Die @-Bombe: Das Schauer-Märchen vom bösen Genie hinter dem apokalyptischen Computervirus

Von Hilmar Schmundt

Nr. 24 – 20.07.2002

Abstract

Wie Computerviren zur schicksalhaften Bedrohung aus dem Cyberspace aufgebauscht wurden. Warum die jugendlichen Kleinkriminellen, die sie schreiben, als böse Genies gelten. Wie eine halbseidene und milliardenschwere Softwareindustrie von der Dämonisierung des groben Unfugs profitiert und die Virenpanik aus wirtschaftlichem Kalkül schürt. Und wie die Mär vom genialen Killervirus zu Abstumpfung, Vertuschung und Fehlinvestitionen führt.

Virenalarm. Wieder einmal. Eine Lawine infizierter E-Mails wälzte sich am 12. Februar 2001 durchs Internet. Mehrere Millionen Computer wurden angesteckt. Und alles nur wegen Anna Kurnikowa. Das Computervirus gleichen Namens verführte die Nutzer mit einem angeblichen Digitalbild der russischen Tennisspielerin. An die zerstörerische Botschaft war eine Datei mit dem vielversprechenden Namen "AnnaKournikova.jpg.vbs" angehängt. Ein Pin-up-Foto? Ein peinlicher Schnappschuss unterhalb der Gürtellinie? Viele Empfänger konnten der E-Mail-Versuchung nicht widerstehen. Mit einem Doppelklick versuchten sie, die Bilddatei zu öffnen. Doch kein Kurnikowa-Foto, nirgends. Stattdessen erwachte unbemerkt eine zerstörerische Kraft zum Leben. "Wurm" nennen Spezialisten den bösartigen Code. Denn anders als gewöhnliche Computerviren reiste er nicht als blinder Passagier mit einer anderen Datei, sondern wand sich selbständig durch die Netze. Der Kurnikowa-Wurm durchstöberte die Festplatte des Nutzers und verschickte Kopien von sich selbst an Empfänger im Adressbuch des E-Mail-Programms Outlook von Microsoft.

Internet-Epidemien breiten sich meist mit der Morgensonne aus und reisen um den Erdball wie eine rabenschwarze Aurora. Als in den USA die Büroangestellten ihre Rechner starteten, fanden viele von ihnen den Kurnikowa-Wurm in ihrem Mailkonto - und traten dann eine Lawine sinnloser Massenmails los, die weltweit die

Firmennetze überfluteten und einige E-Mail-Server lahm legten. Der Schaden betrug nach Schätzungen des FBI allein bei 55 gemeldeten Opfern über 160 000 Dollar. Einen genauen Beleg lieferten die Ermittler dafür nicht. Sie verließen sich auf die vagen und möglicherweise übertriebenen Angaben der Geschädigten. Vieles beruht beim Thema Computerschädlinge auf Hörensagen. Der Topos des Datenterrors ist einer der mythischen Orte der Informationsgesellschaft, ein wahres Horrormärchenland.

Das Märchen vom finalen Killervirus

Es wird einmal, vielleicht schon morgen früh am Bürorechner, zur großen Entscheidungs-Schlacht kommen zwischen den Mächten der Finsternis und den Kräften des Lichts. So will es das Märchen vom finalen Killervirus. Die Rolle des Bösen übernehmen in diesem Moralstück die Virenprogrammierer, namenlose Heerscharen von hochbegabten "Darkside-Hackern", die in schwarzen Messen der Programmierkunst digitale Monstren erschaffen. Ihre Pseudonyme erinnern an die Bösewichter in Fantasy-Comics: "Dark Avenger", "Dark Angel", "Rigor Mortis" oder "Nowhere Man". Ihre Symbole sind düster und stammen aus der Welt der andernorts längst ausgestorbenen Deathmetal-Szene: Totenköpfe, tropfende Blutzspritzen, Giftzeichen. Ihre unheilbringenden Armeen sind tot und lebendig zugleich: Ketten aus Nullen und Einsen, die wie Zombies zum Leben erwachen, wenn sie das Signal zum Angriff erhalten. Oder wie Frankensteins Monster, hinter dem, so will es schon die Romanvorlage von 1818, eben ein hochbegabtes, aber moralisch unterentwickeltes Genie steht. Virenprogramme vermehren sich wie elektronische Lebewesen, das macht ihre Magie aus. Virenprogramme brechen in den geregelten Büroalltag ein wie ein böser Spuk. Sie toben durch die kollektive Fantasie wie Poltergeister - die Rache des Unterbewussten an den Weltbeherrschungsfantasien, die sich um die Effizienzmaschine Computer ranken. Ein falscher Klick genügt, schon ist die Arbeit von Monaten vernichtet und der teure Hightechrechner ist nur noch ein Haufen Sondermüll.

Dies Schauermärchen gehört zum Genre der Weltuntergangsfantasie. Mal angenommen, ein Amazonas-Indianer würde als Ethnologe die Informationsgesellschaft erforschen: Er würde im Mythenkranz vom Killervirus, der bei den Stämmen der Dotcom und der Digerati kursiert, unweigerlich das Wilde Denken seiner Heimat wiedererkennen.

Jahrelang zählten Computerviren zum Geheimwissen weniger Eingeweihter. Doch im ersten Frühling des neuen Jahrtausends verbreitete sich das Hightechmärchen vom Killervirus in Form eins vergifteten Liebesbriefs bis in die entlegensten Teile der vernetzten Weltbewölkerung. "I love you" stand in der Betreffzeile der E-Mail, die sich

von den Philippinen über Hongkong nach Europa und Amerika verbreitete, ein "Teufelsding" aus der "Neuen Unterwelt", eine "@-Bombe", die sich mit Hilfe des Microsoft-Programms Outlook ihre Opfer suchte. Durch die Flut von E-Mails wurden etliche Firmennetze überlastet, auch die von Ford und Siemens und angeblich 80 Prozent der amerikanischen Regierungsbehörden. Die Mittelbayrische Zeitung musste als Notausgabe erscheinen und etliche Geldautomaten spielten verrückt. Der Schaden wurde auf 10 Milliarden Euro geschätzt. Und alles nur durch die vage Verlockung, einen Liebesbrief lesen zu dürfen.

Language is a Virus (William S. Burroughs)

Doch wo das Bedrohliche wuchert, wächst das Rettende auch, das ist die kathartische Grundaussage dieses Moralstücks, das jeden PC zu einer potenziellen Bühne für tragische Datenverluste und dramatische Rettungsversuche macht. Den bösartigen Doktor-Frankensteins steht eine Allianz aus Göttern in Weiß gegenüber. Tag und Nacht wachen die brillanten PC-Doktoren mit vertrauenerweckenden Namen wie "Dr. Solomon" oder "PC-Doctor" über die Unversehrtheit ihrer zahlenden Kunden und wehren den Bannfluch der Bösewichter mit ihren "Gegenmitteln" ("antidotes") ab. Ihr Vokabular ist der Medizin entliehen, sie "impfen" mit "digitalen Immunsystemen" und "Gegenmitteln" gegen die tödlichen "Infektionen". John McAfee, Gründer der gleichnamigen AV-Firma, lässt sich bisweilen sogar gerne mit Stethoskop ablichten. Die PC-Doktoren sind, so will es das Hightech-Gruselmärchen, mindestens genauso genial wie die Heerscharen der Nacht, sie kennen alle Tricks und Kniffe der finsteren Mächte und warnen die Öffentlichkeit ständig und inständig davor, den Versuchungen zu erliegen, die in Form von Kurnikowa-Fotos und Liebesbriefen im Netz unterwegs sind.

