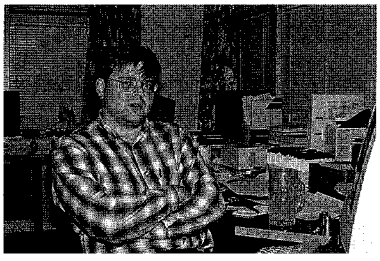
Viren sind wie Sprengstoff – ungefährlich solange sie nicht explodieren.

Ein Gespräch mit Islands Virenexperten Fridrik Skúlason, dem Autor des Virenschutzprogrammes F-PROT.

Jón Halldór Jónasson



Stark steigende Zahl von Viren

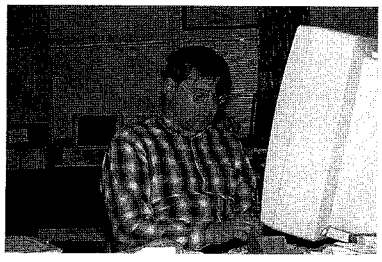
Auf dem Tisch von Fridrik Skúlason liegen eine Menge Viren herum und selbstverständlich sind einige auch in seinem Computern. Im Gegensatz zu den meisten Computerbenutzern fühlt Herr Skúlason sich dabei wohl. Er lebt von Viren. Herr Skúlason hat große Erfahrung darin, Leuten zu helfen, sich gegen Viren zu schützen – und das Unkraut zu beseitigen, falls es in die Computer eindrungen ist. Als er Computerwissenschaft (Informatik) an der Universität in Reykjavik studierte, wurde er häufig zu Hilfe gerufen. Was am Anfang eine Nebenbeschäftigung gewesen ist, hat sich jetzt in einer Firma mit 12 Mitarbeitern etabliert. 'FRISK Software International' heißt die Firma, die im Sommer zwei Jahre alt wurde. Sehr viele kennen mittlerweile auch sein Anti-Virus-Programm: F-PROT. Das F steht für Fridrik und PROT für "protection" (Schutz).

Skúlason freut sich natürlich über den Erfolg seiner Firma, aber er freut sich nicht über die Entwicklung. Nach Skúlason liegt das größte Problem einerseits in der ständig steigenden Zahl von Viren und andererseits darin, daß die Ausbreitung immer schneller vonstatten geht: *"Vor fünf Jahren war es vielleicht ein Virus in zehn Tagen, den ich behandeln mußte, aber heute bekomme ich ungefähr 10 Viren am Tag zugeschickt,"* sagt er und zeigt auf die Diskettenstapel, die überall herumliegen. Obwohl er die Viren auf Disketten aufbewahrt (als Backup : -), bekommt er die meisten über Computernetze.

"Es gibt mittlerweile über 6.000 bekannte Viren und im nächsten Jahr wird die Zahl wahrscheinlich auf 8.000–10.000 steigen," sagt er, fügt aber beruhigend hinzu: *"Es sind nur ca. 100 Viren, die ernste und akute Probleme bereiten können."* Skúlason will Viren trotzdem nicht in gefährliche und ungefährliche unterteilen. Viren seien zwar unterschiedlich aggressiv. Die aggressiven Viren werden meisten schnell entdeckt, während die weniger aggressiven vielleicht eine Zeitlang Kleinigkeiten in Dateien ändern (z.B. jedes zehntausendste Byte).

Schnellere Ausbreitung über Netze

Die andere Seite des Problems ist die schnellere Ausbreitung der Viren. *"Über Computernetze, wie Internet, ist es viel einfacher geworden, einen Virus zu verbreiten. Es ist aber auch viel einfacher, der Ausbreitung nachzugehen."* Der Zeitraum zwischen der Herstellung eines Virus und der ersten Verbreitung ist jedoch viel kürzer geworden, und damit auch die Zeit, die den Anti-Viren-Programmierern für das Erstellen von Schutzprogrammen verbleibt.



Solange sie nicht explodieren ...

Während meines Aufenthalts in Skúlasons Büro in Reykjavik bekam er ein paar Anrufe über seine Hotline, an der selbstverständlich ein knallrotes Telefon hängt. Ein Kollege aus Finnland meldet sich: Es gäbe ein Viren-Angebot auf einem WWW-Server in Amerika. Skúlason wurde gebeten, mit dem Systembetreuer Kontakt aufzunehmen, um ihn zu überreden, mit diesen Unsinn aufzuhören.

