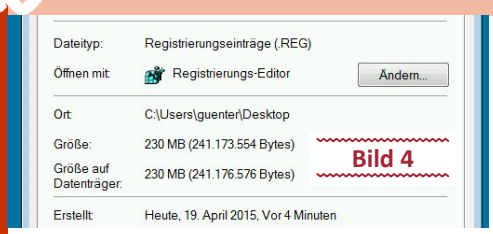

Bild 4

Eine jungfräuliche Registry hat so 15-20 mb. Meine hat ca. 230 (Win7 Pro), was auch nicht wirklich viel ist. **Siehe Bild 4.**

Sobald das System gestartet ist, „liegt“ die Registry (die ja nichts anderes als eine Datenbank darstellt) komplett im Arbeitsspeicher. Wie lange? Bis das System ausgeschalten wird, ganz einfach.

Wäre ja auch unsinnig, nicht den schnellsten Speicher im System zu verwenden.

Jetzt dürfte auch klar sein, warum eine „aufgeblähte“ Registry (mehrere Gigabyte sind da keine Seltenheit) Gift für das System sind.

Auch der größte Arbeitsspeicher ist begrenzt. Und da drin muss die Registry pausenlos werken.

Nochmal, die Registry „verlässt“ nie den Arbeitsspeicher. Außer das System ist ausgeschalten.

Somit ist auch klar, was passiert, wenn Du (oder das System) Software installier(s)t. „Landet“ alles in der Registry.

Hier offenbart sich schon mal der größte Unterschied zu unixoiden Betriebssystemen (Unix, Linux, Mac, Android…).

Bei einer Softwareinstallation unter Windows wird (auch) die Registry größer. Bei einer Softwareinstallation unter Linux wird der verbrauchte Plattenplatz größer.

Natürlich speichert Windows die Programme ferner auf der Festplatte. Im Gegensatz dazu ist es unter Linux aber relativ egal, wie viel Software Du installiert hast. Stimmt nicht ganz, aber zur Veranschaulichung ist der Vergleich okay. Das sind „tote“ Bytes auf der Festplatte unter Linux. Die Registry „schleppt“ eben die komplette Software im Arbeitsspeicher mit.

Der Einfachheit halber sagen wir jetzt dass die Registry mit Ordnern und Files arbeitet. Das ist mal grundlegend falsch, aber leichter zu visualisieren. Ja, die Registry hat auch so gelbe „Ordner“. Vergiss das. Das sind „Container“.

Was Du Dir merken kannst: Wenn ein Teil von der Registry auf der Festplatte gespeichert wird, spricht man von „hives“. (Bienenstöcke). Frag mich nicht warum. Ist so.

Die Registry ist voll von „keys“. Und diese keys sind voll von „values“.

Keys ~ folder (der Einfachheit halber)

values ~ Files (der Einfachheit halber)

Wie viele wissen, gibt es 5 root-keys. **Siehe Bild 5.**

Welcher von den 5 keys ist der kritischste und wichtigste?

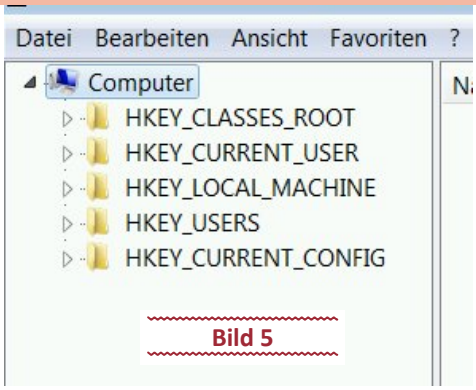

Bild 5

HKLM eindeutig. *(handle to key local machine).*

Dieser Key beinhaltet 7 Subkeys. **Siehe Bild 6.**

Ich habe nur 6 Subkeys, da dieses Win7 in einer virtuellen Maschine läuft und der Key für die Treiber „drivers“ fehlt. Egal.

Fürs Verständnis: Welcher Key ist für einen Hacker interessant?

Die SAM ist für Hacker immer ein primäres Ziel.

Dort drin sind die Usernamen, Passwörter, Gruppen und Security-Zeugs drin. Zwar nicht im Klartext, sondern in hashes. Aber das ist keine wirkliche Hürde.

Der Key „Software“ sollte auch klar sein. Alles, was Du legal oder illegal installierst, manipuliert diesen Key.

Der Vollständigkeit halber:

HKCC > sammelt Infos on the fly. Treiber, Bios…

HKCR > hauptsächlich für Abwärtskompability da.

