VIREN

Regine Buschauer

Am 10. November 1983 testete Fred Cohen an der University of Southern California ein kleines Computerprogramm, das zeigen sollte, wie sich ein Computersystem ›infizieren‹ lässt. Der Versuch war derart erfolgreich, dass er keine Fortsetzung finden durfte; Cohen wurde die weitere Systemnutzung für seine Versuche untersagt. Die Geschichte des Tests und ›ersten Virus‹ wurde Bestandteil von Cohens Dissertation, der sich die Bezeichnung ›Computervirus‹ verdankt, und sie verbreitete sich in kürzester Zeit auch in Deutschland: »Ein amerikanischer Student«, schrieb der »Spiegel« (47/1984), »entwickelte Programme, die in ›gesunden‹ Computern nisten können – wie ein heimtückischer Erreger im menschlichen Körper«. Cohen habe »das Chaos programmiert«.

Die »Zeitschrift für Kommunikations- und EDV-Sicherheit« (»KES«) griff das Thema auf, gefolgt von der »Computerwoche«: »Nach Hackern und Rote Armee Fraktion (RAF) nun virulente Software als weiteres Sicherheitsrisiko: Experten vom Thema Computer-Viren infiziert«, lautete deren Schlagzeile 1985, während die »Zeit« (44/1985) titelte: »Angst vor den Bitnappern«. »Die Viren kommen«, warnte etwas später »c't« (4/1987), die »Wirtschaftswoche« (2/1987) sah »Digitale Horrorbilder« und »PM-Computer« (10/1987) fragte: »Droht uns ein Computer-Aids?« Das Virale der Computer, so kann man folgern, hat auch in dieser medialen Hinsicht Geschichte. Vielleicht liegt es daran, dass heute Nachrichten von einem ›Computervirus‹, einer ›bösartigen Software‹ oder ›Malware‹ eigentümlich aus der Zeit gefallen scheinen.

POP. Kultur und Kritik • Heft 11 Herbst 2017 • S. 29–32 • © transcript

Irritierend jedenfalls war die Meldung von einer »Cyberattacke« und infizierten britischen Spitalsystemen, die am 12.5.2017 der »Guardian« online publizierte, während auf Twitter Bilder betroffener Anzeigetafeln der Deutschen Bahn zu sehen waren, die einen ›Oops‹-Screen im Designstil der 1990er Jahre mit einer Zahlungsaufforderung von $300 in Bitcoin zeigten. Es handle sich um einen erpresserischen Angriff mit der Schadsoftware WannaCry, die sich überaus rasch in bereits hundert Ländern verbreite, meldeten bald die Nachrichtensendungen. Eine Zeit der Verunsicherung und medialen Hochkonjunktur des Themas folgte, bevor WannaCry nach rund zwei Wochen nahezu in Vergessenheit geriet.

Wanna Cry © Sinaida Michalskaja

Einen Monat später dominierte mit Petya (bzw. einer Variation des so bezeichneten Virus, oder möglicherweise auch eines Virus, das als eine solche getarnt war) eine »neue grosse Cyberattacke« (»Echo der Zeit«, 27.6.2017) die Schlagzeilen. Die Debatte konnte fast lückenlos an die im Mai anschließen, etwa daran, dass die Attacken eine »Sicherheitslücke« in Windows-Betriebssystemen ausnutzten. Microsoft wiederum gab der NSA eine »Mitschuld« (»FAZ«, 15.5.2017), denn diese habe die betreffende »Lücke« für »Spionagesoftware« verwendet, die sie sich hatte »entwenden« lassen. Anders als im Mai stand dagegen im Fall des ›neuen‹ Virus von Beginn an fest, dass es sich nicht per E-Mail-Anhang und also durch menschliche Benutzer verbreitete, sondern auch ohne deren Zutun. Auch wurde bekannt, dass es neben der bekannten »Sicherheitslücke« mehrere »andere Lücken« nutzte. Das Virus, zitierte dazu die »FAZ« (28.6.2017) den Chaos Computer Club, »fräst sich durch große Netzwerke und nimmt alles mit«.

Dies ist irritierend, und verblüffend ist an den Berichten zu diesen »Attacken« durch einen (neuen) »Schädling« (br.de, 16.5.2017) auch, wie sehr die Plots und Viren-Narrative denen der 1980er Jahre gleichen. Zwar kann der plane Gegensatz von ›heimtückischem Erreger‹ und ›gesundem Computer‹ – 1984 ausgemalt in der Frühzeit der Vernetzung (und zuvor ein Bild in SciFi-Romanen) – als Bild 2017 kaum überzeugen, er scheint aber dennoch erstaunlich lebendig. Die Darstellung von Microsoft (publiziert von Brad Smith auf dem Blog des Unternehmens; 14.5.2017) hingegen lenkt den Blick auf die »Komplexität und Diversität heutiger IT-Infrastrukturen«. Zum Thema wird neben »Sicherheitslücke« und »Exploits« dadurch auch der globale Handel mit Softwareschwächen. Unternehmensführer und Konsumenten, so Smith, seien leider vertraut mit Ausdrücken wie »zero day« und »phishing« geworden. Dazu verweist der Text auf einen »completely unintended but disconcerting link between [...] nation-state action and organized criminal action«. Nötig sei, wie es im Titel der Meldung heißt, eine »urgent collective action to keep people safe online«.

