Mit Autoruns Programm-Start-Einträge anzeigen und durch Verschieben de-aktivieren

Rudi Theisen, ZAM
15.11.2005

Quellen: http://www.fz-juelich.de/zam/sicherheit/download/freeware.1/pc-tools/AutoRuns/zam-autoruns.htm
und auf dem ZAM PC-Server (nur im JuNet erreichbar)

\\PCSRV\public\JuNetSecCD\win-VERSION.SPRACHE\tools\AutoRuns\zam-autoruns.htm
oder auf der Notfall-CD:\nuetzliches-fuer-PC-Windows\tools\AutoRuns\zam-autoruns.htm

1. Zusammenfassung:

Mit Autoruns sehen Sie die wichtigsten Programm-Start-Aufruf, die nach einem PC-Neustart ausgeführt werden, und können diese per Autoruns sehr einfach entweder verschieben und so vorübergehend für den nächsten PC-Neustart de-aktivieren oder ganz für immer entfernen. Dazu brauchen Sie keine Systemkenntnis zu haben, insbesondere die Registry-Editor-Bedienung nicht zu beherrschen.

- Das Autoruns-Programm braucht man nicht zu installieren; es genügt, das Programm zu starten. Sie können es sogar von einem Server starten. Dann funktioniert nur die Help-Anzeige nicht.
- Autoruns können Sie im Gegensatz zu dem ansonsten funktional ähnlichen Microsoft-Programm MSCONFIG.EXE nicht nur unter Win-XP oder Win Server 2003 einsetzen, sondern unter jedem Windows Betriebssystem, von Win 9x bis Win XP.
- Es untersucht die Registry-Einträge und die Autostart-Einträge des aktuellen Windows-Systems.
  Man kann es deshalb leider nicht unter einer (BartPE-) Notfall-CD sinnvoll einsetzen. Es zeigt zwar auch dort die Start-Einträge an, aber eben die der Notfall-CD, und nicht diejenigen des verdächtigen Windows-Systems, das man mit Hilfe der Notfall-CD bereinigen möchte.
- Autoruns zeigt zwar nicht alle [2], aber bereits die wichtigsten Start-Einträge in den Registry-Verzeichnissen, z.B. in
  - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
  - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
  - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run und in
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Run

  (mit HKLM:=HKEY_LOCAL_MACHINE und HKCU:=HKEY_CURRENT_USER)
  sowie in den Autostart-Verzeichnissen, z.B. in
  - C:\Dokumente und Einstellungen\All Users\Startmenü\Programme\Autostart

  an.
  Hinweis: Welche Registry-Verzeichnisse noch alles überprüft werden, sieht man, wenn man im View-Menü die Option "Include Empty Locations" aktiviert (s. Bild 7.6)
- Mit Autoruns kann man sehr einfach einen Eintrag mal probeweise abschalten. Dazu braucht man nur das betreffende Häkchen zu entfernen und den Rechner neu zu starten.
  Autoruns erstellt direkt beim Entfernen eines Häkchens parallel zu dem betreffenden Datei- bzw. Registry-Verzeichnis das Verzeichnis **Autorunsdisabled** und verschiebt sofort den zu de-aktivierenden Link bzw. das Programm bzw. den Registry-Eintrag in dieses Hilfs-Verzeichnis. Dadurch wird das betreffende Programm nach dem nächsten PC-Neustart nicht mehr gefunden und so auch nicht mehr gestartet.
- Autoruns zeigt die nicht mehr gestarteten Einträge aber auch weiterhin an; sie sind allerdings nicht aktiviert, sprich: Sie haben kein Häkchen gesetzt.
- Wenn Sie merken, daß Sie den betreffenden Programm-Start-Aufruf doch benötigen, dann genügt es, in Autoruns das betreffende Häkchen wieder zu setzen. Autoruns verschiebt dann den betreffenden Aufruf aus dem jeweiligen Autorunsdisabled-Verzeichnis zurück in das richtige Verzeichnis und entfernt das Autorunsdisabled-Verzeichnis dann, wenn es leer ist.
- Doch anstatt einen Eintrag zu verschieben kann man ihn auch mit Autoruns ganz löschen. Dazu markiert man den Eintrag in der Autoruns-Anzeige und löscht ihn entweder mit ==> **Entry** ==> **Delete** oder direkt mit **Strg-D**. Das Löschen muß man dann aber noch explizit bestätigen.

