informiert

„Autorun“ verhindern

Wer kennt das nicht:

Man möchte eigentlich nur eine Datei von einer CD/DVD oder einem USB-Stick holen oder öffnen – doch nach Einlegen des Datenträgers öffnet sich nach langem Suchen erst mal ein Fenster zur Auswahl des Programms, oder es startet sogar ein Programm automatisch, das man momentan eigentlich gar nicht will - „nervende“ Fenster müssen erst geschlossen werden, bis man wirklich an die Daten heran kommt. Besser wäre doch, man öffnet ein Programm und legt dazu einen Datenträger ein, sodass das Programm auch sofort diese Daten nutzen kann, oder der Datenträger wird eingelegt und der Zugriff ist sofort beispielsweise über den Windows-Explorer möglich…

Das Zauberwort heißt „Autoruns deaktivieren“. Wie das geht, was zu beachten ist und welcher große Sicherheitsgewinn damit verbunden ist, soll diese Anleitung zeigen.

Inhalt:

1. Sicherheitsgewinn

Vor allem auf wechselbaren Datenträgern (CD/DVD/USB-Sticks/externen Festplatten…) sind u.U. sogenannte *„Autorun.inf*"–Dateien abgelegt. Diese enthalten Befehle, die dazu führen, dass gezielt Prozesse gestartet werden. Sollte so ein Prozess ein schadhafter sein, kann das schwerwiegende Folgen haben. Natürlich gibt es AV-Programme, die solche Prozesse erkennen und ggf. melden – nur was ist, wenn der erste Prozess dazu dient, genau diesen AV-Scanner abzuschalten ?

Nun stelle man sich vor, auf einem Datenträger befindet sich so ein Programm: **es wird Maleware installiert**, möglicherweise ein Wurm, der ebenfalls auch das Ziel hat, sich beim Einlegen weiterer Datenträger zu verbreiten. Ist *„Autorun*" für das entsprechende Laufwerk aktiviert, so **läuft auch *„Autorun.inf*" eben automatisch ab – dies gilt es zu verhindern !**

Autorun als deaktiviert zu betreiben, **sollte in Firmennetzwerken definitiv Standard** sein !!! Ist das nicht der Fall, so könnte jeder eingelegte private Datenträger zum Kollaps des Firmennetzwerkes führen, da davon ausgegangen werden muss, dass sich nicht jede/r Mitarbeiter/in „sicherheitsverantwortlich" verhalten wird – sei es unbewusst oder aus fehlender Kenntnis zum Problem. Das gilt natürlich auch für private Rechner – sind sie in einem Heim-Netzwerk miteinander verbunden, so natürlich erst recht !!!

2. Nachteile der Einstellung

Wenn der automatische Start der „Autorun.inf" verhindert wird, trifft dies natürlich auch für CDs zu, die zu Installationen von Software dienen – quasi startet das Installationsprogramm NICHT automatisch. Dies ist jedoch nicht so schlimm, denn der Inhalt einer solchen CD kann über den Explorer eingelesen und die entsprechende Datei direkt angewählt werden. Meist nennt sich diese Datei „Setup.exe" – häufig wird diese Vorgehensweise sogar in der Anleitung zur Installation beschrieben.
Dieser Nachteil fällt jedoch mit dem unter Punkt 3. genannten Tool weg.

Dass Inhalte des Datenträgers nicht automatisch dargestellt werden, ist zwar gegeben, aber auch nicht so dramatisch: Man startet das passende Programm und öffnet von dort aus den Datenträger.

Befinden sich Programme auf dem PC, die einen externen Datenträger behandeln, so sind diese in der Regel nicht betroffen von dieser Einstellung. Beispielsweise öffnet sich dennoch das Programm, wenn eine Camera an den PC angeschlossen wird. Ist dies nicht der Fall, so kann die Einstellung präzisiert werden, dazu weiter unten.

Dass Programme lieber allein starten sollen, ist eine „bequeme Ausrede" und sollte dem Sicherheitsgedanken deutlich hinten an stehen – sind Daten oder gar das Betriebssystem erst mal dahin, steht wesentlich mehr Arbeit an als der besagte „Klick mehr" beim Start von Inhalten eines externen Datenträgers.

Die Einstellungen werden in der Registry vorgenommen. Dieses Herzstück von Windows ist mit größter Vorsicht zu behandeln – falsche Veränderungen in der Registry können zum Zusammenbruch des Systems führen. Deshalb der Hinweis: Garantie für Folgen bei Veränderungen in der Registry wird niemand übernehmen, dafür ist jeder selbst verantwortlich. Deshalb sollte bei Vorgaben auch ganz genau den Anweisungen Folge geleistet werden (Schlüssel genau beachten)!

3. Ausgezeichnetes Tool für diese Einstellungen

Für diejenigen, die sich nicht so sicher in der Registry fühlen und es gerne einfacher haben möchten, bietet das Tool **AutoRun Settings von Uwe Sieber**
http://www.uwe-sieber.de/drivetools.html#AutoRunSettings
eine **hervorragende Alternative** !!!

