

# Digitale Infektionen

## Bedrohungen für PCs und mobile Computer

Lutz Stange | Computer- und Medienservice, Hard- und Softwareservice | stange@cms.hu-berlin.de

Schon die Zahlen für 2007 sind beeindruckend: 350.000 neue Bedrohungen aus dem Internet waren zu verzeichnen, das sind über 60% mehr als im Vorjahr. Alle 4 Minuten entsteht ein neuer Malware-Treiber.<sup>1</sup> 38% aller bekannten Angriffe auf Computer wurden im Jahr 2007 veröffentlicht. In Deutschland wurden 2006 3.250 Fälle der Betrugsvariante Phishing gezählt, ohne Berücksichtigung einer angenommenen hohen Dunkelziffer gab es im Jahr 2007 einen Anstieg um ein Viertel.<sup>2</sup>

Aber auch qualitativ entwickelt sich das Bedrohungspotential: Deutlich erkennbar sind eine Professionalisierung der Szene und der Einstieg krimineller Banden mit dem Ziel monetärer Gewinne. Sicherheitslücken werden im Internet zur Versteigerung angeboten. Die Angebote und neuen Möglichkeiten im Web (Stichwort Web 2.0) erhöhen deutlich die Gefahr eingeschleuster Trojaner, die persönliche Informationen direkt an Programmierer weiterleiten, die sie für kriminelle Zwecke missbrauchen. Immer mehr Hacker bauen sich mit Schadprogrammen ihr eigenes Netzwerk auf fremden Rechnern (Bot-Netze). Für Experten ist es nur eine Frage der Zeit, bis sich ein „Super-Wurm“ weltweit über Chat-Programme ausbreiten wird. Die Angriffe, die das Telefonieren über Internet-Verbindungen ermöglicht (VoIP), haben sich 2007 verdoppelt und das ist nur die Spitze des Eisbergs.<sup>3</sup>

1 Jeff Green, Senior Vice President of Product Development and McAfee Avert Labs  
[http://www.mcafee.com/us/security\\_insights/archived/jan\\_2008/si\\_jan1\\_08.html](http://www.mcafee.com/us/security_insights/archived/jan_2008/si_jan1_08.html)

2 Bundesverband der Informationswirtschaft (Bitkom)

3 McAfee, <http://www.mcafee.de/>

An der Humboldt-Universität wurden 2007 knapp 18% des gesamten Softwarebudgets für (am Ende doch unproduktive) Sicherheit ausgegeben.

Über digitale Bedrohungen wurde und wird an vielen Stellen publiziert. Längst ist das Thema von einer Domäne für Freaks zu einem milliardenschweren Industriezweig von Malwareproduzenten, Antivirenherstellern und denjenigen, die dazu veröffentlicht, mutiert. In diesem Artikel sollen ein kurzer Blick auf die Entwicklungsgeschichte geworfen, einige Begriffe erklärt und allgemeine Empfehlungen und Aspekte zu individuellen Sicherheitsvorkehrungen, insbesondere im Zusammenhang mit Malware, erläutert werden. Da die IT-Welt im Allgemeinen und speziell auch die Welt der Computer-Schädlinge besonders kurzlebig sind, kann es sich an dieser Stelle auch nur um eine kurze Bestandsaufnahme handeln.

### Ein kurzer Blick in die Geschichte

Zum Ursprung der Schadenssoftware und zu Jahreszahlen gibt es unterschiedliche Angaben, sicherlich ist dies auch der Frage geschuldet, was in diesem Zusammenhang unter Anfang verstanden wird. Schon in der vom Mathematiker John von Neumann 1949 entwickelten Theorie von selbstreproduzierenden Automaten war latent die Möglichkeit unbeabsichtigter Manipulationen von Verfahren vorhanden. In den sechziger Jahren gab es erste Programme mit (gewollter) Selbstkopie zur Arbeitsorganisation (Wiedereinreihen an das Ende einer Warteschlange). Das in dieser Zeit

