Langwierig ist der Arbeitstag im Zoo der Viren

Wie man seinen Personal Computer von allerlei Schädlingen befreit / Ein Erfahrungsbericht von Fritz Jörn

Was da alles kreucht und fleucht. Man muß nur den Computer offen und ungeschützt lassen wie eine Tiefkühltruhe ohne Strom, das aber ein halbes Jahr lang. Wir bekamen einen der seltenen PCs unter die Finger, der ohne Update, ohne Virenschutz, geschweige denn Firewall, monatelang zu dubiosem Surfen genutzt worden war. Nur die Anwahl von Auslands- und 190er-Nummern war sicherheitshalber geblockt gewesen, damit keine unfreiwilligen externen Kosten entstehen. So konnten Dialer nirgends teuer hinwählen. Jetzt sollte der Rechner an DSL angeschlossen werden, was anstandslos gelang. Eine gewisse Netzsehnsucht haben ja auch die Viren.

Dann aber zeigte sich, daß schon der übliche Windows-Explorer nicht mehr so ganz von Microsoft stammte. Er sah blau aus wie jener, brachte aber fortwährend ungewollt nackte Szenen widerlicher Art. Nun ist der Explorer ja nicht einfach ein Programm wie seine Konkurrenten, sondern fest eingebunden ins Betriebssystem. Ihn in der Systemsteuerung unter Software suchen und löschen geht nicht. Wir mußten schon eine Datei mshtml.dll mitten aus Windows ausätzen. Beim nächsten Start war wenigstens dieser Spuk verscheucht. Dann verpaßten wir dem Rechner sicherheitshalber einen alternativen Browser, Firefox.

Schon jetzt hätte jeder Fachmann die Platte geputzt und den Rechner neu aufgebaut wie einen Schulaufsatz ohne Gliederung. Wir aber wollten einen Blick in den Abgrund tun. Als erstes suchten wir Dialer – ungewollte, zuweilen aber ursprünglich doch gewollte Einwahlprogramme in kostenpflichtige Angebote. Und weil das Internet immer noch zu 99 Prozent auf Treu und Glauben funktioniert, haben wir uns vertrauensvoll ein Programm aus dem Netz dagegen geholt: Spybot. Schauen kann man danach etwa bei der Adresse download.com – der Reichtum an guten, qualitativ professionellen Programmen, die es kostenlos oder fast kostenlos gibt, ist unglaublich. Unsere Dialerprogramme flogen mit Spybot heraus.

Viren soll es schon seit 1983 geben, seit 1986 im PC. Man startete den Rechner von Diskette, und schon konnten sich dort Schädlinge festsetzen. Die Disketten luden zum freien Austausch von Programmen – und Schlimmerem – ein. Bald zog man Rechner von der Festplatte hoch; der verantwortliche Bootsektor ließ sich nicht wie eine Startdiskette schreibschützen. 1995 kamen dann die ersten Viren, die nicht in Programmen saßen: Makroviren in Word-Dokumenten. Inzwischen attakkieren sie von außen, sind verschlüsselt und verstecken sich immer besser.

Seit Windows 98 laufen im PC beliebig viele Programme nebeneinander ab, leider gern auch maliziöse. Wir griffen uns also den „Security Task Manager“, um zu sehen, was wir auf unserem Rechner beim Start alles geladen hatten. Die genannten Hilfsprogramme sind nur Beispiele. Jetzt zeigte sich vielfältige Spyware, die Eingetipptes an bestimmte Internetadressen zu versenden versucht. Neuere Tipp-Trojaner schicken bei interessanten Adressen, etwa Banken, gleich noch die Bildschirmmaske mit, damit am anderen Ende ja gesehen werden kann, wo man das eingetippt hat. Von unserem „Taskman“ werden freilich auch harmlose Plugins wie Popup-Blocker und Virenscanner als Mitläuferprogramme aufgelistet. Dank übersichtlicher Kennzeichnung braucht man nicht viel Geschick, um die richtigen hinauszuwerfen. Manche Böslinge (englisch „Malware“) lassen sich allerdings erst beim nächsten Rechnerstart packen. Überhaupt nahm uns unser Rechnerkehraus, der sich hier so einfach liest, einen Tag Arbeit.