Die Antivirenindustrie lebt sehr gut von der permanenten Bedrohung aus dem Cyberspace. Als das Liebesvirus durchs Internet geisterte, schnellte der Kurs des Antivirenherstellers McAfee um vierzig Prozent in die Höhe. Gräuelmärchen sind bares Geld wert. Daher wird die Branche nicht müde, sich als moralische Instanz zu inszenieren. Penetrant wie puritanische Prediger warnen die Virendoktoren vor der Verunreinigung der Datennetze durch die "Teufelsdinger". So kämpfen die bösen Virengenies und die guten Antivirendoktoren um die wankelmütige Seele des überforderten Märchenhelden namens Ich. Soweit das Horrormärchen.

Doch wer steckt wirklich hinter den apokalyptischen Teufelsdingern, die den Computeralltag zur Hölle zu machen drohen? Der Mythos vom bösen Virengenie hat einen wahren Kern, der weitaus spannender ist als die folkloristische Fiktion.

Der Zauberlehrling oder die Geburt der Viren aus dem Geist der Effizienz

Das furchterregende Genie, das hinter Computerviren steckt, heißt Neumann. John von Neumann, geboren 1903 in Budapest, ging 1930 von Berlin nach Princeton in die USA. Von Neumann war einer der begabtesten Mathematiker des 20. Jahrhunderts, der Inbegriff des rationalen Denkers. Neben Ungarisch, Deutsch und Englisch sprach er vor allem "Mathematisch": Alles, was er betrachtete, wurde ihm zur Formel. Bei Partys zog er sich manchmal in ein stilles Zimmer zurück, um ein paar Gleichungen durchzurechnen. Das Drama der Weltwirtschaft interpretierte er mit den Formeln seiner "Spieltheorie". Die Welt galt ihm grundsätzlich als berechenbar. Für die Hiroshishimabombe berechnete er, wie sie am meisten Schaden anrichten würde. Derlei Gleichungen erforderten leistungsstarke Computer, doch die existierenden Maschinen kamen von Neumann furchtbar unpraktisch vor. Eniac zum Beispiel war ein Kantinengroßes Ungetüm, das weniger als 400 Rechenschritte pro Sekunde schaffte - heutige Aldi-Rechner sind millionenfach schneller. Immer, wenn damals eine neue Formel durchgerechnet werden sollte, musste das schwitzende Bedienungspersonal per Hand allerlei Kabel umstöpseln. Von Neumann entwickelte eine fundamental neue Architektur: Die Aufteilung in Hardware und Software. 1945 stellte er diese Idee in einem "First Draft", diesen ersten Entwurf vor. Alle nachfolgenden Rechnergenerationen basieren auf diesem Prinzip der sogenannten "von-Neumann-Architektur", auch Handys und Digitalkameras.

> "Dieser Virus funktioniert auf Vertrauensbasis. Schicken Sie diese Botschaft an jeden, den Sie kennen, und löschen Sie dann alle Dateien auf Ihrer Festplatte. Vielen Dank für Ihre Mithilfe." (Honor System Virus)

Rechner waren für von Neumann ein Abbild des menschlichen Gehirns, die den "Neuronen im menschlichen Nervensystem" entsprechen, Ein- und Ausgabeschnittstellen beschrieb er als "Organe". Durch seine Trennung von Software und Hardware wurden die Programme frei wie Gedanken, um von einem Elektronenhirn auf ein anderes übertragen zu werden. Das bedeutete eine riesige Arbeitsersparnis.

In diesem Traum von unbegrenzter Effizienz schlummert auch der Kern des Alptraums vom Killervirus, der das Siliziumhirn in den Wahnsinn treibt. Die Effizienz der Elektronenhirne ließe sich sogar noch steigern, wenn "künstliche komplexe Automaten" in der Lage wären, sich selbst fortzupflanzen, so spekulierte von Neumann schon 1949. Mit diesem Prinzip der "Selbstvervielfältigung" hatte von Neumann den Computervirus erfunden - zumindest als theoretische Möglichkeit. Angeblich sollten sich diese "komplizierten Automaten" wie biologische Organismen

verhalten. Lebewesen wie Tiere, Bakterien oder Menschen beschrieb von Neumann in derselben Diktion als "natürliche komplizierte Automaten". In dieser Welt der Abstraktion fühlt sich der Programmierer als Schöpfer von künstlichem Leben. Der Mensch erschafft den Virus nach seinem Bilde.

Gedacht, getan. Bald wurde den digitalen Abziehbildern des Menschen digitales Leben eingehaucht - zunächst hinter den verschlossenen Türen von Elfenbeintürmen. In den Sechziger Jahren spielten Entwickler an den weltberühmten Bell Labs "Core Wars", indem sie kleine Digitalschädlinge auf den Kern des gegnerischen Rechners losließen, um die Kontrolle über das Gerät zu erlangen. Ein anderes Spiel nannte sich "Game of Life". Die Maschine erwacht zum Leben - das ist Stoff, wie gemacht für Romanautoren. Der Sciencefiction-Schreiber John Brunner spann 1975 in seinem Roman "The Shockwave Rider" die Evolution der Digitalorganismen fort. In seinem Szenario frisst sich ein unsterblicher digitaler "Bandwurm" als "Nemesis" durch die Datenbestände einer Orwell-ähnlichen totalitären Gesellschaft und befreit Daten und Menschen. Fortan nannten die Akademiker Programme, die sich nicht nur selbst kopieren, sondern sich obendrein noch von alleine von Maschine zu Maschine bewegen "Wurm".

Würmer galten zunächst als domestizierte Arbeitstiere. 1982 stand zwei Forschern am renommierten Xerox Research Center in Palo Alto eine ebenso mühsame wie langweilige Arbeit bevor: Sie mussten eine neue Software auf allen 100 Rechnern ihres Netzwerkes installieren. John Shoch und Jon Hupp ließen sich von der Romanfantasie inspirieren, bepackten einen "Wurm" mit dem Programm und schickten ihn auf die Reise durchs Netz, damit er für sie die Installation verrichten würde. Es ist eine alte Geschichte, doch bleibt sie ewig neu: den beiden erging es wie dem faulen Zauberlehrling in Goethes gleichnamigen Gedicht, der seine automatischen Besen losschickt zum Wasserholen, aber die Kontrolle über die dienstbaren Geister verliert.

Der Xeroxwurm pflanzte sich zwar fleißig von Rechner zu Rechner fort. Aber sobald er sich eingenistet hatte, brachte er das jeweilige Gerät zum Absturz. Die beiden Forscher bezogen sich allerdings auf eine neuere Variante des Zauberlehrling-Themas und zitieren in einem Fachaufsatz im renommierten Magazin Communications of the ACM ausführlich aus dem Sciencefiction-Roman "The Shockwave Rider". Der Wurm hatte nicht nur Rechner, sondern auch ihre Fantasie angesteckt: "An diesem Punkt möchte man sich eine Szene vorstellen, die direkt aus John Brunners Roman stammen könnte", schreiben sie. "Mitarbeiter, die durch das Gebäude rennen und vergeblich versuchen, den Wurm zu fangen und zu stoppen, bevor er weiterwandert." Fazit: "Leider war das peinliche Resultat für alle klar sichtbar: 100 tote Maschinen über das gesamte Gebäude verteilt."