- Der Help-Text liefert Bedienungs-Hinweise, insb. der Abschnitt "Disabling and Deleting Entries" (s. Bild 7.1).
- Fehler sind an mark@sysinternals.com zu melden.
- Lizenz-Bedingungen: Das Programm darf man nicht ohne Zustimmung von Sysinternals verteilen. Zustimmung erteilt: licensing@sysinternal.com.
  Wir haben keine solche Zustimmung eingeholt. Deshalb bieten wir es auch nicht mehr auf unserem WWW-Server an.

2. Start und erster Überblick über das Autostart-Programm

Hinweis: Die Bilder in diesem Kapitel wurden noch mit der Vers. 6.0 von Autoruns erstellt.

Beschaffen Sie sich den ZIP-File (s. [1]) und packen den aus. Autoruns.exe ist dann sofort nutzbar; es gibt also keine Installation. Sie können Autoruns.exe deshalb auch von Diskette, CD oder USB-Stick ausführen. Wenn Autoruns ausgepackt auf einem Ihnen zugängigen Server liegt (1), können Sie es auch dort starten (2) und Ihren PC damit untersuchen lassen:

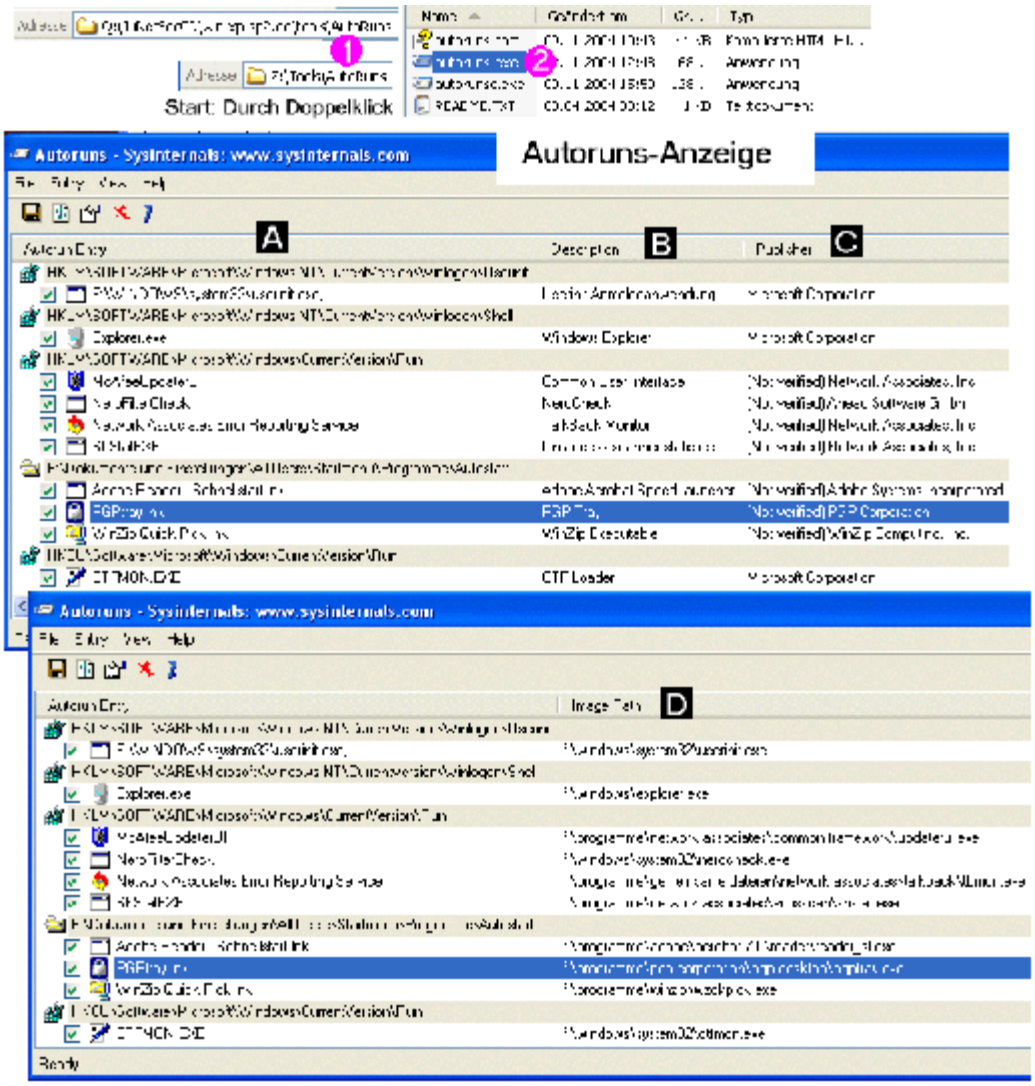

Bild 2 Start von Autoruns.exe und Überblick über die Autoruns-Anzeige

In der "Autoruns Entry"-Spalte (A) sehen Sie, von wo aus die einzelnen Programme beim PC-Neustart gestartet werden.
Die Angaben aus der Description-Spalte (B) und der Publisher-Spalte (C) entnimmt Autoruns aus den Eigenschafts-Einträgen der betreffenden Dateien. Diese Angaben helfen, die jeweiligen Programm besser zuzuordnen und somit die benötigten Programme einfacher zu erkennen (Spreu vom Weizen trennen).

Autoruns zeigt weiterhin in der "Image Path"-Spalte den Programm-Pfad an. Diese Angaben sind sehr wertvoll.

> Hinweis: Wie oft üblich kann man die Reihenfolge der Spalten aber auch einfach durch Ziehen mit der Maus verändern, aber die Anzeige nicht alphabetisch je Spalte sortieren lassen.

Um nun möglichst schnell die Haupt-Anwendungen des Autoruns-Programms zu zeigen, nämlich die De-Aktivierung von Autostart-Programm- und von Registry-Einträgen, werden weitere Details zu den Anzeige-Möglichkeiten dieses Programms ins Kapitel 7 verschoben.

3. De-Aktivierung eines Autostart-Programm-Eintrages

Im folgenden Bild sehen Sie, was Autoruns macht, wenn man einen Autostart-Eintrag de-aktiviert:

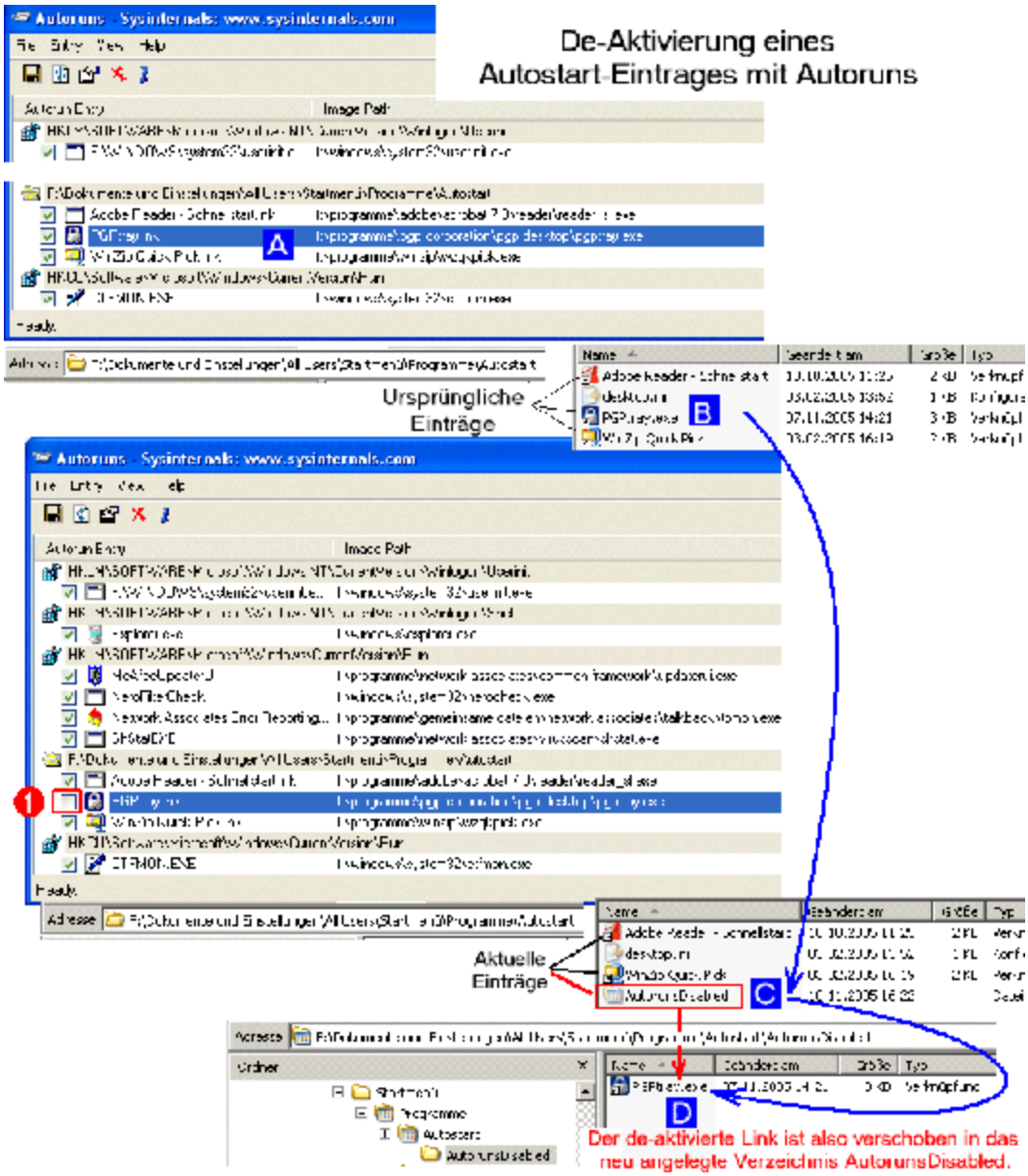

Bild 3.1 De-Aktivierung eines Autostart-Eintrages

Autoruns legt das Verzeichnis **AutorunsDisabled** an (s. C) und verschiebt dorthin den Autostart-Eintrag (s. B und D). Der Prozess (hier: PGPtray.exe) wird durch diese Autostart-Änderung aber nicht beendet:

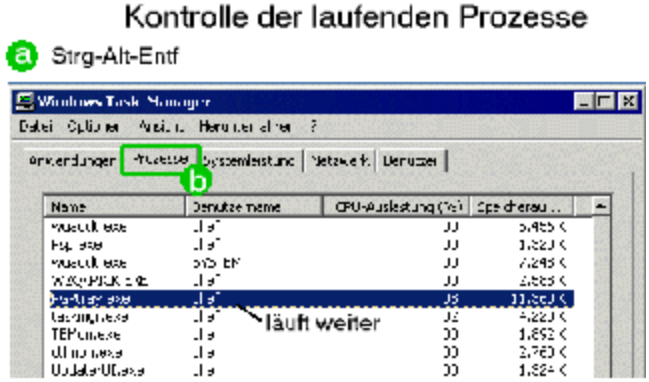

Bild 3.2 Kontrolle der laufenden Prozesse

Erst beim nächsten PC-Neustart würde PGPTray.exe also nicht gestartet.

4. De-Aktivierung eines Programm-Start-Eintrages in der Registry

Die folgenden Bilder zeigen, wie einfach Sie mit Autoruns auch einen über einen Registry-Eintrag veranlaßten Programm-Start dadurch de-aktivieren können, daß Sie den Aufruf innerhalb der Registry in ein neu definiertes **AutorunsDisabled**-Verzeichnis verschieben.

