„VIREN, VIREN!“

Herbert K. ist ein fleißiger Student: Er besucht die Vorlesungen, ist pünktlich, liest die vorgegebenen Texte und trinkt nur selten Bier. Seine einzige Schwäche – sie sei ihm hier verziehen – ist eine junge Dame, die in einer amerikanischen Soap-Opera die Schöne mimt. Natürlich ist Herbert auch ein moderner Student. So nutzt er nicht nur die Bibliotheken zur Quellenforschung, sondern auch das Internet. Und so ergab es sich eines Tages, daß er außer den neuesten Faschismustheorien auch ein Bild der jungen Angebeteten aus dem Internet auf seinen heimischen Rechner herunterlud.

Was K. nicht wußte: Die Computergrafik war mit einem heimtückischen Virus verseucht. Ein Virus ist ein kleines Computerprogramm, welches Dateien infiziert, sich mit ihnen verbindet und sich dann selbständig verbreitet. Harmlose Computerviren beschränken sich auf die bloße Verbreitung. Die bösartigeren Exemplare können jedoch beträchtlichen Schaden anrichten: vom Datenverlust bis zur Beschädigung der Hardware.

Doch zurück zu Herbert K. Er hat die Datei mit dem Virus nun auf seiner Festplatte. Sogleich macht er sich an die Fertigstellung seiner Hausarbeit, wobei ihm die Informationen aus dem Internet sehr hilfreich sind. Der Virus, der sich über den Schleichweg der Grafik auf seiner Festplatte eingenistet hat, infiziert alsbald die Datei mit der Hausarbeit. Am nächsten Tag ist Abgabetermin der Arbeit. Herbert druckt den Text aus, und gibt auch eine Kopie auf Diskette mit ab: Der Seminarleiter will den Text im Internet auch anderen Studenten zur Verfügung stellen. So kam, was kommen mußte: Der Virus findet seinen Weg auf den Rechner des Dozenten, von dort über das institutseigene Netzwerk auf die Rechner der Kollegen, und über die Hausarbeit im Internet auf den Rechner aller, die sich das Elaborat Herberts herunterladen.

So schauerlich diese Geschichte auch klingen mag, sie entbehrt der Grundlagen nicht. Es ist eine traurige Tatsache, daß durch Computerviren bereits ganze Firmen lahmgelegt wurden. Die zunehmende Vernetzung der Computerwelt leistet dem unfreiwillig Vorschub. Der Aufwand, der betrieben wird, um dieser Gefahr zu begegnen ist beträchtlich, die Kosten gehen hierbei leicht in die Hunderttausende. Am Institut für Deutsche Philologie der Georg-August-Universität mußte das Erscheinen eines Tagungsbandes um mehr als ein halbes Jahr verschoben werden, weil durch eingeschleppte Viren mehrere Rechner auf Zeit lahmgelegt wurden. Drucker, Verleger und die wissenschaftliche Welt mußten weiter warten. Denkt man an die Naturwissenschaften, die sich stärker auf den Einsatz von Computern verlassen als beispielsweise die Philologie, wird die Bedrohung unmittelbarer – leicht kann hier die Forschungsarbeit von Wochen und Monaten zerstört werden, Institute geraten im wissenschaftlichen Wettbewerb so unverdient leicht ins Hintertreffen.

Computerviren tauchten erstmals im Jahre 1986 auf. Diese einfach gestrickten Programme waren aber aufgrund einer festen Programmstruktur leicht zu entdecken. Rasch wurden neue Viren geschrieben, die wiederum aufwendigere Programme zum Aufspüren und Entfernen erforderten. Analog zu den bekannten Viren, die Menschen und Tiere befallen, werden auch die Computerviren resistent gegen die zur „Behandlung“ eingesetzten Gegenmittel. Dabei dreht sich die Spirale immer weiter und immer schneller, der Aufwand auf beiden Seiten nimmt stetig zu. Die Inflation zerstörerischer Computerprogramme nimmt zu, mittlerweile gibt es sogar „Viren-Baukästen“ zu erwerben, die es Anwendern ohne Vorkenntnisse erlauben, eigene Viren zu erstellen. Oftmals leisten auch Computerzeitschriften, vermeintlich im Zuge der Aufklärung, gestörten Geistern Vorschub, indem sie ungewollt detaillierte Anleitungen zum Selberbasteln abdrucken. Das Ende dieser Entwicklung ist noch nicht abzusehen. 1996 waren dem Bundesamt für Sicherheit in der Informationstechnik (BSI) alleine 10.000 Viren für das DOS-Betriebssystem bekannt, ähnliches gilt für die Windows-Betriebsysteme, lediglich die Apple Macintosh Rechner blieben bisher weitestgehend von der Heimsuchung verschont. Die Gruppe der Viren-Programmierer ist so vielfältig wie ihre Zahl – vom übermütigen Jugendlichen, über den Datenrowdy, bis hin zu verkannten Computergenies und selbsternannten Techno-Terroristen, die ihren Rachefeldzug gegen die Gesellschaft starten ist alles dabei. In Deutschland ist nach § 303a StGB eine „Datenveränderung“ – also auch durch Viren – schon im Versuch strafbar und wird mit einer Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe geahndet.