Dieses Tool
- ist klein
- muss nicht installiert werden (nur geöffnet)
- funktioniert sehr zuverlässig
- und hat für nicht so versierte User **wesentliche funktionelle Vorteile:**

1.
Es wird ein übergeordneter **HKLM-Schlüssel** erstellt – somit gilt die **Einstellung für alle Benutzer !**

2.
Durch die o.g. Einstellungen funktionieren ebenfalls keine Software-CDs, somit müsste beim Einlegen einer CD, mit der Software installiert werden soll, die entsprechende Setup-Datei manuell aufgerufen/gestartet werden. Wer sich hierbei unsicher fühlt, kann mit diesem Tool das temporäre Problem dadurch lösen, dass er in dem Tool **vor der Nutzung** solch **einer Installations-CD** (oder auch ähnlicher Datenträger) den Haken an entsprechender Stelle wieder setzt und nach dem Vorgang der Installation diesen wieder entfernt. **Eine ständige manuelle Änderung der Registry-Einträge entfällt – somit auch der Gang in die Registry und die Gefahr von risikobehafteten Fehleinstellungen.**

3.
Durch die manuellen Einstellungen in der Registry (vgl. Punkt 3.) ist verhindert worden, dass beim Einlegen eines Datenträgers die „autorun.inf" startet. **Wird das Laufwerk über den Arbeitsplatz aufgerufen, so startet sie dennoch** – es ist erforderlich den Inhalt des Datenträgers über den WIN-Explorer anzeigen zu lassen, um das Problem zu umgehen.

Durch ein WIN-Update im August 2008 (KB 950582) wurde dieser Fehler bereits behoben. Dieses Update wurde nicht automatisch ausgeliefert, hingegen als das **unter Punkt 5.** dieser Anleitung **genannte automatisch ausgelieferte WIN-Update** verteilt. So sollte das Problem eigentlich nicht mehr bestehen. Dennoch **liefert dieses Tool zusätzlich die Möglichkeit, diesen Fehler zu beheben** (vgl. **(B)** und **(C)** in der Abb.).

Nutzung des Tools:

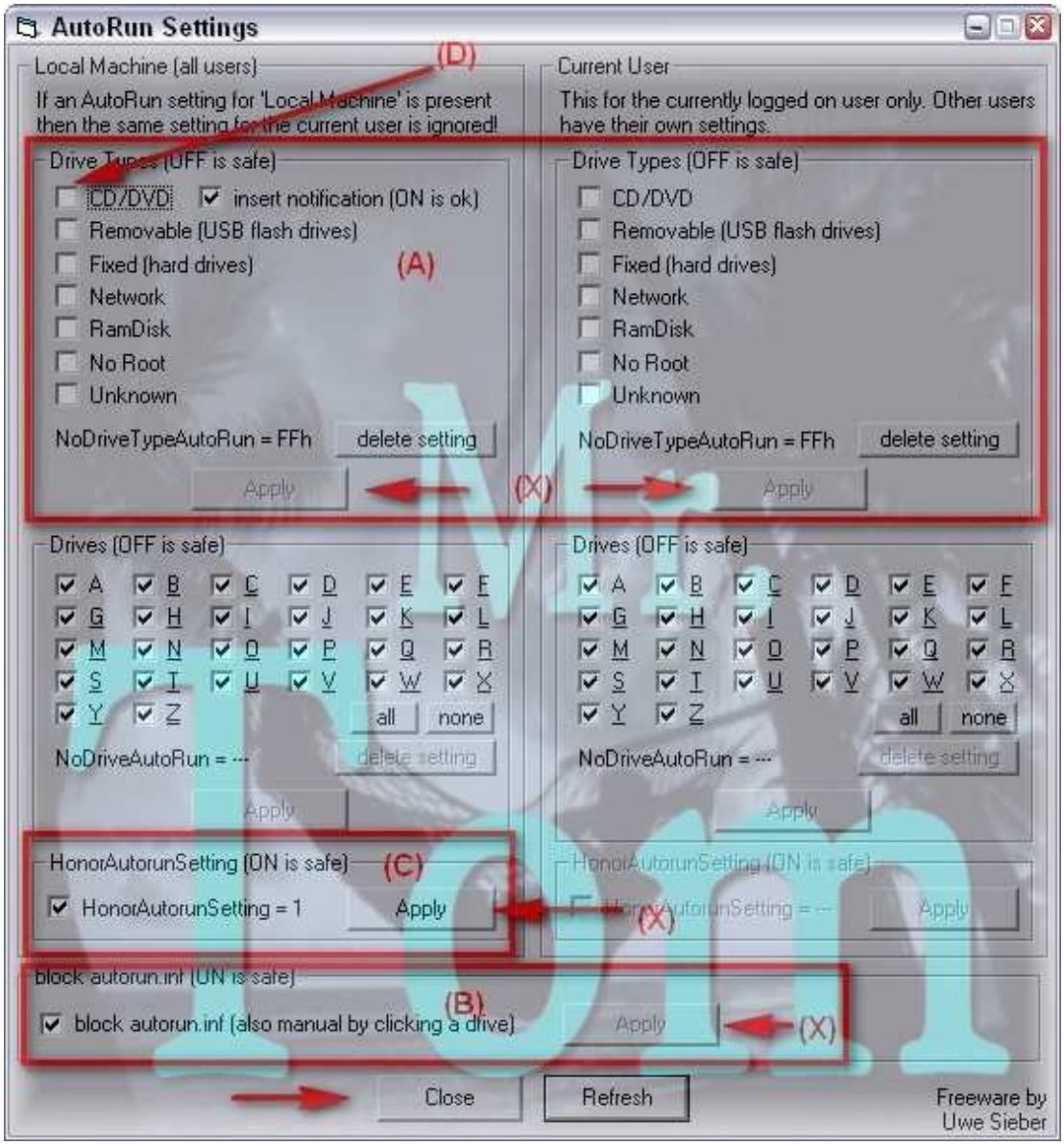
- Datei herunterladen (Tabelle)
- Zip-Datei in Ordner entpacken > Ordner öffnen
- Autorunsettings.exe starten/öffnen
- Folgende Einstellungen vornehmen:

(A) ALLE Haken entfernen, bis auf *„CD/DVD insert notification"*
(X) Klick auf *„Apply"* *(Übernahme der Einstellungen)*

(B) Haken setzen bei *„block autorun.inf(also...)"* *> Damit wird verhindert, dass bei Anklicken des Laufwerkes aus „Arbeitsplatz" heraus dennoch die „autorun.inf" (siehe oben) gestartet/aktiviert wird*
(X) Klick auf *„Apply"* *(Übernahme der Einstellung)*

(C) Haken setzen bei *„HonorAutorunSettiung"*
(X) Klick auf *„Apply"* *(Übernahme der Einstellung)*

*Ist das unter Punkt **5. Update** genannte **WIN-Update (KB 967715)** installiert, so ist bei **(C)** eh der Haken bereits gesetzt und **(B)** verliert seine Bedeutung/Wirkung. Ist das genannte WIN-Update nicht installiert, so erfolgt der Effekt über die Einstellung **(B)** – ein Setzen des Hakens bei **(B)** ist somit logisch, da entweder „egal oder richtig".*



Mit **Klick auf *Close*** das Tool wieder schließen > **FERTIG !**

Die entsprechenden Einträge in der Registry wurden erstellt bzw. geändert (quasi der Vorgang, wie er unter Punkt 4. dieser Anleitung beschrieben wird).

Wenn nun irgendeine Einstellung zurück genommen werden soll, so einfach das **Tool aufrufen > Haken wieder setzen > *Apply* > *Close.***

Soll nun beispielsweise (wie oben) **eine Software–CD doch automatisch starten, so ist der Haken (D) zu setzen > *Apply* > *Close***. Nach der Nutzung dieser Software-CD wird der Haken auf selben weg wieder entfernt.

4. Manuelle Vorgehensweise über die Registry

Es empfiehlt sich, vor Veränderungen der Registry immer **eine Sicherung** derselben **zu erstellen** – entweder von der gesamten Datei oder vom jeweiligen Eintrag, der bearbeitet werden soll.

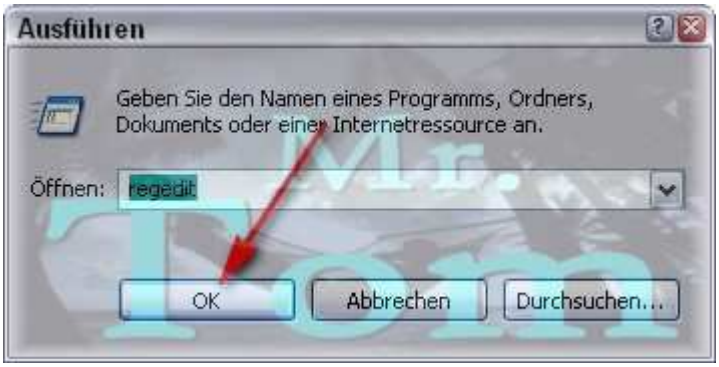
Vorab sollte **im Windows-Explorer** dafür **ein Ordner** eingerichtet werden, in dem später Sicherungen abgelegt werden können – dieser sollte sich außerhalb der Bootpartition befinden.

Hier im Beispiel heißt dieser Ordner „Registry" und liegt im Ordner „SICHERUNGEN" auf der Partition E:/, quasi: **E:\SICHERUNGEN\Registry**

(Das sollte jeder für sein System entsprechend vornehmen !)

4.1. Wie gelange ich in die Registry

Start > *Ausführen* > dort „*regedit*" (ohne „") eingeben:



Klick auf *OK.*

Nach Klick auf *OK* wird die Registry geöffnet. Die Ansicht ähnelt sehr stark dem Windows-Explorer, Einträge sind auf der Oberfläche per Schlüssel strukturiert zu finden (was im Win-Explorer „Pfad" genannt wird, ist in der Registry der „Schlüssel").

