Und er sah, dass es viral war

25 Jahre Michelangelo-Virus: ein Rummel mit Folgen

Am 6. März 1992 hielt die Welt den Atem an. An diesem Tag sollte ein Virus namens Michelangelo auf PCs aktiv werden und Festplatten ratzfatz löschen. Es war der erste Computer-Schädling, der es in die Massenmedien schaffte.

Von Detlef Borchers

Die Tagesschau wollte ein Kamerateam in das im Jahr zuvor gegründete Bundesamt für Sicherheit in der Informationstechnik (BSI) schicken, das den Virus beim Wüten filmen sollte. Auf der anderen Seite des Atlantiks belagerten die Reporter aller großen Sender die Büroräume der Antivirusfirma McAfee in gespannter Erwartung der Katastrophe.

In einem Interview zum Thema Computerviren hatte Firmenchef John McAfee zuvor über den Michelangelo-Virus gesprochen. Gefragt, wie viele Rechner bedroht sind, antwortete McAfee, dass der Virus vielleicht 5000 oder auch 5 Millionen Rechner befallen haben könnte. Das war dem Journalisten zu vage: „Mindestens 5 Millionen Computer gefährdet“ eignete sich weitaus besser als Schlagzeile – eine Sensationsmeldung, die von den Nachrichtenagenturen übernommen wurde.

So wurde Michelangelo zu dem Virus, mit dem das Problem der Computersicherheit beziehungsweise Datensicherung erst-

mals in breiter Öffentlichkeit diskutiert wurde und nicht nur in der IT-Szene. Beim BSI aktivierte man das Referat für „Systembezogene Risikoanalyse“, um Maßnahmen zur Bekämpfung von Michelangelo zu analysieren und auf den Weg zu bringen. Mit dessen damaligem Leiter Frank W. Felzmann unterhielten wir uns für diesen Artikel über das Phänomen Michelangelo.

Mit der 3-Tasten-Maus AM25 der Firma Artec wurden bis Ende Februar 1992 rund 20.000 mit dem Michelangelo-Virus infizierte Treiber-Disketten in den Handel gebracht.

Die Wurzeln

Der Michelangelo-Virus wurde im Februar 1991 von dem australischen Ingenieur und Programmierer Roger Riordan entdeckt und analysiert. Riordan hatte 1989 als Lehrer am Chisholm Institute of Technology ein erstes Antiviren-Programm namens Vet geschrieben. Das löschte den Stoned-Virus, der sich auf den 30 Olivetti-PCs des Lehr-Labors eingenistet hatte. Bedingt durch das leicht inkompatible Olivetti-BIOS löschte Stoned wieder und wieder die Festplatten der Rechner seiner Studenten, was Riordan verärgerte. Eine israelische Firma bot ihm ein AV-Programm an, für 400 Dollar pro PC, erinnert sich Riordan auf seiner Website. Das konnte sich das Institut aber nicht leisten.

PC-Vet vertrieb er zunächst als Shareware über seine Firma Cybec. Tauchten neue Viren auf, speicherte Riordan ihre Signaturen und Löschprozeduren in Vet. Sein Polysearch genannter Algorithmus, der auf der fünften Computer Virus & Security Conference 1992 vorgestellt wurde, konnte parallel nach vielen Signaturen suchen und dann auf die jeweiligen Gegenmaßnahmen verzweigen.

So verfuhr Riordan auch mit dem neuen Virus, der in einem benachbarten Computershop auftauchte und von ihm Anfang 1991 analysiert wurde. Bei dieser Variante des Stoned-Virus entdeckte er, dass der Virus jeweils an einem 6. März aktiv wurde und erzählte dies einem Freund an der Universität. Der merkte an, dass der 6. März sein Geburtstag sei. Riordans Angebot, den Virus nach ihm zu benennen, schlug er aus. Riordan suchte, wer an diesem Tag sonst noch Geburtstag hatte: Michelangelo Buonarroti, Cyrano de Bergerac und Lou Costello standen zur Auswahl. Mit Michelangelo und Vet erzielte Riordan einen Volltreffer. Die australische Antiviren-Firma wuchs und wuchs, bis sie 1999 von Computer Associates aufgekaufte wurde. Von den Erlösen wurde die gemeinnützige Cybec Foundation gegründet, die bis heute Studenten unterstützt.