HKCU > bist Du, wenn Du dich einloggst

HKU > wenn mindestens zwei User eingeloggt sind, kommen die Infos da rein. Interessant für Server.

Zur Wiederholung: Sobald ich eine Portion von der Registry auf meinen Datenträger speichere, spricht man von hives. Wo

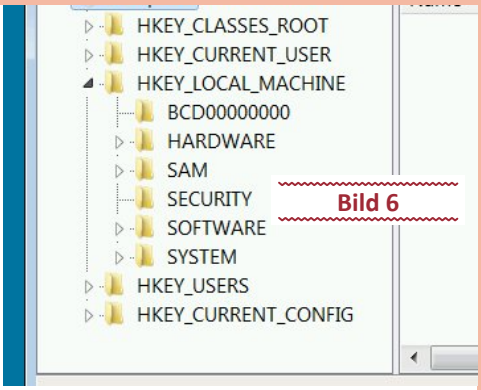

Bild 6

kann man diese jetzt sehen. Da. **Siehe Bild 7.**

C:\windows\system32\config

Da drin sind Deine hives. Ganz wichtig zu merken. Egal, ob XP oder Win10.

Primär sind dort die subkeys von HKLM drin.

Wenn Du morgens um halb 3 nicht schlafen kannst und Dich unruhig im Bett rumwälzt, dreh einfach Deinen PC auf und arbeite Dich durch die Registry. Ist bestimmt genauso einschläfernd, wie wenn Du Dir die „schönsten Nebenbahnstrecken der Welt“ am Fernseher reinziehst. Also passt.

Wer verwendet die Registry? So ziemlich alles in Windows. Kernel, Treiber, SAM, Services, User Interface und third party Anwendungen.

Wer verwendet die Registry nicht?

Portable Applicationen. Logo. Und.net Applicationen. Die bauen nämlich auf den XML-files auf. (Anderes Thema)

Ja, genau die mit dem nervenden „missing Framework…“.

So, und was sind die von Microsoft zugelassenen Tools, um die Registry zu konfigurieren?

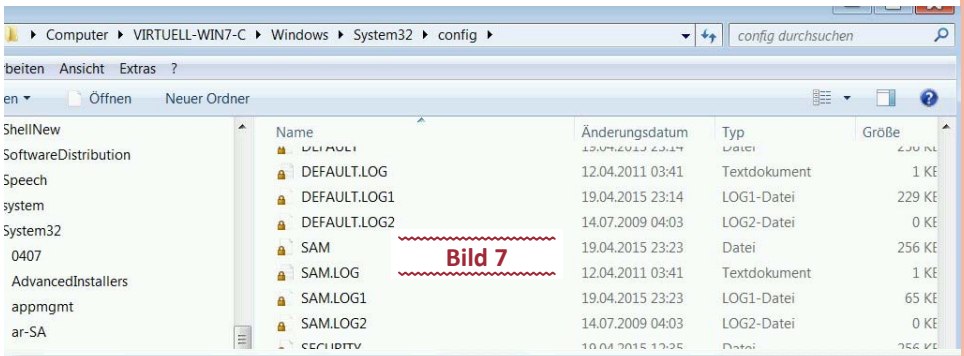

Bild 7

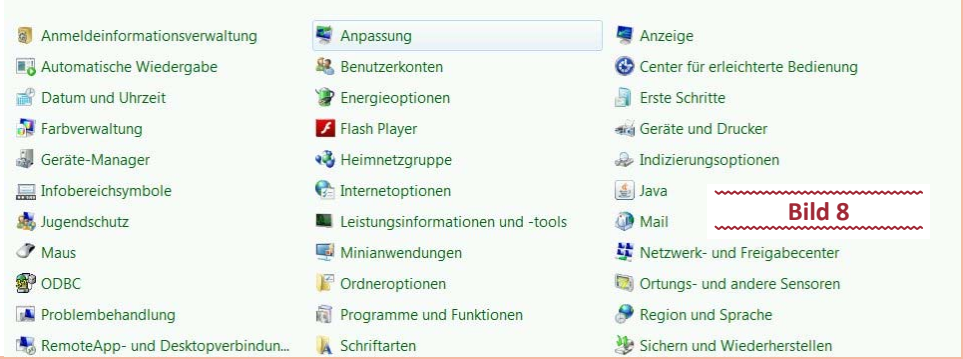

Bild 8