*Viren, Würmer und Trojaner, längst gibt es im Bereich der Malware neben der „elektronischen Graffiti“, neben den Spielereien der „Skriptkiddies“ auch den wirtschaftlich-finanziellen Aspekt, zu dem die verschiedenen Beteiligten (Virenproduzenten, Hersteller von Schutzmaßnahmen, Benutzer) natürlich unterschiedliche Standpunkte haben. Dieser Artikel wirft einen kurzen Blick in die Entwicklungsgeschichte von Malware, erläutert einige mit dieser Thematik im Zusammenhang stehende Begriffe und verweist auf entsprechende konkrete Empfehlungen.*

populäre Computerspiel CORE WARS hatte das Ziel, kostbare Rechenzeit zu stehlen. In den 1970er-Jahren gab es mit CREEPER<sup>4</sup> ein erstes Programm mit unkontrollierter Fortpflanzung im ARPANET. (Als Reaktion darauf gab es dann den REEPER, der den CREEPER verfolgen und ausschalten sollte.) Anfang der 1980er-Jahre tauchte erstmals der Virus-Begriff auf, von Fred Cohen wurde eine Dissertation unter dem Titel „Computer Viruses Theory and Experiments“ veröffentlicht (1984). In ihr wurde ein Virus wie folgt definiert: „A computer virus is a program that can infect other programs by modifying them to include a possibly evolved version of itself“<sup>5</sup>.

Ab dieser Zeit wurden die Zeitabstände für qualitativ neue Entwicklungen immer kürzer<sup>6</sup>. 1986 wurden erste Viren direkt in Umlauf gebracht (PAKISTANI BRAIN für MS-DOS), 1989 gab es erste polymorphe Viren, 1990 erste „Virus Construction Kits“, mit denen selbst Laien auf einfache Weise und menügesteuert Viren produzieren konnten. Die erste große (auch von den Medien erzeugte) Hysterie unter den Computernutzern gab es 1992 mit dem Michelangelo-Virus, die sogar darin gipfelte, möglichst am 6. März (das war dessen Geburtstag und der erwartete Tag des Ausbruchs) den PC nicht einzuschalten.

Immer wieder gab es neue Stars unter den Viren, wie die 1995 in Mode gekommenen (und heute kaum noch eine Rolle spielenden) Makro-Viren, 1999 die Skript-Viren und ab 2002 die Würmer. Seit 2004 spielt der kriminelle Aspekt eine immer größere Rolle. Das hatte u. a. auch dazu geführt, dass die Attacken seltener wahrgenommen wurden, weil sie ansonsten zusätzlich noch geschäftsschädigend gewesen wären.

Die 2000er-Jahre waren geprägt durch „herausragende“ oder populäre Malware, die sich in Bezug auf Verbreitung, Schadensfunktionen, spezielle Sicherheitslücken und/oder Gefahrenpotential besonders hervortaten. Dazu zu

zählen sind beispielsweise die folgenden: LOVELETTER (2000), SIRCAM, CODE RED und NIMDA (2001), KLEZ (2002), SLAMMER und BLASTER (2003), MYDOM, SASSER und SOBER (2004), wieder SOBER in neuen Mutationen (2005), NYXEM und BAGLE (2006).

Nach ersten Gefahren für mobile Handys, die um 2004 auftraten und noch experimentellen Charakter trugen, nehmen diese Bedrohungen mittlerweile deutlich zu. Zurzeit existieren bereits mehr als 200 verschiedene Malware-Programme, Mobilfunkbetreiber berichten von mehreren 10.000 infizierten MMS-Nachrichten pro Woche. „Noch stellen die Schadprogramme keinen übermäßig großen Grund zur Besorgnis dar. Doch Handy-Viren sind nur eine Frage der Zeit. Sobald sich Angebote wie Bezahl-Dienste und Online-Banking per Handy durchsetzen, werden Handy-Viren wie Pilze aus dem Boden schießen“<sup>7</sup>.

In der Entwicklung gab und gibt es bei der kreativen Auseinandersetzung mit diesem Thema kaum noch Grenzen: Die Programmierer von Viren, aus unterschiedlichen und sich wandelnden Motiven, setzen seither neue Maßstäbe in Bezug auf ein erfinderisches Ausspähen von Sicherheitslücken, auf die die Softwarehersteller mit immer stärkeren Sicherheitsmechanismen reagieren. Die Herstellung von Antivirensoftware entwickelt sich, nicht zuletzt auch aufgrund von Verunsicherungen der Anwender, zu einem gigantischen und profitablen Industriezweig. Die Wissenschaft setzt sich mit eigenen Forschungsbereichen und Publikationen aktiv mit diesem Thema auseinander. Zwischen all diesen Giganten wird nun der Anwender zerrieben, der seinen Computer „bloß“ als funktionierendes und sicheres Arbeitsmittel benutzen möchte. Das ist natürlich trotz aller Schreckensszenarien möglich, auch wenn einige Vorsichtsregeln berücksichtigt werden müssen.

## Einige Begriffe<sup>8</sup>

Im Wesentlichen unterscheidet man drei Klassen von Malware: Viren, Würmer und Trojaner. Darüber hinaus gibt es Eindringlinge auf den Computer ohne klassische Vireneigenschaften, die vorrangig kommerziellen Interessen dienen und einen eher finanziellen als technischen Schaden verursachen können. Dazu zählen beispielsweise Spyware und Phishing.