4.2. Sicherung erstellen

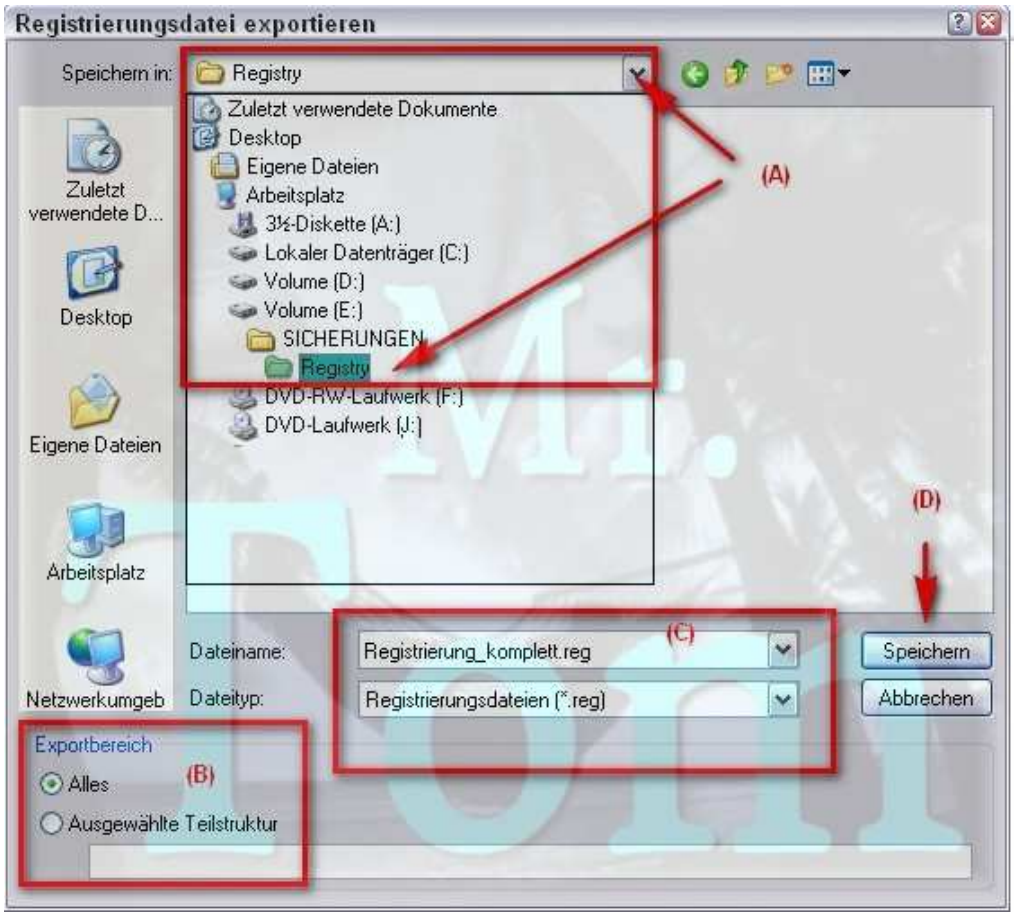
4.2.1. Sicherung der gesamten Registry

Die Sicherung der gesamten Registry ist nicht immer erforderlich, es macht aber Sinn, damit zumindest eine Gesamt-Sicherung vorhanden ist, falls die Einstellungen doch an falscher Stelle erfolgten.

Die Sicherung der gesamten Registry erfolgt über *Datei* > *Exportieren*:

Es öffnet sich ein Fenster, in dem festgelegt wird, wo die Sicherung abgelegt werden soll (siehe Pfad oben) und wie die Datei heißen soll:

Unter **(A)** wird der oben eingerichtete Ordner aufgesucht, der Exportbereich sollte wie in der Abbildung **(B)** angehakt sein, der Name sollte „logisch" vergeben werden **(C)** - dann auf *Speichern* **(D)**:

