeitungsprogramme tauscht, schieben die Mitarbeiter dieses Computer-Gesundheitsamtes mit feuchten Augen die neuesten Virendisketten hin und her.

Die Virenforscher provozieren, was einem vernünftigen Menschen nie einfiele: den Angriff der Viren. Gehen die fleischlosen Tierchen an die Arbeit, werden sie in flagranti erwischt. Das Problem ist, daß Virenprogramme meist unsichtbar sind und zunächst im „Wirtsprogramm" entdeckt und isoliert werden müssen, so daß man sie weiter untersuchen kann. Erlegte Viren werden in dem etwa alle fünf Monate erscheinenden „Viren-Katalog" des Zentrums beschrieben.

Datenkiller

Doch die Forscher sind in der Defensive. Dauert die Programmierung eines Virus zehn Stunden, so ist das Gegenprogramm manchmal erst nach Wochen gefunden. Die Übeltäter vermutet Brunnstein in großer Zahl in

Davon kriegt man's nicht ...
Foto: Fontaine



Bulgarien. Die Programmierer, die in dem armen Land für West-Softwarefirmen tippen, rächen sich mit der Programmierung der Krankheit für die Unterbezahlung. So kommt es vor, daß Viren schon in den Originalprogrammen stecken, die vom Hersteller selbst geliefert werden.

Ein anderer Ansteckungsherd sind PCs am Arbeitsplatz: Unbedarfte Mitarbeiter führen den Kollegen stolz ihr (unwissentlich) infiziertes Computerspiel vor. Einmal im System, breiten sich Viren rasend schnell aus. Brunnstein schwant daher schon eine „Entdemokratisierung der Rechnernutzung": Firmen würden bald nur noch Privilegierte an die Rechner lassen. Doch so bald wird die Flut von Anfragen verzweifelter Nutzer an ihn wohl kaum verebben. Neuester Clou: Viren, die ihr Aussehen dauernd verändern und so den Häschern mit ihren herkömmlichen Methoden regelmäßig durch die Lappen gehen. Simone Fischer-Hübner, Doktorandin zur Rechnersicherheit, befürchtet gar, daß die Zahl der Virenarten weiterhin exponentiell wachsen wird. Allerdings gibt es in der Szene auch viele Märchen: So, daß Computerviren auch für Haustiere gefährlich seien. Auch würde die „Israeli"- Virenfamilie keineswegs von mißgünstigen Palästinensern, sondern plietschen jüdischen Kids am Schulcomputer gebastelt....

Gregor Poniewasz

PC WOCHE, Mo 24.2.92

EXPERTEN SPRECHEN VON ERNSTER BEDROHUNG

Michelangelo-Virus auch in seriöse Software eingeschleust

MÜNCHEN (ch) — Wieder einmal versetzt ein Virus die PC-Szene in Aufregung: Michelangelo soll am 6. März seine destruktive Wirkung entfalten. Im Vergleich zu früheren Virenwarnungen, so versichern die Experten, sei dieses Mal die Gefahr wesentlich höher: Der Virus verbreite sich auch über fabrikneue Software.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) schätzt die Bedrohung immerhin so hoch ein, daß es über den „Kommunikationsplan Informationstechnik Sicherheit" (KITS) eine amtliche Warnung an Behörden und Wirtschaftsunternehmen herausgab. Auch das Microbit Virus Center der Universität Karlsruhe stimmt in die Kassandrarufe ein: Die Kombination von hoher Verbreitung und großem Zerstörungspotential des Virus sei alarmierend, erklärte Microbit-Direktor Christoph Fischer. Der Informatiker hat den Virus 1991 selbst „entdeckt". Der Virus, so Fischer, fragt das Systemdatum ab und entfaltet am Geburtstag des italienischen Renaissance-Malers Michelangelo seine Wirkung, indem er den Master Boot Record der Festplatte unbrauchbar macht und damit den Zugriff auf sämtliche Daten und Programme der Festplatte verhindert.

Die „Ansteckung" erfolgt durch Bootversuche von Disketten aus, die selber gar keine Programme, nicht einmal Daten zu enthalten brauchen — der Virus versteckt sich in dem für den Benutzer nicht unsichtbaren Bootsektor. Die Gefährlichkeit des Schadprogramms wird durch den ungewöhnlichen Umstand erhöht, daß es in Programmen seriöser Hersteller geortet wurde. Selbst große amerikanische PC-Vertreiber mußten in jüngster Zeit eingestehen, mit ihren Produkten auch den Bösewicht an die Kunden weitergegeben zu haben.

Siehe auch Seite 8

Keine Panik bei Anwendern

MÜNCHEN (sm) — Der Michelangelo-Virus ist derzeit in aller Munde. Die großen Unternehmen schützen sich meist nicht speziell vor dem Michelangelo-Virus, sondern setzen generell Sicherheitsprogramme ein.

Die Ost-West-Handelsbank AG in Frankfurt beispielsweise verläßt sich nicht nur auf ein einziges Virensuchprogramm. Denn „einen 100prozentigen Schutz vor Viren gibt es nicht", meint Markus Bingel, PC-Systembetreuer des Unternehmens. Neben dem TNT-Virusprogramm setzt das Bankhaus Netscan Virus V80 von Mc Afee ein. Außerdem wird auch täglich ein Backup angefertigt, über das anschließend der Virenscanner läuft. Auch dagegen, daß Michelangelo über neue Programme ins System gelangen könnte, baut Bingel vor: „Jede neue Software, auch wenn sie direkt vom Hersteller kommt, wird zuerst mit dem Virensuchprogramm gecheckt".

Ähnlich großgeschrieben ist das Thema Datensicherung bei den Mannheimer ÖVA-Versicherungen. Nicht nur zur Michelangelo-Zeit, sondern generell wird das Virenprogramm „Safeguard" von Uti-Maco in Oberursel eingesetzt. Selbst für die 320 im Außendienst verwendeten tragbaren PCs hat Peter Thunsdorff, Leiter der Abteilung Information bei der ÖVA, Vorsorge getroffen: „Wir lassen für die von uns an Außendienstler ausgehändigte Software Prüfzahlen errechnen, die bei jedem Start des Systems neu berechnet und verglichen werden", erklärt er. Der einzelne Mitarbeiter sei auch nicht in der Lage, eigene Software auf seinem Portablen zu installieren.

Der Kosmetikkonzern Beiersdorf verfügt über ein selbstentwickeltes Programm, das die Prüfsumme testet und so das Auftauchen von Viren entdeckt. Deshalb sehen die Verantwortlichen dem 6. März gelassen entgegen: „Wir lassen uns von der Hysterie, die von der Presse und von Antivirus-Softwareherstellern hochgepusht wird, nicht anstecken", beschwichtigt IDV-Leiter Clemens Keuer.

bitte umblättern.....)

PC WOCHE, Mo 24.2.92

VERBREITUNG ERFOLGT ÜBER LEGALE SOFTWARE

Der Michelangelo-Virus ist auch in Deutschland aktiv

MÜNCHEN (ch) — Wer seine Software legal beim Hersteller gekauft hat, konnte bisher davon ausgehen, daß sie auch frei von Viren ist. Diese Gewißheit scheint dahin: Mit Michelangelo hat sich erstmals ein Virus auf legalem Weg im großen Stil verbreitet. Am 6. März soll Michelangelo „zünden".

„Wir haben den Virus in einer VGA-Treibersoftware eines taiwanischen Herstellers entdeckt", sagt Werner Paul, Sachgebietsleiter Computerkriminalität beim Bayerischen Landeskriminalamt in München. Wie der Hersteller heißt, will er allerdings nicht verraten. „In Maustreibern ist er auch schon aufgetaucht", verrät der Kriminalist noch. Aber der Virus ist auch schon in anderen Produkten nachgewiesen worden, beispielsweise in Demo-Disketten für das E-Mail-programm von DaVinci Systems. Der amerikanische PC-Hersteller Leading Edge hat einem Bericht der Tageszeitung Houston Chronicle zufolge eingeräumt, Michelangelo unwissentlich in einer Auflage von mindestens 6000 Stück unters Volk gebracht zu haben — das Programm war bei der Auslieferung gleich auf der Festplatte installiert.

Michelangelo ist aber nicht nur ein amerikanisches Phänomen. Der Virus, dessen Ursprung in den Niederlanden oder Skandinavien vermutet wird, treibt auch hierzulande sein Unwesen. Wie der Virenjäger Klaus Brunnstein von der Universität Hamburg wissen ließ, sind mittlerweile allein auf seinem Schreibtisch rund 100 Fälle von Michelangelo-verseuchten PCs gelandet. Auch der Rat seines Kollegen Fischer aus Karlsruhe ist in letzter Zeit sehr gefragt: „Ich könnte einen wassergekühlten Telefonhörer brauchen", stöhnt der Virusexperte angesichts der Flut von Anfragen.

Die für den PC-User wohl wichtigste Frage dürfte vor diesem Hintergrund wohl lauten, welche Software denn nun von dem Virus betroffen sein könnte. Doch niemand aus der Riege der Virenbekämpfer möchte hier Roß und Reiter nennen. Immerhin war dem Guru zu entlocken, daß es sich mindestens im Fall einer verseuchten Maustreibersoftware nicht um einen taiwanischen, sondern um einen deutschen Hersteller gehandelt habe.

Die Offenlegung von Quellen sei auch gar nicht so sehr das Anliegen des Virus Test Centers, dessen Chef Brunnstein ist. Ihm geht es mehr um präventive Maßnahmen zur Gewährleistung der Sicherheit. „Die Qualitätskontrolle auf der Kopierstrecke, teilweise auch bei den ‚Golden Masters' ist nicht ausreichend. Die Weitergabe des Virus ist zum Teil über sehr namhafte PC-Händler erfolgt", moniert der Experte.

Dabei sei Michelangelo trotz allem noch relativ harmlos. „Wir untersuchen gerade einen Virus, der sich in vier Milliarden verschiedenen Variationen darstellt, da ist jeder Virenscanner machtlos", läßt Brunnstein den Anwender grausen. Michelangelo sei dagegen vergleichsweise einfach zu entdecken. Niemand solle aber auf die Idee kommen, mit einer einfachen Umstellung der Systemuhr auf ein anderes Datum wäre dem Problem beizukommen. Brunnstein: „Am 5. und 7. März zünden andere Viren."

Süddeutsche Zeitung, Do. 27.2.92

NACHGEFRAGT

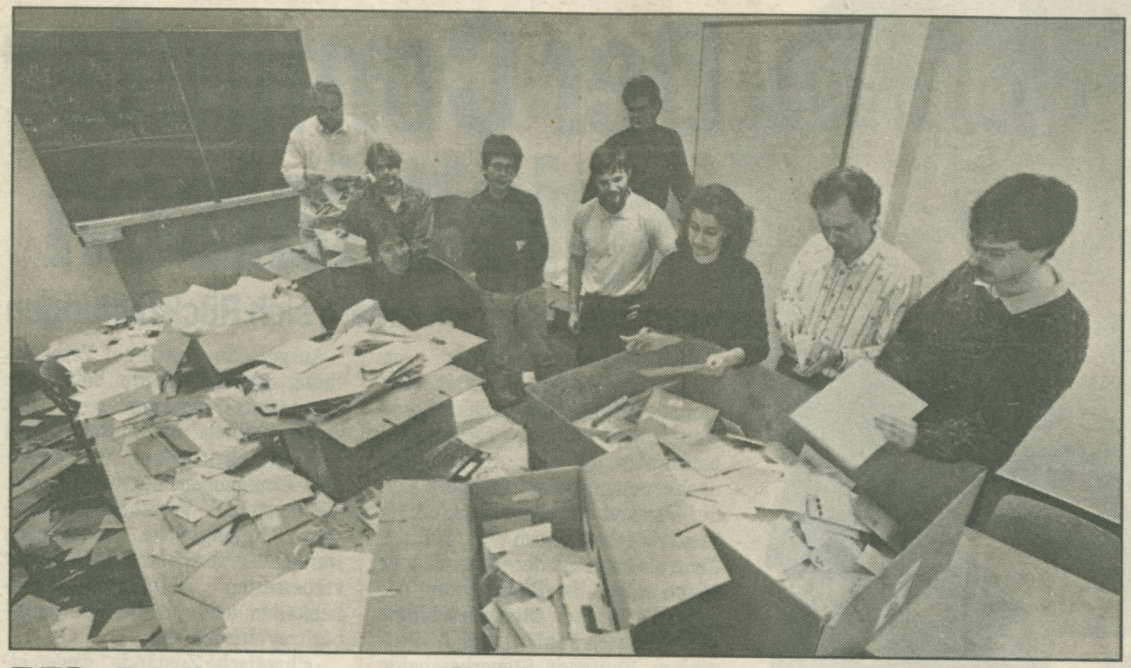
Gefahr durch „Michelangelo"?

Professor Dr. Klaus Brunnstein, Fachbereich Informatik, Universität Hamburg, über die Viren-Sicherheit von Personal-Computern (PC)

SZ: *Pünktlich am 6. März soll der Computervirus „Michelangelo" infizierte PC, die mit dem DOS-Betriebssystem arbeiten, attackieren. Jede Woche kommen zahlreiche neue Viren in Umlauf, ohne daß viel Aufhebens darum gemacht wird. Warum ist vor Michelangelo die Angst so groß?*
BRUNNSTEIN: Früher konnte man Viren weitgehend vermeiden, wenn man nur Software aus verläßlichen Quellen, also aus guten Softwarehäusern verwendete. Mit Michelangelo haben zum ersten Mal die seriösen Hersteller unwissentlich über ihre Produkte Viren an Kunden weitergegeben. PC-Händler haben diese dann mit Treibern von Zusatzgeräten wie Mäusen, Bildschirmen, Platten und Tastaturen in die PC hineinkonfiguriert, so daß bereits neu ausgelieferte PC mit dem Michelangelo-Virus verseucht sind. Deshalb halten wir die Warnung auch für relevant. Weil eben nicht durch no-name-Software-Produkte, etwa aus Taiwan, sondern durch ganz seriöse Fabrikate ein Virus verteilt wurde. Die Qualitätskontrolle, wir nennen das auch Virenfreiheitskontrolle, scheint nicht richtig zu funktionieren.
SZ: *Wie macht sich Michelangelo bemerkbar?*
BRUNNSTEIN: Am 6. März wird dieses Sabotage-Programm, wenn Sie Ihren Rechner gestartet haben, und das System infiziert ist, sofort damit beginnen, Ihre Festplatte - sofern Sie von der Platte geladen haben - zu zerstören. Gestern habe ich von jemandem gehört, der sich seine 80 Megabyte-Platte innerhalb von knapp einer Minute total mit dem Michelangelo-Virus kaputtgemacht hat. Der Virus ist bereits im April 1991 in Schweden und dann im Juni in Holland entdeckt worden.
SZ: *Wer ist durch Michelangelo denn besonders gefährdet?*
BRUNNSTEIN: Das geht querbeet durch die Anwendungen. Bei uns rufen Lehrer an, die sich neue PC oder auch neue Treiber gekauft haben und deren Disketten verseucht waren. Wir haben aber auch besorgte Anrufe aus Unternehmen der freien Wirtschaft.
SZ: *Wo wird Michelangelo aktiv werden?*
BRUNNSTEIN: Vermutlich wird er in Deutschland etwas weniger aktiv sein als beispielsweise in den USA. Das hängt auch damit zusammen, daß die Warnung vom Bundesamt für Sicherheit in der Informationstechnik in Bonn sehr früh herausgegeben wurde, so daß man Gegenmaßnahmen ergreifen kann. In Amerika ist die Warnung bislang über die Medien nicht so verbreitet worden.
SZ: *Kann man schon jetzt erkennen, ob man Michelangelo gespeichert hat?*
BRUNNSTEIN: Auf den verseuchten Disketten und Festplatten sind beispielsweise zwei Kilobyte mehr Speicherplatz besetzt als erwartet. Besser ist jedoch ein Antivirenprogramm. Im Handel werden verschiedene angeboten, die neben anderen Viren auch Michelangelo erkennen und bekämpfen. Außerdem wurde am Microbite Virus-Center der Universität Karlsruhe und auch an unserem Institut in Hamburg einen Antivirus erstellt.
SZ: *Wie kann man sich generell vor diesen Eindringlingen schützen?*
BRUNNSTEIN: PC sind grundsätzlich virenanfällig. Das liegt an der Technologie. Denn das System PC – also Personal Computer – kam 1981 als ein Gerät auf den Markt, mit dem man persönlich seine Daten und Aufzeichnungen bearbeiten kann. Das bedeutet, man ist für die Qualität und die Sicherheit der Programme und Daten persönlich verantwortlich – nicht der Hersteller muß sie schützen. Die Sicherheitsverfahren, wie wir sie in den Großrechnern haben, gibt es nicht beim PC. Der PC ist an sich ein unsicheres Gerät. Wenn ein Unternehmen also solche Apparate einsetzt, ist das mutig. Was man dort bräuchte, sind Computer mit eingebauten Schutzmechanismen. Leider haben die großen Firmen auf die Dezentralisierung mit PC gesetzt, weil die Rechenzentren absolut nicht in der Lage waren, die Benutzeranforderungen zu erfüllen.
SZ: *Wer steckt hinter Michelangelo?*
BRUNNSTEIN: Das wissen wir nicht. Bei Computersabotage dieser Art fehlen jegliche Spuren. Wir wissen auch nicht, ob das Motiv des Programmierers wirklich der Geburtstag des Michelangelo war, denn der Name ist dem Schädling von demjenigen gegeben worden, der ihn als erstes analysiert hat. Das ist wichtig, weil die Wahrscheinlichkeit besteht, daß sich das Datum, an dem er aktiv wird, verändert.
SZ: *Welche Absichten verfolgen die Leute, die Viren programmieren?*
BRUNNSTEIN: Das hängt sehr von der soziokulturellen Umgebung ab. Die gefährlichste Virenfabrik liegt in Bulgarien. Die Leute dort haben nicht unbedingt nach unseren Maßstäben kriminelle Absichten. Bei uns gilt – obwohl sich viele darüber hinweg setzen – die Verletzung des Copyrights von Software als ein Vergehen. Länder wie Bulgarien, Staaten in Asien und die ehemalige UdSSR kennen kein Copyright für Software. Sie haben auch keine Gesetze gegen Computerkriminalität. Ferner wird dort das Programmieren sehr schlecht bezahlt. Einige Viren sind durch Orginalsoftware aus Bulgarien eingeschleppt worden, weil sich die Programmierer für die schlechte Bezahlung rächen wollten.

Die Fragen stellte Angelika Jung-Hüttl

UMWELT · WISSENSCHAFT · TECHNIK
Redaktion:
Martin Urban (verantwortlich)
Lilo Berg, Dr. Jeanne Rubner



Viel Arbeit für die Virus-Experten (l.). Professor Brunnstein (u.) empfiehlt gegen „Michelangelo" Programme von John McAfee (SCAN und CLAEN ab Version 84) sowie von Fridrik Skulason (F-PROT) und Dr. Alan Solomon (Anti Viren Toolkit) in den Versionen ab Oktober 1991. Fotos: Wenzlawski

Michelangelo hält sie auf Trab

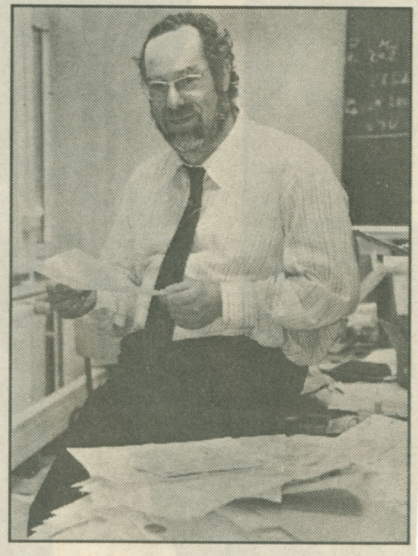
Schon 12 000 Anfragen an das Virus-Test-Center der Uni

Die Angst vor „Michelangelo" wächst: Am 6. März soll der Computervirus zuschlagen, wertvolle Daten der Rechner mit sinnlosen Zeichen überschreiben (MORGENPOST berichtete).

Seitdem das Virus-Test-Center der Hamburger Uni vor dem elektronischen Daten-Killer warnte, steht man dort vor einem kaum lösbaren Problem. Die Briefflut in Panik geratener Computer-Nutzer reißt nicht mehr ab.

„In den vergangenen beiden Tagen haben uns 35 Postsäcke voll mit Anfragen erreicht", sagt Professor Klaus Brunnstein, Leiter des Centers. Nie hätten die Viren-Experten mit einer derartigen Resonanz gerechnet, als sie ein Programm anboten, daß „Michelangelo" erkennen kann. Rund 12 000 Computer-Nutzer haben das bis auf einen Freiumschlag und eine Diskette kostenlose Hilfswerk bisher angefordert.

Hilfe kommt jetzt aus München: Weil die Bearbeitung aller Briefe bis zum Tag X für die Hamburger unmöglich ist, hat sich der Computer-Hersteller Siemens-Nixdorf bereit erklärt, das Virus-Center bei der Bewältigung der Briefflut zu unterstützen. **hh**



Die Welt, Do. 27.2.92

DIE WELT – Nr. 49
Donnerstag, 27. Februar 1992

S. 27

„Michelangelo" löst eine Lawine aus

Nach der Warnung vor dem gefährlichen Computer-Virus „Michelangelo", die gestern auch in der WELT veröffentlicht wurde, brach über den Fachbereich Informatik an der Hamburger Universität eine gewaltige Briefflut herein: „In den vergangenen beiden Tagen haben uns 35 Postsäcke voll mit Anfragen erreicht", sagt Prof. Klaus Brunnstein. Und keiner weiß, ob nicht noch viel mehr kommen werden.

Rund 12 000 Computer-Anwender sind bisher auf das Angebot der Hamburger Viren-Experten eingegangen, ihnen ein Viren-Erkennungsprogramm zu senden, wenn sie einen Freiumschlag mit einer Diskette an die Universität schicken.

„Meine Studenten und Mitarbeiter arbeiten pausenlos, um die Programme zu versenden. Wir sind eigentlich für solche Massen technisch gar nicht ausgerüstet", erklärt Brunnstein. Das Rechenzentrum habe zwei zusätzliche PC bereitgestellt, um den Postberg zu bearbeiten. Rettung kam jetzt aus München: Um den Fachbereich zu entlasten und den Postberg zu bewältigen, hat sich der Computer-Hersteller Siemens-Nixdorf bereit erklärt, einen Großteil der Anfragen zu übernehmen und zu bearbeiten.

„Michelangelo", der Daten auf Disketten und Festplatten zerstört und schon über hundert Fälle von schwerwiegenden Infektionen ausgelöst hat, wird am 6. März aktiv. Er trägt deshalb den Namen des italienischen Renaissance-Künstlers, der an diesem Tag Geburtstag hat. Während die meisten Computer-Viren durch Raubkopien auf Disketten von Rechner zu Rechner übertragen werden, soll „Michelangelo" von Computer und Software-Herstellern verbreitet worden sein, speziell durch Computer-Mäuse aus Asien.

Professor Brunnstein empfiehlt den Computer-Anwendern, sich mit Hilfe professioneller Anti-Viren-Software vor dem „Michelangelo"-Virus und anderen Computer-Viren zu schützen. Zuverlässig seien die Programme von John McAfee (SCAN und CLAEN ab Version 84) sowie von Fridrik Skulason (F-PROT) und Alan Solomon (Anti Viren Toolkit) in den Versionen ab Oktober vergangenen Jahres.

