Viren und Gegenmassnahmen

T. Weissenbach

Wohl kaum jemand wird freiwillig den Befehl «format c:» beim DOS-Prompt eintippen und ihn mittels Enter-Taste zur Ausführung abschicken. Im Falle des «Miss World»-Wurms wird diese Zeichenfolge unbeachtet in die Autoexec.bat-Datei geschrieben (siehe: http://www.sophos.de/virusinfo/analyses/w32missworld.html). Beim nächsten Neustart des Rechners erfolgt, wie «befohlen», die Neuformatierung der Festplatte bzw. der Partition C – je nach Backup-Stand *der* Super-GAU. Aber auch weniger destruktiv wirkende Viren sind ein Ärgernis: so erhalten wir seit über einem Jahr täglich zwei- bis dreimal eine Nachricht von «Schneewittchen und den 7 Zwergen» (siehe: http://www.symantec.com/avcenter/venc/data/w95.hybris.gen.html). Auch andere Skriptviren (Würmer) oder Makroviren (Word- bzw. Excel-Dokumente, z.B. W97/Melissa und seine Varianten: siehe http://www.symantec.com/avcenter/venc/data/melissa.html) breite(te)n sich epidemisch aus. Die Infektion eines Rechners erfolgt heutzutage meist per E-mail bzw. die entsprechenden «Attachments»! Unter http://www.antivir.de/infos/virenkunde.htm werden die verschiedenen Kategorien von Computerviren vorgestellt.

Meines Erachtens gehört ein Viren-Abfang- und Vernichtungssystem seit jeher zur primitivsten Grundausrüstung eines jeden Rechners. Der Kauf eines Virenscanners ist allerdings nur die halbe Miete. Um die Gefahr einer Infektion so früh wie möglich erfassen zu können, muss ein Virenscanner ein Modul, das die sog. Wächterfunktion ausübt, enthalten. Dieses Modul wird automatisch aufgestartet und belegt einen Teil des Arbeitsspeichers. Schalten Sie diese «Wache» nie aus. Im weiteren müssen Sie die Antiviren-Software (Updates der Virensignaturen, allenfalls auch der sog. Scan-Engine) **regelmässig** aktualisieren, Schutz gibt es nur mit aktualisierten Virusbibliotheken! Komfortabel sind Antiviren-Programme, die sich diese Updates quasi-automatisch selbst besorgen. Daneben gibt es noch eine Reihe von weiteren Antivirus-Massnahmen (Makrovirenschutz-Aktivierung bei MS-Office-Programmen, bootfähige Notfalldiskette, Ausschalten der Option «Booten von Diskette» im BIOS, regelmässiges Update und Überprüfen der Sicherheitseinstellungen der Internet-Browser). Selbstverständlich sollten «Attachments» bei E-mails nicht sorg- und gedankenlos geöffnet werden, im Zweifelsfall sollte auch mal eine E-mail von einem bekannten Absender gelöscht werden und beim Absender nachgefragt werden (ich habe von einem schweizerischen Universitätsspital in der Vergangenheit 2mal infizierte «Post» erhalten). Dass die regelmässige, allenfalls tägliche Sicherung der Daten (Backup's) auf einen externen Datenträger zu den Standardvorkehrungen gegen einen Datenverlust gehört, sei hier der Vollständigkeit halber nochmals erwähnt.

Bekannte Antivirus-Programme sind z.B. Network Associates McAfee Virusscan (http://www.nai.com/international/germany/), Symantec Norton Antivirus (http://www.symantec.de/) und Panda Antivirus Platinum (http://www.panda-software.de/). Neben den kostenpflichtigen Programmen lässt sich mit Antivir Personal Edition von H+B EDV (http://www.free-av.de/) ein Freeware-Virenscanner für den privaten Einsatz aus dem Internet holen. Weitere Informationen zu Virenscannern finden sich unter: http://agn-www.informatik.uni-hamburg.de/vtc/de0104.htm, http://www.av-test.org/ und http://www.virusbtn.com/.

Korrespondenz:
Infomed-Verlags-AG
Blumenaustrasse 7
CH-9500 Will

infomed@infomed.org

Aus: Infomed-screen Juli 2001, Nr. 7