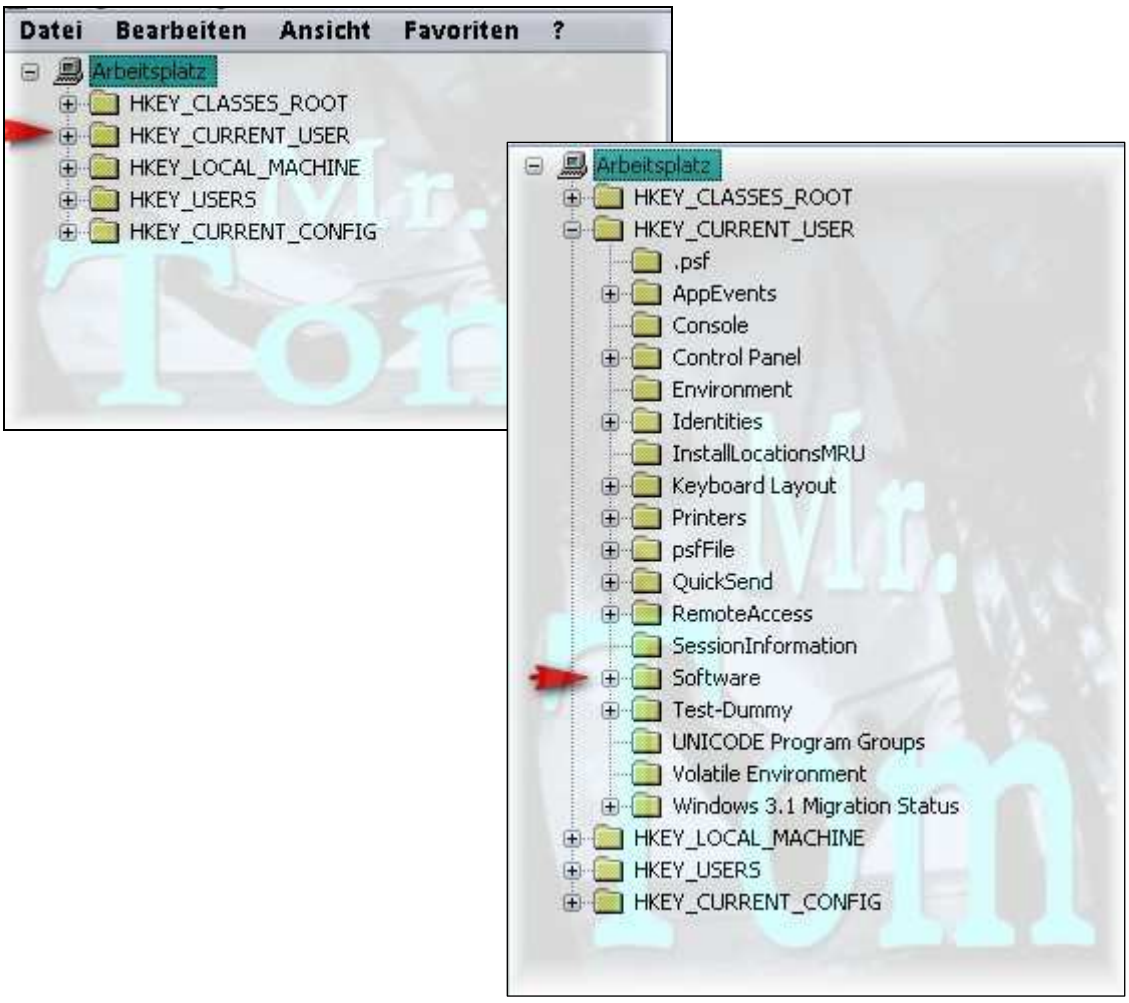


4.2.2. Sicherung des zu bearbeitenden Schlüssels

Dazu hangeln wir uns zu dem Schlüssel durch, den wir später bearbeiten werden:

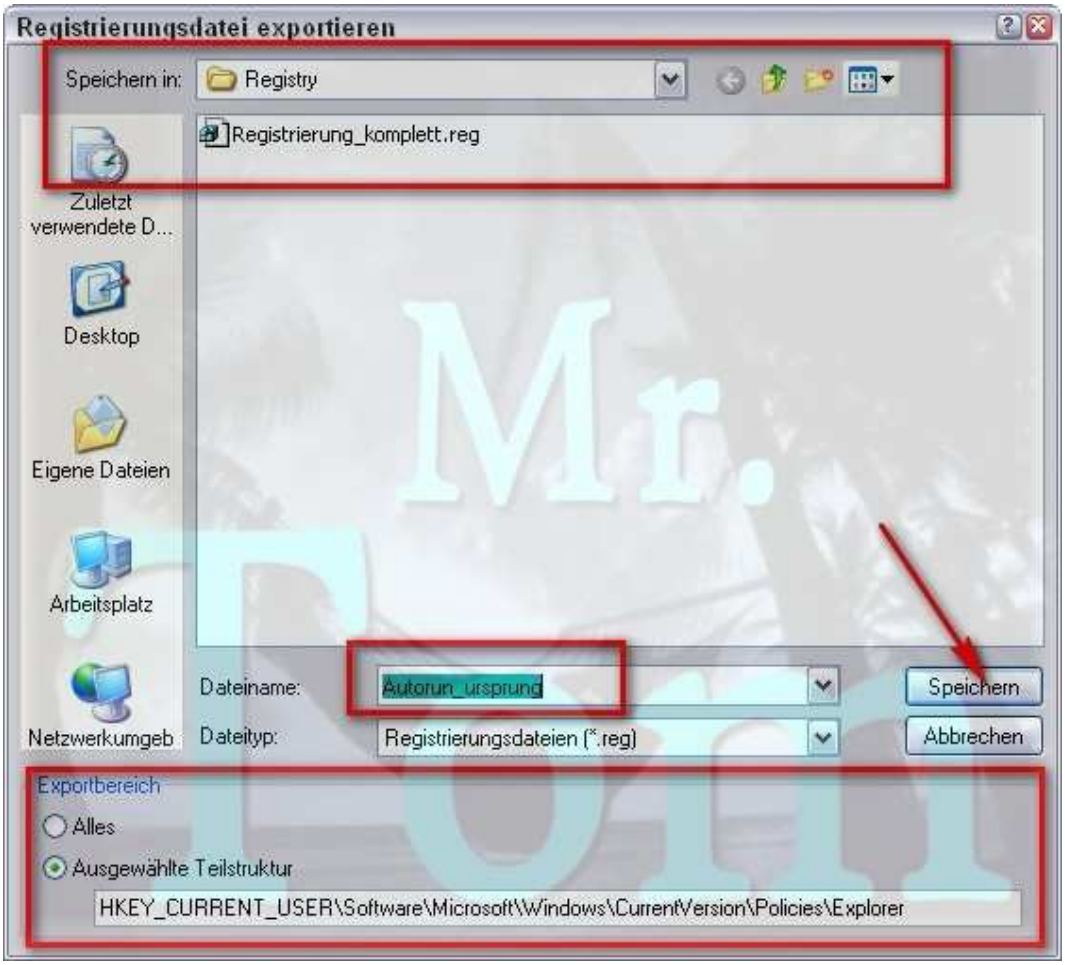
HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Policies\ Explorer