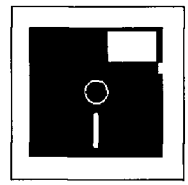
Mit solchen Angeboten wird die Ausbreitung eines Virus drastisch beschleunigt. Skúlason erzählt, daß es vielfach nicht illegal sei, Viren auf diese Art und Weise anzubieten. In Amerika sei das sogar ziemlich häufig. Er erinnert sich an eine Diskussion mit dem Betreuer eines Bullettin Board Systems, der solche Angebote nicht verbieten wollte, weil das gegen die Meinungsfreiheit verstoße.

Mittlerweile gibt es die Möglichkeit Viren auf CD-ROM zu kaufen: 4.000 Viren plus Entwicklungs-Software! Unglaublich, aber wahr.

Skúlason fordert Gesetze, die die Ausbreitung von "schädlicher" Software verbieten oder zumindestens stark einschränken: *"Es ist problematisch zu verbieten, einen Virus zu schreiben oder zu besitzen, aber es muß etwas unternommen werden können, falls der Virus verbreitet wird und Schaden anrichtet. Es sollte auch strafbar sein, wenn es um Fahrlässigkeit geht, z.B. wenn eine Zeitschrift infizierte Disketten verbreitet, weil sie sich nicht darum gekümmert hat, sie zu kontrollieren."* Zusammenfassend sagt Skúlason: *"Viren sind wie Sprengstoff. Sie verursachen keinen Schaden, solange sie nicht explodieren. Trotzdem wird nicht allen erlaubt, mit Sprengstoff zu hantieren. Ich finde schon, daß man eine Erlaubnis haben sollte, um einen Computer-Virus behandeln zu dürfen".*

Hinter jeder Tat steckt ein Täter, aber wer ist der "durchschnittliche" Virenhersteller? *"Jeder, der programmieren kann, ist in der Lage, Viren herzustellen. Viren sind nichts anders als Programme. Der durchschnittliche Virenhersteller ist ungefähr 15 Jahre alt mit einen IQ um 120–140, meistens Jungen mit Schwierigkeiten, sich sozial anzupassen. Die meisten aber hören mit diesem Unsinn auf, wenn sie älter werden und echte Aufgaben bekommen"*, sagt Skúlason. Seiner Erfahrung nach kann man diese Aktivitäten am besten dadurch abstellen, daß man bei den

Jón Halldór Jónasson studiert Informationswissenschaft an der Universität des Saarlandes mit den Nebenfächern Soziologie und Rechtsinformatik. Früher war er als Journalist in Island tätig.



Eltern anruft und die Frage stellt, ob sie gegen einen eventuellen Schaden versichert sind.
Von einigen Virenherstellern bekommt Skúlason deren "Produkte" zugeschickt. Warum? *"Vielleicht suchen sie die Anerkennung, die sie durch die Dokumentation in meinem Virenschutzprogramm bekommen. Aber sonst mache ich mir keine großen Gedanken über deren mentale Zustände oder Motive".*

Vorbeugen ist besser als heilen

Die effektivste Methode, Viren zu bekämpfen, ist die, sich bereits vor dem Befall zu schützen. Das eigene Verhalten entscheidet darüber, ob man von Viren betroffen wird oder nicht. Computer-Viren haben in dieser Hinsicht einiges mit biologischen Viren gemeinsam. Skúlason zählt diese Gemeinsamkeiten auf:

- Die Zahl der Betroffenen ist größer als man sehen kann. Es ist möglich, infiziert zu sein und andere zu infizieren, ohne es zu wissen.
- Eine Epidemie (Seuche) verbreitet sich von einem Punkt aus, wie schnell, hängt davon ab, wie häufig "gefährlicher" Kontakt entsteht und wie infektiös der Virus ist.
- Diejenigen, die viel Kontakt zu anderen haben, ohne vorbeugende Maßnahmen zu treffen, vergrößern die Gefahr, infiziert zu werden. Auch wenn man sich von einer Infektion erholt hat, besteht weiter die Gefahr, wieder infiziert zu werden.