Endlich setzten wir einen Virenscanner ein. Da läßt sich erst einmal das System online kostenlos von außen prüfen, etwa über den Internet Explorer und Symantecs Security Response (unten rechts: check for security risks), sowohl auf Viren als auch auf offene Einfallstore. Die nötige Active-X-Software – sonst ein Risiko – wird dabei automatisch geladen. Bei anderen Außenprüfern wie bei F-Secure.com muß erst der Explorer-Selbstschutz manuell gelockert werden. Wir machten Nägel mit Köpfen und holten uns gleich einen ordentlichen Virenscanner aus dem Netz, Kaspersky. Bezahlt wurde mit der Kreditkarte, gleich verbilligt für zwei Jahre. Während der Virenscannerei kann man Pause machen, muß es aber nicht. Scanner gibt es eine Zeitlang kostenlos, bis sie dann alsbald regelmäßig bezahlt werden müssen. Man bekommt ja auch regelmäßig neue Virendefinitionen dazu. Jedenfalls ging es unserem schwer verseuchten Rechner nach der Virenimmunisierung schon viel, viel besser.

Der Abend war gekommen und damit Zeit, Betriebssystem und „Office“ upzudaten. Das geht gesichert über die Microsoft-Site, dauerte aber in unserem heillos veralteten Fall, wo noch Service Pack 2 und damit 170 Megabyte nötig waren, bis fünf Uhr früh, zumal Microsoft die Daten zum Auffrischen nur tröpfeln ließ. Anschließend hatten wir eine eigene Brandmauer („Firewall“) zwischen uns und dem bösen Internet. Die bot zwar auch der vorgeschaltete DSL-Router, aber so ist Windows auf jeden Fall sicher, nicht etwa zum Zombie-Rechner für Spamversand zu werden. Wie wir später bei F-Secure erfuhren, werden sogar kommerziell Programme angeboten, die durch Ausforschen von allzu offenen Systemen Massenmailings versprechen.

Seine „Büro“-Programme wie Word, Excel oder Outlook auf den neuesten Stand zu bringen wird leider allzuoft vergessen. Das Windows-Update, das sich mit Vorteil automatisch einstellen läßt, enthält nicht das Office-Update. Es kann nicht automatisiert werden. So bleibt oft ein Haupteinfallstor für das Böse, das Mailprogramm Outlook, unkorrigiert. Eine weitere Peinlichkeit beim Office-Update ist, daß zum Schluß die Office-CD verlangt wird. Da beginnt dann das hektische Scheibensuchen.

Nach alldem leisteten wir uns noch einen Blick in die Höhle der dunkelsten Viren, die sich und ihre Dateien jedem normalen Blick ins System entziehen. Sogenannte Rootkit-Viren vergraben sich wie ein Werkzeug (kit) tief im Herzen, in der Wurzel (root) des Betriebssystems. Den Zugang dazu finden sie nur, wenn mit Administratorrechten computert wird, was eigentlich bloß bei Software- und Geräteinstallationen wirklich nötig ist. Wer ahnt schon, daß ein „persönlicher Computer“ hier Hierarchien hat. Das kleine Programm „Blacklight“ von F-Secure leuchtet in diese neuesten Virenverstecke – und fand bei uns dann nichts mehr.

Um den Rechner nun auch noch ein wenig zu tunen, hätten wir die ausgeuferte Registratur bereinigen müssen, etwa mit „Tuneup“, als Download 35 Euro, oder mit einem anderen Registry-Reiniger wie T-Onlines „Registry First Aid“ für 30 Euro. Doch das ist Kür. Am Ende waren wir einigermaßen sicher, daß das System nun eine Zeitlang harten DSL-Surfereien trotzen würde. Was an Resten vom Bösen gewiß noch vorhanden war, das war hoffentlich gut vernarbt wie alte Wunden. Die neuesten Betriebssystemteile und die neuesten Virendefinitionen kommen automatisch aus dem Netz; der Windows-Firewall ist da natürlich kein Hindernis. Laufend werden die Dateien virenüberprüft, einmal jede Woche alle. An Office sollte man von Zeit zu Zeit selbst denken. Und dem Rechner gebe man nach jedem Anschalten und jedem neuen Ankoppeln an DSL ein wenig Vorlaufzeit für seine Sicherheitsarbeiten.