Wir öffnen die Struktur:

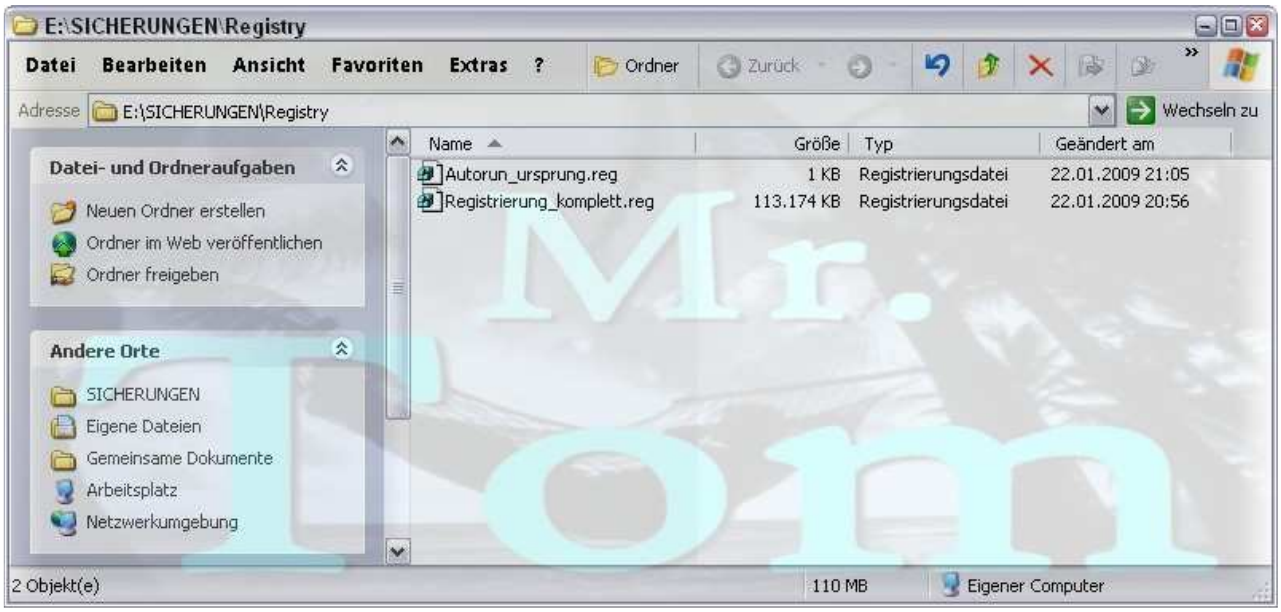


…immer weiter **(vgl. Schlüssel)** bis "Explorer", dort per *Rechtsklick > Exportieren*:

Es öffnet sich wieder das bekannte Fenster, in dem wir wie oben vorgehen, allerdings sollte der Name natürlich anders lauten. Auch der Punkt für den Bereich ist anders gesetzt:



Wird nun der anfangs für die Sicherung erstellte Ordner im Windows-Explorer geöffnet, so sind dort nun die zwei Sicherungs-Dateien zu finden:



Im Fall der Fälle würde man nun eine der beiden einfach doppelt anklicken, um gesicherte Registry-Einträge wiederherzustellen. Die Schlüssel, die sich mit den zugehörigen Einträgen in der Sicherung befinden, überschreiben die aktuellen – also entweder wird nur der betroffene Schlüssel oder die gesamte Registry wiederhergestellt.