McAfee und Norton

In seinen Erinnerungen beschreibt Riordan, wie John McAfee auf einer Australienreise 1991 von Michelangelo erfuhr und verärgert reagierte, als er erfuhr, dass es eine billige Shareware gab, die den Virus entfernte. Noch amüsanter verlief zuvor ein Treffen mit Peter Norton, damals berühmt für die Norton Utilities und den Norton Commander. Von Riordan gefragt, was er denn gegen die Virenplage unternehmen werde, zog Norton vom Leder und tat Computerviren als Gerücht ab („urban hoax“).

Kurz nach seiner Rückkehr in den USA gab Nortons Firma bekannt, ein Produkt namens Norton Antivirus zu entwickeln. Als der Virenscanner erschien, konnte er 30 Viren erkennen, während McAfees Software es schon auf 44 Viren brachte. Der Markt-Durchbruch für Norton Antivirus gelang, als man in der Michelangelo-Panik einen kostenlosen Virenscanner veröffentlichte, der allein Michelangelo aufspürte und vernichtete.

Als das britische Virus-Bulletin Michelangelo im Oktober 1991 zum ersten Mal in seiner „Hitliste“ aufführte, gingen die Viren-Spezialisten von einer moderaten Gefahr aus. Doch die apokalyptischen Warnungen waren längst überall unterwegs. Über die Sensationsmeldung von millionenfacher Schädigung der Rechner verbreitete sich die Warnung vor Michelangelo auch in Deutschland. Besonders laut warnte Professor Klaus Brunnstein, der an der Uni Hamburg ein „Viren-Test-Center“ (VTC) leitete: Am 6. März würden Hunderttausende von Rechnern ihre Daten ins Nirwana schicken. Mit dieser Warnung wurde er für die einen zum „Viren-Papst“, während Kritiker ihn als „Viren-Kassandra“ verspotteten.

c’t hielt sich mit Spekulationen zurück: Eine kurze Meldung im Aktuellteil der Ausgabe 3/1992 wies unter der Überschrift „Michelangelo-Panik“ knapp auf das bevorstehende „Erwachen“ hin und führte Viren-Scanner-Software auf, die Michelangelo bereits erkannte. Auch der Chaos Computer Club gab sich reserviert. In dessen Hauspostille „Datenschleuder“ war von Panikmache die Rede und davon, dass die Sicherheitsbranche im Vorfeld der CeBIT besonders laut trötet.

Ganz so einfach war die Sache jedoch nicht, denn Michelangelo hatte sich vor allem über Treiber-Disketten schneller und weiter verbreitet als frühere PC-Viren. Mit dem Treiber der populären weil billigen Artec-Maus handelte man sich auch den Michelangelo-Virus ein. Die Maus wurde immerhin 20.000-mal verkauft. Auch diverse Treiber für VGA-Grafikkar-

```
                lodsw                           ; check infection
                cmp     ax,[bx+2]               ; is it infected?
                jne     infectharddisk          ; if not, infect HD
checkdate:
                xor     cx,cx                   ; Real time clock get date
                mov     ah,4                    ; get dx = mon/day
                int     1Ah
                cmp     dx,0306h                ; check March 6th
                je      damagestuff             ; if true, damagestuff
                retf                            ; return control to original
                                                ; boot block @ 0:7C00h

damagestuff:                                    ; prepare for int 13h
                xor     dx,dx                   ; head 0, drive 0
                mov     cx,1                    ; track 0, sector 1
smashanothersector:
                mov     ax,0309h                ; ah=03: write al=09 sectors
                ;;      ...

                mov     bx,5000h                ; source is random memory area
                mov     es,bx                   ; at es:bx = 5000h:5000h
                int     13h                     ; Write sectors to drive
                ;;      ...
                xor     dh,dh                   ; go to next head/cylinder
                inc     ch
                jmp     short smashanothersector
```

Der PC-Virus Michelangelo prüft das aktuelle Datum und wird nur am 6. März richtig aktiv.

ten waren infiziert. Besonders pikant: Intel, damals mit einer eigenen Antivirus-Software namens LANProtect im Geschäft, hatte schon 839 Disketten mit seiner LANspool-Software verschickt, ehe jemand im Kopierwerk bemerkte, dass sich Michelangelo im System eingenistet hatte.

