Die Trojaner sind vom Pferd gefallen

Die FAZ schreibt: „Der deutsche Staatstrojaner wurde geknackt“. Auch Heise formuliert „CCC knackt Staatstrojaner“ (von Krempl erwarte ich auch nichts anderes). Der CCC beginnt korrekt „Der Chaos Computer Club (CCC) hat eine eingehende Analyse staatlicher Spionagesoftware vorgenommen“, fährt dann aber leider auch im Medien-Neusprecht fort: „Die untersuchten Trojaner [sic] können nicht nur höchst intime Daten ausleiten, sondern bieten auch eine Fernsteuerungsfunktion zum Nachladen und Ausführen beliebiger weiterer Schadsoftware. Aufgrund von groben Design- und Implementierungsfehlern entstehen außerdem eklatante Sicherheitslücken in den infiltrierten Rechnern, die auch Dritte ausnutzen können.“

Im eigentlichen Bericht (Lesebefehl!) ist es korrekt: „Dem Chaos Computer Club (CCC) wurde Schadsoftware zugespielt, deren Besitzer begründeten Anlaß zu der Vermutung hatten, daß es sich möglicherweise um einen ‚Bundestrojaner‘ handeln könnte.“ (Anführungszeichen! Eben!)

Da fällt mir Wolfgang Fritz Haug ein: „Begriffe sind Abstraktionen, die dann brauchbar sind, wenn sie tatsächliche Bewandtnisse komplexer Gegenstände erfassen. Sie sind analytisch gewonnen Denkbestimmungen, deren Aufgabe es ist, aus dem fürs Denken einzig gangbaren Weg Konkretion zu erreichen.“

„Staatstrojaner“ ist ein Begriff, der ungefähr so seriös ist wie „friedenserzwingende Maßnahme“ für Krieg. Ausserdem wendet sich jeder humanistisch Gebildete mit Grausen ab, weil die sagenhaften Trojaner mitnichten in dem Pferd saßen, sondern die Griechen, und das trojanische Pferd als Computerprogramm dann auch so genannt werden müsste.

Ich habe jetzt das Vergnügen, rational denken zu dürfen, obwohl ich von einer Horde johlender Verschwörungstheoretiker umgeben bin und die wiederum von einer noch größeren Horde von ahnungslosen Dummköpfen, die gar nicht denken wollen.

Die Faz schreibt: *Der Trojaner kann laut der Analyse des Chaos Computer Clubs (CCC) beliebige Überwachungsmodule auf den einmal infiltrierten Computer nachladen – „bis hin zum Großen Lausch- und Spähangriff“, wie CCC-Sprecher Frank Rieger in einem Beitrag für die „Frankfurter Allgemeine Sonntagszeitung“ schreibt.*.

Jetzt mal gaaaanz langsam und genau hinsehen. Die Pointe kommt jetzt:

Die spezielle Überwachungssoftware wird von den Ermittlungsbehörden unter anderem zur sogenannten Quellen-Telekommunikationsüberwachung genutzt. Die Quellen-TKÜ dient dazu, Kommunikation schon auf dem Computer eines Verdächtigen abzufangen, bevor sie verschlüsselt wird. Im Unterschied zur Online-Durchsuchung….

Hier geht es um das Abhören von Internet-Telefonie (Windows! Skype! „Die in den Trojaner eingebauten Funktionen sind das Anfertigen von Screenshots und das Abhören von Skype- und anderen VoIP-Gesprächen, allerdings können auch beliebige Schad-Module nachgeladen und ausgeführt werden.“) und um nicht anderes. Nicht mehr oder weniger. Es geht nicht darum, von fern ein Programm auf einen Rechner zu schleusen (welche IP-Adresse würde diese haben?) und den ohne Wissen des Nutzers fernzusteuern. Das jedoch kann man mit dem vom CCC

analysierten Programm zweifellos („Die Malware bestand aus einer Windows-DLL ohne exportierte Routinen.“ Bekanntlich nutzt *niemand* Linux oder Apple.)