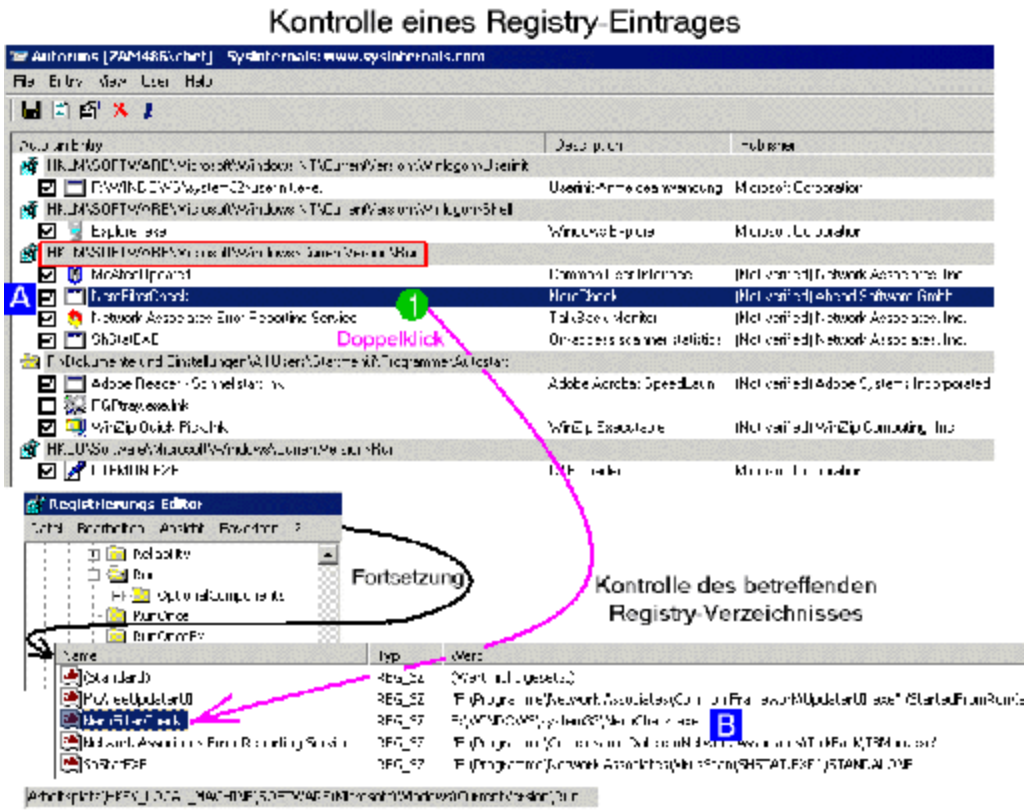

Bild 4.1 Ausgangs-Situation der Registry-Eintragungen

Indem Sie per Autoruns das Häkchen eines Registry-Eintrages entfernen (s. 1 im folgenden Bild), legt Autoruns auch in der Registry wieder parallel zu dem betreffenden Verzeichnis sein **AutorunsDisabled**-Verzeichnis an (C) und verschiebt dorthin den betreffenden Programm-Start (D und E):