Neben der Panik gab es die Vorsorge. Der eifrige Professor Brunnstein gab im Fernsehen bekannt, dass sein VTC eine Reparatur-Diskette mit Software verschicken werde, die Rechner vor dem 6. März prüfen und gegebenenfalls den Virus entfernen werde. Das Resultat: 28 Postsäcke mit Freiumschlägen, in die Studenten im Akkord 18.000 Disketten zum Versand steckten. Die ganze Aktion wurde von Siemens-Nixdorf unterstützt, wobei der Name dieses großzügigen Sponsors nicht in der Öffentlichkeit bekannt werden sollte. Von der Uni Karlsruhe meldete sich der Virenjäger Christoph Fischer und bot eine Antivirus-Diskette an, wenn 5 DM und ein Freiumschlag geschickt werden: Hier wurden 7000 Disketten verschickt.

Das BSI konnte als Behörde wegen wettbewerbsrechtlicher Bedenken keine Disketten verteilen, sondern nur mit Pressemeldungen vor Michelangelo warnen. Frank Felzmann richtete eine „Virus-Hotline“ ein, die vom 17. Februar bis zum 6. März Fragen zu Michelangelo und allgemein zu Computer-Viren beantwortete. Wie man Michelangelo finden könnte, wurde da am häufigsten gefragt. Und ob es Sinn mache, das Datum zu verändern. Wo kein 6. März, da kein Michelangelo. Besonders vorsichtige Naturen schalteten am Freitag, den 6. 3. 1992, den Rechner überhaupt nicht ein.

Am Tag X

Am 6. 3. 1992 schlug Michelangelo tatsächlich zu. Nach den Statistiken des BSI und der Abfrage aller Hotlines gab es in Deutschland insgesamt 95 gemeldete Schadensvorfälle mit 150 Computern, bei denen die Festplatte gelöscht wurde. Der erste Fall in der BSI-Hotline war eine kleinere Druckerei bei Aachen, bei der um 8 Uhr morgens der Computer hochgefahren wurde und der Druckereibesitzer beim Start vor Schreck den Stecker zog. Die Daten auf Laufwerk C waren dahin, doch die Partitionen D (Kunden) und E (Lieferanten) konnten gerettet werden. Die Druckerei besaß keine aktuelle Datensicherung.

Ausgehend von 150 bekanntermaßen betroffenen PCs schätzt Felzmann die Dunkelziffer auf mindestens 1500 Rechner, bei denen Michelangelo Schaden anrichtete. Die Gegenrechnung: Durch die ausführliche Berichterstattung und die verschickten Disketten gab es 770 Fälle mit 1260 PCs, auf denen Michelangelo rechtzeitig erkannt und gelöscht wurde. Mit der gleichen, zehnfachen Dunkelziffer ergibt das rund 12.000 gerettete Computer allein in Deutschland.

Damit war Michelangelo allerdings noch nicht besiegt. Die Folgeschäden waren aber geringer, weil der 6. März in den Folgejahren auf ein Wochenende fiel, an dem kaum beruflich genutzte PCs in Betrieb waren. 1993 wurden dem BSI 50 Schadensfälle gemeldet, 1994 nur noch 20. 1995 trat der Virus nicht mehr messbar auf. PCs wurden mittlerweile mit modernen 3,5-Zoll-Disketten ausgeliefert, mit denen sich Michelangelos nicht mehr verbreiten konnte, weil der Virus Disketten mit 15 Sektoren pro Spur voraussetzte.

Angeregt durch Michelangelo gab das BSI eine Umfrage unter kleinen und mittleren Unternehmen in Auftrag, wie es denn um die Datensicherung bestellt ist. Nur 5 Prozent hatten ein aktuelles Backup, 15 Prozent eine „bedingt aktuelle“ Datensicherung und 80 Prozent überhaupt keine. Die Erfolgsmeldung des BSI vom 11. März 1992 endete deshalb so: „Als positiver Nebeneffekt der Berichterstattung in Presse, Funk und Fernsehen ist im übrigen zu vermerken, dass die Notwendigkeit einer aktuellen Datensicherung vielen Benutzern drastisch vor Augen geführt wurde. Zudem wurden bei der Suche nach ‚Michelangelo‘ auch eine Reihe anderer Computer-Viren noch frühzeitig entdeckt.“

