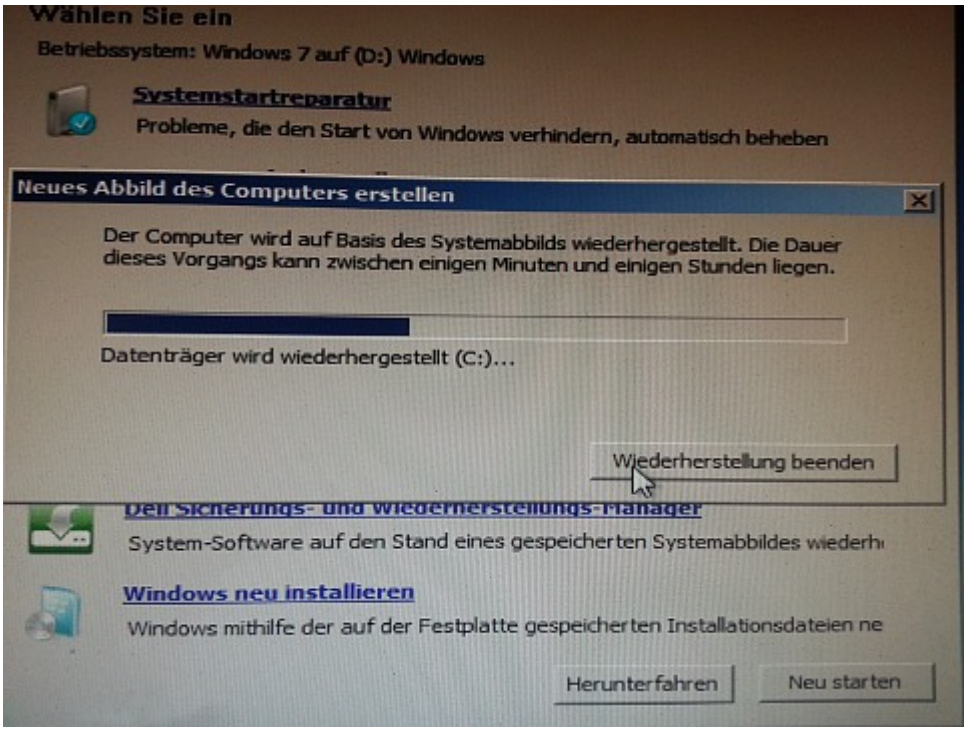
Regedit.exe



Vermutlich werden jetzt die wohlwollenden Stammleserinnen und die geneigten Stammleser hämisch grinsen. Wie allgemein bekannt, besitze ich zwei Windows- und zwei Linux-Rechner. Den Windows-Rechner, den ich meistens nutze, habe ich gestern zerschossen.

Man sollte eben nie, wenn man unkonzentriert ist und mehrere Sachen gleichzeitig tut, mal so eben nebenbei in der regedit.exe herumfummeln. Ein Chirurg entfernt auch nicht ein paar Organe eines Kunden, während er mit der linken Hand am Smartphone daddelt und gleichzeitig wahlweise mit der Narkoseärztin flirtet oder ein Käsebrot isst.

Ich bin ja nicht ganz unerfahren, um nicht zu sagen: ich bin ein Geek, und habe eine dreistellige Mitgliedsnummer aller deutschen Internet-Nutzer, aber wenn selbst der abgesicherte Modus in verschiedenen Versionen nicht dazu führt, dass man sich überhaupt anmelden kann – die Anmeldemaske von Windows 7 erschien, aber keine Nutzerkonten – und noch ein paar eklige Dinge undsoweiter undsofort und wenn nach zwei Stunden

inständigen Fluchens alles vergebens ist, dann wird es Zeit für die Hardcore-Maßnahmen, die man gemeinhin „plattmachen und Backup draufspielen“ nennt. Wo war noch mal das „Medium“ zur Systemwiederherstellung aka *rescue disk*? Zähneknirsch. Nicht vorhanden. (zum Glück hat einer der Laptops auch Windows 7).

Ein mahnendes Wort zu Vorgeschichte. Ich habe noch nie irgendwelche nutzlosen Placebos wie Virenscanner und anderen Regenzauber benutzt. Brauche ich nicht. Ich verhalte mich vernünftig – wie ungefähr ein Promille aller Internet-NutzerInnen. Es gibt keine – in Worten: *keine* Möglichkeit, mir Viren, Würmer, trojanische Pferde, Keylogger, real gar nicht existierende „Bundestrojaner“, Stuxxe und Flame und andere hässliche Programme unterzujubeln. Nein, es ist noch nicht einmal ein Risiko vorhanden. Alles verboten, und auf meinem Rechner geschieht nichts und installiert sich auch nichts, was ich nicht vorher erlaubt hätte. So wäre das eigentlich normal, auch wenn die deutsche Journaille, selbst ernannte „Sicherheits-Experten“ und Hochstapler aller Couleur mit penetranter Belehrungsresistenz den Kauf von „Virenscannern“ ankurbeln. (Und jetzt zu etwas fast ganz Anderem: oder die Pappnasen von der Geschäftstelle des DJV-Bundesverbands mich zwingen wollen, ihren „Newsletter“ in HTML zu lesen, mich also zum Dummen, Risikobehafteten, Bescheuerten und DAU-Mäßigem erziehen wollen: Nein, nein, nein, ihr könnt mich mal kreuzweise.)

Kurz vor der Party zu meinem Geburtstag fiel mir ein, dass es eine Fummelei ersten, zweiten und dritten Grades gewesen wäre, die Kabel meine Lautsprecheranlage an den Linux-Rechner anzuschließen. Außerdem wollte ich ohnehin ein paar Youtube-Videos meiner Sammlung einverleiben – auch solche, die die GEMA meint, mir verbieten zu können und die ich mit Proxtube entsperre.

Chip Online rät zu „Free YouTube Download“ (*„Hinweis: Während der Installation versucht das Setup einige Einstellungen am Browser zu verändern. Bevor Sie auf „Weiter“ klicken, sollten*

Sie daher alle gesetzten Häkchen abwählen.“)

Har har har. Das ist eine Malware, weil eine Browser-Toolbar installiert wird, *obwohl* ich *alles* während der Installation disabled/verboten/untersagt/nicht angekreuzt hatte. Wie kann eine „seriöse“ Website nur so einen abgefuckten Scheiss empfehlen?

Ich habe jedenfalls eine gute Stunde gebraucht, um die Malware rückstandslos zu entsorgen – sogar mit der Systemsteuerung funktionierte das nicht. Auch nach einer Neu-Installation von Firefox erschien die Schadsoftware wieder. Und jetzt, sehr verehrte Leserin und verehrter Leser, habt ihr mein Motiv, in der regedit.exe herumzufummeln, weil ich eh schon dabei war nachzusehen, ob eventuell noch gänzlich tote Leichenteile der Malware übriggeblieben waren.

Leider war mein Backup schon ziemlich alt, und ich habe fast den ganzen Tag gebraucht, um alles auf den aktuellen Stand zu bringen. So etwas wird mir nicht nochmal passieren. Und jetzt kann ich gleich Thunderbird komplett in einen Truecrpt-Container sperren, was ich eh schon lange wollte.