Verirrt im eigenen Gruselmärchen: Die Höllenfahrt des Doktor Joseph Popp

Fast schien es, als hätten die Geister, die von Neumann im Namen der Effizienz und Rationalisierung gerufen hatte, tatsächlich eine Art Eigenleben entwickelt. Die Ähnlichkeit mit biologischen Erregern wurde unübersehbar. 1986 gab der amerikanische Informatiker Fred Cohen den schwer zu bändigenden Hilfsprogrammen in seiner Doktorarbeit ihren Namen und die noch heute gültige Definition: "Ein Computervirus ist ein Programm, das andere infizieren und verändern kann, um ihm Versionen von sich selbst, die auch verändert sein können, hinzuzufügen." Damit waren alle Zutaten für das Gräuelmärchen beisammen: Neunmalkluge Doktoren, die hinter den verschlossenen Türen ihrer Labors künstliche Lebewesen erschaffen, die sich jedoch gegen sie wenden und in einem wütenden Vernichtungsfeldzug die Welt terrorisieren.

Schnell mutierten die Viren von rein akademischen Gedankenspielen zu kleinkriminellen Tatwaffen. Der "Brain"- oder "Pakistani-Virus" verbreitete sich um das Jahr 1986 herum auf möglicherweise über 100 000 Disketten weltweit. Damals waren Disketten mit raubkopierter Software ein beliebtes Mitbringsel aus Drittweltstaaten. Zwei pakistanische Brüder, die in Lahore ein blühendes Raubkopiergeschäft betrieben, waren angeblich einfach neugierig, den Weg ihrer Konterbande über die Welt zu verfolgen, und setzten daher den neuartigen Virus aus als eine Form der automatisierten Marktforschung. Sie hinterließen sogar ihre Telefonnumer im Virencode.

Doch der eigentliche Markt, das stellte sich schnell heraus, lag woanders: nicht im Konsum, sondern im Terror. Besonders aufsehenerregend war die Erpressungskampagne eines Programmierers namens Dr. Joseph Popp, der 1989 vom amerikanischen Cleveland aus 20 000 Disketten mit dem "Aids-Virus" per Post an Computernutzer in Europa verschickte. Die Diskette versprach Informationen zum Thema Aids, aber sobald das Programm lief, verschlüsselte es alle Dateien auf dem Rechner des Opfers und forderte dazu auf, 200 Dollar auf ein Konto in Panama zu überweisen, um den Code zur Freischaltung der eigenen Daten zu erhalten. Doch am Tag, als die ersten Disketten ihre Opfer erreichten, marschierte zufällig ein Großaufgebot der US-Armee in Panama ein und das Computer-Kidnapping floppte. Dr. Popp wurde nach England ausgeliefert. Die Idiotie, die ihn vor den Kadi gebracht hatte, rettete ihn auch. Der Prozess wurde zur Farce und endete ohne Gefängnisstrafe, weil Dr. Popp überzeugend den globalen Dorfdepp mimte und sich bei Gerichtsterminen einen Pappkarton über den Kopf zog.

Derlei grober Unfug, die "Popp"-Kultur sozusagen, zog immer weitere Kreise, die Koevolution von Elektronenhirnen und Elektronenviren vollzog sich mit rasanten Sprüngen. Und stolperte dabei immer wieder über die eigene Wichtigtuerei. In

dutzenden von privaten Mailboxsystemen tauschten Anfang der Neunziger Computerfreaks ihre digitalen Schädlinge aus. Virenschreiber heucheln gern akademisches Interesse vor, um sich vor den Ermittlungsbehörden zu schützen. Sie alle haben eines gemeinsam: Sie sind männlich, zwischen 12 und 30 und arg pubertär. Den Plural von Virus nennen sie "Virii", was wohl Intelligenz vortäuschen soll. Paskell Paris zum Beispiel, ein Krankenpfleger aus Oklahoma, nannte seine Viren-Mailbox wahlweise ganz seriös "The Oklahoma Institute of Virus Research", in der Szene dagegen firmierte sein digitaler Giftschrank als "The Vortex" - der Strudel. "Es gibt viele Wege, Gottgleichheit zu erlangen", versprach der Krankenpfleger in seinem Forum, "wenn du es schaffst, die falschen weltlichen Hemmungen von Ethik und Moral hinter dir zu lassen... etwas zu erschaffen ist immer nett, aber die wahre Macht liegt in der Kraft, zu zerstören." Virenschreiber imaginieren ihre Rechner als Transportmittel ins eigene Herz der Finsternis - und landen dabei meist doch nur wie Dr. Joseph Popp im Innern eines Pappkartons, einer Black Box, aus der ihre Beschwörungen hohl hervortönen.

> Prinzipiell müssen wir uns damit abfinden, dass wir das Problem nicht in den Griff bekommen. Man kann sich allerdings an gewisse Grundsätze halten, was die Disziplin im Umgang mit sensiblen Daten angeht. (Werner Paul. Spezialist für Computerviren und Computerkriminalität im Münchener Landeskriminalamt)

Die Virenschreiber bilden eine Erzählgemeinschaft, deren wichtigste Kommunikationsform die "Kommentarzeilen" sind, die sich inmitten des Virencodes befinden. Normalerweise sollen Kommentarzeilen erläutern, was ein bestimmter Programmabschnitt tut. Virenschreiber dagegen verwenden Kommentarzeilen als Flaschenpost, die fast immer von ihren drei Lieblingsthemen handelt: Ich, ich und nochmals ich. Im zerstörerischen "I-Love-You"-Virus zum Beispiel fand sich das rührende Gestammel: "I hate go school" und "Manila". Tatsächlich kam der Schreiber Onel de Guzman aus der philippinischen Hauptstadt. Sein vermeintlicher Mittäter setzte in eines seiner Frühwerke mal die Drohung ein, einen noch viel gefährlicheren Virus auszusetzen, "wenn ich bis Ende des Monats nicht einen festen Job habe". In einem anderen Virus durften Schriftkkundige folgende altkluge Konfirmandenweisheit zwischen den Zeilen lesen, verfasst in holprigem Englisch: "Watch your thoughts, it becomes word/ Watch your words, it becomes actions/ Watch your actions, it becomes your habit/ Watch your habit, it becomes your character/ Watch your character, it becomes your Destiny". Amen. Gerne und ausführlich wird in Zeitungsmeldungen darüber spekuliert, was diese Digitalgraffiti zu bedeuten haben. Und häufig lässt die Prahlerei im Programmcode ihren Autoren tatsächlich poetische Gerechtigkeit widerfahren - oft führen verräterische Hinweise zur Ergreifung der Täter.