Die Folgen

Wichtiger als der Schutz vor Michelangelo war letztlich die Aufklärungskampagne, zieht der heute pensionierte Virenwarner Felzmann sein Fazit. Auch das britische Virus-Bulletin stufte den „Angriff“ von Michelangelo in seiner Rückschau als „moderat“ ein, ausgehend von 117 PCs, die es am Stichtag nach der Meldung der Computer Crime Unit von Scotland Yard erwischt hatte. Auch in den USA ging es recht glimpflich ab: Statt der befürchteten 5 Millionen wurden zwischen 7000 (Dr. Salomon) und knapp 10.000 Schadensfälle (McAfee) gemeldet. Selbst mit Dunkelziffer ergibt das keine Millionen.

Am schlimmsten traf es die Southern Baptist Church und die Umweltschutzorganisation „Save the Whales“, die beide ihre Spender- und Mitgliederlisten auf den Festplatten verloren. Da keine Backups vorhanden waren, veröffentlichten sie einen Michelangelo-Hilferuf. Zahlreiche Horror-Meldungen entpuppten sich jedoch als Fake News, wie man heute sagen würde. Dazu gehörte etwa, dass die Armee von Uruguay ihre PC-Daten verloren hatte und kampfunfähig sei. Der weltweit größte Michelangelo-Schaden wurde aus Südafrika gemeldet. Dort verteilte eine Firma die jeweils neuesten Preislisten für

Apotheken via infizierter Floppy-Disk. So wurden 1000 Rechner in 450 Apotheken Opfer von Michelangelo.

Der Warner John McAfee stand seinerzeit schwer in der Kritik, auch von Seiten der etwa 12 Firmen, die in den USA Virenscanner verkauften. Dabei lief das Geschäft bombig: Am 4. März notierte der Großhändler Egghead Software, dass die Verkäufe von AV-Produkten gegenüber der Vorwoche um 3000 Prozent zugenommen hatten. Compuserve, der damals führende Online-Anbieter, notierte 49.000 Downloads von Michelangelo-Scannern, die Central Point und Symantec bereithielten. McAfee störte die Kritik überhaupt nicht. Ohne seine Warnung und ohne die Software seiner Firma wäre eine echte Epidemie ausgebrochen, gab er Kontra. Im Oktober 1992 ging McAfee Inc. an die Börse und erzielte beim IPO 42 Millionen US-Dollar. Nicht schlecht für eine 12-Mann-Firma.

In den „Software Engineering Notes“ der ACM erschien das Fazit, dass Michelangelo mehr „Hoax“ denn eine echte Gefahr gewesen sei. Eine echte Gefahr könne von einem Virus erst ausgehen, wenn er etwa gezielt von einer Armee eingesetzt werde. Damit bezog sich der Autor auf eine andere Sensationsnachricht von damals: Im März 1992 meldete die Nachrichtenagentur „U.S. News & Report“, dass die US-Army im Zweiten Golfkrieg einen Virus in den Speicherchips von Druckern versteckt habe, die in den Irak geliefert wurden. Das sollte dann die Kommunikation der Truppen von Saddam Hussein behindert haben.

Die Meldung entpuppte sich letztlich als abgeschriebener Aprilscherz, als echter Hoax. Die zufällige Koinzidenz verdient Beachtung, denn das Märchen von der Virusattacke auf den Irak nannte der aus dem Irak berichtende Star-Reporter Peter Arnett „Hyperwar“. Als 1999 die Zeitschrift Popular Mechanics die Unsinnsgeschichte erneut verbreitete, tauchte erstmals der Begriff „Cyberwar“ in einer größeren Zeitschrift auf. Heute beschäftigen die Öffentlichkeit staatlich unterstützte Hacker wie Sofacy (Fancy Bear, APT28), die in Regierungsnetze eindringen und keine Scheu haben, dabei maßgeschneiderte Malware einzusetzen.

Der oder die Autoren von Michelangelo sind bis heute nicht bekannt.

