Das kurze Leben eines schnellen Wurms

Was bei einem Virenbefall des Rechners zu tun ist / Die unerwünschten Dateien müssen nicht immer ganz entfernt werden

Uns erwischte ein Wurm. Ein besonders schneller Computerwurm im bestens abgesicherten Betriebssystem Windows XP. Es ist darüber nicht zusammengebrochen. Ein paar Beulen, die es innerlich davongetragen hat, hätten gefahrlos als Andenken liegenbleiben können. Wie so oft waren die Warnungen der Experten sehr willkommen – aber maßlos übertrieben. Was tun bei Virenbefall? Das sei hier gefragt und beispielhaft beantwortet.

Eine postfrische Sober-Variante lag am Dienstag um 8 Uhr in der Eingangs-E-Mail. Der Anhang der Nachricht, Tabelle.zip, erschien suspekt, und so wurde er erst einmal in einem Unterverzeichnis gespeichert. Dann ließen wir unseren Virenscanner – einen der feinsten – daran und darin schnüffeln. Doch nachdem dieser zweimal Unbedenklichkeit signalisiert hatte, klickten wir die Datei an. Das war der Sündenfall. Natürlich hätte auffallen müssen, daß sie mit einem gefährlichen exe (execute, führe aus) endete. Bei diesem Ausführen passierte dann scheinbar gar nichts; eine kleine Fehlermeldung sollte anzeigen, daß die Sache nicht dargestellt werden konnte. Also haben wir die Mail in den Papierkorb befördert und weitergearbeitet. Um 10.45 Uhr kam von H+BEDV aus Tettnang – Anbieter des sogar kostenlosen Virenschutzprogramms „Antivir“ – die erste Warnung an die „liebe Redaktion“; Der Virus hinterlasse eine Datei hjgerhds.exe. Und in der Tat brachte ein Suchlauf genau dieses Subjekt auf der Festplatte zutage. Was für ein Ärger! Als erstes verschoben wir, noch aus der Suchliste, den Unhold in den Papierkorb.

Um es gleich zu sagen: Das allein hätte in diesem Fall, wie wohl in vielen, völlig gereicht, um den Schädling auszutrocknen. Als dann um 13 Uhr die Nachricht eintraf, auf der Homepage des Bundesamts für Sicherheit in der Informationstechnik (BSI.de) stehe etwas über den neuen Virus, machten wir uns daran, die Hinterlassenschaften des Wurms zu löschen. Das BSI empfahl, acht Dateien aus dem Windows-Verzeichnis und zwei Einträge in der Registratur zu löschen, das Ganze bei abgeschalteter Systemwiederherstellung im „abgesicherten Modus“. Das ist ein großer, vor allem ungewohnter Aufwand, man verliert alle früheren Absicherungen, und so haben wir die Dateien erst einmal im weiterlaufenden Betrieb gelöscht, ebenso die Registereintragungen. Auffallend war, daß die Adressensammelbüchse des Wurms, concon.www, (noch) leer war und die Dateien genau null Byte groß. Wir starteten das System neu, die Spuren des Wurms blieben permanent getilgt, ein Virenscan zeigte das Ungetüm richtig in unserem Papierkorb an – denn inzwischen hatte auch unser professioneller Virenwarner diesen Wurm schon im Visier. Der war nur ein paar Stunden schneller gewesen.

Die Moral von der Geschicht'? Öffne komische Mails nicht. Und wenn es doch passiert ist, bewahre man Ruhe. Ist der raffinierte Virenmechanismus einmal unterbrochen, etwa dessen automatischer Start durch bloßes Verschieben der auszuführenden Datei unmöglich gemacht, so gibt das höchstens eine Fehlermeldung bei Neustart. Nulldateien kann man getrost als Andenken im System liegenlassen. Und die Prozedur mit dem geschützten Modus ist wirklich nur bei ganz gemeinen Viren nötig. Leider verraten die professionellen Virenwarner nicht, bei welchen, sicherheitshalber. Wir wagen die Empfehlung: Auf jeden Fall die Exe des Virus löschen oder wenigstens verschieben und nach einem Neustart nachsehen, ob sie dauerhaft wegbleibt. Wenn nicht, muß man bei XP die außerordentliche Mühe mit dem Abschalten der Wiederherstellung und dem abgesicherten Modus auf sich nehmen. Anschließend lasse man seinen Virenscanner über das System laufen. Dann ist immer noch Zeit, dessen Löschempfehlungen – relativ bequem – nachzukommen.

Dies zur Beruhigung – und im Gegenzug eine Warnung vor Viren, die da noch kommen werden. Aus der Linux-Welt stammt die Technik der Tarnkappenviren, die scheinbar außerhalb des Betriebssystems Fuß fassen oder sich in veränderten Systemdateien verstecken und so bei normalem Auflisten der Dateien nicht auffallen. Diese „Root Kit“ genannten Viren werden auch von Scannern oft noch nicht erkannt. Sony hat dergleichen – zunächst ebenfalls heimlich – als CD-Kopierschutz genutzt, mußte das Verfahren aber zurückziehen, als bald auch andere Programme auf First4Internets verschwiegenen Mechanismus, XCP – extended copy protection –, aufsetzten. Spezielle Scanner wie Blacklight von F-Secure können ganz vorsichtigen PC-Eltern einigermaßen versichern, daß ihr Rechner nicht klammheimlich aus dem Fenster steigt.

FRITZ JÖRN