Der Virenschreiber von heute zehrt zwar vom Mythos des großen John von Neumann, ähnelt selber aber eher seinem Namensvetter Alfred E. Neumann, der Karikatur eines kindischen Kotzbrockens im Comicheft "Mad." Deshalb verhalten sich manche Virenforscher auch eher wie Sozialarbeiter, die Problemkids bemuttern. Sarah Gordon ist so eine Virenmutti - der einzige weibliche Star der globalen Popp-Kultur. Gordon, die durch ihren sozialpsychologischen Aufsatz "The Generic Virus Writer" bekannt geworden ist, war früher tatsächlich Sozialarbeiterin. Heute ist sie angeblich täglich 10 bis 12 Stunden online, um sich in Virenchats herumzutreiben und mit den Kids zu plaudern. Den typischen, "generischen" Virenschreiber gebe es nicht, sagt sie. Doch alle haben eines gemeinsam: sie genießen die Aufmerksamkeit. An dieser Profilneurose könnte eine neue, ganzheitliche Virentherapie ansetzen, sagt Gordon sinngemäß. Das Image der Virenschreiber müsste von "cool" zu "uncool" umgeformt werden. Das sei nicht schwer, so die virtuelle Sozialarbeiterin weiter, denn Virenschreiben erfordere keine besonderen Fähigkeiten. "Virenschreiber sind nicht zufällig ganz unten in der Hackordnung der Hacker- und Cracker-Subkultur", so Gordon. Wie Recht sie mit ihrer respektlosen Einschätzung hat, zeigt schon ein flüchtiger Blick hinter die alberne Drohkulisse all der größenwahnsinnigen kleinen Möchtegern-von-Neumännlein.

Ein Digitaldepp vor Gericht

September 2001. Der Urheber des Kurnikowa-Wurms steht vor Gericht. Es ist das wohl erste Mal, dass ein Virenautor angeklagt wird, der gar nicht programmieren kann. Vierzig Beobachter und Neugierige verfolgen den Prozess. Ein seltener Ansturm in Leeuwarden, der Provinzhauptstadt von Friesland hoch oben im Norden der Niederlande, wo schwerer Güllegeruch von satten Kuhweiden herüberzieht.

Wer allerdings ein böses Genie erwartet, wird gründlich enttäuscht. Jan de W. ist ein kräftiger Bursche in T-Shirt, schwarzen Jeans und Turnschuhen. Dieser Tage feierte er seinen einundzwanzigsten Geburtstag. "Reden Sie lauter", muss der Vorsitzende Richter ihn immer wieder auffordern, oder auch: "Haben Sie die Frage verstanden?" Doch der Angeklagte sitzt meist so teilnahmslos da wie ein abgestürzter Rechner. Trotzig verschränkt er seine Arme und ähnelt einem Bauernlümmel, der beim Äpfelklauen erwischt worden ist. "Sie müssen jetzt etwas antworten", erinnert ihn der Vorsitzende Richter, und versucht, eine strenge Miene zu machen. Huldvoll lächelt Königin Beatrix dem Angeklagten zu von einem Bild an der Wand hinter dem Richter.

Drei Richter befinden über den neuartigen Fall. Erstmals kommt in dem Musterprozess ein neuer Straftatbestand zur Anwendung, der das Verbreiten von

Computerviren verbietet. Maximales Strafmaß: vier Jahre Freiheitsentzug. Deutschland hat keinen vergleichbaren Paragrafen. Hierzulande ist lediglich das Ausspähen und Verändern von Daten verboten, nicht aber ihre Verbreitung. Dennoch scheint es fast, als sei auch die niederländische Novelle schon wieder veraltet. Denn die Welt der digitalen Plagegeister befindet sich im Umbruch. Selbst gewöhnliche Internet-Surfer können ohne kriminelle Energie zu Schöpfern von Viren und Würmern werden. Der grobe Unfug als Straftatbestand tritt ein ins Zeitalter seiner digitalen Reproduzierbarkeit.

W. jobbt zwar in einem Computerladen, hat aber selbst nicht die Fähigkeiten, eigene Programme zu schreiben. Er benutzte einfach einen vorgefertigten Virenbausatz, den er von einer argentinischen Internetsite heruntergeladen hatte. Der Bausatz namens "VBS Worm Generator" ist ein winziges Programm: nur 540 Kilobyte klein und kinderleicht zu bedienen. Mit wenigen Klicks erstellt es für den Nutzer ein maßgeschneidertes Virus. Geschrieben wurde der Bausatz von einem Programmierer mit dem Pseudonym [k]alamar, angeblich ein Teenager aus Buenos Aires. "Sie müssen zustimmen, dass [k] keine Verantwortung übernimmt für etwaige Schäden", schützt sich der Argentinier vor etwaigen rechtlichen Folgen. "Dieses Programm ist nur zum Lernen gedacht, nicht zum Verbreiten." Auch der grobe Unfug wird ausdifferenziert in der Informationsgesellschaft und teilt sich auf in begabte Schreibtischtäter, die virtuelle Waffen schaffen, und Digitaldeppen, die sie aus Neugier und Dummheit anwenden. Und sich dabei oft selbst ins Knie schießen. Nach wie vor ist der argentinische Wurmgenerator online, regelmäßig kommen neue Versionen heraus. Rechtlich hat [k]alamar tatsächlich nichts zu befürchten.

Anteil der Viren-infizierten E-Mails:

1999: 1 von 1400

2000: 1 von 700

2001: 1 von 300

2004: 1 von 100 (Voraussage)

2008: 1 von 10

2013: 1 von 2

2015: 3 von 4

(Vorhersage der Antiviren-Firma Messagelabs im September 2001)

Virenschreiben gilt als Kavaliersdelikt. Viele Dutzend Bausätze werden kosten- und straffrei auf Websites angeboten, unter skurrilen Namen wie Satanic Brain Virus Tools, Instant Virus Production Kit oder Ye Olde Funky Virus Generator. Mittlerweile beherrschen viele Bausätze allerlei Tricks und Kniffe, die früher zur höheren Schule

des Virenschreibens gehörten: Sie verschlüsseln sich selbst und werden zu so genannten Tarnkappen-Viren, die von älterer Abwehrsoftware kaum erkannt werden können. Oder sie verändern von Generation zu Generation ihren eigenen Code. Dadurch wird das Aufspüren dieser so genannten polymorphen Viren ebenfalls erschwert. Das Verbreiten von Virenbaukästen müsse gestoppt werden, fordert der US-Sicherheitsexperte Richard Smith, "das ist so, als ob man ein geladenes Gewehr an ein Kind verschenkt".

Über 60 000 Varianten dieser potenziellen Waffen wurden bislang im Internet gesichtet, Tendenz steigend. Wöchentlich kommen Dutzende hinzu - und immer mehr werden von Laien mit Fertig-Bausätzen zusammengeklickt. Die meisten der Bausatzviren verstolpern sich schnell an internen Programmierfehlern, und falls sie sich doch verbreiten, hat Antivirensoftware ein leichtes Spiel bei der Analyse.