(ju@ct.de) c't

Michelangelo analysiert

Von Frank W. Felzmann

Der Michelangelo-Virus ist ein Boot-Virus und benötigt zur Verbreitung – im Gegensatz zu einem Datei-Virus – ein physikalisches Medium, konkret eine Diskette. Dabei ist er betriebssystemunabhängig. Theoretisch könnte er auch die Festplatte eines Linux-Systems infizieren. Alles, was er braucht, ist ein Computer mit BIOS, der 80x86-Maschinenbefehle versteht und ausführt. Das Basic Input/Output System stellt die Interrupts 13h für Festplatten-Zugriffe und 1Ah für die Abfrage der Systemzeit bereit.

Findet ein PC beim Systemstart im ersten Disketten-Laufwerk eine Diskette vor, führt er den Code in deren erstem Sektor aus, dem Boot-Sektor. Ist die Diskette mit Michelangelo infiziert, kommt auf diesem Weg dessen viraler Code zum Einsatz. Er prüft zunächst über den Master Boot Record (MBR) der Festplatte, ob diese bereits infiziert ist. Ist dies nicht der Fall, kopiert der Virus den originalen MBR auf Zylinder 0, Kopf 0, Sektor 7. Die Partitionstabelle der Festplatte, die die Aufteilung der Festplatte in Partitionen angibt, wird ans Ende des Virus-Codes gehängt, woraufhin sich der Virus selbst in den MBR schreibt. Nach der Infektion der Festplatte übergibt Michelangelo die Kontrolle an den originalen MBR – das System startet wie gewohnt.

```
000000      ·<·MSDOS5.0·····
000010      ···@·····------
000020      ·····)··H·VOLUM
000030      E-NAMEFAT12   ·3
000040      ·····|···x·6·7·V
                . . . . . .
                . . . . . .
                . . . . . .
000190      ·····$|·6%|·····
0001A0      Kein System oder
0001B0       Laufwerksfehler
0001C0      ··Wechseln und T
0001D0      aste drücken···I
```

```
000000      ···········.···P
000010      ··u·3·····?··u·X
000020      ··.·····------X
000030      ·.·.··PSQR··VW··
000040      ··------------3·
                . . . . . .
                . . . . . .
                . . . . . .
000190      ·····r··------!
0001A0      ·····3··------
0001B0      ------------er
0001C0      ··Wechseln und T
0001D0      aste drücken···I
```

Der Boot-Sektor einer DOS-Diskette vor und nach der Infektion.

Doch künftig infiziert der Computer alle in das Laufwerk A: eingelegten, beschreibbaren Disketten. Dazu klinkt sich Michelangelo dauerhaft in den Festplatten-Interrupt 13h ein – eine Technik, die zu DOS-Zeiten für Treiber in Form von TSR-Programmen weitverbreitet war (Terminate, Stay Resident). Zur Infektion wird der originale Boot-Sektor einer Diskette mit 360 KByte Kapazität ans Ende des Hauptverzeichnisses ausgelagert. Das überschreibt unter Umständen dort vorhandene Verzeichniseinträge und kann bereits zu Datenverlust führen. Anschließend überschreibt der Virus den Anfang des Boot-Sektors mit seinem Code. Diese Infektion war jedoch auf die Anfang der Neunziger noch verbreiteten 5,25"-„Floppy Disks“ mit einer Kapazität von maximal 1,2 MByte (HD) beschränkt. Auf die wenig später aufkommenden, harten 3,5"-Disketten war Michelangelo nicht vorbereitet, weshalb er sich darüber nicht ausbreiten konnte.

Wurde ein infizierter Rechner am 6. März eines Jahres gestartet, überschrieb Michelangelo Bereiche der ersten Festplatte, die unter anderem wichtige Verwaltungsinformationen wie die File Allocation Table (FAT) enthielten. Ohne deren Dateizuordnung kam die Schadfunktion für die meisten Betroffenen einem kompletten Datenverlust gleich – sofern keine aktuelle Datensicherung existierte. Lediglich bei Festplatten mit mehreren Partitionen konnten mit einigem Aufwand und Glück die Partitionen D:, E: et cetera gerettet werden.

Angesichts der ausschließlich über Disketten stattfindenden Infektion verbreitete sich Michelangelo erstaunlich schnell. Ausschlaggebend war wohl, dass es dem Autor gelang, Michelangelo auf den Master-Disketten einiger Kopieranstalten in Taiwan zu platzieren. So kamen mit günstiger Hardware auch Tausende von virenverseuchten Treiber-Disketten in Umlauf.