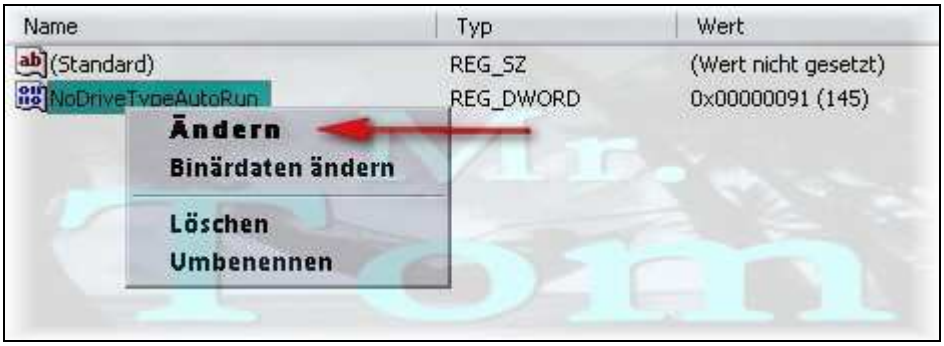
Zu Beachten:
Sollte die Wiederherstellung erst nach längerer Zeit vorgenommen werden, ist Vorsicht zu genießen: Ein Zurücksetzen ***der gesamten Registry*** *kann zur Folge haben, dass aktuelle Einträge verschwinden, die in der Zwischenzeit hinzugefügt wurden ! Deshalb ist es ratsam, bei evtl. erneuten anderweitigen Eingriffen in die Registry die Sicherung der gesamten Registry zu erneuern.*
Die Sicherung des einzelnen Schlüssels, der anschließend bearbeitet werden soll, ist natürlich aufzuheben – sollten Veränderungen nicht zum erhofften Erfolg führen, beeinflusst ein Wiederherstellen schließlich NICHT die gesamte Registry, sondern eben nur den gesicherten Schlüssel. Auch aus diesem Grund sollte allein schon aus dem Namen der Sicherung hervorgehen, um welchen Schlüssel es sich handelt.

4.3. Einstellung von Autorun

In der nun folgenden Einstellung werden wir **Autorun** (**nicht zu verwechseln mit „Autoplay" !!!!**) **für alle Laufwerke deaktivieren**.

In dem bereits gefundenen Schlüssel befindet sich ein Eintrag „NoDriveTypeAutoRun":

Den Wert dieses Eintrages gilt es nun zu ändern - dazu auf den Eintrag mit *Rechtsklick > Ändern*:



Es wird der Wert in "Hexadezimal" angezeigt:

Wir *wechseln in "**Dezimal**",* sehen den Standardwert (für XP ***145***):

Und ändern **diesen** auf ***255***, dann auf ***OK***

Nun sollte der neue Wert des Eintrages auch im Registry-Fenster zu sehen sein:

Die Registry (Fenster) kann nun geschlossen werden.

Beim Einlegen von CDs oder USB-Sticks kann sofort über den Explorer oder von anderen entsprechenden Programmen auf den Inhalt zugegriffen werden – **Prozesse (eben auch „böse"), die auf dem Datenträger liegen, werden nicht automatisch starten, da die *„Autorun.inf"* nicht beachtet wird!**

Der Wert **255** ergibt sich aus der Tatsache, dass **Autorun eben auf allen Laufwerken deaktiviert** werden soll. Woher dieser Wert kommt, wie er entsteht, was er aussagt - und - wie er sein muss, wenn aus bestimmten Gründen doch Laufwerke *„Autorun"* erlauben sollen, ist z.B. dieser Seite zu entnehmen:
http://www.winfaq.de/faq_html/Content/tip0000/onlinefaq.php?h=tip0055.htm

Eine weitere Anleitung mit noch zusätzlichen Tipps ist hier zu finden:
http://forum.avira.com/wbb/index.php?page=Thread&threadID=78989
…dort wird auch beschrieben, wie ein „Globaler Eintrag" unter HKLM (der alle Einstellungen unter HKCU überlagert) zu erstellen ist und wie man trotz der o.g. Einstellung ein evtl. Fehlverhalten beim Einlegen **ehemalig benutzter** Datenträger beheben kann. Diese Tipps (v.a. der des „Globalen Eintrages") können **von Bedeutung sein, wenn** auf dem PC **weitere v.a. eingeschränkte Benutzerkonten** vorhanden sind!

Viele werden sich sagen: „so etwas interessiert mich nicht", „dafür habe ich keine Zeit", „ich verstehe eh nichts davon"…
Um aber mal aufzuzeigen, welche Folgen das haben kann und wie machtlos der User ohne diese Veränderung der Einstellung eigentlich dem Datenträger ausgeliefert ist, soll der **Test unter Punkt 6.** dieser Anleitung dienen.