Der Kurnikowa-Wurm war eher eine Ausnahme. Er verbreitete sich rasend schnell. Glücklicherweise war der Erreger relativ harmlos und vernichtete keine Daten oder Hardware, sondern nur Arbeitszeit. "Wir haben im Schnitt alle drei Monate eine große Virusepidemie im Internet", berichtet Howard Fuhs, ein Sicherheitsberater aus Wiesbaden. Im Netz gibt es bereits Kalender, auf denen ähnlich wie bei einem Wetterbericht täglich die Aktivierungstermine von lauernden Viren vermeldet werden, oft sind es zwei bis drei pro Tag. Derzeit werden die digitalen Nervensägen auch allmählich in modernen Mobiltelefonen und auf elektronischen Terminkalendern heimisch. Von Neumanns "selbstreproduzierende Automaten" sind heute so selbstverständlich geworden wie Regen in London. Man richtet sich eben drauf ein und sagt sich: Es gibt kein schlechtes Wetter, nur schlechte Kleidung. Um so unverständlicher ist es, dass immer noch Surfer ohne aktuelle Virenscanner unterwegs sind und sich von Schadprogrammen überrumpeln lassen.

Angeblich wollte der Urheber des Kurnikowa-Virenangriffs genau vor solcher Naivität warnen. "Die Leute sind so dumm", sagte er in einem Interview mit dem Onlinemagazin Wired.com, "Sie sind selber Schuld, wenn sie auf Viren hereinfallen." Doch er selbst war genauso leichtsinnig wie die Internet-Experten und -Nutzer, denen er eine Lehre erteilen wollte. W. hatte vergessen, seine Kurnikowa-Fanpage rechtzeitig vom Netz zu nehmen, auf der er vom "besten Tennisstar der Welt" schwärmte, mitsamt E-Mail-Adresse, Namen und Wohnort: "Ich heiße Jan und wohne in Sneek (Friesland)."

Jan de W. gab weiteren Online-Zeitschriften Interviews über seinen Virus. Spätestens dadurch flog er auf. Bevor er festgenommen wurde, ging er zwei Tage nach der Tat gemeinsam mit seinen Eltern zur Polizeistation von Sneek und zeigte sich an.

Mit diesem Geständnis sprang die akute Virusinfektion auf Siebold Hartkamp über, den Bürgermeister von Sneek. Spontan bot er dem Bausatz-Lümmel einen Job an. "Solche Leute können wir in unserer Computerabteilung gut gebrauchen",

schwärmte der Bürgermeister wie in einem Friesenwitz, "plötzlich steht unsere Stadt auf der digitalen Weltkarte."

Die Verhandlung um den Bausatz-Wurm war nach nur zwei Stunden abgeschlossen. "Ich plädiere auf Freispruch", sagte der Verteidiger. Bösartige Software sei heute etwas ganz Normales: "Viren sind Teil vom Internet-Game."

Die Richter gaben ihm weitgehend Recht, als sie zwei Wochen später das Urteil verkündeten, eine eher symbolische Strafe: 150 Stunden gemeinnützige Arbeit sowie die Konfiszierung der CD, auf der der Schuldige seinen Virenzoo gespeichert hatte. Ganz so, als könnten die Richter stellvertretend für den dusseligen Jan de W. wenigstens dessen digitale Plagegeister dingfest machen.

Anatomie eines Märchens: Im Netz der Panikindustrie

Spätestens nach dem Prozess gegen den Virenlümmel aus Friesland fällt es schwer, an die Bedrohlichkeit genialer junger Von-Neumännchen hinter den "Teufelsdingern" zu glauben. Der Virenkomplex ist nicht irgendeine Randerscheinung der Computerisierung. Der Umgang mit der Virenproblematik ist ein Gradmesser für das Erwachsenwerden der Wissensgesellschaft. Derzeit befinden sich alle beteiligten Akteure tief in die Wahnwelt ihres eigenen Märchens verstrickt: die Virenschreiber genau wie die Antivirenindustrie, die Netzwerkbetreuer genau wie die Medien.

Jahrzehntelang fand die Forschung an Viren und an ihrer Abwehr sowie ein- und denselben akademischen Labors statt. Daher haben die Antivirenberater einen fast ebenso schlechten Ruf die Virenschreiber selber. Die AV-Industrie sei geprägt von "schamlosen Tricksereien, hirnlosem Geschwätz, das sich als Vernunft tarnt, ätzender Vulgarität, lächerlichen Kleinkriegen, schmutzigen Tricks", schreibt George Smith, ein Netzbeschmutzer und Sicherheitsberater aus Kalifornien, in seiner schonungslosen Abrechnung "The Virus Creation Labs". Jahrzehntelang ließ sich in im schmutzigen Codekrieg nicht genau sagen, wer auf welcher Seite der Front steht. Denn ohne Viren keine Antivirenindustrie. Virenschreiber sehen sich oft in einem sportlichen Wettbewerb mit Virenscannern, und fühlen sich anerkannt, wenn ihr armseliges kleines Virus erkannt wird vom Schutzprogramm.

Virenfreunde wie Mark Washburn schrieben sowohl Viren als auch Antivirenprogramme, Dealer wie John Buchanan vertickten ihre teilweise selber geschriebenen Sammlungen gegen Geld. Hackertools und Vireninformationen tauchten sogar auf einer öffentlichen Verwaltungs-Mailbox der Sicherheitsberaterin

einer US-Behörde auf. Ein gewisser "Dark Angel" widmete daher seinen Virengenerator großherzig "sowohl der Virusgemeinde wie auch der Antivirusgemeinde, die beide davon profitieren werden..." Wer derlei Freunde hat, braucht keine Feinde.

Um sich von ihren Zulieferbetrieben, den Virenschreibern, zu unterscheiden, inszenieren sich die Hersteller von Antivirensoftware ebenfalls als Comichelden: Sie sind die Götter in Weiß, die unermüdlich gegen den bunten Mutantenzoo aus Viren, Würmern und Trojanischen Pferden kämpfen.

Die Gründergeneration der AV-Industrie rekrutierte sich oft aus schillernden Persönlichkeiten wie John McAfee, der versucht hatte, eine Art virtuellen Safe-Sex-Swingerclub aufzuziehen, indem er eine Datenbank aufbaute, in der sich Silicon-Valley-Bewohner eintragen lassen konnten, wenn sie beim Aids-Test HIV-negativ getestet wurden. Doch das Geschäft lief nicht so recht, und so verlegte er sich lieber auf Digitalviren. Der Durchbruch für seine Firma McAfee kam 1992, als alle Welt vor dem mythischen Michelangelo-Virus erzitterte, das sich über eine Floppydisk verbreitete. Am 6. März, dem Geburtstag des Malers Michelangelo, würde der Virus zum Leben erwachen und große Teile der Festplatte mit sinnlosen Daten überschreiben. Die junge Antivirenindustrie tat alles, um die Panik zu schüren, und fütterte die sensationshungrige Presse mit leckeren Zitaten. Fünf Millionen Computer waren angeblich infiziert, "Millionen von PC könnten am Freitag abstürzen," schrieb USA Today, und die sonst eher skeptische Washington Post warnte: "Tödlicher Virus richtet morgen ein Chaos an." Michelangelos Geburtstag kam und ging, doch der Weltuntergang blieb aus. Das sei der Presse und ihren Warnungen zu verdanken, orakelte daraufhin McAfee, die Medien hätten eine Medaille verdient. Dabei gehörten sie eigentlich an den Pranger.

Virenmärchen scheinen immun zu sein gegen Widerlegungen, denn immer, wenn sie sich als heiße Luft erweisen, wird das Ausbleiben der Katastrophe als ihr Verdienst in die Große Erzählung vom Kampf gegen das Böse interpretiert. Ein alter Kniff aus der Trickkiste aller falschen Propheten. Doch diese clevere Erzählstrategie der Gräuelmärchenonkels hat sehr reale Auswirkungen: McAfee verkaufte allein im Februar und März des Michelangelo-Jahres 68 Prozent mehr Firmenlizenzen als bisher. Seitdem gehören überzogene Kassandrarufe zum festen Repertoire der Branche.