Computeranwender können sich auch an die Karlsruher Firma BFK (Humboldtstraße 35, 7500 Karlsruhe) wenden. Dort bekommt man gegen fünf Mark in Briefmarken ein „Anti-Michelangelo-Programm". Die Düsseldorfer Firma Hoffmann Datenschutz bietet gegen Einsendung einer Leerdiskette und eines Freiumschlags kostenlos ein Programm, das nach Angaben der Firma den „Michelangelo" bekämpft. lno

BILD, Do. 27.2.92

Impfung schützt vor Computer-Virus

Der Fachbereich Informatik der Hamburger Universität steht vor einem Chaos: In den vergangenen Tagen gingen dort 35 Postsäcke ein. „Alles Anfragen zum Computer-Virus ‚Michelangelo'", sagt der Hamburger Computer-Spezialist Professor Klaus Brunnstein. Der Virus wird am 6. März sämtliche Daten auf Disketten und Festplatten zerstören. Rund 12 000 Computer-Anwender haben sich von Brunnstein bereits ein Viren-Erkennungsprogramm zusenden lassen (per Diskette und Freiumschlag). Ein Anti-Viren-Programm wie das von John McAfee (Scan und Claen Version ab 84) schützt vor den gefährlichen Computer-Viren. bim

U N I V E R S I T Ä T   H A M B U R G

Fachbereich Informatik
Arbeitsbereich AGN
Virus Test Center
Telefon: 040 / 54715-234
040 / 54715-235
Telefax: 040 / 54715-226

Universität Hamburg - FBI / VTC
Vogt-Kölln-Str. 30, 2000 Hamburg 54

Pressemitteilung 28.02.1992

"Michelangelo"

0. Allgemeines

Das Virus Test Center der Universität Hamburg unter Leitung von Prof. Dr. Klaus Brunnstein beschäftigt sich seit seiner Gründung im Jahre 1988 mit den Themenkreisen Computer-Sicherheit, Datenschutz und Aufklärung von Computer-Unfällen.

Neben der Entwicklung von Techniken zur Erkennung und Bekämpfung von "bösartiger Software" werden die in diesem Themenbereich anfallenden Informationen gesammelt, ausgewertet und veröffentlicht.

!!!
Aufgrund der Flut von Anfragen (auch über Telefon und FAX) bitten wir alle Vertreter der Medien, auf eine Veröffentlichung unserer Anschrift sowie unserer Telefon- und Faxnummern zu verzichten.
Das VTC richtet demnächst eine VIRUS-HOTLINE und -BERATUNG ein.
Die Telefon-Nummern hierfür werden baldmöglichst bekanntgegeben.
!!!

1. Was ist "Michelangelo"?

"Michelangelo" ist ein Computervirus, der sich im BOOT-Sektor von Festplatten und Disketten festsetzt.

BETROFFEN SIND AUSSCHLIESSLICH RECHNER, DIE MIT DEM BETRIEBSSYSTEM DOS (MS-DOS oder DR-DOS UND EMULATIONEN) ARBEITEN.

Der Virus wird bei jedem Rechnerstart resident (im Hauptspeicher abgelegt) - von dort aus verbreitet er sich bei jedem Diskettenzugriff auf die gerade eingelegte Diskette, sofern diese nicht schreibgeschützt ist.

Dieser Verbreitungszyklus schlägt bei Erreichen des Systemdatums "06.03.xxxx" in eine zerstörerische Phase um: das Medium (Festplatte oder Diskette), von dem geBOOTet (gestartet) wurde, wird überschrieben.

Ist dies geschehen, sind die auf dem Medium gespeicherten Daten in den meisten Fällen unrettbar verloren. Nur ein Backup kann hier (relativ) schnell helfen. Die in einigen Ausnahmefällen mögliche teilweise Datenrettung ohne Backup ist sehr aufwendig und extrem kostenintensiv.
Privatanwender dürften diese Ausgaben nicht tragen können.

"Michelangelo" stellt deshalb eine große Gefahr dar, weil der Virus - entgegen der bisher bekannten Verbreitungskanäle - auch mit professioneller Originalsoftware weitergegeben wurde.
Das VTC verweist in diesem Zusammenhang auch auf das von Prof. Dr. Klaus Brunnstein herausgegebene Virus-Telex März 1992.

2. Welche Folgen hatte die "Michelangelo-Kampagne"?

Das VTC erhielt innerhalb einer Woche ca. 14.000 Anfragen (Schätzung) mit der Bitte um Zusendung eines Antivirus gegen "Michelangelo".

Die Bearbeitung dieser Postmengen wurde von durchschnittlich fünfzehn Studenten, drei Wissenschaftlichen Mitarbeitern und unserer völlig gestreßten Sekretärin übernommen.

Ein Teil der seit Donnerstag, 27.02.1992 eingehenden Post wird zur Entlastung des Arbeitsbereiches durch die Firma Siemens-Nixdorf, München weiterverarbeitet.

3. Hilfen gegen "Michelangelo"

"Michelangelo" wird durch die folgenden Antivirus-Programme erkannt und beseitigt:

Scan/Clean, Mc Affee	(ab Version V84) (neuester Stand: V87)
Dr. Solomons Antivirus Toolkit	(ab Version 10/91)
F-PROT von Fridik Skulason	(ab Version 2.00)

Computeranwender, die mindestens eines dieser Programme einsetzen, benötigen das vom VTC entwickelte Programm NTIMICH nicht !!!

Das Programm F-PROT (entwickelt von Fridrik Skulason) ist als Shareware-Version erhältlich.

Als Alternative bieten die Verbraucherzentralen gegen eine Schutzgebühr von DM 2,-- einen Antivirus an (Sendung "WiSo" vom 27.02.1992).

Das vom VTC (Morton Swimmer) entwickelte Programm stellt nur eine "Notlösung" dar: es erkennt ausschließlich "Michelangelo", während die übrigen obengenannten Programme auch weitere nicht weniger gefährliche Viren entlarven können.

Der von Christoph Fischer (Microbit Virus Center, Uni Karlsruhe) entwickelte Scanner erkennt und beseitigt ebenfalls "Michelangelo", erkennt darüberhinaus auch mögliche, bisher nicht aufgetretene Varianten (CLONES) mit verändertem Auslösedatum.

Computernutzer, die das vom VTC entwickelte NTIMICH trotzdem benötigen, können es voraussichtlich ab Samstag, 29.02.1992 über BTX als Telesoftware "downloaden". Wählen Sie hierzu bitte im BTX-System *55155# oder *RTL#.

4. Weitere Gefahren

Mit Ablauf des 6. März 1992 sind keineswegs alle Gefahren überstanden. Die nächsten gefährlichen Daten folgen unmittelbar: wie im von Morton Swimmer entwickelten Virenkalender nachzulesen ist, werden am Donnerstag, 12. März 1992 (Thursday 12 th) sowie am

FREITAG, 13. März 1992

(mehrere Jerusalem- / Israeli-Viren) weitere Schwerpunkte im Bereich der Virenangriffe zu erwarten sein.

Die derzeit auf dem Markt verfügbaren Viren-Scanner stellen im Hinblick auf kommende Entwicklungen im Bereich der Viren-Angriffe in absehbarer Zeit keinen wirkungsvollen Schutz mehr dar, da bereits die ersten "mutierenden" polymorphen Viren aufgetreten sind.

Kennzeichen dieser neuen Tarnung ist, daß durch wechselnde Erscheinungsformen der Viren (im Gespräch sind ca. 4 Milliarden Formen je Virus) die jetzt übliche Virensuche durch Mustervergleich unmöglich wird.

Das VTC kann zur Zeit gegen diese neue Art von Viren nur die Überprüfung von Dateien durch Ermittlung von Prüfsummen empfehlen.

5. Das VTC in Zukunft

Das VTC wird auf der CeBIT 1992 in Hannover nach 1991 zum zweiten Mal als "Virus-Notdienst" vertreten sein - an dieser Stelle ein Dank an die Deutsche Messe AG, die die Teilnahme an der CeBIT ermöglicht hat.

Auf dem Stand des VTC wird die Wirkung von Viren anhand einiger Beispiele demonstriert werden. Darüberhinaus werden Messebesucher Gelegenheit zu Gesprächen mit Mitgliedern des VTC haben - bitte haben Sie jedoch dafür Verständnis, daß nur in besonderen Notfällen komplette Lösungen vom VTC erstellt werden können.

6. Last but not least...

Sie werden nach Abschluß dieser Veranstaltung jeweils eine Diskette mit den Antivirus-Programmen NTIMICH (Uni HH, M. Swimmer) und F-PROT (F. Skulason) erhalten.

F-PROT ist Shareware, NTIMICH unterliegt dem Copyright von M. Swimmer. Sie dürfen

(nur kostenlos)

weitergegeben werden.

Desweiteren enthalten die Disketten einen Auszug aus dem aktuellen Virus-Katalog, um Ihnen einen kleinen Überblick über die dokumentierten Virus-Typen zu ermöglichen.

Wir, das Team vom VTC, danken für die Unterstützung durch die Medien und die Sponsoren.

Hamburg, 28. Februar 1992

Krieg im Computer:

Hamburger Morgenpost, Sa. 29.2.92

Der Generalangriff auf Michelangelo

In sieben Tagen ist es soweit: „Virus" wird aktiv Uni und Verbraucherzentrale bieten Gegenmittel an

Hamburg – Um den echten reißen sich die Kunstliebhaber in aller Welt, doch diesen Michelangelo will wirklich niemand haben: Der Gedanke an den 6. März läßt Millionen Computernutzer in aller Welt erschauern. Denn wenn die Systeme auf das Datum des 517. Geburtstags des Bildhauers und Architekten umschalten, wird sein Computervirus-Namensvetter zuschlagen, Daten zerstören, Rechner lahmlegen – und damit riesige Schäden hinterlassen.

Daten-Doktoren und Viren-Experten schieben seit Wochen Überstunden, um verschnupfte Computer noch zu kurieren, bevor der Zerstörer seine Arbeit aufnimmt. Besonders in Hamburg sind die Rechner-Reiniger aktiv: Seit Tagen kämpfen Studenten am Virus-Test-Center (VTC) der Hamburger Uni gegen die Briefflut hilfesuchender Computernutzer an. VTC-Leiter Professor Klaus Brunnstein hatte angeboten, kostenlose Hilfe für erkrankte Elektronik zu liefern (MORGENPOST berichtete).

Der Tag, den Computer-User fürchten: Am 6.März 1992 wird das „Michelangelo-Virus" aktiv. Riesige Datennetze sind von der Vernichtung bedroht

Statt studiert wird nun ständig kopiert. Das Anti-Michelangelo Programm mit dem wenig einprägsamen Namen NTIMICH wird in der Uni auf eingesandte Disketten kopiert und an die bisher 15 000 Bittsteller zurückgesandt. Erfunden wurde der Viruskiller vom Studenten und VTC-Mitarbeiter Morton Swimmer. „Wir konnten jetzt 3000 Anfragen an Siemens-Nixdorf weitergeben. Die anderen Anfragen werden wir bis Montag geschafft haben."

Wo und wie genau Michelangelo entstand, liegt noch im dunkeln. Eine Spur führt nach Taiwan. Doch nicht nur dort gibt es Saboteure, die zerstörerische Chaos-Programme schreiben und für ihre Verbreitung sorgen. In der Regel gelangen die Viren über eine Diskette in das Computersystem. Dort nisten sie sich ein, werden meist zu einem programmierten Zeitpunkt tätig. Sie löschen wertvolle Zeichen, überschreiben sie mit Sinnlosem. Für große Unternehmen können so Millionen-Verluste entstehen.

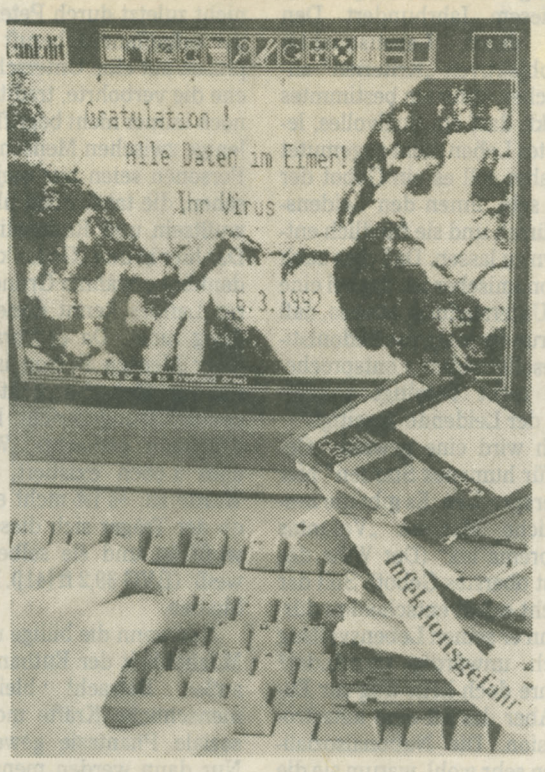
Selbst Original-Software namhafter Hersteller ist nicht immun – auch in den Disketten-Kopierwerken wurden schon Viren entdeckt. Wer noch erste Hilfe in letzter Minute braucht, dem stehen in Hamburg neben dem überarbeiteten VTC andere Möglichkeiten zur Verfügung: Ab Montag gibt es in der Verbraucherzentrale 1500-Virus-Killer-Disketten zum Sonderpreis, einige Buchhandlungen bieten an, die möglichen Hilfsprogramme kostenlos zu kopieren.

Doch selbst wenn Michelangelo wirklich stirbt, ist die Gefahr nicht vorüber. Die Viren-Flut nimmt zu. Heute sind 1500 bekannt, am Jahresende rechnet Professor Brunnstein mit 2000 bis 4000. Und für jeden neuen Virus muß ein neuer Killer gefunden werden. Übrigens: Schon am 12. und 13. März werden die Angriffe weiterer Viren erwartet.

Heiko Haupt

Die Welt, Sa. 29.2.92

Heute in der WELT



Mit Kill-Programmen gegen „Michelangelo“

„Michelangelo“ ist ein stiller Vertreter seiner Art, nistet sich ein – und wartet auf seinen großen Auftritt: „Michelangelo“ ist ein Computervirus, das am 6. März, dem Geburtstag des Renaissancekünstlers (oben seine „Erschaffung Adams“ in der Sixtinischen Kapelle in Rom), Personal Computern weltweit großen Schaden zufügen könnte. Woher es stammt, weiß niemand genau; es zu bekämpfen sind viele angetreten – mit Virus-Aufspür- und Kill-Programmen.

Seite 3

Bitte umblättern ....>

Welt

Samstag, 29. Februar 1992 – Nr. 51

Zittern vor dem schwarzen Freitag und Michelangelo

Ein kleiner Störenfried mit möglicherweise großer Wirkung: der Computervirus „Michelangelo". So sehr er am kommenden Freitag versuchen wird, überall auf der Welt mühsam gesammelte Informationen zu vernichten, so widerspenstig hat sich inzwischen eine Verteidigungslinie gegen den elektronischen Eindringling gebildet.

Von DIETER THIERBACH

Droht den Besitzern von Personal Computern ein schwarzer Freitag? Informatiker befürchten: Ein Computervirus namens „Michelangelo" könnte am 6. März Millionen von Personal Computern auf der ganzen Welt einen erheblichen Schaden zufügen. Am 517. Geburtstag des Künstlers könnten auch in Deutschland, wo rund fünf Millionen IBM-kompatible Rechner auf Büroschreibtischen, in Großraumbüros, in Laboren und im privaten Bereich stehen, schätzungsweise einige zehntausend Computer geschädigt werden. Bisher hatten es die PC-Fachleute einzelner Firmen mit Viren zu tun, relativ harmlosen elektronischen Eindringlingen, die mehr oder weniger originelle Sprüche oder Grafiken auf den Bildschirm zauberten.

Beliebt ist auch der Trick, die Computertastatur umzustricken: Fortan erscheint beim Druck auf das X ein U auf dem Bildschirm, oder es piept schrill, wenn die Leertaste gedrückt wird. Jeder dritte Virusbefall verursacht jedoch schwerwiegende Probleme. „Dark Avenger", dunkler Rächer, oder „Joshi" heißen zwei der digitalen Schädlinge, die Daten auf Nimmerwiedersehen verschwinden lassen. Im Vergleich zu den Resultaten einer Studie von Anfang 1991 hat sich das Auftreten dieser elektronischen Terroristen verdoppelt.

Woher genau „Michelangelo" stammt und wann genau er zum ersten Mal sein Unwesen getrieben hat, ist nicht nachzuvollziehen. Irgendwo sitzt oder sitzen mehrere „Computerkriminelle", die sich vermutlich die Hände reiben, wenn sie Abläufe bei Banken, Firmen, Institutionen durcheinanderbringen können. Schweden und die Niederlande werden als Ursprungsländer für den Datenkiller genannt. Im Gegensatz zu den meisten seiner rund 1400 „Kollegen" ist „Michelangelo" ein eher stiller Vertreter, der sich unerkannt im Computer einnistet und auf seinen großen Auftritt wartet.

Auch „Michelangelo" ist ein kurzes Programm, das jemand an den Anfang eines nützlichen Programms geschrieben hat. Ein Zeitbombenmechanismus tritt in Kraft, der Zünder ist das Datum, in diesem Fall der 6. März, von der eingebauten Uhr eines jeden Computers ausgelöst.

Übertragen wird das Virus, wenn der Benutzer seinen Rechner mit einer infizierten Diskette startet. Das Virus überschreibt am 6. März bei befallenen Rechnern wichtige Systembereiche, die zur Steuerung der Programmabläufe notwendig sind. Auch wertvolle Pläne und Korrespondenz bleiben nicht verschont. Tabellen, Adressen, Lagerlisten – soll plötzlich alles verschwunden sein? Die mühsam erworbenen Daten sind in der Regel unwiderruflich verloren. „Im Extremfall kann sogar die gesamte Festplatte überschrieben werden", so Horst Samsel vom Bonner Bundesamt für Sicherheit in der Informationstechnik (BSI).

Was tun? Am kommenden Freitag den PC lieber erst gar nicht einzuschalten wäre mit Sicherheit die einfachste Methode, in der beruflichen Praxis jedoch kaum anzuwenden. Zumal nach einem Jahr, wieder am 6. März, „Michelangelo" erneut virulent wäre. Ein Tip: Zur Vorsicht alle Dateien von der Festplatte auf einzelne Disketten kopieren und in Sicherheit bringen.

Die einzig wirksame Überprüfung der eigenen Datenbestände auf Virusbefall mit anschließender Therapie besteht in der Anwendung eines geeigneten „Virus-Kill-Programms". Konventionelle Virenerkennungsprogramme helfen da wenig, es sei denn, sie sind in den vergangenen drei Monaten erstellt worden und weisen in ihrer Dokumentation einen Anti-„Michelangelo" auf. Verängstigten Besitzern von Personal Computern helfen jetzt die Verbraucherberatungsstellen weiter: Seit gestern gibt es – gegen einen Obulus von zwei Mark – das einzig wirksame Medikament, „Michelangelo" den Garaus zu machen. „So einen Ansturm haben wir noch nicht erlebt", berichtet eine Mitarbeiterin der Düsseldorfer Zentrale. „Die Leute haben schon am frühen Morgen unsere Räume gestürmt." Die ersten 600 Disketten mit einem Virus-Aufspür-und-Kill-Programm waren im Nu weg.

Andere städtische Verbraucherberatungsstellen sitzen zur Zeit noch auf dem trockenen. Am Dienstag werden neue Disketten erwartet. Raubkopierer machen sich im Fall „Michelangelo" verdient, wenn sie als Präventivmaßnahme das Programm weitergeben. Die Anwendung ist denkbar einfach: Nachdem die Festplatte durchforstet worden ist, empfiehlt es sich, den gesamten Bestand an Disketten auf Befall zu überprüfen.

Mit viel Glück und Geduld erreicht man unter eigens eingerichteten Telefonnummern, den Hotlines, fachkundige Informatiker, die Tips und Rezepte zur Überlistung von „Michelangelo" geben. So auch beim BSI (0228–9582444), das eine bundesweite Warnung vor dem Virus herausgegeben hat. „Unsere Hotline bleibt während der Dienstzeiten auf jeden Fall bis zum 6. März geschaltet", versichert Horst Samsel. Auch in Hamburg (040–54715405) und Karlsruhe (0721–376422) stehen Experten zur Verfügung.

Auch wenn der schwarze Freitag unbeschadet vorübergehen sollte: Mindestens jedesmal, wenn neue Software eingeführt wird, sollte mit einem Virenerkennungsprogramm das System überprüft werden, zu Hause wie im Betrieb. Obwohl die Mehrheit solche Programme besitzt, war – so eine Umfrage in den USA – ein solches nur auf etwa 15 Prozent der Personal Computer auch tatsächlich installiert.

Als bedenklich wird von Informatikern immer wieder die Sorglosigkeit der Anwender beim Umgang mit ihren Daten eingestuft. Die gravierenden Lücken in der Computersicherheit, auch früher bereits offen zutage getreten, müssen ihrer Meinung nach endlich dazu führen, auf nationaler und internationaler Ebene die Standards für die Datensicherheit zu verbessern.

Hamburger Abendblatt, Sa. 29.2.92

Anti-Virus gegen „Michelangelo“

Computerexperte gibt Tips zum Umgang mit dem Sabotageprogramm

Ganz Deutschland liegt im Fieber – wegen der Computerviren. „Die Hysterie ist übertrieben, aber heilsam“, meint Prof. Klaus Brunnstein, Leiter des Virus-Test-Centers der Uni Hamburg. „Computerviren hält jetzt niemand mehr für einen Witz.“

Brunnstein hatte als erster vor dem Sabotage-Programm „Michelangelo“ gewarnt, das am 6. März bei infizierten Personal-Computern alle Daten löschen soll. „In Deutschland trifft es etwa 50 000, also ein Prozent aller PC's“, sagt Brunnstein. „Michelangelo ist relativ harmlos – andere Viren schlagen das ganze Jahr über zu.“ Jeder siebte Computer ist infiziert. Jährlich vervierfacht sich die Zahl der Computer-Viren, sagt Brunnstein.

„Michelangelo“ schleicht sich ein, wenn eine infizierte Diskette beim Systemstart im Laufwerk steckt. Selbst auf Original-Software und bei Service-Firmen, die Viren bekämpfen, wurde „Michelangelo“ entdeckt.

Bereits jetzt hat der Virus das Hamburger Uni-Institut lahmgelegt: 15 000 Briefe von Hilfesuchenden allein in der vergangenen Woche, pausenlos klingelte das Telefon.

Vor dem Verlust wichtiger Daten kann nur Sorgfalt schützen. Das Virus-Test-Center rät:

- Daten von der Festplatte regelmäßig auf Disketten sichern.
- Regelmäßig ein aktuelles Anti-Virus-Programm anwenden. Zuverlässig: „Dr. Solomons“ und „Skulasons“. Einen günstigen „Anti-Michelangelo“ gibt es bei den Verbraucherzentralen.

Brunnsteins Fazit: „Verlassen Sie sich nie auf Computer.“

Computer-Virus „Michelangelo“ bedroht 60 Millionen Personalcomputer

Von IRA KOCH

Hamburg

Am kommenden Freitag droht weltweit rund 60 Millionen Personalcomputern (PC) die Zerstörung ihrer gespeicherten Daten. „Michelangelo“, ein Computer-Sabotage-Programm, soll – pünktlich zum 517. Geburtstag des italienischen Bildhauers, Malers und Architekten – am 6. März aktiv werden.

Ist ein PC mit „Michelangelo“ infiziert und wird am Freitag in Betrieb genommen, zerstört das Virus binnen Minuten einen Großteil der auf Diskette oder Festplatte gespeicherten Daten. Die Folge: Der Bildschirm bleibt dunkel, Dateneingabe oder -abrufung sind ausgeschlossen.

Klaus Brunnstein, Leiter des 1988 eingerichteten Virus-Test-Centers (VTC) der Universität Hamburg, glaubt, „daß in Amerika rund 25 Prozent der PC, in England 30 und Deutschland bundesweit rund 15 Prozent der PC mit ‚Michelangelo‘ verseucht sind“. In absoluten Zahlen: Allein in Deutschland könnten am kommenden Freitag mehr als eine halbe Million PC nicht mehr rechnen wollen.

Grund für den „ungewöhnlich hohen Durchseuchungsgrad“ (Brunnstein) ist die Verbreitungsweise von „Michelangelo“: Das Virus hat auch Originaldisketten von Herstellern befallen. Andere Computerviren werden meist durch Raubkopien in Umlauf gebracht.