5. Update

Microsoft hat am 24.02.2009 ein Update herausgebracht. Durch dieses WIN-Update wird die o.g. Änderung in der Registry als Änderung auch über HKLM gesichert: es wird ein Eintrag erstellt:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer/**HonnorAutoRunSetting**

Hintergrund:
Einstellungen unter HKLM (HKEY_LOCAL_MACHINE) stehen in ihrer Wirkung über denen in HKCU (HKEY_CURRENT_USER). Die o.g. Änderung erfolgte unter HKCU. Durch dieses WIN-Update wird die o.g. Änderung in der Registry als Änderung auch über HKLM gesichert.

Somit wird empfohlen, das **Update** mit der **KB 967715** zu installieren.

Sollte das Update bereits installiert sein, so müsste dies gelistet sein:
- entweder unter Systemsteuerung>Software (was evtl. durch Reg-Cleaner beseitigt wurde) , dann aber
- als Ordner: C:\WINDOWS\hf_mig\KB967715
- der o.g. Regeintrag (unter HKLM) ist bereits vorhanden

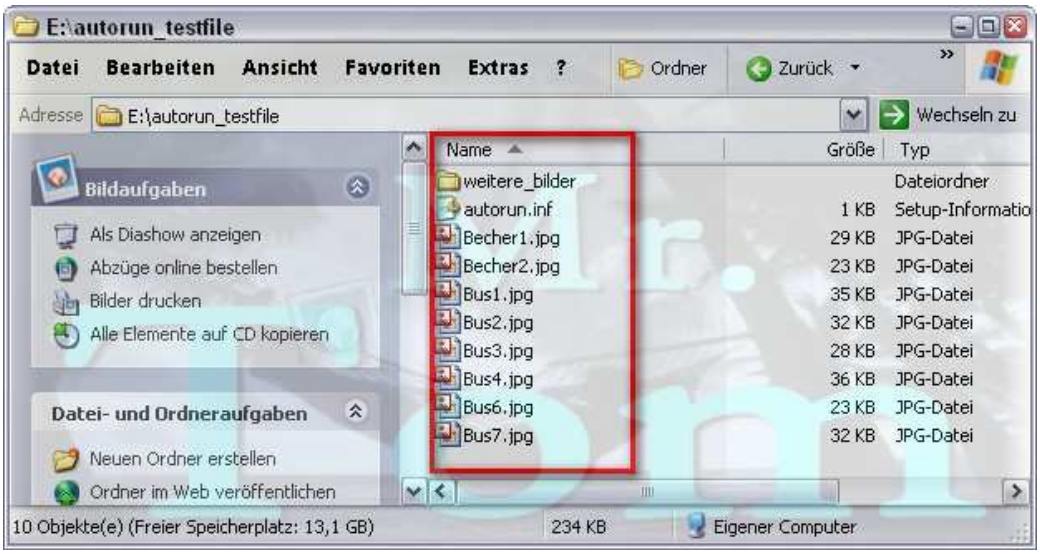
6. Testen

Um die Wirkungsweise dieser Einstellung zu verdeutlichen, liegt im Netz eine Zip-Datei *„autorun_testfile.zip"* bereit, die zum Download zu erreichen ist unter:

http://www.webmrtom.de/ablagen/autorun_testfile.zip

Dieser Test ist **völlig harmlos** und wird **KEINE Veränderungen am System** vornehmen, die evtl. zurück gesetzt werden müssten, verdeutlicht aber hoffentlich den **Sicherheitsgewinn**:

- Die Zip-Datei downloaden
- Zip-Datei entpacken in einen Ordner (vorzugsweise „Entpacken nach…" wählen)
- Den Zielordner öffnen
- Den **kompletten Inhalt** dieses Ordners (nicht den Ordner selbst):



auf eine CD brennen.

Bitte eine leere CD und keinen USB-Stick **verwenden** (evtl. für diesen Datenträger notwendige Daten könnten überschrieben werden)! Eine Verwendung eines **wiederbeschreibbaren** Rohlings (CD-R**W**) wäre ja auch möglich, so müsste man dafür keinen Datenträger „verschwenden", da der Inhalt ja wieder löschbar ist. Sich diese CD aufzuheben für Tests anderer PCs wäre aber auch denkbar.

- Nach dem Brennen der oben eingerahmten Dateien den Datenträger erneut in das Laufwerk einlegen
- Ergebnisse vergleichen

Je nach Einstellungen der

Werte:	**255** nach dieser Anleitung *oder* **Andere vorher** (Voreinstellung für XP **145**)
des **Eintrages:**	**NoDriveTypeAutoRun**
Unter dem **Schlüssel**:	**HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Policies\ Explorer**

oder eben der gesetzten/nicht gesetzten Haken im **Punkt 3. beschriebenen Tool** wird die Reaktion/Wirkung am PC eine andere sein. Zwar kann man in beiden Fällen Bilder auf der CD betrachten – allerdings wartet bei der Einstellung *ohne Deaktivierung von Autorun* (für XP *145*) eine kleine Überraschung auf den Tester.

Hinweis: beim Wechsel zwischen den zwei verschiedenen Einstellungen wird die Veränderung in der Registry **erst nach einem PC-Neustart wirksam !!!**