Scheint so, als würde deine Alpträume jetzt wahr. (Anzeige des Smash-Virus, bevor er den gesamten Inhalt der Festplatte löscht)

Die Olympischen Winterspiele 1994 in Lillehammer zum Beispiel sollten angeblich gefährdet sein durch den "Olympic Aids"-Virus. Nichts passierte. Dabei hätte schon die Bekennerbotschaft stutzig machen können, die im Code versteckt war: "Dieser Virus wurde nur geschrieben, um Angst und Publicity zu erzeugen." Der virale

Olympiateilnehmer erreichte sein Ziel - mit wortmächtiger Unterstützung der Medien.

Im Juli 2001 warnte das amerikanische National Infrastructure Protection Center (NIPC) eindringlichst vor dem Wurm Code Red, der sich nicht durch die Rechner der Endbenutzer schlängelte, sondern über professionelle Server verbreitete. Das FBI riet sogar dazu, sich während der Zeit des erwarteten Angriffs vom Internet abzukoppeln. Daraufhin waren Websites wie die des Pentagon waren zeitweilig gar nicht nicht zu erreichen - eine weitaus größere Beeinträchtigung als der Virus selbst herbeigeführt hätte. Denn Code Red brachte das Internet nicht zum Erliegen, wie die Hype-Industrie prophezeit hatte. Die Kassandras lagen wieder einmal daneben, und Insider tauften Code Red in "Code Dead" um. Zwar wurde an dem betreffenden Termin das Netz langsamer. Aber das lag nicht an dem Virus, sondern an einem Kabelbrand. Ein Güterzug war in Baltimore entgleist und hatte in einem Tunnel die Kabel von sieben großen Internetprovidern angeschmort.

Hoaxes: Virenprofis warnen vor Virenwarnungen

Längst kursieren Parodien auf die lächerlichen Windei-Warnungen der Antivirenindustrie:

> "ACHTUNG!! Noch während Sie seelenruhig diesen Artikel lesen, könnte Ihr Rechner von einen ELEKTRONISCHEN Virus KLEINGESCHREDDERT werden. Schicken Sie diese Mail SOFORT an ALLE Menschen, die Sie kennen!!!"

Online-Veteranen kennen derartig hysterische Warnungen, die immer wieder im elektronischen Postkasten landen, häufig von aufgeschreckten Bekannten weitergeleitet. Die Gefahren, vor denen diese E-Mails warnen, existieren nicht. Doch bis der Empfänger das gemerkt hat, haben die Mitteilungen ihre Aufgabe bereits erfüllt: seine Zeit gestohlen. "Hoaxes" heißen die Windei-Warnungen auf Neudeutsch - im Klartext: "Verarschungen". Wichtigstes Stilelement ist der ausgiebige Gebrauch von Ausrufungszeichen, Großbuchstaben und pseudotechnischem Science-Fiction-Geschwafel: "Der Prozessor wird in eine n-komplexe, unendliche Binärschleife geschickt", orakelt etwa die Warnung vor dem (nicht existierenden) "Good Times"-Virus, einem stilbildenden Klassiker des Genres, der anno 1994 für viel unnötige Aufregung sorgte. Meist kulminieren Hoaxes in der Aufforderung, die Mail an möglichst viele Menschen zu versenden.

In Deutschland ist seit Jahren immer wieder der "Telefonmissbrauch"-Hoax virulent. Er warnt Mobiltelefonierer davor, eine bestimmte Nummer einzugeben (meist die 09 oder 90), da sonst die SIM-Karte ausgelesen werden könnte und später die Telefonkosten "ins Unermessliche" steigen würden. Ein "Klingelstreich" mit Folgen:

Beim Mobilfunkanbieter T-Mobile gehen seither immer wieder besorgte Anrufe ein. "Einmal in die Welt gesetzt, ist ein Hoax nicht mehr zu stoppen", sagt Pressesprecher Stephan Althoff genervt. "Ein Scherz bekommt im Internet ein Eigenleben."

Der SIM-Karten-Jokus zum Beispiel geht schon seit Anfang 1998 um: Da grassierte er laut Althoff in Irland. "Als man dort Entwarnung gab, schwappte der Hoax auf den Kontinent rüber, anfangs vor allem in die Alpenrepubliken." Im Jahr 1999 eroberte er Deutschland, wo er immer wieder von neuem auszubrechen scheint. "Wir haben mal drei Monate Ruhe, dann kommt er wieder", so Althoff. Der Grund: Immer neue Handy- und Internet-Nutzer kommen dazu und kennen das abgedroschene Seemannsgarn der alteingesessenen Netzbürger noch nicht. Einem Hoax auf den Leim zu gehen gleicht einer Äquatortaufe im Meer der Daten und Frequenzen.

Im Hoax wiederholen sich viele wahre Begebenheiten der Virengeschichte als Farce - und nehmen eine ganz eigene Realität an. "Unsere Hotline hat mehr mit Hoaxes zu kämpfen als mit echten Viren", heißt es auf der Homepage von Sophos, einem Antivirenprogramm-Hersteller. "Obwohl es keine offiziellen Studien darüber gibt, wird geschätzt, dass ein Hoax mehr Schaden anrichten kann als ein echter Virus." Die amerikanische EDV-Eingreiftruppe Computer Incident Advisory Capability (CIAC) nennt mögliche Schäden: Der E-Mail-Verkehr schwelle unnötig an, und der Produktivitätsverlust sei enorm, wenn Tausende von hoch bezahlten Büromitarbeitern auch nur eine Minute mit dem Lesen und Löschen eines Hoaxes verbringen - was häufig vorkommt. Wenn das von Neumann wüsste, er würde wahrscheinlich entzückt ein paar neue Gleichungen formulieren: Wie das Signalgewitter eines epileptischen Anfalls jagen die Unsinnsmeldungen durchs Zentralnervensystem des Internet - vor allem, weil viele User schneller klicken als denken. Unzensiert huschen so finstere Phantasmen durchs Netz. Und Spekulationen über das Warum und Woher klingen bisweilen selbst wie Hirngespinste: "Es gibt Gerüchte, dass die Versender von Werbe-Mails absichtlich Hoaxes und Kettenbriefe anzetteln, um E-Mail-Adressen zu sammeln", munkelt das CIAC - nur um gleich einzuschränken: "Natürlich könnte auch das wiederum ein Hoax sein."

"Hoaxes sind kein technisches, sondern ein soziologisches Phänomen", sagt Frank Ziemann, ein Berliner Netzwerkspezialist, der einen kostenlosen Hoax-Newsletter an über 12 000 Abonnenten verschickt. "Die meisten Hoaxes kommen von Kids, die zu doof sind, echte Viren zu programmieren." Und das, man denke an Jan de W., will schon etwas heißen.