Computer-Viren sind destruktive Programme, die andere Programme verändern („infizieren“) können, wobei sie eine (möglicherweise mutierte) Kopie von sich selbst einfügen, sich somit von einem Speichermedium zu einem anderen kopieren und Schäden an Daten, Programmen, Rechnerkonfigurationen und Arbeitsabläufen verursachen können. (Während der Begriff Virus in der Medizin in der sächlichen Form verwendet wird, hat sich bei dem Computer-Virus das männliche Genus eingebürgert.)

In Analogie zum biologischen Virus zeichnen sich Computerviren also durch folgende drei Eigenschaften aus:

- Es gibt einen Wirt (ein Programm), in den sich der Virus einnistet.
- Der Virus reproduziert sich.
- Der Virus hat eine Schadensfunktion.

Die Klasse der Viren untergliedert sich in Bootsektor-Viren (Bsp.: MICHELANGELO von 1992), Datei-Viren (Bsp.: TREMOR von 1993), Makro-Viren (Bsp.: MELISSA von 1999) und Skript-Viren (Bsp.: JS/GIGGER-A von 2002).

Würmer sind keine Viren im eigentlichen Sinne, da sie keine Wirtsprogramme benötigen, sondern ausschließlich sich selbst kopieren (Bsp.: WORM von 2004). Im Gegensatz zu Viren und Trojanischen Pferden infizieren sie keinen fremden Code, um sich fortzupflanzen.

Trojanische Pferde (Trojaner) sind auch keine Viren im eigentlichen Sinne (da sie sich i. d. R. nicht selbst reproduzieren), sondern Programme mit Virenfunktionalität, die sich hinter dem Namen von bekannter (harmloser) Software verstecken (Bsp.: KORG von 2004). Der Be-

4 <http://de.wikipedia.org/wiki/Creeper-Virus>

5 <http://www.eecs.umich.edu/~aprakash/eecs588/handouts/cohen-viruses.html>

6 Eine gute Zusammenfassung der Virenchronik steht auf den Web-Seiten des BSI. [http://www.bsi-fuer-buerger.de/viren/04\\_06.htm](http://www.bsi-fuer-buerger.de/viren/04_06.htm)

7 Eugene Kaspersky, CEO Kaspersky Lab

8 Ein ausführliches Glossar zu Malware-Begriffen finden Sie unter [http://www.cms.hu-berlin.de/dl/software/viren/malware/index\\_html](http://www.cms.hu-berlin.de/dl/software/viren/malware/index_html)

griff Trojaner wird gelegentlich synonym für Spionage-Software verwendet. Besondere Kennzeichen sind, dass sie oftmals lange Zeit unentdeckt bleiben und von „innen nach außen“ wirken.

Spyware sind Programme, die persönliche Daten von Computer-Nutzern ohne deren Wissen versenden. Die am häufigsten vorkommende Spyware sind Adware-Cookies bzw. Adware-Programme. Diese stellen nach dem Start einer Applikation Anzeigenwerbung dar und übermitteln dabei unerlaubt Daten an Dritte. Spyware hat vordergründig keine zerstörerische Funktion, kann in vielen Fällen aber zu Problemen (Systemabstürzen, Ressourcenverbrauch) führen. Spyware kann auch aktiv werden und das Verhalten des Anwenders beeinflussen, z. B. Suchen auf vorgegebene Seiten umlenken, Funktionen des Browsers verändern oder Bannerwerbung und Pop-ups in anderen Anwendungen auslösen.

Phishing ist Trickbetrug per E-Mail. Es wird versucht, über fingierte E-Mails auf gefälschte Bank- oder eBay-nachempfundene Webseiten zu locken, um dort die Zugangsdaten abzunehmen.

## Was kann man dagegen tun?

Sowohl die Publikations- als auch die Internetseiten sind voll von Hinweisen, gegen diese Gefahren Sicherheitsvorkehrungen zu treffen (siehe Internet-Informationsquellen am Ende des Artikels). Auch das hier vorliegende CMS-Journal dient letztendlich diesem Zweck. Grundsätzlich ist zu berücksichtigen, dass Empfehlungen oftmals natürlich auch einen kommerziellen Hintergrund haben und somit auch auf das Portemonnaie der Computerbenutzer zielen.