Die Zahnpasta ist leider aus der Tube, auch wenn sogar die FAZ darauf hinweist, dass die real gar nicht existierende „Online-Durchsuchung“ etwas anderes sei als die so genannte „Quellen-TKÜ“. Beide Begriffe stammen ohnehin aus dem Wörterbuch des Unmenschen, sind Propaganda und wurden vom Ministerium für Wahrheit in die Welt gesetzt, was bei der übergroßen Zahl der regimetreuen Medien zu der irrigen Annahme führt, man dürfe auch nur diese Begriffe benutzen.

„Der CCC betonte, die sogenannte Quellen-TKÜ dürfe ausschließlich für das Abhören von Internettelefonie verwendet werden“, schreibt Heise. Richtig, aber die Ermittler handelten offenbar nach der Maxime „legal, illegal, scheißegal“. Ich habe nichts anderes erwartet. Die Schad- und Spionagesoftware macht auch genau das, was man von ihr erwartet: „So kann der Trojaner über das Netz weitere Programme nachladen und ferngesteuert zur Ausführung bringen“. (Gemeint ist: das Trojanische Pferd).

Die ausgeleiteten Bildschirmfotos und Audio-Daten sind auf inkompetente Art und Weise verschlüsselt, die Kommandos von der Steuersoftware an den Trojaner sind gar vollständig unverschlüssselt. Weder die Kommandos an den Trojaner noch dessen Antworten sind durch irgendeine Form der Authentifizierung oder auch nur Integritätssicherung geschützt. So können nicht nur unbefugte Dritte den Trojaner fernsteuern, sondern bereits nur mäßig begabte Angreifer sich den Behörden gegenüber als eine bestimmte Instanz des Trojaners ausgeben und gefälschte Daten abliefern. Es ist sogar ein Angriff auf die behördliche Infrastruktur denkbar.

Avanti Dilettanti. Das ist eigentlich eine gute Nachricht, denn sie straft diejenigen Lügen, die glauben, „die da oben“ hätten von irgendwas eine Ahnung. Wie stellte sich das BKA-

Chef Ziercke das vor mit der „Online-Durchsuchung“:

Dieses Programm, was wir da entwickeln, muss ein Unikat sein, darf keine Schadsoftware sein, darf sich nicht selbst verbreiten können und muss unter der Kontrolle dessen stehen, der es tatsächlich einbringt, wobei die Frage des Einbringens die spannendste Frage für alle überhaupt ist. Ich kann Ihnen hier öffentlich nicht beantworten, wie wir da konkret vorgehen würden. Sie können sich die abstrakten Möglichkeiten vorstellen, mit dem man über einen Trojaner, über eine Mail oder über eine Internetseite jemanden aufsucht. Wenn man ihnen erzählt hat, was für eine tolle Website das ist oder eine Seite mit ihren Familienangehörigen, die bei einem Unfall verletzt worden sind, sodass sie dann tatsächlich die Seite anklicken.

Sehr hübsch ist das Fazit im CCC-Bericht: „Wir sind hocherfreut, daß sich für die moralisch fragwürdige Tätigkeit der Programmierung der Computerwanze keine fähiger Experte gewinnen ließ und die Aufgabe am Ende bei studentischen Hilfskräften mit noch nicht entwickeltem festen Moralfundament hängenblieb.“

Jetzt aber Butter bei die Fische: „Wir haben keine Erkenntnisse über das Verfahren, wie die Schadsoftware auf dem Zielrechner installiert wurde. Eine naheliegende Vermutung ist, daß die Angreifer dafür physischen Zugriff auf den Rechner hatten.“

Anders geht es nicht. Daher muss ich auch kein Wort meines Buches zurücknehmen. Und nicht nur das: Wie sollen Ermittler die IP-Adresse einen Rechners herausfinden? Was machen sie, wenn Linux zum Einsatz kommt? Egal: Das dumme Volk denkt, „sie“ wären ohnehin schon drin. diesen Einrdruck zu vermitteln, sind die Medien ja da. Das war jetzt *meine* Verschwörungstheorie.

Update: Nein Zeit online, die „Online-Durchsuchung“

funktioniert eben nicht – nur mit physischen Zugriff auf einen Rechner – und das nur bei Windows 32 Bit, und auch nur bei Internet-Telefonie. Es ist zum Haare Ausraufen.