Der Ursprung einiger Hoaxes entpuppt sich als Aprilscherz in einer Zeitung, wie etwa die Meldung, dass die USA noch vor dem Golfkrieg Drucker mit manipulierten Chips in den Irak lieferten, um dort Rechner der Flugabwehr zu infizieren. Andere Hoaxes

scheinen einen wahren Kern zu haben, der durch das Prinzip der stillen Post immer weiter verfälscht worden ist.

Selbst harmlose Scherze wie der "Honor System"-Hoax können verunsichern, wenn ein Netzneuling das Humorige daran nicht gleich kapiert: "Dieser Virus funktioniert auf Vertrauensbasis. Schicken Sie diese Botschaft an jeden, den Sie kennen, und löschen Sie dann alle Dateien auf Ihrer Festplatte. Vielen Dank für Ihre Mithilfe."

Mit derlei Fantasieviren, die sich losgelöst von der Realität von Hirn zu Hirn hangeln, kehrt die computerisierte Gesellschaft zu ihren Wurzeln zurück: Zu den Gedankenexperimenten des John von Neumann zum Computer als Gehirn-Nachbau und zu "komplexen Automaten", die sich selber vermehren können. Gedanken selbst werden infektiös und werden so wirksam wie Computerviren.

Einerseits sind sie Teil des Virenproblems, andererseits könnten sie Teil der Lösung sein: Hoaxes sind ein Crashkurs in Sachen Skepsis. Gerade ihre absurde Fantastik macht sie zum perfekten Lehrmaterial für die Stiftung Märchentest. Wer dies Genre kapiert, hat auch die meisten anderen Hightechmärchen durchschaut. Doch mit Skepsis allein ist das reale Virenproblem noch nicht gelöst.

Asymmetrische Attacken

Es scheint paradox: Wie kann es sein, dass ein paar hundert spätpubertäre Neumännchen die klügsten Köpfen der milliardenschweren Computerbranche als jammernde Statisten durch ihre Comicheld-Fantasien hetzen?

Zwei Antworten bieten sich an, die eine einfach, die zweite überzeugend. Zuerst die einfache: Die Nutzer sind immer noch erstaunlich naiv. Kaum jemand scheint dazugelernt zu haben, seit der verheerende "I-Love-You"-Virus im Jahr 2000 mehrere Millionen Rechner attackierte. Wer sich seitdem ohne ein aktuelles Virenschutzprogramm ins Internet begibt, handelt grob fahrlässig, so als wäre das Internet immer noch das nette globale Dorf, das es nie gewesen ist.

Rein technisch ist der Virenschutz banal. So einfach, wie sich Viren erstellen lassen, lassen sie sich auch erkennen von sogenannten "Virenscannern" oder Antivirus-Tools (AV). AV-Programme sind im Grunde genommen Volltext-Suchmaschinen, welche einfach jedes Programm, das auf einem Rechner installiert wird, nach verräterischen Codezeilen oder auffälligem Verhalten durchsuchen. Kein Virenprogramm kann je alle Viren erkennen, aber durch die Kombination von zweien und durch regelmäßige Updates ließe sich fast jede globale Epidemie im Keim ersticken.

Dennoch verzichten immer noch viele Internetnutzer auf diese Programme, oder verschludern einfach, sie zu aktualisieren. Denn zwei Märchen schaukeln sich gegenseitig hoch. Der Alptraum vom Teufelsvirus, gegen den nur Beten hilft auf der einen Seite. Auf der anderen Seite das Idyll vom schmusigen globalen Dorf, in dem keine Hütte ein Türschloss braucht. Der Effekt sind Milliardenschäden, die sich leicht verhindern ließen. Virenschutzprogramme müssten eigentlich so selbstverständlich sein wie eine verschließbare Wohnungstür in New York, ein Regenschirm in London oder ein Fahrradschloss in Amsterdam.

Angesichts des viralen Dauerbeschusses geht allerdings auch ein erhebliches Sicherheitsrisiko von den Profis aus: von verschusselten Netzwerkbetreuern, im Fachjargon Systemadministratoren oder einfach Admin genannt, die als Hausmeister des Netzes die Server der Webseiten am Laufen halten. Im September 2001 verbreitete sich zum Beispiel ein neuer Internet-Wurm mit rasender Geschwindigkeit. Der Nimda-Virus benutzt Software aus dem Hause Microsoft, um die PC ahnungsloser Surfer zu manipulieren. Nimdas neuer Trick: Schon das Aufrufen einer Webseite genügt unter Umständen, und schon ist der Rechner infiziert. Diese Sicherheitslücke war seit über einem Jahr bekannt. Doch viele Admins verschliefen es, die Lücke mit einem kleinen Zusatzprogramm zu schließen. Wie jeder Virus war auch Nimda eine Art interaktive Botschaft: Der geheimnisvolle Name Nimda ist einfach "Admin", rückwärts gelesen.

So drehen sich alle munter im Teufelskreis ohne Ausgang: Die Virenschreiber fühlen sich angestachelt, soviel Doofheit auszunutzen, die Antivirenhersteller warnen vor der Infokalypse, um ihre Produkte zu verkaufen, und die Medien sind dankbar für die regelmäßigen Schlagzeilen. Naive Internetnutzer wiederum fühlen sich einerseits bestens unterhalten von den Horrormärchen. Neulinge fühlen ein Grundgefühl bestätigt: Dass sie machtlos sind gegenüber den Tücken der Technik. Und werden es dadurch wirklich. Dies Horrormärchen dürfte einer der teuersten Fortsetzungsromane der Geschichte sein mit milliardenschweren Produktionskosten pro Jahr.

Neben dieser gleichsam moralischen Erklärung für die Hilflosigkeit der Informationsgesellschaft gegenüber den Virenattacken gibt es eine strategische: die Asymmetrie der Angriffe. Viren funktionieren asymmetrisch, denn mit geringem Aufwand wird eine gigantische Wirkung erzielt. Ein einzelner kleiner Jan de W. lässt von Sneek aus seine automatische Schadensroutine Tag und Nacht millionenfach für sich arbeiten. Ein derartig effizientes Vorgehen schwebte auch von Neumann vor, als er die dienstbaren Geister erdachte. Der Virenschutz dagegen funktioniert immer noch weitgehend manuell: Mit großem Aufwand wird geringer Nutzen erzielt, durch mühsame Hand- und Kopfarbeit von Millionen von Netzwerkberkbetreuern, Sicherheitsberatern und Einzelnutzern. Immer, wenn wieder irgendein lächerlicher Friesenvirus durchs Netz geistert, muss an Millionen von Rechnern eine neue Sicherheitsmaßnahme ergriffen werden.

Zwei Produktionsformen treffen bei Virenepidemien aufeinander, ähnlich wie im amerikanischen Bürgerkrieg, als der industrielle Norden 1865 den agrarischen Süden besiegte, vor allem durch die Überlegenheit der Industrie. Die Virenkids spielen Nordstaaten und piesacken mit ihrem vollautomatischen Virenunfug eine veraltete Frühform der Informationsgesellschaft, die auf einzelkämpferische Informationshandwerker setzt. Auch die schärfsten Gesetze können an dieser grundlegenden Asymmetrie nichts ändern. Solange die Virenabwehr nicht ebenso vollautomatisch funktioniert wie die Attacken, werden immer wieder Virenstürme von Ost nach West durch die globalen Netze toben mit den ersten Sonnenstrahlen. Solange die Informationsgesellschaft auf Handarbeit setzt, ergeht es ihr wie den Südstaaten: Sie bleibt Opfer ihrer archaischen Produktionsweise sowie der eigenen Selbstverzauberung.

