Starke Argumente gegen Virenscanner

Spiegel online hat heute einen hanebüchenen Artikel im Programm, in dem sich Zitate wie dieses finden:
72 Prozent haben der Studie zufolge ein Virenschutzprogramm auf ihrem Rechner installiert, um sich vor Kriminellen und Hackern zu schützen. 28 Prozent aber haben demzufolge aber eben keines. Selbst mit einer simplen virenverseuchten Website könnten Kriminelle diesen Nutzern sehr leicht Schadsoftware unterjubeln. Etwa Erpresserprogramme wie den sogenannten BKA-Trojaner.

Wie kann man so einen Quatsch nur veröffentlichen? Ich habe es aber aufgegeben argumentieren zu wollen. Die Befürworter von so genannten „Virenschutzprogrammen“ sind genau so belehrungsresistent und bescheuert wie die Angehörigen der Glaubensgemeinschaft Freier Markt(TM).

Hier einige Argumente *gegen* Virenschutzprogramme, die ich in meinen Seminaren anführe.

Erstes Argument: Ein Windows-Nutzer (Version Vista ff) wird penetrant dazu aufgefordert, den so genannten „Defender“ zu aktivieren – „eine Sicherheitssoftware der Firma Microsoft zur Erkennung von potenziell unerwünschter Software (vorwiegend Spyware)“.

Wenn diese „Sicherheitssoftware“ etwas nützte, warum sollte man noch zusätzliche „Antivirenprogramme“ installieren? Was ist denn eigentlich das Geschäftsmodell der Hersteller wie Kaspersky oder McAfee, da Windows Defender doch behauptet, es schütze die Rechner gegen schädliche Software? Und was ist das Motiv der Leute, die deren „Sicherheitssoftware“ benutzen? „Doppelt hält besser“, „einem geschenkten Gaul schaut man nicht ins Maul“ oder „man kann nie wissen“?

Zweites Argument: Antivirenprogramme tun nicht das, was sie behaupten, und sie wirken nicht hinreichend. Um das zu belegen, muss man nur den einschlägigen Wikipedia-Eintrag lesen:

Virenscanner können prinzipiell nur bekannte Schadprogramme (Viren, Würmer, Trojaner etc.) bzw. Schadlogiken (engl. Evil Intelligence) erkennen und somit nicht vor allen Viren und Würmern schützen. Daher können Virenscanner generell nur als Ergänzung zu allgemeinen Vorsichtsmaßnahmen betrachtet werden, die Vorsicht und aufmerksames Handeln bei der Internetnutzung nicht entbehrlich macht. So fand die Stiftung Warentest bei einem „internationalen Gemeinschaftstest" von 18 Antivirusprogrammen Anfang 2012 mit 1.800 eingesetzten „aktuellen" Schädlingen Werte von 36 bis 96 % aufgespürten Signaturen.

Das Ergebnis der Stiftung Warentest ist übrigens transparent und für die Lobby der Antivirensoftware-Hersteller vernichtend.

Drittes Argument: Die Hersteller der Antivirenprogramme spähen selbst die Rechner der Nutzer aus und erhalten sensible Informationen nicht nur über alle installieren Programme. Man sollte zum Beispiel die „Lizenzbedingungen" Kasperkys studieren.

Viertes Argument: Die so genannte „Sicherheitssoftware" oder die Antivirenprogramme sind oft selbst schädlich oder versagen kläglich, wenn es darauf ankommt. Beispiele: „Windows Defender ermöglicht Einbruch in Windows-Systeme" (Heise, 05.04.2013). „Antiviren-Software AVG hielt Systemdatei für Trojaner" (Heise, 14.03.2013). „Why Antivirus Companies Like Mine Failed to Catch Flame and Stuxnet" (Wired, 06.01.2012). „Apple lehnt Antivirensoftware von Kaspersky für iOS ab" (TNW, 05.02.2013).

Fünftes Argument: Die Lobby der Antivirenprogramm-Hersteller versucht, ihre Produkte heimlich und auf Umwegen auf den

Rechnern unerfahrener Nutzer zu installieren, zum Beispiel über Updates anderer Programme. IT-Portale warnen ausdrücklich davor. (Heise, 27.02.2013) Das ist definitiv kein seriöses Geschäftsgebaren.

Sechstes Argument: Unerfahrene Nutzer, die sich durch die Propaganda der Lobby für Antivirenprogramme einschüchtern lassen oder auf die dämliche und unkritische Berichterstattung der Mainstream-Medien hereinfallen, werden mit den Ergebnissen der „Prüfung“ ohnehin wenig anfangen können.

Siebtes Argument: Wer sich vernünftig verhält, braucht keine zusätzliche Software, um irgendetwas abzusichern.