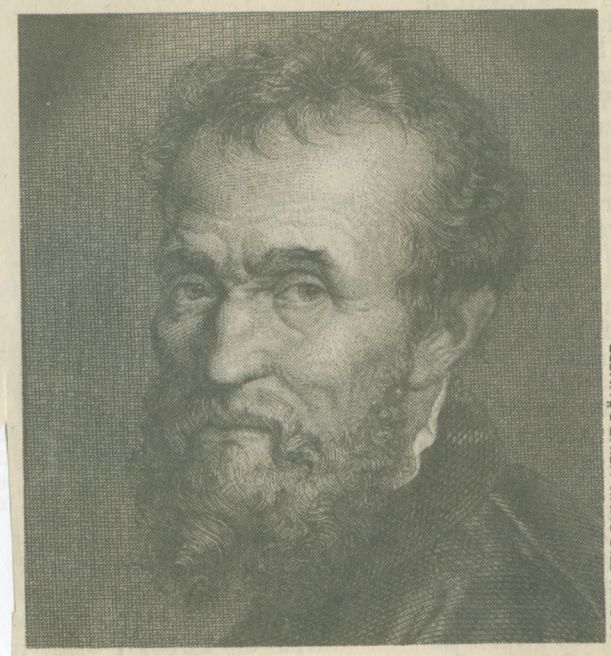
So verkaufte ein großes Kaufhaus in Hamburg bis vor wenigen Tagen Computer-Mäuse einer Firma aus Taiwan mit „Michelangelo“-verseuchter Diskette.

Oder: Ein Servicetechniker eines Hamburger Software-Hauses installierte bei einem Kunden ein neues Software-Programm. Mitarbeiter untersuchten die Neuerwerbung auf „Michelangelo“ und wurden fündig: Der Service-Mann hatte mit einer verseuchten Wartungsdiskette gearbeitet. Vorher war er mit derselben Diskette bei einer Hamburger Großbank tätig gewesen.

Sicheren Schutz vor dem Daten-Crash bieten allein Antivirus-Programme, sogenannte „Scanner“, die „Michelangelo“ erkennen und eliminieren. Morton Swimmer, VTC-Mitarbeiter, entwickelte ein Viruskiller-Notprogramm und bescherte seinem Institut fast den Notstand: Nach dem öffentlich verkündeten Angebot der kostenlosen Abgabe des Killer-Programms gingen im Fachbereich Informatik seit vergangener Woche 29 Postsäcke mit mehr als 15 000 Anfragen nach Disketten ein.

Gleichwohl: „Mein Programm“, sagt Morton Swimmer, „eliminiert nur ‚Michelangelo‘.“ Andere Scanner erkannten auch weitere, „nicht weniger gefährliche“ Viren – von denen den VTC-Experten derzeit rund 1500 bekannt sind.

Viele der Viren stammen aus Bulgarien. Der Grund: Bulgarische Computer-Spezialisten würden „sehr schlecht bezahlt“ und hätten „extrem wenig zu tun“ (Brunnstein). Um im Westen bekannt zu werden und Computer-Firmen auf ihre Talente aufmerksam zu machen, hätten sich viele bulgarische Programmierer auf Viren-Produktion spezialisiert.



ARCHIV, TELE-BUNK, HEINZ RÖHNERT

Klaus Brunnstein, Hamburger Informatik-Professor

Michelangelo, (1475–1564), italienischer Maler, Bildhauer und Architekt, gab dem Virus seinen Namen

Brunnstein: „Viren sind nicht Scherzartikel, sondern eine ernstzunehmende Gefahr.“ Bei „optimistischer Schätzung“ rechnet er Ende dieses Jahres mit 2000 bekannten Viren, „realistisch gesehen werden es 4000 sein“. Zum Vergleich: 1987 waren gerade drei Sabotage-Programme bekannt.

Eine zusätzliche Gefahr sind „mutierte“, leicht veränderte Viren – nach Schätzungen des VTC je vier Milliarden Formen pro Virus – die nicht mehr sicher von den Antivirus-Programmen erkannt und ausgeschaltet werden können. „In Zukunft“, so Morton Swimmer, „kann kein PC-Anwender mehr vor einem Computer-Virus sicher sein.“ Sein Rat, um möglichem Datenverlust zu entgehen: „Regelmäßige und permanente Datensicherung.“

Dazu rät auch Claus Fassnacht, Leiter der Datenschutz- und Informationssicherung bei IBM Stuttgart, und weiter: „Programme nur aus zuverlässigen Quellen kaufen, auf Schreibschutz achten, Computerspiele vermeiden und den Zugang zum eigenen Computer kontrollieren.“ Die Verwendung von aktuellem Anti-Virus-Software hält auch er für unvermeidlich.

Denn: „Bei rund 2000 verschiedenen Virustypen“, so Kuno Brem, Sprecher der IBM Hamburg, „besteht statistisch die Wahrscheinlichkeit, daß täglich fünf Viren aktiv werden.“

So ist die Gefahr eines Datencrash nach „Michelangelo“ nicht vorbei: Nach einem von Morton Swimmer entwickelten Virus-Kalender 1992 werden am 10., 13. und 14. März weitere „Michelangelo“-ähnliche Viren aktiv.

Und – wie jeden Sonntag bis ins Jahr 2020 – treibt der „Sunday-Virus“ sein Unwesen. Bei infizierten Rechnern erscheint auf dem Bildschirm der Text: „Heute ist Sonntag, warum arbeitest Du so hart?“ Anschließend wird das System bis Sonntag 24 Uhr blockiert.

Der „Viren-Kalender 1992“ des Hamburger Virus-Test-Centers. Er zeigt, wann Sabotage-Programme aktiv werden könnten

Sabotage-Program soll Freitag aktiviert werden – Daten werden zerstört – s dener als Rettung – Neue Crash-Daten im März

Welt am Sonntag, 1.3.92

Welt am Sonntag, 1.3.92

Unternehmen und Armee rüsten gegen Computer-Virus „Michelangelo“

r. **Hamburg**

Deutsche Unternehmen und die Bundeswehr nehmen Warnungen vor dem Computer-Virus „Michelangelo“ ernst, und sie bereiten entsprechende Maßnahmen vor. Das ergab eine Umfrage von WELT am SONNTAG bei führenden deutschen Firmen und den Streitkräften.

„Michelangelo“ ist ein Sabotage-Programm, das die in Computern gespeicherten Daten zerstört. Das Virus befällt allerdings ausschließlich Personalcomputer (PC). Informatik-Experten befürchten, daß es am kommenden Freitag, dem Geburtstag Michelangelos, aktiv wird.

Sollte ein PC mit dem Virus infiziert sein und am kommenden Freitag in Betrieb genommen werden, wird, so das Szenario von Informatikern, das Virus in Minutenfrist die auf Diskette oder Festplatte gespeicherten Daten unaufhaltsam zerstören. Dann bleibt der Bildschirm dunkel, der Computer reagiert auf keine Befehle mehr.

Das Virus wurde erstmals im April 1991 in Holland entdeckt. In den vergangenen zehn Monaten hat es sich mehr als alle bekannten Computer-Viren zuvor in Deutschland verbreitet. Frank Felzmann, Computer-Experte beim Bundesamt für Sicherheit in der Informationstechnik (BSI) gegenüber WELT am SONNTAG: „Der Durchseuchungsgrad hat eine neue Qualität erreicht.“ Der Hamburger Informatik-Professor Klaus Brunnstein schätzt, das allein in Deutschland rund 500 000 Personalcomputer von „Michelangelo“ befallen sind.

Unternehmen wie Mercedes Benz, VW, Deutsche Bank oder BASF haben in ihren Computer-Netzen spezielle „Killer-Programme“ gegen „Michelangelo“ eingesetzt. Mercedes will überdies einen Viren-Frühwarndienst einrichten, BASF beschäftigt bereits eine „Virenjägerin“.

Das Bundesverteidigungsministerium hat ebenfalls einen besonderen Maßnahmekatalog gegen Computerviren entwickelt sowie das Abwehr-Programm gegen „Michelangelo“ an die militärischen Stäbe verteilt.

Seite 6: „Michelangelo“

bitte umblättern .....>

Welt am Sonntag, 1.3.92

Frühwarndienst bei Mercedes BASF mit Virenjägerin

M.K. **Hamburg**

Dies sind die Ergebnisse einer WELT am SONNTAG-Umfrage bei deutschen Unternehmen zu „Michelangelo" und der Gefahr von Computer-Viren:

Der **Gerling-Versicherungskonzern** in Köln hatte bereits mehrfach Viren im PC-Bereich. Einmal kroch dort ein Wurm über die Bildschirme, ein anderes Mal arbeiteten die Rechner langsamer.

Bei **Mercedes Benz** wurden Viren bislang immer früh genug erkannt. Dort ist ein Viren-Frühwarndienst geplant. Zudem werden regelmäßig Viren-Suchprogramme eingesetzt.

Die Computer der **Volkswagen AG** wurden mit Stichproben auf „Michelangelo" getestet, bis gestern wurde das Virus aber nicht gefunden.

Peter Dietlmaier, Sprecher der **Deutschen Bank**: „Mit Sicherheit kann man davon ausgehen, daß bei uns schon mal Viren aktiv wurden. Schaden ist nicht bekannt." Das Geldinstitut sei mit Scan-Programmen auf „Michelangelo" vorbereitet.

Die **BASF** hat für die mehr als 12 000 PCs im Unternehmen eine „Virenjägerin" eingestellt. Die 28jährige Informatikerin Esther Armbrust entdeckt pro Monat rund ein Dutzend Sabotage-Programme. Gleichwohl wurde BASF schon von Viren heimgesucht: Beim „Herbstlaub" fielen die Ziffern auf dem Bildschirm herunter wie Laub. Bei „Marihuana" erschienen die Worte: „Your PC is stoned now. Legalise Marihuana."

Virusabwehr-Programm an die militärischen Stäbe

MJI **Hamburg**

Vom Befall mit dem „Michelangelo-Virus" sind auch die für die äußere und innere Sicherheit der Bundesrepublik Deutschland zuständigen Behördencomputer des Verteidigungsministeriums und des Bundeskriminalamts (BKA) betroffen. Beide Häuser wurden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bonn vor dem Virus gewarnt.

Nach Informationen von WELT am SONNTAG werden sowohl die Warnungen als auch mögliche Schäden von der Hardthöhe ernst genommen. Inzwischen hat der für die Rechner und Datenverarbeitung zuständige Organisationsstab 2 der Hardthöhe und der Bundeswehr einen entsprechenden Maßnahmenkatalog sowie ein extra vom BSI für „Michelangelo" entwickeltes Virusabwehr-Programm an die militärischen Stäbe verteilt.

Da „Michelangelo" nur auf PC aktiviert wird, sollen die für die Einsatzführung der Bundeswehr, die zentrale Aufklärung und Frühwarnung zuständigen Großrechner nicht betroffen sein. Diese arbeiten mit einer anderen Betriebssprache und sind von außen nur schwer für Fremddatenträger zugänglich. Die Einsatzführung der deutschen Streitkräfte, hieß es sowohl bei der Bundeswehr wie beim BSI, sei nicht infrage gestellt.

Das BKA in Wiesbaden teilte auf Anfrage mit, auch dort werde die zentrale Datenverarbeitung über Großrechner abgewickelt, so daß die Funktionsfähigkeit der Behörde nicht gefährdet sei.

Die Computer Zeitung, Mi. 4.3.92

Prophylaxe gegen „Michelangelo“

Karlsruhe (rr). Fünf Millionen DOS-PCs sind in Deutschland am 6. März potentieller Tatort des Virus „Michelangelo“. Wenn der Rechner erkrankt ist, hilft kein Kraut mehr.

Das Geburtsdatum des Renaissancekünstlers Michelangelo Buonarotti (6. März 1475) dürfte sich so manchem PC-Anwender einprägen: Der an diesem Tage aktivierte, zwei K große Virus „Michelangelo“ löscht auf infizierten PCs rigoros Daten von Festplatte und Diskette. Verbreitet hat sich das im vergangenen Jahr aufgetauchte Sabotageprogramm nicht nur über Raubkopien: Originale Maus-Treibersoftware (Artec), Standardsoftware sowie Festplatten neu ausgelieferter PCs (Leading Edge Products) waren verseucht.

Da der Virus sofort nach dem Booten seine zerstörerische Wirkung entfaltet, hilft nur die prophylaktische Prüfung und Beseitigung mit Anti-Viren-Programmen, wie sie die Viren Test Centren der Universitäten Hamburg und Karlsruhe (BFK Karlsruhe) anbieten.

Per Backup gesicherte Daten lassen sich auch nachträglich „reinigen“.

BILD, Mi. 4.3.92

Gestatten, Michelangelo

Ich lasse am 6. März die Computerwelt untergehen

Info Michelangelo

Michelangelo Buonarroti (1475 bis 1564), italienischer Maler, Bildhauer und Baumeister der Hochrenaissance. Berühmteste Werke des tiefreligiösen Meisters: die Sixtinische Kapelle im Vatikan, sein zum Kampf bereiter „David". Für seine Lebensgefährtin Vittoria Colonna schrieb er wunderbare Liebesgedichte.

Michelangelo leiht dem Virus seinen Namen. Er wäre am 6. März 517 Jahre alt geworden – und genau an diesem Tag soll das Virus weltweit 50 Millionen Computer lahmlegen ...

Von CLAUS-PETER BRUNS

Man kann es nicht sehen, man kann es nicht hören – aber es will übermorgen die Computer-Welt untergehen lassen: Gestatten, Michelangelo, das geheimnisvolle Computervirus!

Was ist überhaupt ein Computervirus? Ein Sabotage-Programm, das alle gespeicherten Daten verändern bzw. zerstören kann. Weltweit kursieren 2000 Computerviren, schätzt Prof. Klaus Brunnstein, Leiter des Hamburger „Virus-Test-Centers".

Was ist das Besondere an Michelangelo? Michelangelo gehört zur Gattung der „Killer-Viren": In wenigen Minuten zerstört es alle gespeicherten Informationen.

Wo kommt Michelangelo her? Darüber rätseln die Computerexperten. Prof. Brunnstein hält es für möglich, daß bulgarische Computer-Spezialisten es erschaffen haben – sie sind schlecht bezahlt, haben wenig zu tun.

Wie funktioniert Michelangelo? Der „Erfinder" von Michelangelo programmierte das Virus mit dem Befehl: „Alles zerstören – am 6. März!" Dann schob er das Virus-Programm in so viele Computer wie nur möglich. Die Übertragung des Virus geht dann so: Das „Ram", eine Art Kurzzeitgedächtnis des Computers, speichert das Virus; wenn der Computer vor Einlegen einer neuen Diskette (= Arbeitsprogramm) nicht ausgeschaltet wird, befällt das gespeicherte Virus diese Diskette – und diese wiederum befällt weitere Disketten ... Hauptüberträger: Computerspiele, weil sie oft zwischendurch eingeschoben werden!

Wen bedroht Michelangelo? Weltweit 50 Millionen Personal-Computer (vor allem von IBM), in Deutschland 500 000 – schätzt Prof. Brunnstein. Betroffen sind auch die Personal-Computer des Verteidigungsministeriums.

Was kann man gegen Michelangelo tun? Große Unternehmen und auch das Verteidigungsministerium schützen sich mit speziell erarbeiteten „Anti-Viren-Programmen". Sie löschen den vom Virus-Programm gegebenen Befehl („alles zerstören"). Der private Computer-Besitzer kann sie für 100 Mark im Fachhandel kaufen.

Hamburger Abendblatt, Do. 5.3.92

„Michelangelo“: Das erste prominente Opfer

Der Computer-Virus „Michelangelo“ hat sein erstes prominentes Opfer gefunden. Wolfgang Toepfer (26), Enkel von Hamburgs Ehrenbürger Alfred C. Toepfer, muß einen Teil seiner Diplom-Arbeit im Fach Betriebswirtschaft neu schreiben, weil „Michelangelo“ am Dienstag die Dateien seines Computers zerstört hat. Toepfer, Student in Düsseldorf: „Plötzlich war alles weg, was ich gespeichert hatte. Nur Glück, daß ich vergangene Woche von den meisten Kapiteln der Arbeit eine Sicherheitskopie angefertigt hatte.“

Zum Verhängnis wurde Toepfer eine modifizierte Version des Killer-Virus. Das „Michelangelo“-Original soll erst morgen, am 517. Geburtstag des italienischen Malers und Bildhauers, zuschlagen. Der Hamburger Informatiker Prof. Klaus Brunnstein hatte bereits vor Wochen gewarnt, daß mehrere Abarten „Michelangelos“ mit unterschiedlichen Daten in Umlauf seien.

Nur neun Tage später, am 15. März, steht den Benutzern IBM-kompatibler Computer übrigens der nächste Ärger ins Haus. An diesem Termin wird der Virus „Maltese Amoeba“ (oder auch „Eresh“) aktiv. Er meldet sich mit den blumigen Worten: „In einem Sandkorn die Welt betrachten, und in einer Blume den Himmel. Halt' die Endlosigkeit in einer Hand und die Unendlichkeit in einer Stunde.“ Anschließend werden alle Daten gelöscht. ar

Gefährlicher Virus attackiert Rechner

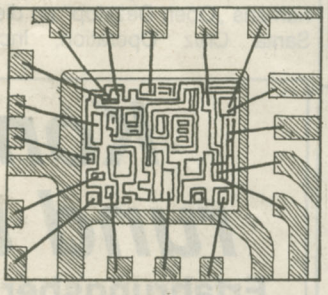
An Michelangelos Geburtstag wird Sabotage-Software aktiv

Der gefährliche Computervirus „Michelangelo" wird am 6. März infizierte Personal-Computer attackieren und Daten zerstören. Internationale Computer-Experten warnen vor dieser Sabotage-Software, die Rechner mit dem Betriebssystem MS-DOS befällt.

Dieser Virus breitet sich in einer unglaublichen Geschwindigkeit aus", sagt Prof. Klaus Brunnstein von der Universität Hamburg. Der berühmte italienische Bildhauer, Maler und Architekt Michelangelo, nach dem der Virus benannt wurde, kam am 6. März 1475 zur Welt.

Amerikanische Computer-Experten befürchten, daß weltweit hunderttausende Computer von der Virus-Attacke betroffen sein könnten. Das Sabotage-Programm löscht willkürlich Daten auf der Festplatte und überschreibt sie mit nutzlosen Zeichen. Der Zerstörmechanismus wird aktiviert, wenn das Systemdatum des Rechners den 6. März erreicht hat. Das geschah bereits im vergangenen März, doch waren damals nach Angaben von Experten nur wenige Computer infiziert.

Nach Ansicht von John McAfee, einem weltweit renommierten Anti-Virus-Experten aus dem kalifornischen Santa Clara, tauchte „Michelangelo" das erste Mal im Februar 1991 in



den Niederlanden auf. Andere Quellen nennen zwei junge Schweizer Informatikstudenten als Urheber. Der Virus breitet sich laut McAfee über die Disketten aus. „Wenn erst einmal das Betriebssystem auf der Festplatte infiziert ist, dann wird der Virus auf jede Diskette übertragen, die der Benutzer auf diesem Rechner einsetzt."

Um der Bedrohung durch „Michelangelo" zu entgehen, empfehlen die Experten, die Daten der Festplatte schrittweise zu sichern. Die neuesten Anti-Virenprogramme seien in der Lage, ihn zu entdecken. Benutzer in Deutschland, deren Rechner infiziert sind, können sich an die Viren-Test-Zentren in Karlsruhe oder Hamburg wenden. Prof. Brunnstein, der Leiter des Hamburger Zentrums, warnt die Benutzer davor, lediglich das Systemdatum der Rechner zu verändern, um so den möglicherweise verhängnisvollen Geburtstag von Michelangelo zu umgehen. „Es tauchen immer wieder Varianten von Computer-Viren auf, die beispielsweise einen Tag früher oder später loslegen."

??, ? XX.Y.92

Briefflut nach Warnung vor „Michelangelo“

Uni Hamburg bot Virus-Erkennungsprogramm an

Hamburg. Nach der Warnung vor dem gefährlichen Computer-Virus „Michelangelo“ steht der Fachbereich Informatik an der Hamburger Universität vor einem kaum lösbaren Problem: Die Universitätsmitarbeiter müssen eine immense Briefflut bewältigen. „In den vergangenen beiden Tagen haben uns 35 Postsäcke voll mit Anfragen erreicht“, sagte Prof. Klaus Brunnstein. „Michelangelo“, der Daten auf Disketten und Festplatten zerstört, wird – wie mehrfach berichtet – am 6. März, dem Geburtstag des italienischen Renaissance-Künstlers, aktiv. Der Informatiker schätzt, daß rund 12 000 Computer-Anwender auf das Angebot der Hamburger Viren-Experten eingegangen sind, ihnen gegen Freiumschlag und Diskette ein Viren-Erkennungsprogramm zu senden. Brunnstein empfahl den Computer-Anwendern, sich mit Hilfe professioneller Anti-Viren-Software vor dem „Michelangelo-Virus“ und anderen Viren zu schützen, die böswillig in die Computerprogramme eingeschleust und zum Teil unbeabsichtigt verbreitet wurden.

??, ? XX.Y.92

Programm aus Olbernhau killt „Michelangelo“-Computervirus

Verbessertes Anti-Virenprogramm „säubert“ Rechner

OLBERNHAU (WI). Schutz vor dem „Michelangelo“-Computervirus: Der Betreiber einer EDV-Schule in Olbernhau im Erzgebirgskreis Marienberg hat ein herkömmliches Anti-Virenprogramm so weiterentwickelt, daß es nun den Virus vernichten kann.

Der Virus aktiviert sich bei befallenen Rechnern am 6. März, dem Geburtstag des Malers Michelangelo. Der Virus überschreibt wichtige Systembereiche. Die Festplatte muß neu formatiert werden und die gespeicherten Daten gehen verloren.

Dietrich Schwenker hatte auf über 30 Computern seines „Freien Bildungs College“ den tückischen Virus entdeckt. Drei Tage kämpfte er mit seinen Mitarbeitern, um den Virus unschädlich zu machen. „Der Virus setzt sich an der untersten Einrichtungsstufe von Datenträgern fest“, erläutert Schwenker. „Auf normalem Wege ist er nicht zu zerstören, ohne die Festplatte, und damit alle Daten zu löschen.“

Doch mit ihren weiter entwickelten Programmen können die Olberhauer EDV-Spezialisten nun den Virus innerhalb weniger Minuten erkennen und zerstören - ohne andere Programme zu beeinträchtigen. Schwenker möchte auch anderen Computerbesitzern im Bezirk helfen. Zum Selbstkostenpreis untersuchen und „säubern“ seine Mitarbeiter die Rechner (Telefon: 07668/2194).

Hamburger Morgenpost, Fr. 6.3.92

Heute greift „Michelangelo“ an

Computer-Virus seit Mitternacht aktiv – Hamburger gelassen

Schlägt „Michelangelo“ heute zu? Mit dem Datumswechsel zum 6. März – dem 517. Geburtstag des italienischen Malers – soll das Computer-Virus in Datenbanken wüten, Informationen auf „verseuchten“ Disketten und Festplatten zerstören. Doch in Hamburg fürchtet sich kaum jemand vor dem „Killer-Programm“.

Experten schätzen, daß weltweit rund fünf Millionen Personal-Computer (PC) vom Datenkiller befallen sind. Das Bundesamt für Sicherheit in der Informationstechnik rechnet bundesweit mit 10 000 viruskranken PC. Professor Klaus Brunnstein, Leiter des Viren-Test-Centrums Hamburg, hält die Zahl 50 000 für realistischer.

Doch Banken und Versicherungen in Hamburg sehen „Michelangelos“ Angriff gelassen entgegen. Haspa-Pressesprecher Ulrich Sommerfeld: „Er wird bei uns keinen Schaden anrichten. Wir haben Such-Programme laufen lassen, das Virus nicht gefunden. Außerdem sichern wir die Daten nochmal extra.“ Auch bei der Deutschen Bank ist zu erfahren: „Michelangelo macht uns nicht nervös.“ Anja Siegfried aus der Abteilung „Electronic Banking“ der Commerzbank: „Die Kunden-Daten sind nicht auf PC, sondern im Rechenzentrum gespeichert.“

Gerhard Wittmann von der Allianz-Versicherung: „99 Prozent unserer Daten sind in Großrechnern gespeichert. Was wir auf den Arbeitsplatzrechnern haben, sichern wir.“

Auch beim Deutschen Ring – die Hauptverwaltung verfügt über 350 Personal-Computer – bleibt man cool: „Wir haben die Warnungen ernst genommen, nach Michelangelo gefahndet. Wir sind aber nicht fündig geworden“, so Manfred Schmidt. Keine Sorge bei der Volksfürsorge: „Wir haben ein internes Daten-Verarbeitungs-Netz mit Großrechner“, weiß Pressesprecher Bernd Jeschonnek.