Dumpfe Rotzlöffel wie Jan de W. sind Lehrmeister in Sachen Modernisierung, ohne es zu wollen und ohne es zu wissen. Es gilt nur, zwischen den Zeilen der Virenprogramme zu lesen. Neben den pubertäten Graffiti ihrer Autoren verbreiten sie eine zweite Botschaft: das Evangelium von der Software-Automatisierung und ihres Apostels St. John von Neumann.

Technisch ist die Infrastruktur für einen weitgehend automatischen Virenschutz längst vorhanden. Doch kaum ein Privatkunde macht von dem Angebot Gebrauch, den eigenen Rechner durch automatische Updates schützen zu lassen. "Das setzt eine intensive Vertrauensverhältnis voraus", sagt Klaus Brunnstein, Gründer des Virus Test-Centers (VTC) an der Uni Hamburg. "Und dieses Vertrauen genießt die Antivirenindustrie anscheinend nicht." Das Märchen, das die Gräuelmärchenonkels streuen, um das Problem zu lösen, wird so selber zum Problem. Denn durch die Panikmache verspielen die Antivirenhersteller ihre Glaubwürdigkeit. Der Vertrauensverlust wiederum verhindert die dringend notwendige Automatisierung.

Die Branche hat sich in ihren eigenen Virenmärchen verheddert. Nun wird es höchste Zeit, die eigene Rolle und das eigene Image zu überdenken. Es wandelt sich vom Leitbild des Wunderheilers und Exorzisten zum Selbstverständnis einer staubtrockenen Polzeibehörde. Ein solcher Imagewandel bedürfte nicht einmal großer Fantasiearbeit. Denn im Alltag der Antivirenindustrie geht es längst so stinklangweilig zu, wie man es von einer zuverlässigen Schutzinstanz erwarten darf. Nun müsste sich diese Sensation des Alltags nur noch herumsprechen.

Sara und die Virenverwalter

Wo die automatische Bedrohung wächst, wird auch die Rettung automatisiert. "Darf ich vorstellen, das ist meine wichtigste Kollegin", sagt André Post, Informatiker bei

der Antivirenfirma Symantec in der Europafiliale im holländischen Städtchen Leiden. Sara ist Tag und Nacht im Einsatz und erledigt fast alle Virenmeldungen. Sara ist der Inbegriff der Antivirenindustrie, ein einziger Blick auf sie genügt, um die gesamte Branche zu begreifen. Sara sieht nichtssagend aus: ein Schrank mit ein paar Rechnern darin. Sara ist eine Virendatenbank, von der sich je eine Kopie im kalifornischen Cupertino und in Leiden befindet, in gut verschlossenen Sicherheitsräumen. Automatisch schicken die Rechner von Symantec-Kunden aus aller Welt verdächtige Software an Sara. Sara vergleicht sie mit den Beschreibungen aller bekannten Viren. Wenn das eingeschickte Virus bekannt ist, verschickt Sara binnen einer Minute automatisch das digitale Heilmittel per Internet an den Rechner des Kunden. Gefahr erkannt, Gefahr gebannt, vollautomatisch und ohne dass Anbieter oder Kunde davon etwas merken würden. Über 95 Prozent aller Virenmeldungen werden so abgearbeitet.

Für die restlichen fünf Prozent sind André Post und seine zwei Kollegen zuständig. An speziellen "Infektionsrechnern" nehmen sie die dubiosen Dateien unter die Lupe. Die Maschinen stehen völlig isoliert in einem speziellen Raum, und sind nicht einmal mit dem Firmennetz verbunden. Pro Tag untersucht Post rund 15 verdächtige Dateien. Wenn er morgens mit der Arbeit anfängt, kopiert er sie auf eine Diskette und trägt sie per Hand zu seinem Infektionsrechner.

Den Kurnikowa-Virus zum Beispiel bekam er um zehn nach elf, erzählt er. Eine Viertelstunde später war der Wurm seziert. Post hatte sich einfach die 50 Zeilen Code angesehen und festgestellt, welche Zeile ein typisches Erkennungsmerkmal ist: in diesem Fall war es der Programmbefehl, sich selbst an alle Mailadressen zu versenden. Er markierte diese verräterische Codezeile als sogenannten "Fingerabdruck" und sandte sie an Sara. Fertig war die Impfung, auch sie in vielen Fällen vollautomatisch: wenn der Nutzer das betreffende Feld anklickt, holt sich sein Rechner vor jeder Internetsitzung automatisch die neuesten Fingerabdrücke auf die lokale Festplatte. "Digital Immune System" heißt diese Technik.

Selbst der "I-Love-You"-Virus war nach zehn Minuten analysiert, sagt Post. Doch damit fing die eigentliche Arbeit erst an: Interviews vom Morgen bis zum Abend. "Ein Großteil meiner Arbeit ist Pressearbeit", sagt Post. Der Onkel Doktor ist immer auch ein Märchen- und Medienonkel, das wird in der Informationsgesellschaft einfach von ihm erwartet.

"Jaaa, ich habe hier einen Windows-Wurm", frohlockt sein Kollege Neal Hindocha irgendwann am Nachmittag. Es scheint schön zu sein, gebraucht zu werden in Zeiten der automatisierten Gefahrenabwehr. Vier Informatiker sitzen in der Leidener Filiale, um die Fingerabdrücke digitaler Eindringlinge zu nehmen. Sie blättern in Zeitschriften, trinken Kaffee, spielen zwischendurch Schach. Hier stemmen sich keine Datentetektive gegen den Ansturm der apokalyptischen Viren. Hier erledigt eine geordnete Virenverwaltung den täglichen Kleinkram. Die Virenerkennung selbst

macht in der Sicherheitsindustrie noch die wenigste Arbeit und dürfte im Prozentbereich liegen. Auf die vier Virensammler in Leiden kommen fast 200 Mitarbeiter, die in endlosen Gängen auf vier Stockwerken Verträge abwickeln, telefonische Beratungsgespräche führen, Pressearbeit machen oder in der Kantine Kaffee kochen.

Der neue Windows-Wurm, so stellt sich schließlich heraus, war keiner, sondern nur ein Fehlalarm. "Die meisten Viren, die wir bekommen, sind gar keine", sagt Hindocha leicht resigniert. Um fünf ist Feierabend, denn die Symantec-Zentrale im Silicon Valley übernimmt nun. Wer in der Virenindustrie die atemlose Verbrecherjagd hart am Abgrund der Datenapokalypse vermutet, sollte lieber einen Science-Fiction-Roman lesen. Oder wahlweise die atemlosen Pressemitteilungen von Finjan und FBI und NIPC und all den anderen Alleinunterhaltern.

Selten machen die Virenverwalter bei Symantec Überstunden. Nur die Datenbank Sara hält die Stellung. So lieblos und automatisiert, wie die unbegabten Virenkids mit ein paar Mausklicks ihre globalen Klingelstreiche zusammenpfuschen, so vollautomatisch putzt Sara das Netz wieder sauber.

***

Dieser Text ist ein Ausschnitt aus Hilmar Schmundts 2002 im Argon-Verlag erschienen Buch Hightechmärchen.