Wie der einzelne Benutzer sich schützen kann, muß im Zusammenhang mit seiner Arbeitsumgebung betrachtet werden. *"Es gibt extreme, fast paranoide Lösungen, zum Beispiel wenn jeder Mitarbeiter seinen Computer nur mit einem an seiner Armlehne befestigten Schlüssel einschalten darf"*, sagt Skulason. *"Meiner Meinung nach ist das ein etwas übertriebenes Verfahren, aber jeder Manager sollte sich darüber Gedanken machen, wer an den Computern darf und wie er das darf. Außer Anti-Viren-Schutzprogrammen (wie F-PROT), gibt es hier auch andere Möglichkeiten, wie etwa sogenannte 'integrity checker', die ständig Vergleiche anstellen und sich melden, wenn etwas an den Programmen verändert worden ist. In Betrieben, in denen man häufig Programme ändert oder neue installiert, führt ein solcher 'integrity checker' allerdings öfters zum Fehlalarm. Eine weitere Möglichkeit ist ein sogenannter 'behavior blocker', der virenartige Vorgänge meldet und blockiert."*

Das oberste Gebot für Schutzmaßnahmen, die verhindern, von Viren hart betroffen zu werden, ist es, regelmäßig Backups zu machen. *"Erstens sollte man ein Backup machen, zweitens noch ein Backup und dann drittens ein extra Backup"*, betont Skúlason und fügt ironisch dazu, daß das auch eine sehr gute Methode sei, eigene Dateien gegen sich selbst zu schützen, weil es in der Tat wahrscheinlicher sei, irgendetwas selber zu löschen, als von einem Virus betroffen zu werden. Wie oft man ein Backup tätigt, hängt ganz davon ab, wie wichtig uns die eigenen Daten sind.
"Und", betont Skúlason mit erhobenem Zeigefinger, *"die Backups muß man an einen sicheren Ort aufbewahren, am besten in einem anderen Gebäude."*

Welches Anti-Viren-Programm?

Häufig wird Skúlason die Frage gestellt, wieviele Viren sein Anti-Virus-Programm F-PROT finden kann. Auf diese Frage gibt es keine genaue Antwort. In F-PROT werden die bekannten Viren in Viren-Familien klassifiziert (zur Zeit ungefähr 1.6OO Familien) und jede Familie besteht aus 1–150 Viren. Es kann vorkommen, daß F-PROT einen Virus findet, obwohl es ihn nicht als eigenständigen Virus identifiziert hat, aber es meldet einen neuen oder modifizierten Virus. Die Anti-Viren-Programme klassifizieren die Viren sehr unterschiedlich. F-PROT gruppiert z.B. Jerusalem, AntiCAD und Fu Manchu in dieselbe Familie, während andere Schutzprogramme jeden dieser Viren als einzelne Familie betrachten.

Wieviele Viren ein Anti-Viren-Programm finden kann, ist also kein brauchbares Kriterium für die Qualität eines Programmes. Aber nach welchen Kriterien sollte man sich dann richten? Was für ein Anti-Viren-Programm sollte man auswählen? Der Rat von Fridrik Skúlason lautet: Man sollte *mehrere* verwenden. Das verbessert die Möglichkeiten, einen vorhandenen Virus zu finden. *"Es gibt keine einfache Methode um zu beurteilen, ob ein Virenschutzprogramm gut ist oder nicht. Meiner Meinung nach findet ein gutes Virenschutzprogramm nicht notwendigerweise die meisten Viren, sondern die meisten bisher unbekannten Viren. Ein gutes Programm ist auch einfach zu bedienen"*, sagt Skúlason. "Es gibt Vergleichstudien über Anti-Viren-Schutzprogramme, und am besten stützt man sich auf solche Studien, z.B. von der Virenschutzzentrale in Hamburg oder anderen anerkannten Test-Zentren."

Skúlasons Vertriebsphilosophie

F-PROT hat viel Lob und Anerkennung bekommen. Unter anderem hat Microsoft sich das Programm für den internen Schutz angeschafft. Skúlason legt großen Wert darauf, seine Software preiswert zu verkaufen. Für Privatleute ist das Programm sogar kostenlos. Diese "freeware policy" hat den einfachen Grund, daß er nur wenig Geld für Marketing hat. "Freie Software für Privatleute" ist deshalb seine Strategie, damit jeder sich überzeugen kann, ob das Programm gut ist oder nicht. Von Unternehmen und Behörden fordert er Bezahlung, aber teuer ist es auch hier nicht. Skúlason will seine Software lieber preiswert verkaufen und viele Kunden haben, als hohe Preise zu fordern und viele Raubkopien fürchten zu müssen.