Oliver Schmid

BILD, Fr. 6.3.92

Michelangelo: Ist Ihr PC heute abgestürzt? Einer weiß Rat

Computer-Praxis Dr. Virus

Von BIRGIT MARQUARDT

Bildschirm schwarz, Datenspeicher „rasiert", alle Programme futsch? Pech, Virus „Michelangelo" hat, wie für heute vorhergesagt, Ihren Computer angesteckt. Damit's nicht wieder passiert, klemmen Sie Ihren PC untern Arm, und ab nach Lokstedt zu Professor Klaus Brunnstein (54), in seine Computer-Praxis.

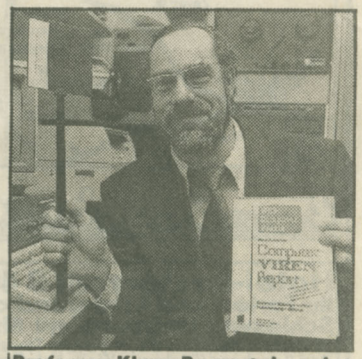
„Dr. Virus" hat einen Bart, Geheimratsecken, kluge braune Augen blinzeln hinter einem goldenen Brillengestell. „Ich habe Medizin gegen 207 Viren, aber da sind 1300 Daten-Killer, gegen die kein Kraut gewachsen ist", sagt Brunnstein.

Wenn plötzlich die russische Nationalhymne aus dem PC dudelt, ein Krankenwagen mit Tatütata quer über den Bildschirm blinkt, Buchstaben wie Schneeflocken nach unten purzeln, haben „Freitag der 13.", „Herbstlaub" oder „Ohropax" zugeschlagen.

„Das sind noch die Harmlosen", sagt Brunnstein, Professor an der Hamburger Uni und international vielgefragter Viren-Spezialist. „Die Bösartigen fressen ganze Datenspeicher. Das kann für Firmen Millionenverluste bedeuten."

Das Europäische Patentamt München verschickte versehentlich Disketten, die mit dem Virus „Stoned" infiziert waren. „Da stand plötzlich 'legalisiert Marihuana' auf dem Bildschirm, dann stürzte das Programm ab." Damit dem Weltkonzern Siemens nichts Ähnliches passiert, hat Brunnstein dort einen Vertrag als „Viren-Feuerwehr".

Brunnstein („Ich bin Wahl-Blankeneser") war einer der Virus-Pioniere, forschte schon in den 70ern. Gegen die Daten-Pest wettert er öffentlich so leidenschaftlich, daß ihn ein Hamburger Lokalsender „glitschfüßige Tarantel" nannte. Brunnstein: „Mißgunst ist ein Virus, gegen den es nie ein Programm geben wird."



Professor Klaus Brunnstein zeigt seine „Viren-Klatsche": eine Diskette an einem Plastikstengel. Rechts seine Datenschutz-Broschüre. Foto: Fabian Posselt

Fanfarenstöße für das Computervirus „Michelangelo“

Tarnen, täuschen, Daten löschen / Mit Umsicht, Disziplin und Hilfsprogrammen kann man sich schützen / Von Hans-Heinrich Pardey

FRANKFURT, 5. März. Diesmal trägt die Gefahr den Namen Michelangelo. Man muß „diesmal“ sagen, weil es nicht das erste Mal ist, daß ein Computer-Virus große öffentliche Beachtung rund um den Globus findet. Jetzt wissen auch Leute, die mit dem Kulturkalender sonst nichts im Sinn haben, daß der Renaissance-Meister am 6. März geboren wurde. Steht die Uhr eines zum Industriestandard kompatiblen Personal Computers auf diesem Datum, verwüstet das Programm, dem der Name des Künstlers gegeben wurde, das aber sonst nichts mit ihm zu tun hat, Datenträger, auf denen es sich hat einnisten können. Etwas Besonderes sind an Michelangelo vielleicht die Verbreitungswege, vielleicht auch der Grad der Verbreitung, aber im übrigen verläuft der Rummel um „Michelangelo“ nach einem bewährten Muster, das schon den Auftritt anderer Computer-Viren in Szene setzte.

Wenn der Schädling der Fachwelt für geraume Zeit bekannt ist, ertönt zu einem Zeitpunkt, der durch das Näherrücken des verhängnisvollen Datums die Drohung ernster erscheinen läßt, ein warnender Fanfarenstoß. Im Falle „Michelangelos“ lagen Monate zwischen der Entdeckung und der Warnung, „Millionen Personal Computer“ seien bedroht. Das ist so richtig wie übertrieben: Tatsächlich kann ein Virus, das für den mit etwa siebzig Millionen installierten Rechnern verbreitetsten Computer-Typ der Welt geschrieben wurde, jeden dieser Computer heimsuchen. Allerdings findet diese „Ansteckung“ nicht durch einen digitalen Pesthauch statt und trifft nicht zwangsläufig jeden der Rechner. Man mag sich fragen, ob der von Fachleuten als gefährlich eingestufte Grad der „Michelangelo“-Verbreitung eine Folge längeren Abwartens war. Doch solange der 6. März noch in einiger Entfernung lag, interessierte sich auch kaum jemand dafür, daß die Computer-Virologen einen neuen Schädling in ihre Kataloge aufgenommen hatten.

Schließlich könnte man ein paarmal im Jahr auf den Virus „Freitag der Dreizehnte“ warnend hinweisen. Dabei sind die „datumsorientierten“ Schadensstifter eine Minderheit unter den – mit allen Varianten – auf grob anderthalbtausend geschätzten Erscheinungsformen von Virenprogrammen. Die Wiederkehr von Todestagen in der Familie Kennedy ist genauso Auslöser für ein Computer-Virus namens „Dead Kennedys“ wie alle Tage, deren Datum eine Null an der zweiten Stelle hat, für einen anderen. Wesentlich weniger öffentlichkeitswirksam sind die Computer-Viren, die rechnerinterne Vorgänge zählen – wann auf einem bestimmten Rechner ein Virus Schaden stiftet, der nach einer programmierten Anzahl von Festplattenzugriffen aktiv wird, das läßt sich nicht vorhersagen.

Was man biomorph Viren nennt, sind kleine Computer-Programme, die sich selbst reproduzieren können. Man unterscheidet sie nach der Art, wo und wie sie sich verbergen, und danach, welche Sektoren der Speichermedien oder welche Dateien von ihnen angegriffen werden. Inhalt des Viren-Programms ist zum einen, eine Kopie von sich selbst, manchmal auch eine trickreiche Modifizierung zu schaffen. Dieser Programm-Teil besitzt die Fähigkeit, andere mögliche Opfer zu erkennen, festzustellen, ob diese schon „infiziert“ wurden, die Infektion vorzunehmen und Tarn-Maßnahmen zu treffen. Die unselige Berühmtheit, zu der Computer-Viren gelangen, liegt in einem anderen Teil des Programms: dort wird geprüft, ob bestimmte Auslösebedingungen gegeben sind, und falls das der Fall ist, beginnt eine mehr oder weniger schädliche Aktion.

Da es sich um Programme handelt, kann man den Computer-Speicher, die für die Verwaltung von Disketten und Festplatten wichtigen Sektoren, die Dateien und Programme nach verräterischen Bestandteilen bekannter Viren-Programme absuchen. Das tun sogenannte „Viren-Scanner“, Programme, auf die nach dem warnenden Fanfaren-Stoß stets hingewiesen wird. Findet man Spuren eines Virus, ist der nächste Schritt, ihn zu entfernen und nach Möglichkeit die gesäuberten Dateien wieder zu reparieren. Das tun andere Hilfsprogramme. Dieses Verfahren hat den Vorteil, sehr rasch zu arbeiten, aber auch Nachteile: Erstens muß der Scanner immer auf dem neuesten Stand sein; nur was er kennt, kann er finden. Außerdem kommt sein Einsatz möglicherweise zu spät, denn es gibt Fälle, in denen allein die „Infektion“ zu Beschädigungen von Daten führt. Also wurden Programme entwickelt, die dauernd auf der Wacht liegen und jede kritische Operation des Rechners verbellen. Das kann ziemlich lästig sein, weil solche Programme sofort alle Aktivitäten stoppen, wenn etwa ein ihnen unbekanntes Programm einen Kopiervorgang starten will – obwohl dieser Wunsch harmlos sein kann. Einen vollständigen Schutz, der noch dazu bequem ist, gibt es nicht: Aber mit Disziplin und Umsicht kann man dem Schlimmsten vorbeugen.

Die entscheidende Schwachstelle eines PC, der allerdings auch konstruktiv und von der Anlage seines Betriebssystems her nicht gerade ein Fort Knox für Daten ist, bleibt der Mensch: Computer-Viren entwickeln sich nicht „von allein“, sie leben genausowenig wie irgendein anderes Programm. Sie werden von Menschen – deren Motive zwischen Geltungssucht und fachlichem Interesse changieren mögen – geschrieben und bedürfen, um den Schaden anzurichten, der in den Anweisungen des Codes steckt, immer eines Menschen, etwa eines, der auf einem fremden Rechner „eben mal schnell eine Diskette kopieren“ will. Das eigentliche Wirtstier des Computer-Virus ist der gedankenlose, um das Risiko unbekümmerte Benutzer – und das ist in der Welt der persönlichen Computer die vorherrschende Spezies. Es ist heller Wahnsinn, auf einem PC, der existentiell wichtiges Material – nehmen wir einmal an: die einzige druckfertige Version einer Doktorarbeit – speichert, Software aus dunkler Quelle zu kopieren oder zu starten, ohne alle Schotten dicht zu machen.

So hat der gern als Sensation konsumierte Komplex Computer-Viren durchaus ernste Aspekte: Von einem Spielzeug ist der Personal Computer zu einer immer leistungsfähigeren Maschine geworden. Entsprechend wichtiger wurden die ihm übertragenen Aufgaben. Das macht eine bessere Sicherung, als sie bisher möglich ist, gerade in der „dezentralen Datenverarbeitung“ dringend nötig – nötiger als eine um ein paar Megahertz höhere Taktfrequenz.

Frankfurter Allgemeine Zeitung, Fr. 6.3.92

Hamburger Morgenpost, Sa. 7.3.92

Michelangelo – nur ein Bluff?

Die Angst war unbegründet: In Hamburg stürzte der Computer-Virus ab

Hamburg – Wochenlang hielt uns „Michelangelo", der Computer-Virus mit dem wohlklingenden Künstler-Namen, in Atem. Gestern war es soweit: Am 6. März, dem 517. Geburtstag des italienischen Bildhauers und Malers Michelangelo Buonarroti, sollte der Virus weltweit alle Personal-Computer (PC) lahmlegen. Was passierte? Fast nichts. Nur ein Bluff?

Ganz anders sieht das Professor Klaus Brunnstein vom Viren-Test-Zentrum an der Universität Hamburg: „Nur dank unserer Warnungen ist so wenig passiert." Seine Mitarbeiter kämpften sich in den vergangenen Wochen durch 40 Postsäcke mit 20 000 Zuschriften. Anfragen kamen vom Bundesverteidigungsministerium, einzelnen Firmen und verzweifelten Privatpersonen.

Das Bonner Bundesamt für Sicherheit in der Informationstechnik (BSI) konnte noch rechtzeitig 1000 infizierte PC's kurieren. Das BSI rechnete mit bundesweit 10 000, Brunnstein mit rund 50 000 erkrankten PC's: „Hamburg gehörte zu den verseuchtesten Gebieten."

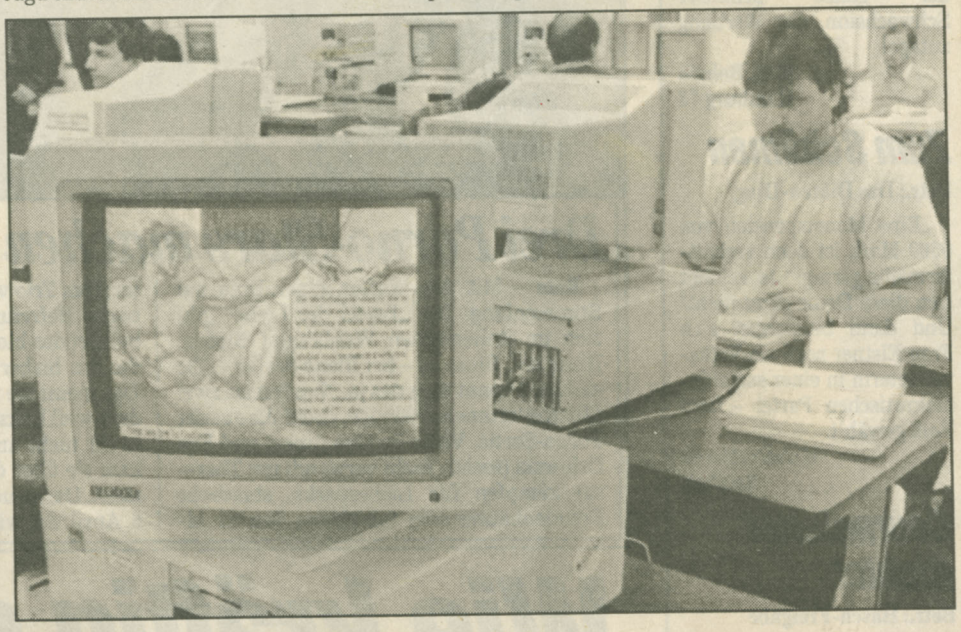
Komisch. Nur vier Hamburger Patienten meldeten in den vergangenen zwei Tagen datenzerstörende Virus-Attaken. Bei Behörden, Banken und Versicherungen flimmerten die Bildschirme wie immer. Auch die vorangegangene Virus-Jagd endete ohne Beute.

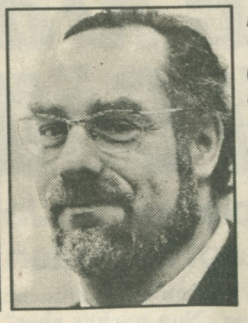
Lediglich die Hamburger Hypotheken-Bank wurde fündig. Vor etwa einer Woche stieß der Computer-Experte des Bankhauses, Jan Feddern, bei einer routinemäßigen Kontrolle auf einen Daten-Killer: „In einem unserer 60 PC's haben wir den Tequila-Virus entdeckt und sofort unschädlich gemacht. Michelangelo haben wir nicht gefunden."

Pech hatten dagegen die Stadtverwaltung von Gladstone in Australien sowie die Schweizer Unis St.Gallen und Zürich; krank meldeten sich auch 1300 Rechner in Südafrika – vor allem in Apotheken.

„Außer Spesen nichts gewesen." Das ist das Resümée für Deutschland von Steffen-Wernery vom Hamburger Chaos-Computer-Club. Der Rummel um „Michelangelo" sei sicherlich nicht zufällig vor der Cebit, der weltweit größten Computer-Messe losgegangen. Sie beginnt am Dienstag in Hannover.

Die Rostocker IBM-Filiale meldete nach Hamburg: „Michelangelo ist hier nicht aufgetaucht, aber eben hat ein Kollege eine Tasse Kaffee über die Tastatur geschüttet." **ols/caj**





Keine Angst mehr vor „Michelangelo" (o.): Steffen Wernery (li.) vom Chaos-Computer-Club hält das Virus-Fieber für einen Riesen-Bluff. Informatikprofessor Klaus Brunnstein (re.) dagegen warnt weiter vor Daten-Killern

Brunnstein warnt vor PC's

Hamburg – Durch Viren in Personal-Computern würden in Zukunft „riesige wirtschaftliche Schäden entstehen", glaubt der Hamburger Informatik-Professor Klaus Brunnstein. „Dagegen ist Michelangelo ein kleiner Fisch." Die Computer seien „eine enorme Gefahr für die Gesellschaft", denn „sie sind nicht beherrschbar". Wie in der Anfangszeit von Aids werde die Gefahr völlig unterschätzt. Sein Rat: „Schafft die PC's ab."

Hamburger Abendblatt, Sa. 7.3.92

In Hamburg setzte das Virus nur wenige Computer außer Gefecht

„Michelangelo": Das Chaos blieb aus

Alle hatten vor einem Computer-Virus gewarnt – im Kaufhof an der Mönckebergstraße passierte es: Als der Kaufhausdetektiv Michael Heinz am Freitag, 6. März, seinen Computer einschalten wollte, ging nichts mehr. „Die Kiste ging kurz an, und dann war's erledigt", sagt Heinz.

„Wir hatten am Vorabend glücklicherweise alle Daten auf Diskette abgespeichert", sagt der Detektiv, der für Kaufhof als Subunternehmer arbeitet. Ob „Michelangelo" oder ein anderes Computer-Virus seinem Rechner den K.-o.-Schlag versetzt hat, weiß er nicht. Dabei hatte der Kaufhof besorgten Kunden kostenlos ein Anti-Viren-Programm kopiert.

Der große Zusammenbruch der Personal-Computer aber ist ausgeblieben. „Die Warnungen haben die Leute dazu gebracht, ihre Viren zu entdecken und zu eliminieren", sagte der Hamburger Professor Klaus Brunnstein, der vor einem Monat als erster in Deutschland Alarm geschlagen hatte. Bei Brunnsteins Virus-Test-Center haben sich zehn Privatleute gemeldet, denen „Michelangelo" in den letzten beiden Tagen die Daten von der Festplatte geräumt hatte.

Einer wollte das Virus überlisten und stellte am 5. das Datum seines Rechners auf den 6. März vor – das aktivierte das Virus sofort, und alle gespeicherten Daten waren futsch. Bei einigen wurde das Virus schon am 5. März ausgelöst, weil der Kalender ihrer Computer das Schaltjahr vergessen hatte und den 29. Februar zum März zählte.

Auch in einer Hamburger Behörde schlug das Virus zu: Ein Beamter hatte eine infizierte Spieldiskette eingeschleppt, mit der er sich – streng verboten natürlich – die Langeweile während des Dienstes vertrieb.

Den Uni-Instituten in Hamburg und Karlsruhe und dem Bonner Bundesamt für Computer-Sicherheit seien bisher mehr als 5000 Infektionen bekanntgeworden, rechtfertigte Brunnstein den Alarm. Sein Institut hatte kostenlos 18 000 Disketten mit einem Antivirus verschickt. „Hätten wir nicht gewarnt, säßen die jetzt dumm da", sagte Brunnstein.

Der Hamburger Chaos-Computer-Club hatte die Warnungen vor „Michelangelo" als „Witz des Jahres" bezeichnet. Einer der Sprecher, Steffen Wernery, hatte in den „Tagesthemen" behauptet, hinter der „Virenpanik" kurz vor der CeBIT in Hannover (vom 11. bis 18. März) stecke eine „Marketing-Philosophie", um die Umsätze der „Entseuchungs-Branche" in die Höhe zu treiben.

In Hamburg und der ganzen Welt haben Universitäten eifrig vor dem Computer-Virus „Michelangelo" gewarnt, das nun immer am 6. März zuschlagen soll, dem Geburtstag des Malers Michelangelo Buonarotti. Das abgebildete Plakat hängt in der Universität von Newark im US-Bundesstaat New Jersey und zeigt einen Ausschnitt von Michelangelos Deckenfresko in der Sixtinischen Kapelle in Rom. Der Text besagt, daß vermutlich 80 Prozent der dortigen Uni-Programme von „Michelangelo" befallen sind. Foto: AP

Brunnstein hat diese „idiotische Berichterstattung so geärgert", daß er in Zukunft nicht mehr öffentlich warnen und seine Hilfe anbieten will. „Die Universität soll nicht in den Verdacht kommen, irgend jemandes Sache zu betreiben."

DIETMAR HIPP

Hamburger Abendblatt, Sa. 7.3.92

„Michelangelo“ schonte die Deutschen

hip **Hamburg** – „Michelangelo“ hat die Computer weitgehend verschont. In Deutschland wurden nur 50 Fälle bekannt, in denen das Virus bei Personal-Computern am Freitag Daten vernichtete.

In der Mehrzahl handelte es sich um mittelständische Betriebe und um Computer von Privatpersonen. Bei einer Firma im Ruhrgebiet seien 75 Rechner ausgefallen, so das Bonner „Bundesamt für Sicherheit in der Informationstechnik“ (BSI). In Behörden hat das Virus nur in zwei Fällen zugeschlagen: in Hamburg und in Nordrhein-Westfalen. Das ergab eine Umfrage der Wickert-Institute.

Ähnlich waren die Schäden auch in anderen europäischen Ländern, in Asien, Australien, dem Nahen Osten und den USA. Katastrophal wirkte sich das Virus in Südafrika aus, wo mehr als 1000 Computer versagten. In Uruguay löschte das Virus nach Zeitungsberichten Geheimdienstinformationen eines Militärinstituts.

Seit den ersten Meldungen über „Michelangelo“ seien „dreimal so viele Viren entdeckt worden wie im gesamten Jahr 1991“, sagte Paul Langemeyer, Vorsitzender der Europäischen Anti-Viren-Organisation EICAR.

Kritiker hatten den Viren-Alarm als „größten Public-Relations-Schwindel in der Computergeschichte“ bezeichnet.

„Im Gespräch“ Seite 2, Bericht Seite10

IM GESPRÄCH

Computer-Viren

Das Bild vom „Virus“ paßt – das ist auch das einzig Gute, was sich über Computerviren sagen läßt. Einmal in Umlauf gebracht, breiten sich die Sabotageprogramme aus, indem sie sich selbst vervielfältigen, Disketten und Computer infizieren.

Manche Viren löschen einzelne Programme oder die ganze Festplatte, schleichend oder zu einem bestimmten Datum. Andere füllen einfach den Speicher mit „Datenmüll“. Ein eher harmloses Virus macht nur sonntags den Computer unbrauchbar, mit der Meldung: „Hey, es ist Sonntag, warum schuftest du? Geh raus, viel Spaß!“

Viren verbreiten sich über kopierte oder weitergereichte Programme. Wirklich sichere Quellen gibt es nicht: Wer nur lizensierte Original-Disketten benutzt, ist zwar relativ sicher – aber selbst dort tauchten schon Viren auf.

Manche betrachten es als „Sport“, Rechner und Experten mit neuen Viren zu überlisten. In Deutschland ist diese Computersabotage strafbar – es drohen bis zu zwei Jahre Haft. Besonders Taiwan und Bulgarien gelten als Viren-Ursprungsländer.

Zur Zeit sind weltweit etwa 1200 Viren bekannt. Die Zahl der Viren steigt jährlich um das Zwei- bis Vierfache. Anti-Viren-Programme, die Infektionen aufspüren und unschädlich machen sollen, müssen deshalb ständig aktualisiert werden. Solche „Viren-Killer“ bieten der Handel und Service-Unternehmen an, bei den Verbraucherzentralen gibt es ein Programm schon für zwei Mark. Virus-Institute der Universitäten Hamburg und Karlsruhe beraten im Notfall, ebenso das Bonner „Bundesamt für Sicherheit in der Informationstechnik“.

Wer regelmäßig seine Daten von der Festplatte auf Disketten abspeichert und Anti-Viren-Programme einsetzt, geht auf Nummer Sicher. Je schlimmer ein Datenverlust wäre, desto sorgfältiger sollte man sein. hip

bitte umblättern.....>

Die Welt, Sa. 7.3.92

„Michelangelo" griff 10 000 Rechner an

MICHAEL SIMM, **Bonn**

Die von einigen Experten angekündigte massenhafte Zerstörung wichtiger Daten durch den Computervirus „Michelangelo" blieb gestern weitgehend aus. Gleichwohl schätzte der Präsident des amerikanischen Industrieverbandes Computerviren, daß weltweit mindestens 10 000 IBM-kompatible Rechner Opfer des Virus wurden. Dieser Zahl stehen etwa fünf Millionen PC gegenüber, die „Michelangelo" hätte befallen können.