## Betriebssystem

Das größte Sorgenkind an dieser Stelle ist Microsoft Windows. Auch wenn die Fa. Microsoft in immer kürzer werdenden Abständen auf erkannte Sicherheitslücken reagiert<sup>9</sup>, stellt natürlich ein Angriff auf das weltweit mit Abstand meistge-

nutzte Betriebssystem ein lohnendes Ziel dar. Mit dem Service Pack 2 bei Windows XP wurde ein großer Schritt in Richtung Systemsicherheit vollzogen. Dort ist insbesondere die bereitgestellte Firewall zu nennen. Auch wenn Windows Vista seit seiner Einführung keinen guten Ruf genießt, hat Microsoft in Fragen Sicherheit doch einen weiteren großen Schritt vollzogen. Dabei sind insbesondere die verstärkte Absicherung des Systems, der Qualitätssprung in der Funktionalität der Firewall, die Benutzerkontensteuerung (User Account Control, UAC) und der bereitgestellte Windows-Defender (Schutz vor Spyware) zu nennen<sup>10</sup>.

Ein Einzelaspekt ist das Verwenden ausschließlich sicherer Passwörter<sup>11</sup>. Mit Hilfe moderner Rechnerkapazitäten kann man mit mehr oder weniger Aufwand jedes geläufige Passwort erraten. Da sich komplizierte Passwortstrukturen aber nicht oder schwer merken lassen und diese dann doch auf einem Zettel unter der Tastatur abgelegt werden, sei an dieser Stelle an die alten Dichter erinnert: Man denke sich eine Gedichtzeile aus, separiere alle Anfangsbuchstaben (inkl. Groß- und Kleinschreibung), Ziffern und Satzzeichen und bilde daraus das Passwort. Kann man hier erkennen, welcher Goethe-Vers sich hinter „StKrRs,RadH,“ verbirgt?

Für Detailinformationen zu Sicherheitseinstellungen in Betriebssystemen sei auf die entsprechenden Artikel in diesem Heft verwiesen.

## Anwendungsprogramme

In Anwendungsprogrammen sind vor deren Benutzung Einstellungen zu wählen, die nicht unbedingt den Standard-Einstellungen der jeweiligen Hersteller entsprechen. Insbesondere trifft das auf die „systemnahen“ Programme, wie z. B. Windows Explorer, sowie die direkt mit dem Internet verbundenen Programme,

wie z. B. Browser, Mailer, zu. Auch hier wird auf entsprechende Artikel in diesem Heft verwiesen.

## Anti-Virensoftware

Obwohl Malware ein Problem darstellt, sollte ihre Bedeutung nicht überbewertet werden. Die häufigste Ursache für ein „nicht ordnungsgemäßes Funktionieren“ des Computers sind Benutzerfehler, gefolgt von Hardwarefehlern und Softwarefehlern. Viren & Co. kommen erst an vierter Stelle.

Die Erkennung von Angriffen durch Anti-Virensoftware (Virens Scanner) kann man grundsätzlich nach drei Formen der Erkennung klassifizieren:

- **Signatur Based Detection**  
Diese ist nur bei bekannten Angriffen (bei so genannten Zoo-Viren) wirksam, da der Datenverkehr gegen einen Satz von Signaturen abgeglichen wird. Sie bildet den Kern der meisten aktuellen Virens Scanner. Der wichtigste Vorteil dieser Vorgehensweise (wenn sie auch nicht perfekt ist) besteht in der Einfachheit des Konzepts: Sobald ein Virus entdeckt wird, fügt der Hersteller seinem Produkt die Erkennungsfunktionalität hinzu. Die wesentlichen Nachteile sind ihre im Grunde rein reaktive Natur und dass in der Regel neue und komplexe Angriffe nicht erkannt werden.
- **Anomaly Detection**  
Diese wirkt gegen unbekannte oder erstmals auftretende Angriffe. Es wird versucht, das Kurz- und Langzeitverhalten der zu schützenden Systeme in Profilen zu erlernen. Bei signifikanten Abweichungen von diesen definierten Standardwerten werden dann Alarmglocken generiert oder der Verkehr geblockt.
- **Denial of Service Detection**  
Hier wird der Datenverkehr auf Schwellwertüberschreitungen hin untersucht. Diese Schwellwerte werden sowohl vom Administrator definiert als auch vom gelernten Verhalten abgeleitet.

Es gibt grundsätzlich zwei Möglichkeiten, die Zeitpunkte des Scannens festzulegen:

<sup>9</sup> Anzahl behobener Sicherheitslücken in Windows XP: 2005 – ca. 60, 2006 - 133

<sup>10</sup> c't 03/2008, S. 92 ff

<sup>11</sup> einen Passwortcheck kann man bspw. durchführen unter <https://passwortcheck.datenschutz.ch/check.php?lang=de>

- On Demand

Auf Aufforderung werden Dateien, Ordner oder ganze (Netz-)Laufwerke gescannt. Diese Prüfung spielt insbesondere bei einem befürchteten Befall eine Rolle, weil sie der Fehlerlokalisierung und -beseitigung dient.