Über den spezifischen Fokus dieser Aussagen hinaus reflektiert sich darin das Virale als eine Figur eher der unvorhergesehenen Links und verschwommenen Grenzen. Dass sich davon Software selbst nicht ausnehmen lässt, hat 2007 Jussi Parikka (»Digital Contagions«) eingehend thematisiert. Viren, so eine Kernthese von Parikkas medienarchäologischer Arbeit, sind weniger als ein abgrenzbares Feld der »Malware« zu begreifen; vielmehr ist das Virale ein immer schon inhärenter Bestandteil digitaler Vernetzung und ihrer »historisch-kulturellen Assemblage«. Viren und ihre »Contagion« sind, folgt man Parikkas Argumentation, für die digitale Netzwerkkultur und deren Spannungsfelder eines flexibilisierten Sicherheitsmanagements geradezu konstitutiv.

Aus medienhistorischer Sicht verweist Parikkas Arbeit damit zum einen auf das grundlegende Thema der digitalen Sicherheit. So betonte Fred Cohen,

dass es, mathematisch gesehen, keine Sicherheit vor Viren geben könne. »Gegen Computer-Viren ist innerhalb des Systems kein Kraut gewachsen«, schrieb »KES« (3/1985) – es sei denn, man wolle jeden Datenfluss unterbinden. Sicherheit präsentierte sich so als eine permanente und nicht endliche Aufgabe. Historisch steht für eine solche, grundlegende Frage der Sicherheit vor allem das Problem des Debugging. »All the large software systems that exist contain ›bugs‹«, hielt J.C.R. Licklider 1969 in einem Beitrag unter dem Titel »Underestimates and Overexpectations« fest. Donald MacKenzie hat in einem Aufsatz (»A Worm in the Bud?«, 2000) von einem seitdem virulenten »safety-case problem« des Software-Engineering gesprochen, das sich nach Dick Hamlet (1994) mit einem Fischteich vergleichen ließe – man könne an einem ganzen Tag keine Fische fangen, aber daraus nicht schließen, dass keine mehr da seien.

Zum anderen erweitert sich medienhistorisch, richtet man den Blick auf die Jahrzehnte vor Cohens Arbeit, das Bild des Computervirus – denn Viren sind, als Formen der Selbstreproduktion, ein virulentes Thema seit der Frühzeit des Computing. John von Neumann gilt in diesem Sinne als ›Vater‹ nicht nur der Von-Neumann-Architektur digitaler Computer, sondern – mit seiner Arbeit »Theory and Organization of Complicated Automata« (1949) – auch einer Theorie selbstreproduzierender Programme bzw. Computerviren. Überlegungen zu »Viren« stellte zur selben Zeit Norbert Wiener in seinem populären Buch »The Human Use of Human Beings« (1950) an. Aus der Sicht der kybernetischen Analogie von Lebewesen und Maschinen repräsentierten Viren für Wiener gleichsam eine Minimalform lebendiger Phänomene, definiert durch ihre Fähigkeiten zu persistieren, sich zu vermehren und zu organisieren. Viren kann man deshalb auch als ein ›Cyber‹-Phänomen im historisch-wörtlicheren Sinne begreifen: Sie sind, wie John Johnston (2008) in seiner medienhistorischen Arbeit zu Kybernetik, Artificial Life und AI folgert, Beispiel für eine »Allure of Machinic Life«. Computerviren partizipieren offenkundig an einer Faszination des Artifiziellen im Nexus zwischen Organismus und Maschine.

WannaCry konnte laut Medienberichten von einem Sicherheitsexperten zufällig durch einen ›kill switch‹ in seiner Verbreitung gestoppt werden. Von den neueren ›Virus-Angriffen‹ ist Vergleichbares nicht bekannt; es wird an die Verantwortung aller appelliert, gegen bekannte Schwachstellen (›Vulnerabilities‹) ›Patches‹ zu installieren und den Schutz der eigenen Systeme laufend auf dem neuesten Stand zu halten. Dies sind zweifellos metaphorische Bilder. Sie sprechen als solche für sich und mithin davon, weshalb eine »collective action to keep people safe online« (Microsoft) auch künftig andere Bilder voraussetzt. ◆