Zuvor hatten der Hamburger Professor Klaus Brunnstein vom Virus Test Center der Universität und Klaus Fischer (Universität Karlsruhe) vor den Folgen des Computervirus gewarnt, der darauf programmiert ist, am 6. März, dem Geburtstag des Renaissancekünstlers Michelangelo, loszuschlagen. Das Virusprogramm, das nach Erkenntnissen von Interpol in Taiwan seinen Ursprung hat, sollte an diesem Schlüsseldatum auf jedem infizierten Computer nach dem Einschalten sämtliche Dateien überschreiben und damit unbrauchbar machen.

Allein in Hamburg gab es nach der Warnung innerhalb weniger Tage 15 000 Anfragen besorgter PC-Benutzer. In beiden deutschen Notfallzentren wurden bis Donnerstag abend fast 1000 Infektionen gemeldet und anschließend beseitigt. Am Freitag kam es dann doch zu rund 50 Fällen, in denen der Virus Computerdaten beschädigte. In einem Fall waren 75 Rechner einer Firma im Ruhrgebiet betroffen.

Ähnlich war die Situation in den meisten westlichen Ländern. In Südafrika dagegen hinterließ der Virus verheerende Zerstörungen bei rund 1000 Firmen und privaten Anwendern. Nach Auskunft des Unternehmens Computer Help Line wurden vor allem Apotheken geschädigt, „bei denen trotz unserer Warnung niemand Vorkehrungen getroffen hat". In Japan hat der Virus nach Angaben des Software-Hauses Lonrho International die Rechner von mindestens fünf Firmen angegriffen, darunter ein Industriekonzern und ein Computerhändler.

Aus Australien und Neuseeland wurden nur vereinzelte Infektionen ohne nenneswerte Schäden gemeldet. Die Zahl der neugierigen Reporter, so hieß es, habe die Zahl der Opfer bei weitem Überschritten. Brunnstein macht die breite Berichterstattung dafür verantwortlich, daß der 6. März für die meisten Computerbesitzer glimpflich verlief. Ein Sprecher des Hamburger Chaos Computer Clubs beschuldigte dagegen die Hersteller von Anti-Viren-Programmen, im Vorfeld der Hannover Computer-Messe CeBIT eine Kampagne geführt zu haben mit dem Ziel, die Verkaufszahlen zu erhöhen.

Der Absatz der Programme, die zwischen 50 und 800 Mark kosten und ständig durch neue Versionen ersetzt werden müssen, stieg in den letzten Tagen sprunghaft an. Die Fachzeitschrift „PC Professionell" etwa stellte in ihrer Februar-Ausgabe 19 Anti-Viren-Pakete vor, weist aber ausdrücklich darauf hin, daß beim ausschließlichen Gebrauch von Originalsoftware für nichtvernetzte PC keinerlei Gefahr besteht.

Schutz vor „Michelangelo" hätte auch eine billigere Methode gebracht: Um einen Anschlag am Geburtstag des Namensgebers zu vermeiden, hätte es genügt, die Uhr des Rechners auf den 7. März vorzustellen.

Winsen/Luhe (Stadtanzeiger?), 7./8.3.92

„Michelangelo"-Warnungen verhinderten zum Teil Millionenschäden

Geburtsdatum löste weltweit Panik aus

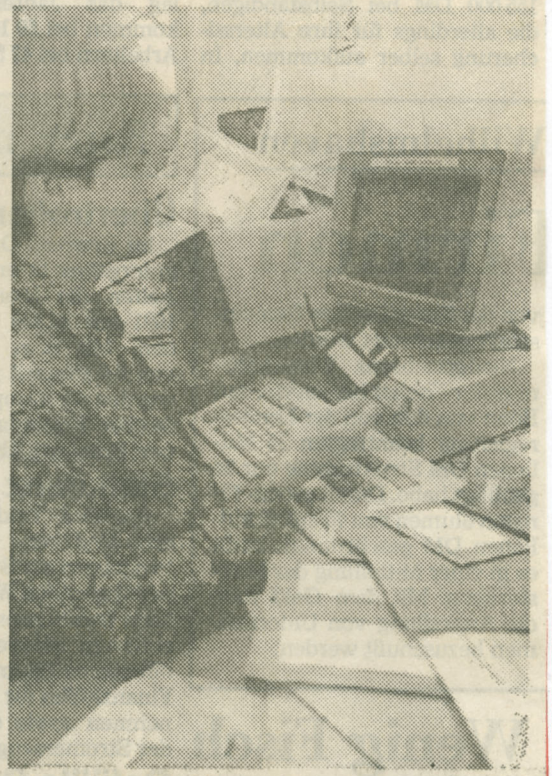
Von C. Dernbach

Hamburg. Das gefürchtete Computer-Virus „Michelangelo" hat gestern international zugeschlagen. Dennoch feiern die Fachleute zur Bekämpfung von Computer-Viren einen Erfolg: „Die beharrlichen Warnungen vor ‚Michelangelo' haben in Deutschland größere Schäden verhindert", freut sich der Viren-Experte des Bonner Bundesamtes für Sicherheit in der Informationstechnik (BSI), Frank Felzmann.

Gestern, am Geburtstag des italienischen Renaissance-Künstlers Michelangelo Buonarotti, wurden in der Bundesrepublik nur vereinzelt Aktionen des Sabotage-Programms bekannt. Tausende Infektionen waren rechtzeitig entdeckt worden. In Japan und Südafrika fielen dagegen die Daten zahlreicher Personal Computer (PC) dem Virus zum Opfer.

Die Aufklärungs-Kampagne der „Viren Test Centren" an den Universitäten in Hamburg und Karlsruhe und des BSI hatte in der Öffentlichkeit vereinzelt sogar zu Panikreaktionen geführt. In Kiel belagerten hunderte Anwender regelrecht die Verbraucherzentrale, die ein Anti-Viren-Programm angeboten hatte. Zum hohen Bekanntheitsgrad des Virus hatten der einprägsame Name und das feststehende Auslösedatum beigetragen. Dabei ist „Michelangelo" nur einer von rund 1 500 Computer-Viren, die die IBM-kompatiblen PC befallen können.

An der Universität Hamburg verbrachten Studenten freiwillig Hunderte von Stunden im Viren-Test-Centrum, um besorgten PC-Benutzern Anti-Viren-Programme zu kopieren und die Flut der Anfragen zu beantworten. Ohne die spontane Hilfe der Studenten wäre die feste Mannschaft des Centrums unter der Leitung von Prof. Brunnstein in den Massen der Zusendungen versackt. „Michelangelo" macht nach Auffassung der Experten exemplarisch deutlich, daß die wertvollen Daten in den Computern gefährdet sind. Prof. Brunnstein: „Viele PC-Anwender merken jetzt endlich, daß sie quasi ein Auto ohne Bremse gekauft haben."



Informatikstudent Ulf untersucht eingeschickte Disketten auf Viren. An der Hamburger Universität waren 32 Postsäcke mit Anfragen eingegangen, seitdem vor „Michelangelo" gewarnt wurde. Foto: dpa

Münchener AZ, ?? XX.Y.92

Computer infiziert? So killen Sie den Michelangelo-Virus

● Computer-Freaks zittern vor Michelangelo – der elektronische Virus zerstört genau am 6. März alle infizierten Programme. Betroffen sind mehr PCs und Software als man denkt: „Grundsätzlich sollte jeder etwas dagegen tun", sagt Klaus Brunnstein, Professor für Datensi-

cherheit. Sein Virus-Testcenter bietet kostenlos Testprogramme an, mit deren Hilfe Michelangelo erkannt und verbannt werden kann.

Michelangelo – so genannt, weil der italienische Maler am 6. März zur Welt kam – überschreibt in infizierten Computern wichtige Systembereiche mit nutzlosen Zeichen, zerstört Daten. Computer werden sofort gestört, wenn der Rechner mit einer infizierten Diskette gestartet wird. Auch wenn der Startversuch nicht erfolgreich ist, wird der Virus aktiviert und kann die Festplatte infizieren, die dann neu eingerichtet werden muß. Hat sich der Virus in einem Rechner eingenistet, wird jede Diskette, die nicht schreibgeschützt ist, bei ihrer Verwendung infiziert – und kann andere Computer „anstecken".

So bekommt man das Programm, das Michelangelo entlarvt: Diskette und frankierten Rückumschlag an die Uni Hamburg, Virus-Testcenter, Vogt-Kölln-Straße 30, 2000 Hamburg 54, schicken.

Berliner Verlag GmbH & Co

Wochenpost

Mauerstraße 86–88, O-1080 Berlin

Universität Hamburg
Prof. Klaus Brunnstein
Institut für Informatik
Vogt-Kölln-Str. 30
2000 Hamburg 54

S. 29

Pressesammlung

Berlin, 11.3.1992

Sehr geehrter Herr Brunnstein,

auf Seite 29 der aktuellen Ausgabe der WOCHENPOST finden Sie einen Artikel, der Sie interessieren dürfte.

Wir würden uns freuen, wenn die Lektüre unserer Zeitung bei Ihnen Interesse für unsere Arbeit weckt und verbleiben

mit freundlichen Grüßen

Ihre WOCHENPOST Redaktion

Angelika Neubauer

i.A. Angelika Neubauer

Redaktion
Wochenpost
REGINE HALENTZ

privat: Regine Halentz
Zingster Straße 2
O-1093 Berlin
Telefon: 9 22 58 27

Mauerstraße 86–88
O-1080 Berlin
Telefon: 2 31 01 146
Telefax: 2 31 01 159

PC WOCHE, Mo. 9.3.92

Wer hilft bei Virenbefall?

Wegen der vielen Anfragen zu Gegenmaßnahmen gegen den Michelangelo-Virus (siehe PC WOCHE Nr. 8/92, Seiten 1 und 8), veröffentlichen wir die Adressen unabhängiger Institute und Behörden, die im Falle eines vermuteten Befalls ihre Hilfe anbieten. Im übrigen erkennen die meisten Virensuchprogramme, die nicht älter als etwa ein halbes Jahr sind, auch den Michelangelo-Virus.

— Bundesamt für Sicherheit in der Informationstechnik
Am Nippenkreuz 19
5300 Bonn
Sondertelefon 02 28/ 95 82-444

— Virus Test Center
Universität Hamburg,
Fachbereich Informatik
Vogt-Kölln-Str. 30
2000 Hamburg 54
Telefon 040/ 547 15-0
Prof. Dr. Klaus Brunnstein, Dipl.-Informatikerin Simone Fischer-Hübner

— Microbit Virus Center
Technische Universität Karlsruhe
Rechenzentrum
Kaiserstr. 12
7500 Karlsruhe 1
Telefon 07 21/ 37 64 22
Dipl.-Informatiker Christoph Fischer

LESERBRIEF

Zu unseren Beiträgen über den Michelangelo-Virus, PC WOCHE 8/92, Seiten 1 und 8:

Es ist sehr begrüßenswert, wenn die Presse in objektiver Weise über Computerviren aufklärt, wie dies in der PC WOCHE vom 24. 2. geschah. Der Michelangelo-Virus stellt eine doch recht hohe Gefahr dar, wenn auch die Diskussion um diesen Virus durch Panikmache in anderen Medien übermäßig angeheizt wurde.

Neben der objektiven Darstellung der Problematik fielen uns aber auch sehr bedenkliche Äußerungen des Herrn Prof. Brunnstein, Universität Hamburg, auf. Unreflektierte Stellungnahmen wie „Wir untersuchen gerade einen Virus, der sich in vier Milliarden Variationen darstellt, da ist jeder Virusscanner machtlos", sind pure Panikmache und zeigen bestenfalls Herrn Brunnsteins mangelnde Sachkunde auf.

Aus Hamburg wurde dem staunenden Auditorium der Computermagazin-Leser bereits mehrfach der Untergang der Datenverarbeitung prophezeit (zum Beispiel im Zusammenhang mit dem Dbase-Virus), durch bekanntermaßen mangelnde Untersuchungsqualität der Universität Hamburg verursachte Gerüchte haben bereits öfter zu bedenklichen Fehlmeldungen geführt. So verstieg sich Brunnstein zu Warnungen über den Dark Avenger Virus (der Virus werde schon bei bloßen Lesezugriffen aktiv, es bleibe dem Anwender „nur noch Beten" übrig etc.).

Ein sensibles Gebiet wie die Antivirus-Branche verlangt nach seriöser Aufklärung statt nach der wilden Verstreuung kolportierter Panikmeldungen. Wer jenseits jedes wissenschaftlichen Anspruchs vorgibt, „Virusforschung" zu betreiben, muß sich auch über die damit übernommene Verantwortung den Nichtfachleuten gegenüber im klaren sein. Es kann nicht angehen, daß man die Betroffenen mit Sprüchen wie „man kann nur noch beten", „da ist jeder Virenscanner machtlos" oder „bisher größter Anschlag auf die EDV", verunsichert. Zudem sind all diese Behauptungen sachlich falsch. Tatsache ist, daß bisher noch jeder Virus von Scannern erkannt werden kann, sofern man nicht die unzeitgemäßen Klassifizierungsansätze der Uni Hamburg verwendet. Und noch jedem Virus konnte man bisher beikommen.

Sehr schlimm ist auch, daß Herr Brunnstein in Ihrem Beitrag weiter behauptet, nicht einmal das Verstellen der Systemuhr sei eine Hilfe, denn „am 5. und 7. März zünden andere Viren".

Abgesehen von der unsachlichen, suggestiven Wortwahl („zünden") ist das völliger Unsinn, denn immerhin ist der Michelangelo nach sehr vorsichtigen Schätzungen auf mindestens 10 000 Systemen im Bundesgebiet verbreitet (dank Firmen wie dem Maushersteller Artec). Dagegen sind die ohne Namen erwähnten anderen beiden Viren in Deutschland höchstens in Brunnsteins Labor stark verbreitet — nach unseren Unterlagen wird zu diesem Zeitpunkt keiner der in Deutschland verbreiteten Viren aktiv. Zudem muß man das Problem in Relation zur potentiellen Zerstörung sehen: Der Michelangelo ist einer der destruktivsten Viren, die in der letzten Zeit erschienen sind.

Unser Rat also — trotz Brunnstein: Ja, verstellen Sie das Systemdatum. Und selbst wenn ein anderer Virus dann aktiv werden sollte, das Risiko und die eventuellen Zerstörungen sind in jedem Fall geringer als beim Michelangelo.

Bedauerlich ist, daß Herr Brunnstein durch sachfremde und teilweise völlig unbegründete Äußerungen in der Regel nur Hoffnungen bei den Anwendern zerstört, statt seriöse Ratschläge zu geben, die dem Benutzer weiterhelfen. Während Herr Brunnstein sich selbst durch sein Verhalten jegliche Kompetenz abspricht, hat die Antivirusbranche in aller Stille Tausende von Anwendern mit kostenloser Software versorgt. In aller Stille deshalb, weil die (Tages)-Presse lieber spektakulären Äußerungen und kolportierten Gerüchten nachgeht.

Joachim Günster, Geschäftsführer der EPG, Unternehmensberatung GmbH.

Zur Info:
EPG, Unternehmensberatung GmbH
vertreibt das
Carmel Turbo AntiVirus-Progr.

Wochenpost, O-Berlin, Do. 12.3.92

COMPUTERVIREN

Italienischer Datensalat

Seit Wochen hatte der »Tag X« den rechnergestützten Teil der Menschheit je nach Gemütslage amüsiert oder verunsichert: Am 6. März, dem 517. Geburtstag von Michelangelo, sollte in IBM- oder IBM-kompatiblen Personal-Computern ein Monster aktiviert werden, so es sich überhaupt in das Programm einnisten konnte. Was man nie genau weiß. Über Austausch von Daten, Kopieren von Spielen, Verarbeitungsprogrammen und dergleichen können sich vor allem PCs unbemerkt mit Störprogrammen, sogenannten Viren, infizieren. Die Computer-Welt ist beinahe machtlos.

An bestimmten Tagen, Freitag, dem 13. etwa, mischen sich diese virulenten Erzeugnisse übermütiger oder frustrierter Programmierer ungebeten in die Software ein, lassen Herbstlaub fallen, leiern »Tankee Doodle«, auch: »An der schönen blauen Donau« oder fordern – immer sonntags – auf dem Bildschirm kategorisch: »Heut ist Sonntag! Du arbeitest zuviel!« Oft sind die künstlichen Erreger harmlos und lassen einen etwa montags wieder arbeiten. Manche sind gefährlich und gehen an die Substanz. Sie zerstören Programme und Datenbestände. Michelangelo, der die PCs am 6. März – wenngleich nicht so heftig wie erwartet – quälte, zerstörte Festplattenspeicher, allerdings nicht vollständig. Dennoch: Der Bildschirm bleibt dunkel.

1200 Arten von Computer-Viren zählen die Spezialisten, die elektronischen Mikroben haben sich binnen eines Jahres verdoppelt, und im nächsten Jahr werden es wiederum doppelt so viele sein. Weltweit schlossen sich Computerexperten gegen diese Computer-Peiniger in der Gruppe »Caro« zusammen. Sie tauschen – verschlüsselt und per Diplomatenpost – die Charakteristika der neuesten Virus-Varianten aus, um sofort Gegenprogramme zu entwickeln. Zu ihnen zählt Professor Klaus Brunnstein, Informatiker an der Hamburger Universität, der seinen Studenten ein Virus-Forschungszentrum einrichtete.

Brunnstein war es auch, der die deutsche Presse über Michelangelo informierte und dann entnervten PC-Nutzern seine Hilfe anbot: ein Such- und Killerprogramm, mit dem dem heimtückischen Italiener das Handwerk gelegt werden kann. Das ZDF-Magazin WISO berichtete im Februar über das prekäre Ereignis und verschickte über die Verbraucherzentralen bundesweit 100 000 Programmdisketten gegen sämtliche bekannte Viren. Brunnsteins Studenten hatten bis zum Vorabend des 6. März 48 Postsäcke mit Hilferufen gelehrt und insgesamt 18 000 Such- und Killerdisketten kostenlos verschickt.

Sicher war auch Hysterie dabei, meint der Experte Brunnstein vor allem zu den Zeitungsberichten über Michelangelo. Doch in gewisser Weise stelle der Import, »höchstwahrscheinlich aus Taiwan und nicht aus Schweden, wo er 1991 das erste Mal auftauchte«, eine neue Generation von Computer-Viren dar. Der Infektionsweg führt nicht mehr nur über Raub-Kopien oder fremde Spielprogramme, sondern über ganz seriöse Firmen. Die lassen oft Treiberprogramme für Tastaturen oder Mäuse beziehungsweise auch Software auswärts kopieren und vernachlässigen danach offenbar die Kontrolle der Disketten.

Brunnstein schätzt, daß in etwa einem Prozent der fünf bis sechs Millionen in Deutsch-

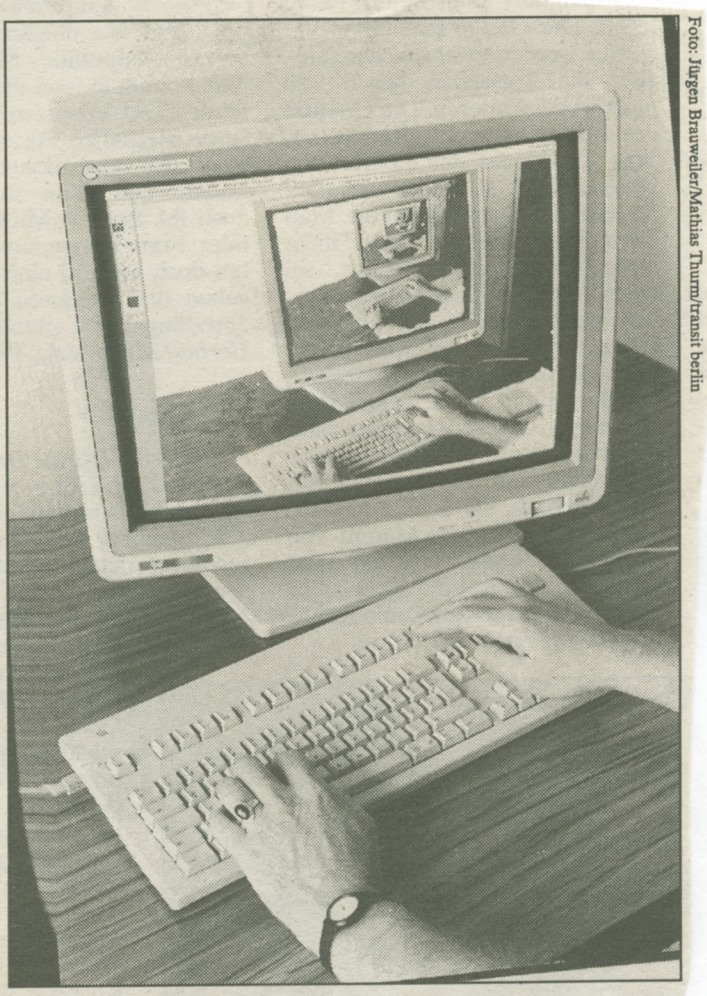


Foto: Jürgen Brauweiler/Mathias Thurm/transit berlin

Die erwartete »Michelangelo«-Epidemie ist ausgeblieben.

land installierten PC das Michelangelo-Virus nistete. Daß am 6. März die meisten mit ihren Computern arbeiten konnten, führt Brunnstein auf die rechtzeitige Warnung und die Vorsorge zurück. Notwendig sei sie zweifelsohne gewesen: Seit der Bekanntgabe über die Presseagenturen UPI und dpa Ende Januar meldeten sich im Hamburger Zentrum bei Brunnstein hundert PC-Besitzer pro Woche, die das Virus fanden.

Insgesamt säßen in mindestens einer halben Million PCs in Deutschland mindestens eine Art dieser elektronischen Quälgeister, sagt Professor Brunnstein. Infiziert waren z. B. rund tausend Datenträger, die das Europäische Patentamt in München im vergangenen Sommer an Behörden versandte. Vor sogenannten Sicherheitsbereichen machen Computerviren nicht halt. 1990, an einem Freitag, dem 13., verschwand in einem »kernenergetischen Betrieb« (Brunnstein) ein Kontrollprogramm. Konkreter wird Brunnstein nicht, und auch das neue, weitgehend noch unbekannte Bonner »Bundesamt für Sicherheit in der Informationstechnik« hüllt sich über solche bedenklichen Vorgänge besser in Schweigen.

»Die PC sind Fahrräder ohne Bremse, auf denen wir sitzen, und nun merken wir, daß es bergab geht«, meint Klaus Brunnstein. Für den Umgang mit Firmendaten, Konstruktionsunterlagen und dergleichen sind Personal-Computer völlig ungeeignet, da die Daten prinzipiell ungeschützt sind. Großrechner sind weitaus weniger anfällig, weshalb vor allem Banken, Versicherungen, große Unternehmen, die damit arbeiten, weniger gefährdet sind. Der öffentliche Bereich aber mit seiner immensen Bürokratie habe sich derart massiv von den PC abhängig gemacht, daß er den Folgen nicht mehr ausweichen könne. Für diesen Teil der Gesellschaft sieht Brunnstein schwarz, zumal die Vernetzung der Systeme untereinander kräftig voranschreitet.

Der letzte Tag X schonte noch einmal unseren Glauben an den technischen Fortschritt. Der nächste steht vor der Tür: Freitag, der 13.

Regine Halentz

Therapie gegen PC-Viren

Shareware-Bibliotheken
Nicht wenige Händler nutzen die Angst vor PC-Viren aus und bieten – vor allem in solchen Kampagnen wie gegen Michelangelo – Anti-Programme für Hunderte von Mark an. Dabei geben sogenannte Shareware-Bibliotheken solche Programme für einige Tage kostenlos ab. Hat der Kunde sie geprüft, erhält er gegen einen bestimmten Beitrag (25 Dollar z. B. für das Programm des amerikanischen Virus-Papstes John McAfee) ein bis zwei Jahre lang regelmäßig aktualisierte Anti-Virus-Versionen.