Doch sollte man die Gefahr durch die kleinen Computerschädlinge weder überbewerten noch unterschätzen. Viele der Programme sind unschädlich, und bewirken meist wenig mehr als das Abspielen einer Nachricht oder einer Tonfolge. Viele Anwender lassen sich jedoch schon davon in Panik versetzen. Aus Angst formatierte Festplatten – natürlich ohne vorher Sicherungskopien erstellt zu haben – sind leider keine Einzelfälle. Dabei gibt es ausgefeilte kommerzielle Produkte, die gut vor einer Dateninfektion zu schützen vermögen. Vor einer Investition sollte man hier nicht zurückschrecken – die vielfach angebotenen Shareware- oder Freeware-Programme (d.h. Software, die kostenlos ist, bzw. kostenlos ausprobiert werden darf), entdecken mitunter noch nicht einmal die einfachsten und ältesten Vertreter von Computerviren. Zahlreiche Tests haben erwiesen, daß viele Billigprodukte vor Virenbefall ungefähr genauso zuverlässig schützen, wie Handauflegen Krebs therapiert. Bevor man sich ein Schutzprogramm zulegt, sollte man sich in Testberichten u.ä. über deren Wirksamkeit informieren. Es sind sogar schon Fälle aufgetreten, wo ein vermeintliches Testprogramm sich als Infektionsherd erwies – es war bereits „serienmäßig“ von seinem Programmierer mit den tückischen Programmen versehen worden. Die Schäden sind in solchen Fällen verheerend.

Gute Schutzprogramme vermögen es, auch vor unbekannten Viren zu warnen. Eines dieser Programme ist „Canary“, das sich eines alten Tricks der Bergleute bedient: Diese führten stets einen Käfig mit einem Kanarienvogel mit sich untertage. Dieser hatte die Aufgabe vor giftigen Gasen oder vor einer zu hohen CO_2 Konzentration in der Luft zu warnen. Das System war denkbar einfach: Fiel der Vogel tot von der Stange, drohte Gefahr. – Ganz ähnlich funktioniert auch „Canary“ – seine einzige Aufgabe besteht darin, sich von einem Virus infizieren zu lassen. Danach informiert es den Anwender: „Der Vogel ist gestorben“, d.h. es liegt eine Virusinfektion vor, und nun sollte man sich alsbald um die Bekämpfung kümmern, gegebenenfalls mit einem Update der Anti-Viren-Software. – Trotz alledem: Laut Statistik des BSI ist der mit über 35% verbreitetste Virus immer noch der „Parity Boot Virus“, seit Jahren ein alter Bekannter in diesem Geschäft. Doch wie im richtigen Leben gilt hier: Wer sich schützt, vermeidet gefährliche Infektionen.

Dabei ist zumindest ein Schutz vor Computerviren relativ leicht zu erreichen: Nie Disketten ohne aktivierten Schreibschutz in andere Computer einführen, keine Daten aus fragwürdigen Quellen (Internet) oder Raubkopien installieren, einen Virenscanner installieren, der regelmäßig Festplatte, Speicher und Wechselmedien untersucht. Wer sich und andere nicht selbst schützt, kann leicht für eine Epidemie mitverantwortlich sein. Und die Gesetzmäßigkeit, daß unangenehme Dinge immer nur „den anderen“ passieren, gilt auch für Personalcomputer nicht. Oder würden sie sich freuen, wenn sich beim Speichern ihrer Arbeit ein Dialogfenster öffnet, das ihnen mit knappen Worten verkündet, daß die Festplatte gerade formatiert wird?

Virenbefall ist unangenehm, Selbstschutz so einfach. fra

Ausführliche Informationen zum Themen Computerviren und Datenschutz findet man auf den Seiten des Bundesamtes für Sicherheit in der Infromationstechnik unter http://www.bsi.de.