- On Access

Auch wenn diese Form deutlich Ressourcen des PCs frisst, sollte diese Funktion standardmäßig eingeschaltet sein. Sie bietet, natürlich eine Aktualität der Erkennungsfunktionalität vorausgesetzt, einen großen Schutz vor Neubefall aus verschiedensten Quellen.

Ein großes Problem stellen Bereinigung und Reparatur dar. Die Entfernung eines Virus und seiner vielleicht erfolgten zerstörerischen Funktionen im System (!) kann einer „Operation am Herzen“ entsprechen: Der Patient bleibt nicht ansprechbar. Leider bekommt man von den Marketing-Abteilungen der Hersteller auch nur unzureichend Informationen über Qualitäten des Produktes in dieser Frage. Letztendlich bleibt dem Nutzer nur die Möglichkeit, den möglichen Schaden vom schwächsten bis zum stärksten Mittel zu beseitigen, auch auf die Gefahr hin, dass das Ausgangssystem damit unbrauchbar wird:

1. Ruhe bewahren
2. falls nicht ausreichend, dann: sich bei Malware-Erkennung über konkrete Auswirkungen und Maßnahmen informieren, ggf. den Anweisungen zur Fehlerbeseitigung folgen
3. falls nicht ausreichend, dann: Befall mit dem Virens scanner beseitigen
4. falls nicht ausreichend, dann: Datei/Anwendung löschen und wieder herstellen
5. falls nicht ausreichend, dann: System neu installieren bzw. von einer Sicherung wieder herstellen
6. falls nicht ausreichend, dann: Festplatte formatieren, FDISK ausführen

Nach der (hoffentlich) erfolgreichen Beseitigung des Malware-Befalls sollte in jedem Fall ein „On Demand“-Scan nachfolgen.

## Fazit

Ein aktiver Schutz der eigenen Installation ist unerlässlich. Hierzu gibt es eine Vielzahl kostenpflichtiger aber auch kostenfreier Angebote, so dass eine Absicherung des Systems für jeden Computerbenutzer möglich ist. Mitglieder der HU sollten sich nach den Vorgaben zentraler (Sicherheits-) Richtlinien richten und können sowohl im Dienst, als auch im Privatbereich, zentrale Angebote zum Virenschutz nutzen.<sup>12</sup>

Gerade auf dem Gebiet der Computersicherheit ist auf die Aktualität der getroffenen Maßnahmen besonders zu achten.

## Einige Informationsquellen im Internet

Bundesamt für Sicherheit in der Informationstechnik (BSI):

<http://www.bsi-fuer-buerger.de>

<http://www.bsi.de>

<http://www.buerger-cert.de>

Glossar zu Malware-Begriffen (HU):

[http://www.cms.hu-berlin.de/dl/software/viren/malware/index\\_html](http://www.cms.hu-berlin.de/dl/software/viren/malware/index_html)

Virus Test Center (VTC) der Universität Hamburg:

<http://agn-www.informatik.uni-hamburg.de/vtc>

Informationsseiten des Heise-Verlages:

<http://www.heise.de/ct/antivirus>

Virus-Datenbank des Perkomp-Verlages:

<http://www.percomp.de/virusinformationen.html>

Informationen zu Hoaxen (TU Berlin):

<http://www.hoax-info.de>

## AV-Software - Kostenlos für Privat

AntiVir Personal Edition:

<http://www.free-av.de> F-Prot für DOS:

<http://www.f-prot.com>

Bitdefender Free Edition:

<http://www.bitdefender.de>

Weitere Informationen über kostenfreie Scanner:

<http://www.heise.de/security/dienste/antivirus/links.shtml>

## AV-Software – kostenlos und online

VirusTotal:

<http://www.virustotal.com/>

Jotti:

<http://virusscan.jotti.org/de/>

Ikarus:

<http://www.ikarus-software.at/portal/modules.php?name=Content&pa=showpage&pid=4>

## Anti-Spyware-Software

Ad-Aware SE Personal:

<http://www.lavasoft.com>

für den Privatgebrauch kostenfrei

Spybot Search&Destroy:

<http://www.spybot.info/de/download>

<sup>12</sup> [http://www.cms.hu-berlin.de/dl/software/viren/antisoftware/index\\_html](http://www.cms.hu-berlin.de/dl/software/viren/antisoftware/index_html)