Anti-Virus-Steckkarte
Sie erweitert die Hardware des PC und verhindert den Zugriff fremder Programme (Viren) auf den Datenträger. Damit wird der reguläre Zugriff des Nutzers umständlicher, erfordert mehr Arbeitsschritte.

6. März 1992
In Deutschland verwüstete Michelangelo in einer Firma im Ruhrgebiet die Daten von 75 PC. Neun weitere, harmlosere Fälle wurden bekannt. In den USA versagten an einer Universität mehrere tausend PC. Reuter gab rund 50 Fälle in Australien bekannt, darunter bei einer Fluggesellschaft und im Bergbau. Erbarmen hatte der Renaissance-Künstler mit seinem Geburtsland: Aus Italien wurde kein einziger Fall gemeldet.

Das Ausmaß der Verseuchung durch Computerviren
Deutschland: 15 Prozent von knapp sechs Millionen PC,
USA: 25 Prozent von 35 Mio PC,
Großbritannien: 30 bis 35 Prozent von vier Millionen PC.

Für IBM-kompatible PC existieren die meisten Viren (1200). Macintosh-Nutzer müssen nur 30 Viren befürchten. Das letzte davon ersannen zwei New Yorker Schüler, die, seltener Fall, von der Polizei überführt wurden.

PC WOCHE, Mo. 16.3.92

KOMMENTAR DER WOCHE

Das Geschäft mit der Angst

Von Wolfram Haase

Hat sich Michelangelo bei Ihnen gemeldet? Nein? Kennen Sie jemanden, dem er ernsthaft Schaden zugefügt hat? Nicht? Wir auch nicht. Geschädigt hat er allenfalls die Reputation sogenannter Sicherheitsspezialisten, die glauben, mit der Angst der Anwender gute Geschäfte machen zu müssen.

Jedesmal wenn bei den Sicherheitsspezialisten Ruhe einkehrt, wird — Gott sei's gedankt — in den Medien, am besten in einem angesehenen TV-Wirtschaftsmagazin, ein Virus plaziert. Dieser befällt dann sicherheitsbewußte, aber kaufunwillige Anwender und reißt sie aus ihrer Lethargie. Im Einzelfall sind die Sicherheitsverantwortlichen zwar samt und sonders davon überzeugt, daß alles Humbug ist und bei ihren PCs nichts passieren wird. Aber ausschließen können sie ein gewisses Restrisiko doch nicht. Also wird rasch der neueste Virenscanner angeschafft, der denn auch bestätigt, daß alles in Ordnung ist. Und so mancher Händler oder Distributor der Antivirenprogramme kann sich die Hände reiben: Er hat seinen Halbjahresumsatz schon im ersten Quartal „im Kasten". Sollte das Geschäft wieder einschlafen — kein Problem, der nächste Virus kommt bestimmt, beispielsweise am Freitag, dem 13.

Zur Ehrenrettung der einschlägigen Branche sei angemerkt, daß die Mehrheit der Unternehmen seriös ist und vor übertriebener Hysterie gewarnt hat. Sie beobachtet mit Mißmut die Marktschreierei einzelner Wichtigtuer, die nicht aufklären, sondern ihr Spielchen mit verunsicherten PC-Anwendern treiben. Und die Seriösen fürchten ob solcher Machenschaften zu Recht um ihre Glaubwürdigkeit. Denn, je mehr die Anwender auf einen derartigen Fehlalarm hereinfallen, desto sorgloser gehen sie danach mit dem Virus-Problem um. Und damit werden sie leichtes Opfer für ganz normale, aber durchaus bedrohliche Viren, die ihre destruktiven Aktivitäten nicht weltweit an einem Tag entfalten, sondern im verborgenen tagtäglich mehr und mehr Schaden anrichten.

Hamburger Abendblatt, Mi. 18.3.92

Immer häufiger dringen Computerviren in fabrikneue Programme ein

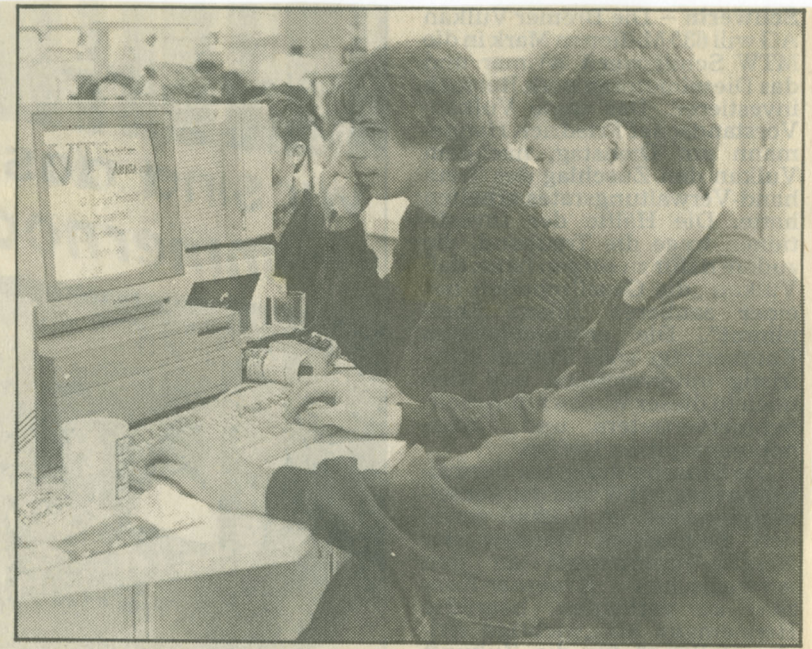
„Kein Wort an die Öffentlichkeit"

Von JONATHAN WEISE und ANDREA KADEN

Hannover – Das Krankenzimmer für virenverseuchte Computer befindet sich in Halle 18 auf dem Hannoveraner Messegelände der CeBIT: Es ist der Stand des Instituts für Informatik der Hamburger Universität. Dem Erste-Hilfe-Team gehören Mitarbeiter des Instituts an sowie Informatik-Studenten. Ihre Patienten sind die Datenträger des 20. Jahrhunderts: Disketten und Festplatten.

Diese Gehirne der Computer werden immer häufiger von Viren infiziert – elektronischen Krankheitserregern. Bei der Suche nach wirksamen Mitteln gegen die programmierten Unpäßlichkeiten wird man in Software-Apotheken reichlich bedient. Doch vor der Therapie heißt es, sich genau zu informieren.

Wie kommt ein Virus in einen Computer? Überträger kann jedes Software-Produkt sein. Vor allem Raubkopien von Programmen trugen bis vor wenigen Jahren die gefährlichen Erreger in gesunde Rechner. Auch fabrikneue Programme sind zuneh-



Hamburger Studenten spüren auf der CeBIT Computerviren auf. Der durch sie verursachte Schaden wird immer größer. Foto: SCHÜTZE

CeBIT'92 HANNOVER
11. – 18. MÄRZ 1992

mend befallen. „Sie infizieren andere Programme auf allen erreichbaren Datenträgern", sagt Gerald Hackenberg, Virus-Forscher bei Siemens. „Dabei wird eine Kopie des Virusprogramms in vorhandene Dateien eingefügt."

In den USA hatten Computer-Experten bereits 1984 erste elektronische Erreger gefunden. Fast spielerischen Charakters stellten sich die Viren als „Trojanische Pferde" oder „Würmer" auf den Bildschirmen dar. „In Deutschland war das 1987 zum erstenmal der Fall", erinnert sich Wolf-Dieter Jahn, wissenschaftlicher Mitarbeiter des Hamburger Informatik-Instituts. Der Virus „Herbstlaub" beispielsweise ließ Buchstaben auf dem Bildschirm herunterfallen, und beim Rot-Kreuz-Virus raste ein Krankenwagen mit Tatütata über alle Buchstaben, die dabei gelöscht wurden. Zu den gutmütigen Einbrechern zählt auch ein erst vor wenigen Wochen in Hamburg aufgetauchter Virus, der auf den Bildschirm die Parole schmiert: „Hafenstraße bleibt!"

Die meisten heute grassierenden Viren wirken zerstörerisch. Sie löschen vorhandene Daten oder vermehren sich so schnell, daß nicht nur einzelne Personalcomputer, sondern sogar ganze Großrechenanlagen überlastet zusammenbrechen. So konnte sich in den USA der „Internet-Wurm" so fleißig selbst kopieren, daß ein ganzes Netzwerk lahmgelegt wurde.

Die Angaben der Computer-Experten über die Zahl der bisher weltweit aufgetauchten Viren schwanken zwischen 1200 und 1500. Täglich kommen durchschnittlich vier neue dazu. Der Aufbau der Virenprogramme wird dabei immer besser. Gleichzeitig wird es immer komplizierter, die Viren zu erkennen.

Die Entdeckung der Viren wird auch dadurch erschwert, daß sich viele selbst verändern können. Die meisten dieser Viren besitzen bis zu vier Milliarden Verwandlungsmöglichkeiten. Nach Schätzungen von Experten sind in Amerika bereits etwa 25 Prozent aller Personalcomputer von Viren befallen, in Großbritannien 35 Prozent, in Deutschland aber nur 15 Prozent. Wolf-Dieter Jahn sagt: „Hierzulande besteht ein höheres Sicherheitsbewußtsein."

Wie hoch der von Viren verursachte Schaden in der Wirtschaft ist, weiß niemand genau. Denn die Betroffenen schweigen meist. „Kein Wort an die Presse", lautet das oberste Gebot, das der amerikanische Virendoktor Allan Solomon allen Unternehmern zu beherzigen rät.

Die beste Vorsorge gegen Computerviren ist Datenhygiene. Fachleute empfehlen, Disketten mit einem Schreibschutz zu versehen, unbekannte Programme zu meiden, Disketten nicht länger als nötig im Laufwerk zu lassen, Backup-Disketten anzulegen und den Zugriff auf das Netzwerk einzuschränken.

Neue Programme sollte man außerdem am besten erst in einem isolierten Quarantänerechner ausprobieren. Haben sich trotz aller Schutzmaßnahmen Viren eingenistet, hilft nur noch der Griff zu einem Anti-Viren-Programm aus der Programm-Apotheke. Diese Anti-Viren-Programme sollen einen Virus aufspüren und vernichten, bevor er ausbrechen und Schäden anrichten kann.

Solche Medikamente, die Namen tragen wie Blocker, Wächter oder Doktoren, gibt es zu Preisen zwischen 200 und 500 Mark im Handel. Wolf-Dieter Jahn warnt aber vor blindem Vertrauen in die Anti-Körper: „Viele Anti-Viren-Programme haben nur ein gutes Escheinungsbild, bekämpfen aber den Virus nicht wirksam."

Auf der CeBIT empfehlen Jahn und seine Kollegen Ratsuchenden das Programm „F-Prot" aus Island, das einige Händler kostenlos anbieten, und „Dr. Solomons Anti-Viren Toolkit" aus Großbritannien, das zwischen 200 bis 300 Mark kosten soll.

Unternehmen rät Jahn, den „Up-Date-Service" zu nutzen, den viele Hersteller von Anti-Viren-Software anbieten: Im Abonnement bekommt der Kunde alle zwei, drei Monate aktualisierte Gegenprogramme.

Der Viren-Notdienst der Hamburger Universität hat auf den sieben Messetagen der CeBIT relativ geruhsame Stunden. „Mit infizierten Programmen ist kein Aussteller zu uns gekommen", sagt Matthias Jänicken am Stand in Halle 18.

Rat suchen vor allem die Besucher. Jänicken bilanziert: „300 bis 400 Gespräche täglich waren keine Ausnahme". Besucher kamen mit Disketten an den Stand. Fast jedes Programm war mit einem Virus infiziert. Matthias Jänickens wichtigster Tip: „Regelmäßige Datensicherung."

386SX zu gewinnen

F9856E

HFL 8,50 LFR 170 ÖS 55,- SFR 7,- DM 7,-

PCPraxis

Großer Windows 3.1 SONDERTEIL

- Was bringt TrueType?
- Mehr Power durch richtige Installation
- Das kann der neue Datei-Manager

Kaufberatung: Festplatten

NEU

Scanner

Sound-Karten

OCR-Texterkennung für wenig Geld

PC Tuning:

So machen Sie Ihren PC fit für MULTIMEDIA

Utility-Trickkiste

PC schneller machen – ohne Hardware

TIPS & TRICKS

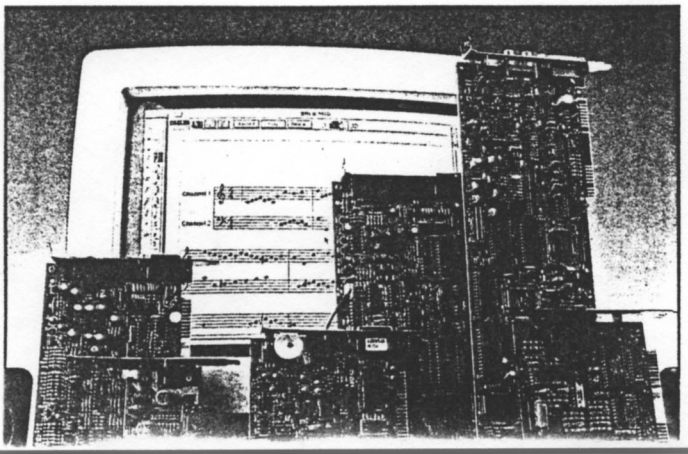
- Makros mit Word
- Works für Windows
- Paradox
- Faxen mit dem PC
- Grafiken mit Excel
- GeoWorks 1.2

INHALT

M A I

Scanner
Möchten Sie Bilder und Texte in den PC einlesen? In unserem Praxistest zeigen wir, was Scanner aus verschiedenen Leistungsklassen können
52

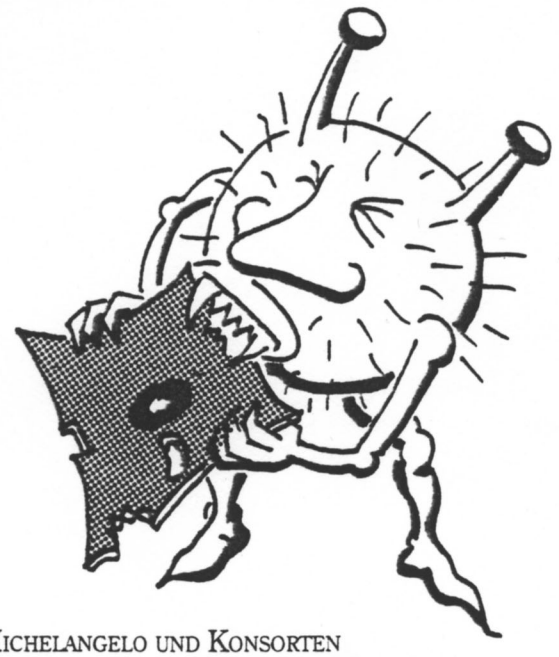
Sound-Karten
Mit Sound-Karten wird der PC richtig Multimedia-fähig - wir haben sechs Karten für Sie getestet
58



AKTUELL

KURZTESTS

PRAXISTEST



MICHELANGELO UND KONSORTEN

Viren – Panikmache oder ernste Gefahr?

Pünktlich zur CeBIT '92 geisterte ein neues Schlagwort durch Fachpresse und andere Medien: Michelangelo. Selbst das Fernsehen nahm sich des Problems an und verunsicherte manchen Anwender, der sich am 6. März kaum traute, den Rechner einzuschalten. Sind Viren eine konkrete Bedrohung oder nur Geschäftemacherei? Wir sind dieser Frage nachgegangen.

Bereits am Vorabend des 6. März beschlich mich ein leichtes Unbehagen. Morgen würde es soweit sein, morgen würde ein gewaltiges Armageddon über die gesamte PC-Welt hereinbrechen – und mein Rechner mittendrin. Oder würde ich verschont bleiben? Die ganze Nacht wälzte ich mich ruhelos in den Kissen, um dann übernächtigt und unrasiert ins Büro zu fahren. Vor meinem geistigen Auge sah ich zerstörte Festplatten, für immer verlorene Texte, wichtige Daten, verschwunden im Nirwana der Bits und Bytes.

Dann war es soweit, der Griff zum Netzschalter des PCs. Der anlaufende Lüfter und das Herunterzählen des Arbeitsspeichers kamen kaum gegen mein lautstark pochendes Herz an. Jetzt geschah es: Das Netzwerk begrüßte mich wie immer mit einem fröhlichen „Guten Morgen", die AUTOEXEC .BAT wurde wie stets abgearbeitet und brachte mich in meine Standardarbeitsumgebung. Keine Spur von Unregelmäßigkeiten oder ungewöhnlichen Vorkommnissen. Holla, noch mal davongekommen!

Aber wie mochte es Kollegen ergangen sein? Schließlich hatte der Virenpapst McAffee von etwa 1,5 Millionen weltweit verseuchten PCs gesprochen. In der Bundesrepublik sollten 6%, also rund 350.000 Personalcomputer mit Michelangelo infiziert sein – zumindest behauptete dies eine Pressemitteilung der Firma boeder in Flörsheim.

Meine Rundrufaktion bei Kollegen, Firmen und Presseagenturen brachte allerdings kau etwas zutage. Überall wur gemeldet: „Business as usua Einzig eine Werbeagentur w tatsächlich betroffen, die D ten konnten aber Dank ein Backups problemlos gerett werden. Jetzt war ich natürli verwirrt. Wo waren denn die Katastrophen, wo war d wirtschaftliche Schaden Milliardenhöhe, den Pessin sten vorausgesagt hatte

Dr. Viktor Mayer-Schönberger, Generalbevollmächtigter Ikarus Software

Michelangelo regt den Zuschauer zur Phantasie an: der alte Meister ebenso wie sein computer-viraler Konterpart. Selbsternannte Experten und auf so manche schnelle Mark bedachte Software-Hersteller wurden nicht müde, die große Katastrophe heraufzubeschwören. Von 5 Millionen verseuchten PCs war die Rede. Kurz vor dem berüchtigten 6. März riefen hunderte durch diese Horrormeldungen verunsicherte PC-Anwender in unserem Unternehmen an, um die Lage zu klären. Keiner wollte so recht glauben, daß Michelangelo nicht das Ende des PCs bringen wird.

Und dann kam der 6. März und ging vorüber, ohne daß die Katastrophe hereinbrach. Bei uns trafen lediglich 9 Michelangelo-Meldungen ein. Am 6. März hielten wir auch telefonisch ständig Kontakt mit der NCSA, der amerikanischen Dachorganisation für Virenschutz und Datensicherheit. Auch dort trafen die Schadensmeldungen nur äußerst spärlich ein: einige betroffene PCs in Australien, ein Dutzend in England, unter 10 in Holland. Tragisch ist dabei nur der Fall des Anwenders, der das Systemdatum vor dem 6. März einen Tag zurücksetzte und dann am 7. März beim Hochfahren vergaß, das Datum zu ändern. Ihn erwischte Michelangelo mit einem Tag Verspätung, unvorbereitet und vernichtend.

Überrascht von den Schadensmeldungen war keiner von uns. Michelangelo ist – im Gegensatz zu wilden Gerüchten – als Boot-Sektorvirus nicht leicht zu bekommen (Hand aufs Herz: Wann haben Sie zum letzten Mal von einer unbekannten Diskette gebootet?), seine Verbreitung daher gering. Und der Rummel um den Virus war nicht mehr als das: ein Rummel.

Freilich: Auch wenn nichts passiert ist und lediglich ein paar Panikmacher in der Branche ein gutes Geschäft gemacht haben, bleibt doch ein bitterer Nachgeschmack. Denn mit der zerplatzten Seifenblase der Michelangelo-Katastrophe ist leider auch ein Gutteil der Glaubwürdigkeit für Virenvorsorge dahin. Zu viele PC-Anwender haben die eindimensionale Taktik mancher Hersteller erkannt und beschlossen, daß Virenschutz nicht so wichtig ist. Verdenken kann man das dem Anwender nicht, auch wenn er sich damit in einer gefährlichen Sicherheit wiegt.

AUSWAHL VON VIRENSCHUTZPROGRAMMEN

Produkt	Hersteller/Vertrieb	Preis
Central Point Anti Virus 1.1	Central Point Software, München	DM 341,-
Norton Anti-Virus 2.0	Symantec, Düsseldorf	DM 299,-
Dr. Solomons Anti-Virus Toolkit	MSPI, München	DM 299,-
Certus Novi	Megabyte, München	DM 345,-
McAfee V86	u.a. Deutsche Software Bibliothek, Gröbenzell	Kopiergebühr

Oder waren durch die Warnmeldungen der Medien die Anwender sensibilisiert und hatten mit Hilfe von Virenschutzprogrammen Michelangelo frühzeitig eliminiert?

Etwas war auf jeden Fall dran an Michelangelo. Erstmals sollten hier auch Originalprogramme in größeren Mengen mit diesem Virus verseucht worden sein, so daß große Mengen dieser Disketten in Umlauf gekommen seien. Da es sich bei Michelangelo aber um einen Bootsektor-Virus handelt, konnte die Gefahr eigentlich nur bei Betriebssystemen wie zum Beispiel DOS zu suchen sein, da in der Regel nur hier der Rechner von Diskette hochgefahren wird.

Branchenriesen wie Microsoft veranlaßte das sogleich zu Pressemeldungen, daß bei ihren Produkten nicht mit einem Befall zu rechnen sei. Geschäftsführer Dr. Jochen Hainк: „MS-DOS wird definitiv nicht mit Viren ausgeliefert."

Eindeutig festzuhalten bleibt, daß das Medienspektakel „Michelangelo" die Verkäufe von Virenschutz-Programmen immens in die Höhe getrieben hat. Daß Viren eine konkrete Bedrohung darstellen, soll gar nicht geleugnet werden. Aber gerade Michelangelo ist als Bootsektor-Virus nicht so schnell zu bekommen. Außerdem: es gibt eine ganze Reihe von Viren, die an ein bestimmtes Systemdatum gebunden sind und die in ihrer Gefährlichkeit in nichts hinter Michelangelo zurückstehen. Wer hat zum Beispiel vom „Freitag dem 13. Virus" gesprochen, der mitten zur CeBIT-Zeit sein Unwesen trieb und kaum wahrgenommen wurde? Steffen Wernery, einer der Sprecher des Hamburger Chaos Computer Club, unterstellt gar eine Irreführung des Verbrauchers, in dem bei jedem neuen Virus durch Panikmeldungen die Verkaufszahlen für Entseuchungsprogramme und Fachinformationsdienste in die Höhe getrieben würden.

Was kann der Anwender tun, der mit teils unseriösen Methoden vor einer zwar vorhandenen, aber oft überschätzten Gefahr geängstigt wird? Der Einsatz eines Virenscanners bzw. eines Programms, das den Boot-Sektor überwacht, ist auf jeden Fall zu empfehlen. Auch mich hat eine solche

Was ist Michelangelo?

Michelangelo ist ein speicherresidentes Bootvirus-Programm, das zwar einige sehr raffinierte Strategien verwendet, um sich zu verbreiten und auch über ein nicht unerhebliches Zerstörungspotential verfügt, aber streckenweise so primitiv programmiert ist, daß eine Entdeckung auch für einen Laien problemlos möglich ist. Der Virus schreibt sich bei einem Boot-Vorgang von einer infizierten Disk in den Partitionssektor einer vorhandenen Festplatte und sichert den ursprünglichen Inhalt im Sektor Sieben.

Von nun an ist der Virus nach jedem Boot-Vorgang von der Festplatte im Speicher aktiv und fängt die Datenträgerzugriffe ab. Entdeckt es bei einem Zugriff auf eine Diskette einen nicht infizierten Boot-Sektor, so wird dieser Boot-Sektor (je nach Diskettentyp) im Sektor 3 oder 14 auf Seite 1 gesichert und dann vom Virus überschrieben. Hat die Systemuhr beim Booten das Datum 6.3., so wird die gesamte FAT der Festplatte gelöscht. Die Daten sind zwar noch vorhanden, aber das Restaurieren lohnt sich in den seltensten Fällen.

Erkennung im Arbeitsspeicher:

Rufen Sie den Befehl MEM oder CHKDSK auf. Beide Kommandos liefern Ihnen als Ergebnis unter anderem die Größe des Arbeitsspeichers. In einem System mit 640 KB oder mehr Hauptspeicher (und das sind heute 99,9% aller PCs) lautet das Ergebnis 655.360 Bytes. Sollten Sie eine Differenz von ca. 2 KB feststellen, so liegt der Verdacht nahe, daß sich ein Virus im Arbeitsspeicher befindet.

Um diesen Verdacht zu erhärten – es gibt nämlich noch einige andere Gründe, warum der Arbeitsspeicher reduziert wird – sollten Sie einen Virenscanner einsetzen. Aber auch mit Programmen wie PC Tools oder Norton Utilities kann man die Hex-Kennung des Virus suchen (als eine Zeile eingeben):

581F9C2EFF1E0A009CE80B009
DCA0200581F

Was ist zu tun?

Booten Sie zunächst Ihren Rechner mit einer schreibgeschützten Original-Diskette. Bei Disketten ist die Handhabung nun recht einfach: Entweder wenden Sie das Kommando SYS auf die betroffene Disk an – dadurch wird ein neuer Bootsektor auf die Disk geschrieben – oder Sie kopieren alle Files mit XCOPY /S in ein DUMMY-Unterverzeichnis Ihrer Festplatte, formatieren dann die Disk und kopieren danach alle Files wieder zurück.

Problematischer wird es bei einer infizierten Festplatte, denn das einzige DOS-Programm, das in der Lage ist, den Sektor Null einer Festplatte zu lesen oder zu schreiben ist FDISK – und neu geschrieben wird der Sektor nur dann, wenn Sie alle Partitionen löschen und danach neu anlegen. Das heißt aber auch: Ein komplettes BACKUP und RESTORE sind notwendig.
(Ralf Burger)

Dr. Klaus Brunnstein,
Professor f. Anwendungen der Informatik,
Universität Hamburg

Die derzeit rund 1.300 Computer-Viren auf PCs stellen eine spürbare, wenn auch selten massive Bedrohung der Informationsverarbeitung in Unternehmen, Behörden, Organisationen, Schulen sowie zuhause dar. Immerhin gelten nach einigen Erhebungen etwa 25% der US-PCs als verseucht, während die Rate hierzulande bei 10 bis 15% liegen dürfte. Bei Überprüfungen werden oft Viren wie Stoned, Cascade oder Jerusalem gefunden.

Bis zum Herbst 1991 galt die Erkenntnis, daß selber schuld sei, wer Viren habe: Viren wurden vorwiegend über illegal oder „billig" erhaltene Disketten übertragen. Als jedoch im Dezember 1991 mehrere kommerzielle Disketten sowie neu konfigurierte PC-Systeme in USA und Europa mit dem erstmals im Februar 1991 in Australien entdeckten Michelangelo-Virus verkauft wurden, hielten die Computer-Notfall-Teams in USA und Deutschland eine Warnung der Benutzer für geboten.

Die Warnung wurde von interessierter Seite erheblich übertrieben, etwa als J.McAfee von 1,5 Mio. befallener PCs redete. Kein Wunder, daß DV-unerfahrene Journalisten dies weiter aufbauschten. Die Mahnungen deutscher Stellen, daß höchstens 0,5 bis 1% der 5 Mio. PCs in Deutschland betroffen seien, wurden dagegen nicht berichtet.

Immerhin hat die Hysterie viele Anwender zur Überprüfung ihrer Programme und – oft erstmalig – zur Datensicherheit bewegt. In rund 10.000 PCs wurden nach BSI-Angaben der Virus rechtzeitig entdeckt, so daß am 6. März nur rund 1.500 Abstürze erfolgten. Die erfreulich besonnene Reaktion vieler Anwender ist die schönste Belohnung für die Warner, die sich aber jetzt dem medialen Zorn für eine entgangene Katastrophe ausgesetzt sehen. Denn: Only Bad News Is Good News (Presse-Grundsatz).

Software schon einmal vor einem Virus bewahrt. Jetzt müssen Sie aber nicht gleich zum teuersten Profi-Programm greifen, das zu haben ist.

Auch im Shareware-Bereich bieten viele Anbieter gute Virenschutzprogramme an, die Sie für ein paar Mark Kopiergebühr bekommen können. Leider sind solche Programme immer nur so gut wie ihre Aktualität, das heißt, um regelmäßige Updates kommen Sie kaum herum. Wenn Sie sich jedoch nicht in Mailboxen einloggen, Ihren PC alleine nutzen und nur Originalsoftware benutzen, habe ich einen noch besseren Tip: Sparen Sie sich das Geld für eine Virenschutz-Software, denn in diesem Fall ist die Wahrscheinlichkeit, sich einen Virus einzufangen, wirklich nahezu gleich Null.

Wenn Sie mehr über Viren wissen wollen, können Sie bei der Deutschen Software Bibliothek, Gröbenzell, kostenlos eine Info-Broschüre anfordern (solange der Vorrat reicht). (haf) ■

Viren erkennen mit Batch-Dateien

Auch mit den einfachen Mitteln der DOS-Oberfläche kann effektiver Virenschutz betrieben werden. Unser Leser Andreas Eickmeier aus Lemgo zeigt Ihnen wie.

Ein Virus setzt sich häufig in EXE- oder COM-Dateien fest, hierbei verändert sich die Größe der Dateien. Mit den Programmen ERST.BAT werden die Größen der EXE- und COM-Dateien mit Hilfe des DIR-Befehls in die Dateien Temp.$$$ und Memo.$$$ geschrieben. Hierzu müssen die Verzeichnisse und Unterverzeichnisse der Festplatte in den Dateien ERST.BAT und VERG.BAT in die Klammern der For..in..do-Schleife eingetragen werden. Der COPY-Befehl faßt die Dateien Temp.$$$ und Memo.$$$ zusammen. Anschließend werden die Zeilen, die den String EXE und COM besitzen, in die Datei MEMO.TXT geschrieben.

Das Programm ERST.BAT braucht nach dem ersten Start nur wieder gestartet zu werden, wenn neue Unterverzeichnisse hinzugekommen sind. Beim Aufruf von VERG.BAT werden die Größen der EXE- und COM-Dateien in die Datei MEMO2.TXT eingetragen. Unterschiede werden nun Dank des DOS-Befehls FC aufgezeigt.

Auch die bekannten Viren-Codes können mit einer Batch-Datei gesucht werden. Dazu müssen jedoch die üblichen Hex-Werte mit einer Tabelle in ASCII-Werte umgewandelt werden. Bei den meisten Codes muß außerdem in Etappen nach Teilstücken der Virenkennung gesucht werden, weil es für das Hex-Zeichen „00" keine Entsprechung in ASCII gibt. Hier muß dann ein Schnitt gemacht werden. Die Datei SCAN.BAT sucht im aktuellen Unterverzeichnis nach Viren.

erst.bat

```
for %%x in (dos dos\bat) do
   dir c:\%%x\*.exe
   >>temp.$$$
for %%x in (dos dos\bat) do
   dir c:\%%x\*.com
   >>memo.$$$
copy temp.$$$ + memo.$$$
find /n „EXE" temp.$$$
   >memo.txt
find /n „COM" temp.$$$
   >>memo.txt
del memo.$$$
del temp.$$$
echo ende
```

verg.bat

```
for %%x in (dos dos\bat) do
   dir c:\%%x\*.exe
   >>temp.$$$
for %%x in (dos dos\bat) do
   dir c:\%%x\*.com
   >>memo.$$$
copy temp.$$$ + memo.$$$
find /n „EXE" temp.$$$
   >memo2.txt
find /n „COM" temp.$$$
   >>memo2.txt
fc /c /l memo2.txt
   memo.txt | more
del memo.$$$
del temp.$$$
```

scan.bat

```
for %%b in (*.com) do find /n
   „%1" %%b
for %%b in (*.exe) do find /n
   „%1" %%b
```

DATENBANK

Microsoft kauft Fox Software

Die Windows-Datenbank Cirrus geistert nach wie vor durch die Medien, Alpha-Versionen sind bereits im Umlauf. Jetzt möchte Microsoft nicht nur ein Stückchen vom Datenbank-Kuchen, sondern gleich die dominierende Rolle übernehmen. Unterstützen soll dabei das Know-How der Firma Fox Software, die mit FoxPro 2.0 ein innovatives Produkt auf dem Markt hat, das dBase das Fürchten lehren soll. Die Übernahme durch Microsoft soll kurz bevorstehen, es geht um Aktien im Wert von 173,4 Millionen Dollar. Die größte Übernahme, die Microsoft je getätigt hat, bringt Bill Gates endlich in eine starke Position im Datenbankmarkt, wo man bislang keine Rolle gespielt hatte. (haf) ■

Nach der Medien-Kampagne um Michelangelo

Wie Anwender und Hersteller mit Computerviren umgehen sollten

Nach Jerusalem und Datacrime löste im Februar 1992 der Michelangelo-Virus eine dritte Medienwelle aus. Obwohl größere Schäden verhindert wurden, verbreiteten Presse, Funk und Fernsehen nach dem 6. März 1992 Kritik an denjenigen, die eine sachliche Warnung ausgesprochen hatten. Günter Mußtopf* beschreibt an Beispielen die von Michelangelo verursachten Schäden, setzt sich kritisch mit den Auswirkungen der Medienkampagne auseinander und unterbreitet Vorschläge für einen wirksamen Schutz vor Sabotage-Software.

Die Warnung vor Datenverlust durch das Michelangelo-Virus war ein voller Erfolg: Viele mit diesem Festplattenkiller verseuchte PCs konnten rechtzeitig gesäubert werden. Dadurch fielen nach den Ermittlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) am 6. März in Deutschland weniger PCs aus als befürchtet worden war. Die Folgen der spektakulären Berichterstattung vor und nach dem 6. März bedürfen aber einer kritischen Analyse, um daraus konstruktive Vorschläge für künftige vorbeugende Maßnahmen abzuleiten.

Michelangelo problemlos erkennbar

Das zur Stoned-Familie gehörende Michelangelo-Virus, im Februar 1991 in Australien entdeckt, verfügt über keinerlei bemerkenswerte Eigenschaften. Es ist nur eines von heute über 1500 DOS-Viren und besitzt weder spezielle Tarnkappen-Mechanismen noch bereitet seine Erkennung Probleme. Da es durch keinerlei Effekte vor seinem Aggressionsdatum auf sich aufmerksam macht, konnte es sich in der vergleichsweise langen Inkubationszeit von etwa elf Monaten international verbreiten, so daß am 6. März 1992 Tausende von PC-Massenspeichern durch seinen Ausbruch bedroht waren.

Gute Viren-Suchprogramme erkennen das Michelangelo-Virus schon seit dem Frühsommer 1991. Obwohl er nur durch einen Kalt- oder Warmstart von einer infizierten Diskette in den Speicher und den Partition-Record einer Festplatte gelangen kann, waren weltweit viele PCs infiziert. Das BSI schätzte auf der Basis einer Umfrage, daß in Deutschland mindestens 10 000 PCs verseucht waren. Die zahlreichen Anrufe bei der Hot-line des Viren-Service Hamburg bestätigten diese Angabe. Nicht nur private Anwender, Freiberufler oder kleine Unternehmen, sondern auch große Firmen wie Siemens-Nixdorf und die deutsche BP, die weitgehende Maßnahmen zum Schutz gegen Viren eingeführt haben, berichteten vom Auftreten des Michelangelo-Virus in ihrem Haus.

Boot-Viren können sich weder in PC-Netzwerken ausbreiten noch aus Mailbox-Systemen direkt importiert werden. Das wirksamste Transportmittel für die internationale Ausbreitung waren deshalb infizierte Originaldisketten, beispielsweise mit Treibern für VGA-Karten, Mäuse oder Modems. Shareware- oder Public-Domain-Software trug nach bisherigen Erkenntnissen allerdings nicht zu dieser Entwicklung bei.

Dagegen förderte fehlende oder mangelhafte Prüfung der produzierten Disketten durch einige Kopieranstalten und kommerzielle Hersteller die internationale Verbreitung des Virus. In einem Fall setzte beispielsweise eine Kopieranstalt einen Viren-Scanner zur Prüfung ein, der bereits anderthalb Jahre alt war und Michelangelo nicht erkennen konnte. Von dem Auftraggeber wurden deshalb von September 1991 bis Januar 1992 Tausende permanent schreibgeschützte Maustreiber-Disketten inklusive Michelangelo versandt. Natürlich trugen auch PC-Anwender zur Verbreitung bei: Das Virus kopiert sich auf jede nicht schreibgeschützte Diskette im Laufwerk A, auf die von einem infizierten PC zugegriffen wird. Dadurch kann das Virus auch Datendisketten für seine Ausbreitung nutzen.

Zwei Fälle aus der täglichen Praxis der Viren-Hot-lines verdeutlichen die Wirksamkeit der Vorsorge und die schädlichen Folgen von zuviel Vertrauen: Kassenärztliche Vereinigungen (KV) erhalten in zunehmenden Maße die Abrechnungsdaten von Ärzten auf Disketten. Eine KV, die alle eingehenden Disketten auf Viren prüft, stellte am 5. März fest, daß eine an diesem Tag eingegangene Datendiskette mit Michelangelo infiziert war. Der Arzt konnte noch rechtzeitig gewarnt werden, so daß am 6. März bei ihm kein Schaden entstand.

Eine Druckerei, die grundsätzlich nur Lizenzprogramme einsetzt und stets Originaldisketten für die Installation benutzt, fühlte sich vor Viren

*Günter Mußtopf ist als aktiver Virenschützer Direktor des European Institute for Anti-Virus Research und Geschäftsführer des Computerfachverlages Percomp in Hamburg.

sicher — eine Prüfung fand deshalb nicht statt. Am 6. März schlug Michelangelo zu und löschte eine Festplatte, auf der die Kundendatenbank des Unternehmens abgelegt war; leider besaß das Unternehmen keine aktuelle Datensicherung.

Warnungen verhinderten größere Schäden

Durch die Warnung in den Medien wurden sehr viele PCs vor dem Ausbruchsdatum auf Viren geprüft, so daß infizierte Systeme rechtzeitig gesäubert werden konnten. In den Virus-Test-Zentren an den Universitäten Hamburg, Karlsruhe und beim BSI in Bonn gingen etwa 1000 Meldungen ein.

Eine Umfrage des BSI bei den genannten Instituten in der Woche vom 10. März ergab, daß am 6. März etwa 50 und in der darauffolgenden Woche noch einmal 50 Schäden durch Michelangelo gemeldet wurden. Die Dunkelziffer dürfte in diesem Fall allerdings sehr hoch sein: Nur sehr wenige Betroffene sind nach einer solchen Medienwelle aus Angst vor einer Blamage bereit, Schäden durch das Michelangelo-Virus zuzugeben.

Aus dem Raum Zürich wurde bekannt, daß eine Michelangelo-Variante bereits am 1. März Festplatten zerstörte. Aus USA kam die Meldung, daß das Virus teilweise bereits am 5. März aktiv gewesen sei, weil einige PCs ein Kalenderprogramm enthielten, das kein Schaltjahr kennt. Nicht zuletzt wurden Varianten gefunden, deren Aggressionsdatum auf einen späteren Zeitpunkt abgeändert war.

Viren-Warner sitzen zwischen zwei Stühlen

Michelangelo hat sich nicht nur in Deutschland stark ausgebreitet. Beispielsweise wird in Meldungen aus Südafrika von 1000 durch Michelangelo geschädigten PCs berichtet.

Die Meldungen von „dpa", die auf die Gefahr aufmerksam machten, waren weitgehend fachlich richtig. Leider traf dies aber für andere Medien nicht zu.

Die Phantasie von Journalisten und Redakteuren blühte. Unqualifizierte Aussagen von Interview-Partnern verunsicherten die PC-Anwender zusätzlich.

Trotzdem hatten die vielen Meldungen über das Virus eine weitgehend positive Wirkung. In vielen Unternehmen wurde „Frühjahrsputz" gemacht. Dabei fand man nicht nur viele Michelangelo-Viren, sondern auch andere mehr oder weniger harmlose Sabotage-Programme wurden entfernt.

Die Autoren von Viren-Warnungen setzen sich zwischen zwei Stühle:

Ist die Warnung erfolgreich, das heißt werden Schäden weitgehend verhindert, stellen Besserwisser hinterher fest, daß diese Aktion unnötig war oder anderen Zwecken diente.

Hat die Warnung dagegen keinen Erfolg oder wird nicht gewarnt, verursacht das Virus also größere Schäden, wird den Fachleuten Unfähigkeit nachgesagt.

Die Warnung vor Michelangelo war voll und ganz berechtigt. Die durch eine Umfrage gestützte Schätzung des BSI der vor dem 6. März infizierten PCs bestätigt die große Gefahr. Selbst wenn man davon ausgeht, daß im Fall einer fehlenden Warnung kein allgemeiner Daten-GAU aufgetreten wäre, wurden doch größere Schäden verhindert.

Ursache für die Kritik an Viren-Warnungen ist nicht zuletzt, daß der sachliche Gegenstand einer solchen Meldung häufig mit den darauf basierenden spekulativen Hochrechnungen der möglichen Schäden verwechselt wird. Journalisten tun mit dem Versuch, Daten über die Anzahl infizierter PCs und die erwartete Höhe möglicher Schäden zu ermitteln, ein übriges. Die nach einer derartigen Medienwelle sicher notwendige kritische Analyse der präventiven Maßnahmen sollte primär prüfen, ob die Warnung größere Schäden verhindern konnte.

Verharmlosung birgt Gefahren

Eine Verharmlosung der Virengefahr nach der Michelangelo-Medienwelle birgt Gefahren. Der alte Schlendrian wird sich in vielen Unternehmen schnell wieder ausbreiten. Schlimmer noch: Viren-Autoren haben aus der Michelangelo-Welle sicher gelernt, daß die Verbreitung eines Virus unübersehbar gefördert wird, wenn möglichst viele Monate zwischen dem Aussetzen eines Virus und der ersten Aggression verstreichen. Ausgefeilte Tarnkappen-Eigenschaften ebenso wie Techniken, die das zuverlässige Erkennen und Analysieren von Viren erschweren dürften, werden sich bei weiteren Virenwellen bemerkbar machen. Der Zeitbedarf für die Erweiterung von Werkzeugen zur Virenbekämpfung und die Geschwindigkeit von Viren-Scannern wird sich zuungunsten der PC-Anwender spürbar verschlechtern. Die Vorwarnzeit verkürzt sich dadurch wesentlich, und der Zeitbedarf für Abwehrmaßnahmen steigt.

Bedacht werden muß auch, daß viele PC-Anwender aus den Medien zunächst furchterregende Berichte vorgesetzt bekamen und nach dem Schreckenstag aus den gleichen Quellen erfuhren, daß dies nur eine gezielte Kampagne war, um die Umsätze von Viren-Scannern zu erhöhen. Tritt künftig ein neues besonders aggressives Virus auf, dürfte deshalb eine Warnung bei vielen PC-Anwendern — in Erinnerung an Michelangelo — auf taube Ohren stoßen.

Einen perfekten Schutz gegen Viren gibt es bisher nur in der Werbung einiger Anbieter von Anti-Viren-Produkten.

FORTSETZUNG AUF SEITE 56 ►

Wie Anwender und Hersteller ...

► FORTSETZUNG VON SEITE 55

Sie behaupten beispielsweise, daß sie auch alle neuen, bisher noch unbekannten Viren erkennen und entfernen können. Tatsächlich aber sind Viren-Forschungsgruppen und Hersteller von Anti-Viren-Produkten heute immer noch gezwungen, neue Sabotage-Programme sowie deren Techniken zum überwiegenden Teil manuell zu analysieren und die eigenen Verfahren beziehungsweise Werkzeuge entsprechend zu erweitern. Sie bleiben so lange in dieser unangenehmen Verteidigungsstellung, bis neue Hardware-Architekturen und sichere Betriebssysteme beim Endanwender verfügbar sind. In der Diskussion künftiger Gefahren darf nicht vergessen werden, daß Viren nur eine Abart von Sabotage-Software darstellen. Würmer und Trojanische Pferde sowie verwandte Anomalien sollten ebenfalls Berücksichtigung finden. Würmer können beispielsweise in Netzwerken für den Transport von Viren benutzt werden.

Der Wettlauf von Virus-Test-Zentren, Herstellern und Anwendern gegen die Viren-Autoren hat vor dem Erreichen einer endgültigen Lösung nur Aussicht auf Erfolg, wenn nicht nur der Software-Hygiene mehr Beachtung geschenkt wird, sondern auch eine konstruktive Kooperation zwischen Forschungsgruppen, Herstellern und Anwendern Schritt für Schritt aufgebaut wird. Die beiden zu diesem Zweck gegründeten Organisationen Caro (Computer Anti Virus Researcher Organization) und Eicar (European Institute for Anti-Virus Research) werden dieses Bestreben nach besten Kräften fördern.

Unabhängig von den internationalen Bemühungen der einschlägigen Forschungsgruppen können aber auch erfahrene Fachleute einen wichtigen Beitrag zur wirksamen Bekämpfung von Viren leisten. Einige konkrete Vorschläge, die baldmöglichst von den angesprochenen Gruppen in Angriff genommen werden sollten:

— Kopieranstalten und Hersteller müssen die Endkontrolle von Disketten auf Viren wirksamer durchführen. Parolen wie „Setzen Sie nur Originaldisketten etablierter Hersteller ein" oder „Verwenden Sie keine Public-Domain- beziehungsweise Shareware-Programme" sind zwar aus wirtschaftlicher Sicht verständlich, reichen aber bei weitem nicht aus.

— Hersteller sollten ihre Maßnahmen zur Qualitätssicherung während der Entwicklung und vor der Auslieferung offenlegen. Die Forderungen des BSI an Originaldisketten, sollten erfüllt werden.

— Disketten können beim Kopiervorgang nicht mehr infiziert werden, wenn Kopieranstalten keine MS-DOS-Systeme einsetzen.

— Nicht nur die Master-Disketten, sondern auch die von der Kopieranstalt gelieferten Kopien müssen vom Hersteller auf Viren geprüft werden.

— Der Standard-Lieferumfang von PCs sollte erweitert werden: Ein guter Viren-Scanner, der die BSI-Forderungen erfüllt, gehört zu jedem PC. Die laufende Aktualisierung kann durch einen Update-Vertrag sichergestellt werden, den der PC-Anwender abschließen muß.

— Das mit dem PC gelieferte Handbuch sollte eine leicht verständliche Einführung in die Datensicherheit und die Bekämpfung von Viren enthalten.

PC-Anwender können den Kampf unterstützen

Diese Forderung im Interesse der Sicherheit der Benutzer ist — analog dazu — bei anderen technischen Geräten bereits selbstverständlich geworden: Sicherheitsgurte gehören zu jedem PKW. Für die PC-Hardware müssen — ebenso wie für jedes andere elektrische Gerät — die Vorschriften des VDE und des FTZ erfüllt werden. Sicher dürfte es mittelfristig möglich sein, PC-Hersteller durch gesetzliche Vorschriften zur Lieferung von Viren-Suchprogrammen zu zwingen — eine freiwillige und schnelle Erfüllung dieser Forderung wäre allerdings wünschenswert.

Auch PC-Anwender können die Bekämpfung von Viren wirksam unterstützen. Das regelmäßige Sichern der Daten von der Festplatte und das Prüfen fremder Disketten auf Viren wird bei vielen Anwendern allmählich zur Routine. Darüber hinaus können sie weitere Beiträge leisten:

— Wird der Boot-Sektor jeder fremden, nicht schreibgeschützten Diskette vor ihrer ersten Benutzung auf dem eigenen PC durch einen virenfreien „Standard"-Boot-Sektor überschrieben, haben Viren, die sich ausschließlich durch den Boot-Sektor ausbreiten, keine Chance mehr.

— Jede fremde Diskette — gleichgültig, ob sie bootfähig ist oder nicht — sollte vor der ersten Benutzung mit einem aktuellen Viren-Scanner geprüft werden. Dies gilt auch für Disketten, die nur Daten enthalten.

— Jede Diskette, die für einen anderen PC-Anwender gedacht ist, sollte mit einem aktuellen Scanner geprüft werden.

— Hersteller und Anwender sollten Lieferanten, Partner und Kunden schnell über Viren-Unfälle informieren: Wird ein Virus gefunden, so sollten sofort alle Unternehmen und Personen in Kenntnis gesetzt werden, mit denen Disketten ausgetauscht oder die Disketten erhalten haben.

Der Wahrheitsgehalt der in den Medien über Michelangelo verbreiteten Infomationen war sehr unterschiedlich. Die meisten PC-Anwender sind jedoch kaum in der Lage, die Richtigkeit solcher Meldungen zu beurteilen. Für eine Notsituation müssen deshalb andere Wege gefunden werden. PC-Anwender korrekt zu informieren. Die Forschungsgruppen könnten in Zusammenarbeit mit Eicar, dem BSI und den Notfall-Zentren (CERT) die Informationen über die Bekämpfung eines neuen Virus kritisch prüfen und aufbereiten. Da konventionelle Telefon-Hot-lines — wie die Erfahrungen mit Michelangelo zeigen — zu schnell überlastet sind, bieten sich für diese Aufgabe elektronische Medien an:

— Ein telefonischer Ansagedienst der Telekom kann rund um die Uhr Gefährdete und Betroffene informieren.

— Der Dienst läßt sich auch durch einen kostenpflichtigen Fax-Service ergänzen.

— Selbstverständlich kann auch ein Service per Electronic Mail und Btx eingerichtet werden.

Michelangelo und der 6. März haben trotz des Medienwirbels bewiesen, daß keinerlei Anlaß zur Panik besteht. Das BSI will zusammen mit Herstellern, Anwendern, Instituten und Organisationen Empfehlungen für die Bekämpfung von Computer-Viren und verwandten Anomalien zusammenstellen. ◆

Viren

Erste Forschungsarbeit aufgetaucht

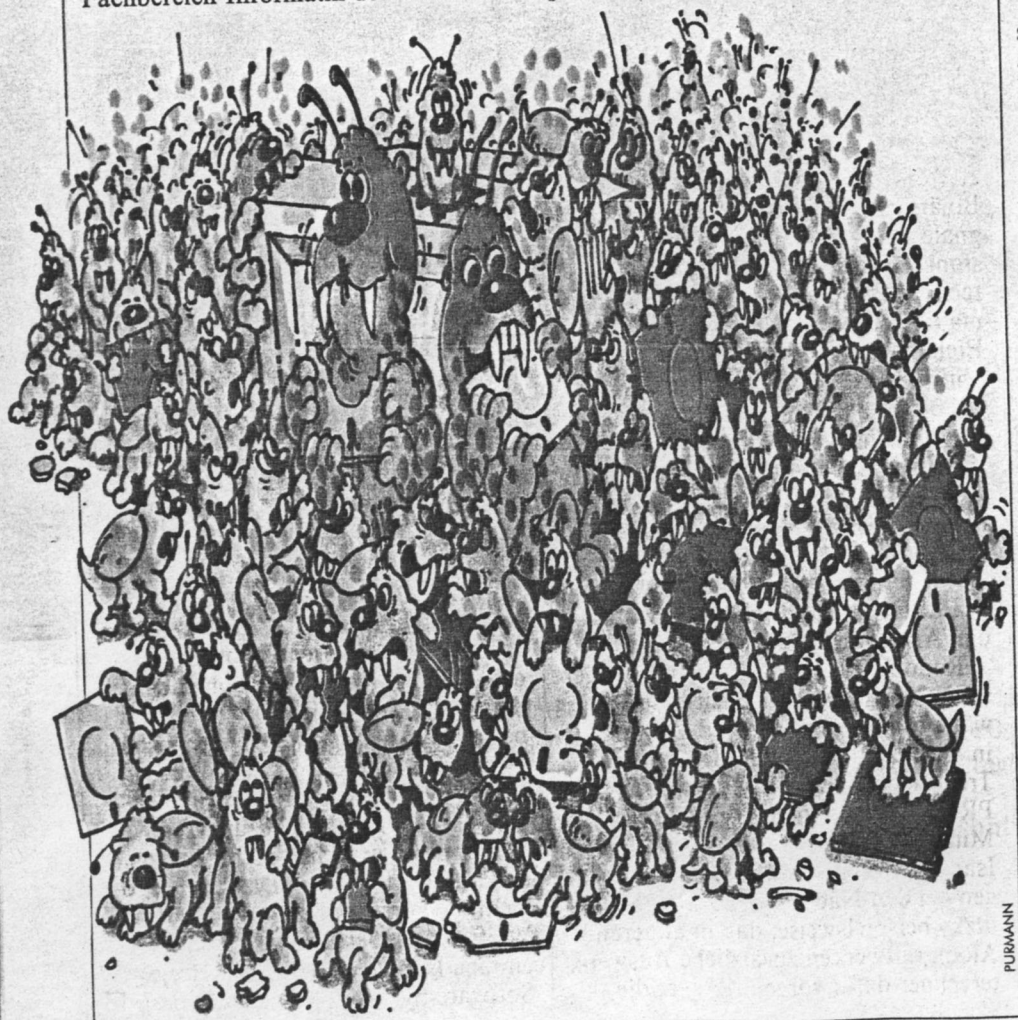
Fred Cohen gilt seit 1984 als Entdecker von Computerviren. Doch schon 1980 zog ein deutscher Informatikstudent die Analogie zwischen lebenden Viren und mutierenden, selbstreproduzierenden Programmen.

Programmierte Vermehrung

Selbstreproduzierende Programme kommen als Träger von Leben auf Computerebene durchaus in Frage." Dieser ungewöhnliche Satz stammt aus einer Diplomarbeit, die über zehn Jahre als unzugänglich galt und CHIP nun vorliegt. Das Besondere an dieser wissenschaftlichen Schrift: Ihr Verfasser, Jürgen Kraus, reichte das 221 Seiten starke Werk bereits im Februar 1980 bei Professor Volker Klaus am Fachbereich Informatik der Universität Dortmund zur Begutachtung ein. Es enthielt sogar Listings von virenähnlichen, selbstreproduzierenden Programmen in den Programmiersprachen Simula, Pascal und Siemens-Assembler.

Die Arbeit mit dem Titel „Selbstreproduktion bei Programmen" schloß Kraus also vier Jahre vor der Veröffentlichung von Fred Cohens Arbeit „Computer Viruses – Theory and Experiments" ab. Aber erst Cohen versetzte die Fachleute mit dem Thema Computerviren in helle Aufregung und löste zugleich einen beachtlichen Medienrummel aus. Nicht ohne Grund: Der Amerikaner verdeutlichte zum ersten Mal das Gefahrenpotential, das in den Viren steckt. Um die Arbeit von Kraus hingegen blieb es still – sie verschwand im Universitätsarchiv. Der Student habe, so Professor Klaus, „seine Arbeit nicht zur Veröffentlichung freigegeben". Kraus hielt lediglich einen Vortrag am Fachbereich.

Die in dem Werk enthaltenen Beispielprogramme testete er, wie er in seiner Abhandlung schreibt, auf dem universitätseigenen Siemens-Rechner Typ 77 38 der Abteilung Informatik.



PURMANN

Lange Nächte im Labor

Damals war es unmöglich, auf eigenen Geräten zu programmieren; der PC wurde schließlich erst 1981 von IBM vorgestellt.

Für den Studenten Jürgen Kraus stand wegen der kostbaren Rechenzeit am Computer auch nicht das „Spielen" (siehe Kasten) im Mittelpunkt, sondern etwas ganz anderes: Er wollte die Existenz selbstreproduzierender Programme beweisen, ihre Eigenschaften diskutieren und konkretes Verhalten wie Mutation in verschiedenen Programmiersprachen analysieren.

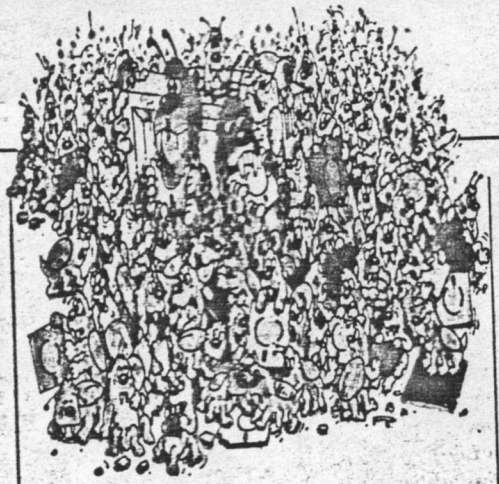
Doch die Diplomarbeit ist noch unter einem anderen Gesichtspunkt interessant: In der Bibliographie wird eine Fülle biologischer Literatur angeführt. Kraus benutzt dieses wissenschaftliche Material, um eine für das Jahr 1980 erstaunliche Gedankenverbindung zu untermauern: Er zieht die Analogie zu lebenden Organismen. Seine Argumentation stützt sich auf zwei charakteristische Eigenschaften lebender Zellen: einerseits die identische Reproduktion auf eigene Veranlassung (Autoreproduktion), andererseits die Möglichkeit der fehlerhaften Reproduktion (Mutation).

Dazu schreibt er: „Obwohl Viren keine Lebewesen sind, läßt sich an ihnen Evolution beobachten. Die Gründe dafür sind:

– Viren sind zur Mutation fähig,
– Viren befinden sich ebenfalls in einem Kampf ums Dasein und sind daher der Selektion unterworfen. Es liegt der Schluß nahe, daß Evolution

Viren

Erste Forschungsarbeit aufgetaucht



auch bei selbstreproduzierenden Programmen möglich ist, falls diese der Mutation und Selektion gleichzeitig ausgesetzt sind."

Dieser theoretische Ansatz weist einige logische Mängel auf – dessen ist sich Kraus bewußt. Er beugt deshalb einer Fehlinterpretation seiner Arbeit vor, wenn er schreibt: „Ich möchte deshalb nicht Leben in Programmen definieren. Die abschließenden Kapitel der vorliegenden Arbeit sind eher als ein erster Versuch zur Erschließung des dargelegten Problemkreises, verbunden mit einigen Denkmöglichkeiten, zu verstehen."

Der junge Informatiker überträgt in der Diplomarbeit die Theorie der lebenden Zelle auf selbstreproduzierende Programme. Zum Kampf ums Überleben schreibt er: „In einem Modell behaupten sich diejenigen Programme, die in der Vorrangmatrix eine günstige Stellung einnehmen, also relativ leicht Speicherplatz für ihre Kopien finden. Sie zeichnen sich durch eine kurze Reproduktionszeit aus. In meinem Modell besteht also ein Selektionsdruck in Richtung auf kurze Reproduktionszeit und günstige Stellung in der Vorrangmatrix."

Im abschließenden Teil der Arbeit kommt er zu der Einsicht, daß seine selbstreproduzierenden Programme bei den wissenschaftlich definierten Schlüsselprozessen des biologischen Lebens nur Entsprechungen in den

Nicht vergleichbar mit lebenden Organismen

beiden Punkten „Mutation" und „Reproduktion" finden. Kraus räumt ein: „Selbstreproduzierende Programme lassen sich somit auch nicht mit lebendigen Organismen vergleichen." Derselben Ansicht ist auch Professor Klaus: Er hält diesen Ansatz auch heute noch für „die jugendliche Spielerei eines Studenten".

Dennoch entwickelt Kraus – ob Spielerei oder nicht – einen Gedanken, der das Phänomen Computervirus im Kern bereits beschreibt. „Die Biologie kennt jedoch Strukturen, die durchaus einen Vergleich mit selbstreproduzierenden Programmen zulassen." An dieser Stelle taucht das erste Mal der Begriff „Viren" auf – im Sinne einfachster Organismen, die über keinen eigenen Stoffwechsel verfügen. „Erst wenn Viren in eine Zelle eindringen, zeigen sie Lebenserscheinungen in Form von Mutation und Reproduktion (...) Diese Zusammenhänge sind in ähnlicher Form auch in selbstreproduzierenden Programmen festzustellen."

Kraus geht aber nicht – wie Cohen vier Jahre später – auf das Sicherheitsproblem ein, sondern konzentriert sich auf den Beweis und die Konstruktion möglichst einfacher, selbstreproduzierender Programme. Die bisher bekannten Programmlistings mit diesen Eigenschaften seien bis dahin sehr kompliziert und lang gewesen, erläutert Professor Volker Klaus. Damit wird klar: Die Diplomarbeit beschreibt tatsächlich theoretische Ansätze für jene Codes, die als Viren ihr Unwesen in Speicher und Festplatte treiben. Denn erst kurze Codes machen Viren gefährlich, weil sie sich zunächst unbemerkt verbreiten können.

Dieses Verhalten ist die Grundlage für Cohens Arbeit von 1984: Bereits in der Einleitung seines Aufsatzes weist Fred Cohen auf Viren als Sicherheitsrisiko für Computer hin. Die Viren sind für ihn deshalb interessant, weil sie die Fähigkeit besitzen, sich in Programme einzunisten und sie dann ihrerseits zu Schadensprogrammen – Viren – umzuschreiben.

Fred Cohen sah die Gefahr voraus, die von der Verbreitung solcher Schadensprogramme ausging – und schlug Alarm. Das Resultat: Virensuchprogramme finden heutzutage reißenden Absatz. Die Arbeit von Kraus dagegen verstaubte im Archiv und geriet in Vergessenheit. Professor Klaus, der inzwischen an der Universität Stuttgart lehrt, kann sich aber noch gut an die Arbeit erinnern. Dabei findet er eines höchst verwunderlich: „Vor einigen Jahren ist mein Exemplar der Diplomarbeit aus meinem Büro einfach verschwunden."

Patricia Müller

Tatort: Schlachtfeld Speicherplatz

In den sechziger Jahren entwickelten die drei jungen Programmierer H. Douglas McIlroy, Victor Vysottsky und Robert Morris in den AT&T Bell Laboratories einen ungewöhnlichen Zeitvertreib: den Kern-Krieg (Core Wars). Die drei Männer kannten sich hervorragend im Kernspeicher (Core Memory) ihrer Rechner aus. Jeder Spieler programmierte kleine, selbstreproduzierende Programme, sogenannte Organismen, die er im Speicher auf die seines Spielgegners losließ. Der Organismus, der nach einer bestimmten Spielzeit die Oberhand hatte, gewann. Bis 1983 hielten die Core-War-Fans ihr Spiel streng geheim – bis Ken Thompson, der die Urversion von Unix programmiert hatte, auspackte. Als Thompson eine Auszeichnung der Industrie erhielt, trat er vors Mikrofon und sprach zum ersten Mal öffentlich über Core Wars. Die Core Wars waren jedoch keine echten Virenprogramme im heutigen Sinn, da sie sich zwar im Speicher des Rechners breitmachten, aber keine anderen Programme überfielen.

Viren tauchen heutzutage als Boot- oder File-Viren auf. Als File-Viren infizieren sie alle ausführbaren Dateien von Programmen, also Dateien, die auf .com, .sys, .ovl, .bin oder .exe enden. Dabei hängen sie sich in den meisten Fällen an das Ende einer Datei und werden bei deren Aufruf aktiv. Boot-Viren benutzen als Wirt den Boot-Sektor der Festplatte oder Diskette. Sie kopieren sich beim Hochfahren des Systems in den Speicher des Rechners und gehen dann dort an ihr Zerstörungswerk. Im gleichen Jahr wurde auf einem amerikanischen Rechner unter dem Betriebssystem Unix ein künstlicher Virus für die Vorführung in der Öffentlichkeit geboren. Bei diesem Schadensprogramm handelte es sich um einen Virus, der zu Demonstrationszwecken künstlich in das Betriebssystem eingepflanzt worden war. Dort durfte er sich unter strengster Aufsicht der Professoren am Unix-Befehl VD vergreifen, der Verzeichnisse grafisch anzeigt.

Virenforum

Linkviren

Linkviren heißen nicht so, weil sich der arglose PC-Nutzer von ihnen gelinkt fühlt, sondern wegen der Art ihrer Fortpflanzung. CHIP erklärt, wie solch ein Virus vorgeht.

Die zersägte Dame

Was ist das denn – ein Computervirus? Die Frage ist berechtigt, da es inzwischen viele Arten dieser schädlichen Programme gibt und dem Anwender längst nicht mehr klar ist, womit er es im Einzelfall zu tun hat.

Schemata, die Vielzahl von Viren einzuteilen und zu klassifizieren, gibt es mehrere. Da ist zum Beispiel von verschiedenen Viren-Generationen die Rede. Die Forscher sind sich jedoch nicht immer einig, wie viele es überhaupt gibt. Ein anderes gebräuchliches Schema ist die Einteilung in überschreibende, Link-, Boot- und Partitionsviren.

Die überschreibenden Viren sind schnell abgehandelt. Sie vermehren sich, indem sie sich auf den Anfang einer EXE- oder COM-Datei kopieren. Der ursprüngliche Programmcode der infizierten Software wird dadurch zerstört, und das Anwendungs- oder Systemprogramm ist nicht mehr zu reparieren. Nach Durchlauf des Viruscodes stürzt die befallene Software ab oder produziert Fehlermeldungen. Solche Viren waren durch ihre auffällige Wirkung meist leicht und schnell zu erkennen. Aus diesem Grund sind sie inzwischen auch so gut wie ausgestorben.

Die elegantere Methode ist, den Virus derart in den Programmcode einzufügen, daß die Software funktionsfähig bleibt. Diese Art Viren hat man Linkviren genannt. Bekannte Vertreter ihrer Art sind etwa Eddi, dBase oder Herbstlaub.

Die eine Art Linkviren schreibt sich in der Hoffnung, schlechter erkannt zu werden, mitten in die Software hinein. Den überschriebenen Teil kopieren sie zuvor einfach ans Ende des Programms, so daß er erhalten bleibt. Wird so ein Programm gestartet, macht sich der Virus zunächst speicherresident und fügt das ausgeschnittene Stück des Anwendungsprogramms wieder in seine ursprüngliche Position ein. Damit überschreibt er zwar auch sich selbst, das stört ihn jedoch nicht weiter, da er sich ja schon im Hauptspeicher weiterkopiert hat und von da aus sein verderbliches Werk fortsetzen kann. Der Nachteil dieser Methode ist der Zeitaufwand des Hin- und Herkopierens.

Eine noch fiesere Variante: Der Virus zerlegt sich in Einzelteile und verfährt mit diesen wie beschrieben, überschreibt also mit seinen Einzelteilen das Opfer an verschiedenen Stellen. Die fügt er alle nacheinander am Programmende wieder an. Er benötigt allerdings auch ein entsprechend großes Wirtsprogramm. Ein derart „zerrupftes" Programm ist kaum mehr zu restaurieren, auch die Analyse ist stark erschwert.

Die dritte und weitaus verbreitetste Art von Linkviren sind solche, die sich einfach an vorhandene Software anhängen und am Anfang des Programmcodes ihres Opfers einen Sprungbefehl auf sich selbst einbauen. Damit stellt der Virus sicher, daß er zuerst abgearbeitet wird. Danach erst beginnt das gestartete Programm. Ist von Linkviren die Rede, meint man im allgemeinen diese Variante. Durch ihren einfachen Anhänge-Mechanismus sind sie auch relativ einfach zu entfernen. Ein populärer Vertreter dieser Gattung ist zum Beispiel der Dark Avenger.

Dann ist noch eine Variante möglich, bei der der Virus einen Teil seiner selbst auf einem externen Speichermedium auslagert. Dadurch kann er den Teil, der sichtbar im Code des befallenen Programms sitzt, möglichst klein halten und so die Wahrscheinlichkeit einer Entdekkung um ein Vielfaches herabsetzen.

Programmcode als Puzzle

Nun wären Linkviren ganz einfach daran zu erkennen, daß sie das Wirtsprogramm sichtbar verlängern, erkennbar an der geänderten Größe im Verzeichniseintrag von DOS. Die gewieften Viren bedenken jedoch auch dies: Sie verändern die Dateilänge im Directory, indem sie den Eintrag entsprechend modifizieren oder indem sie Zugriffe des Systems abfangen, dann von der tatsächlichen Dateilänge jedesmal ihre eigene Länge abziehen und erst den geänderten Wert weitergeben. Nach dieser Technik der Verschleierung nennt man solche Viren auch Tarnkappen- oder Stealth-Viren. Ganz allgemein ist damit gemeint, daß ein Virus dem Anwender vorgaukeln kann, er wäre gar nicht vorhanden und hätte keine Auswirkungen. Neben der Dateilänge kann ein Virus auch Dateiattribute oder Speicherbereiche verschleiern oder sie verändern.

Weitere Arten von Viren wären noch die Bootsektor- und die Partitionsviren. Sie werden sich in einer späteren Folge des Virenforums vorstellen. *Joachim Pich*

Neues von der Virenfront

Antiviren-BIOS: Intel-Konkurrent American Megatrends (AMI) hat eine neue Version seines Hi-Flex-BIOS angekündigt. Das neue BIOS ist am Datum 6. 6. 1992 zu erkennen. Eine der wesentlichen neuen Funktionen ist ein Bootsektorschutz. Das neue BIOS überwacht auf Wunsch alle Schreibzugriffe. Damit besteht die Chance, Bootviren rechtzeitig zu erkennen. Versucht ein Programm, auf Sektor 1 der Festplatte zu schreiben, unterbricht das BIOS den Schreibzugriff und meldet dies dem Anwender in einer Dialogbox. Dann muß der Anwender entscheiden, ob dieser Zugriff berechtigt ist oder nicht. Ein ausgesprochener Virenschutz ist dies natürlich nicht. Aber bisher existierenden Bootviren kann damit das Leben schwer gemacht werden.

Freitag der 13.: In der Schweiz lieferten zwei PC-Händler und ein Softwarehaus mit ihren Produkten unbemerkt einen neuen Virus an ihre Kunden aus. Er hört vorläufig auf den Namen Swiss Phönix und überschreibt am 13. November die ersten dreizehn Zylinder der Festplatte. Auf dem Bildschirm gibt der Virus die Meldung „Phönix" aus. Die Antivirensoftware F-Prot erkennt Swiss Phönix ab Version 2.04c.

24./5.3.93 Welt?

Schlägt Computervirus Michelangelo wieder zu?

Von PETER MICHALSKI

London – Michelangelo geht wieder um. Der Zeitzünder-Eindringling ist auf den kommenden Samstag programmiert, den 518. Geburtstag des Renaissance-Meisters aus Vinci. Allein in Deutschland suchte er am 6. März vergangenen Jahres „einige zehntausend" IBM- und IBM-kompatible PCs heim und vernichtete oder verstümmelte die Festplattendaten.

In England wurden mehr als 200 Datenanlagen betroffen, darunter die der meisten Banken, des Innen- und des Außenministeriums. Daß es nicht noch mehr Opfer gab, führt Scotland Yard nur auf den Erfolg einer Warnkampagne des Dezernats Computerdelikte zurück.

Der erste Computervirus wurde 1987 an der amerikanischen Universität Delaware ausgemacht. Heute sind weltweit nahezu 2000 verschiedene Erreger bekannt. Nach Vermutung von Experten kommen jeden Monat 150 neue dazu. Für 1993 sagen Fachleute etwa jedem sechsten PC Virusbefall voraus, rund zwölf Millionen Geräte. „Wenn der Trend so weitergeht, haben wir es in drei Jahren mit über 10 000 Viren zu tun", prophezeit Andy Campbell vom Londoner Virenbekämpfungsunternehmen Reflex Magnetics. Gut die Hälfte aller britischen Firmen, die in einer Untersuchung der Unternehmensberatung Price Waterhouse unter die Lupe genommen wurden, bestätigte finanzielle Einbußen infolge Computerpannen.

Vorbeugen ist weder billig noch leicht – aber immer noch einfacher, als den Virenschreibern das Handwerk zu legen. Die Verhaftung von sechs jungen Erreger-Erfindern im Februar in England gilt als das erste Mal in der Computergeschichte, daß eine Erzeugerbande dingfest gemacht worden ist. Ihr „Verein echt gemeiner Viren" (ARCV), eine Gruppe von 15- bis 24jährigen aus vier verschiedenen Städten, soll seit Weihnachten zwischen 30 und 50 Viren über ein „schwarzes Brett" bis nach Amerika in Umlauf gebracht haben.