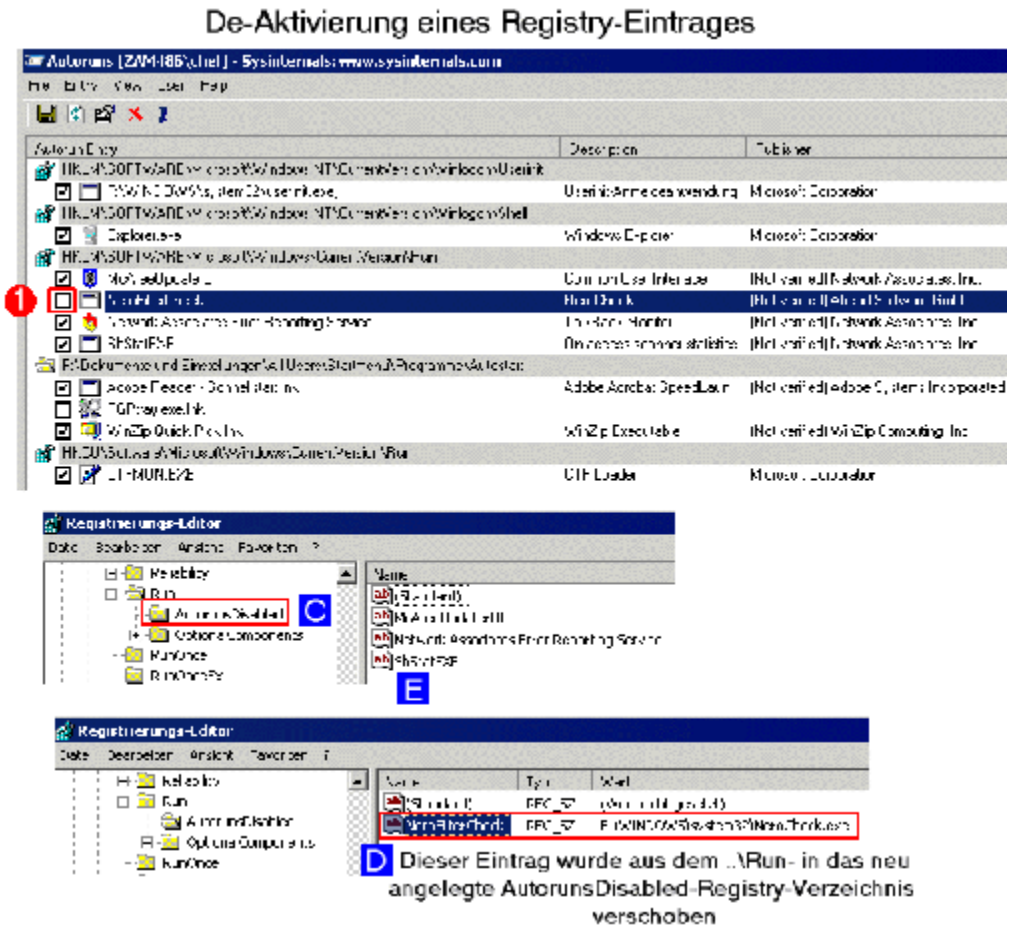

Bild 4.2 De-Aktivierung eines Registry-Eintrages

Beim nächsten PC-Neustart würde dieses Programm (hier: NeroCheck.exe) durch diese Verschiebung innerhalb der Registry nicht mehr gestartet.

5. Re-Aktivierung eines mit AutoRuns de-aktivierten Programm-Starts

Wenn Sie nach dem nächsten PC-Neustart nun aber feststellen, daß Sie ein de-aktiviertes Programm doch benötigen, dann können Sie dessen De-Aktivierung wieder einfach mit dem AutoRuns-Programm rückgängig machen. Dieses zeigt Ihnen ja alle de-aktivierten Programme ohne Häkchen an. Sie brauchen nur das betreffende Häkchen wieder zu setzen und schon verschiebt AutoRuns den betreffenden Start-Eintrag aus seinem AutorunsDisabled-Verzeichnis zurück in das betreffende Verzeichnis. Das wird im folgenden exemplarisch für den im vorherigen Kapitel de-aktivieren Eintrag in einem Registry-Verzeichnis gezeigt:

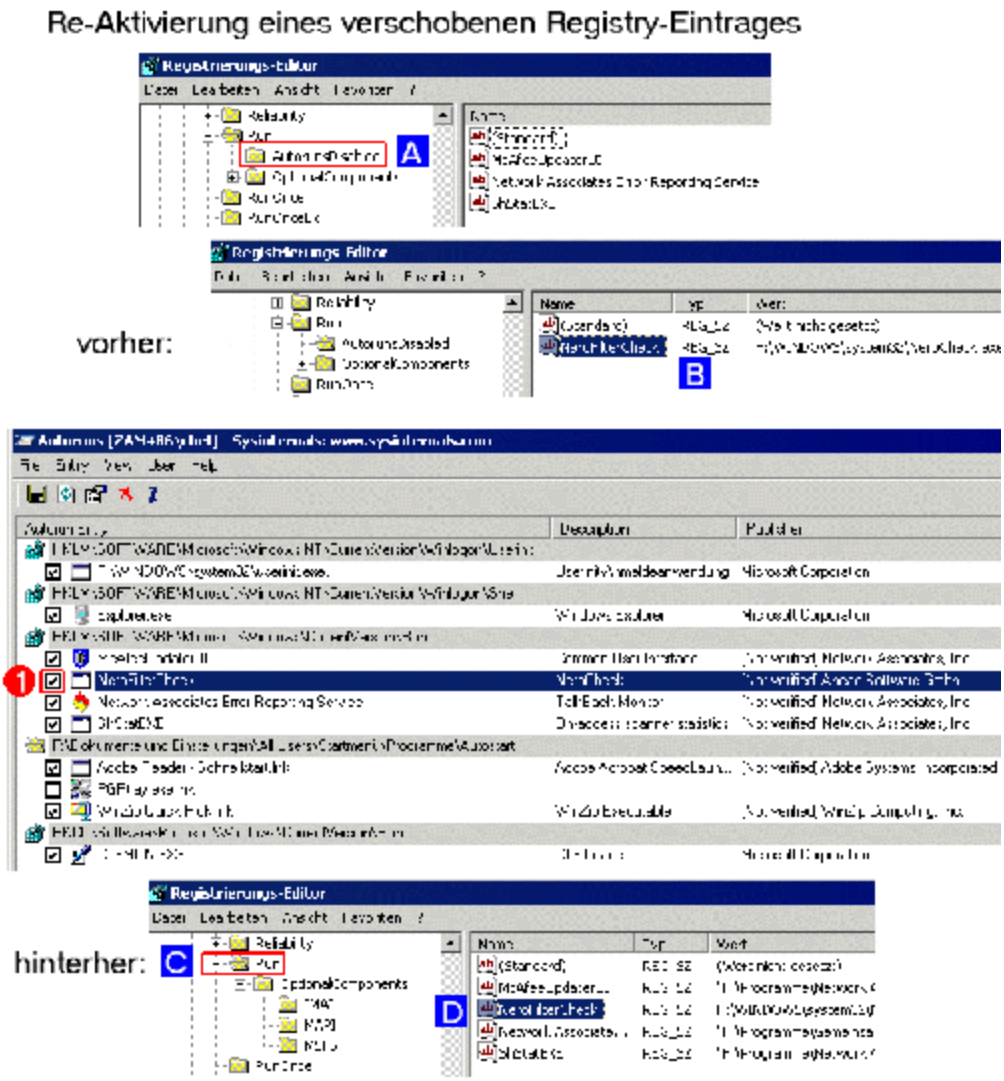

Bild 5. Re-Aktivierung eines Registry-Eintrages

Wenn das betreffende AutorunsDisabled-Verzeichnis durch diese Rückverschiebung leer wird, wird es automatisch gelöscht.

6. Löschung eines Autostart-Programm-Eintrages

Erst wenn Sie ganz sicher sind, daß Sie ein Programm nicht mehr automatisch nach einem PC-Neustart starten wollen, sollten Sie den betreffenden Startauf mit Hilfe des Autoruns-Programm ganz löschen. Das wird im folgenden Bild exemplarisch für einen Autostart-Programm-Aufruf gezeigt:

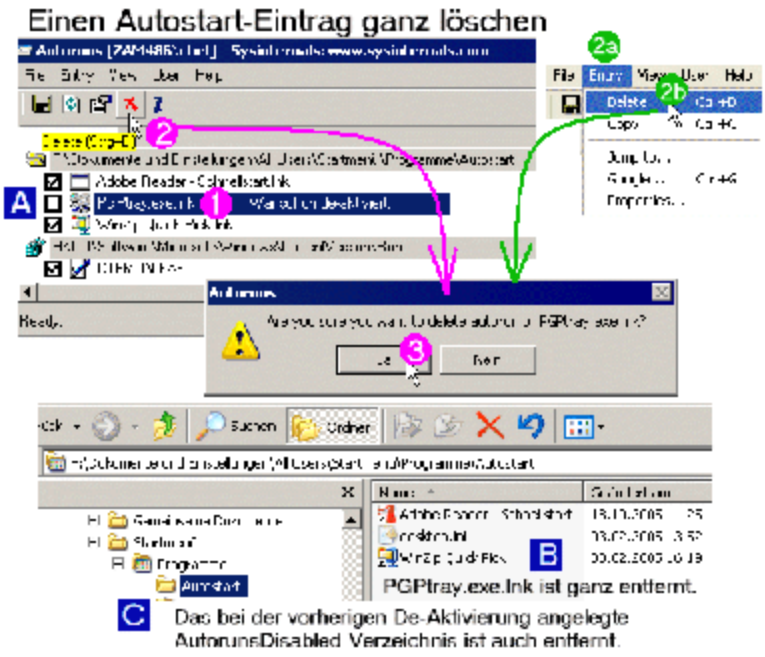

Bild 6 Löschung eines Autostart-Programm-Eintrages

Bei diesem Beispiel war der Programm-Eintrag bereits vorher de-aktiviert (A). Das ist aber für die Löschung nicht nötig.

7. Detailierterer Einblick in die Bedienung und Anzeigen des Autoruns-Programms, Version 6.0

Hinweis: Die Bilder in diesem Kapitel wurden noch mit der Vers. 6.0 von Autoruns erstellt.

Ein ersten Überblick über das Autoruns-Programm wurde bereits im Kap. 2 gegeben. Nun sollen weiteres Anzeige-Möglichkeiten des Autoruns-Programs vorgestellt werden, denn es kann viel mehr, als man auf den ersten Blick vermutet.

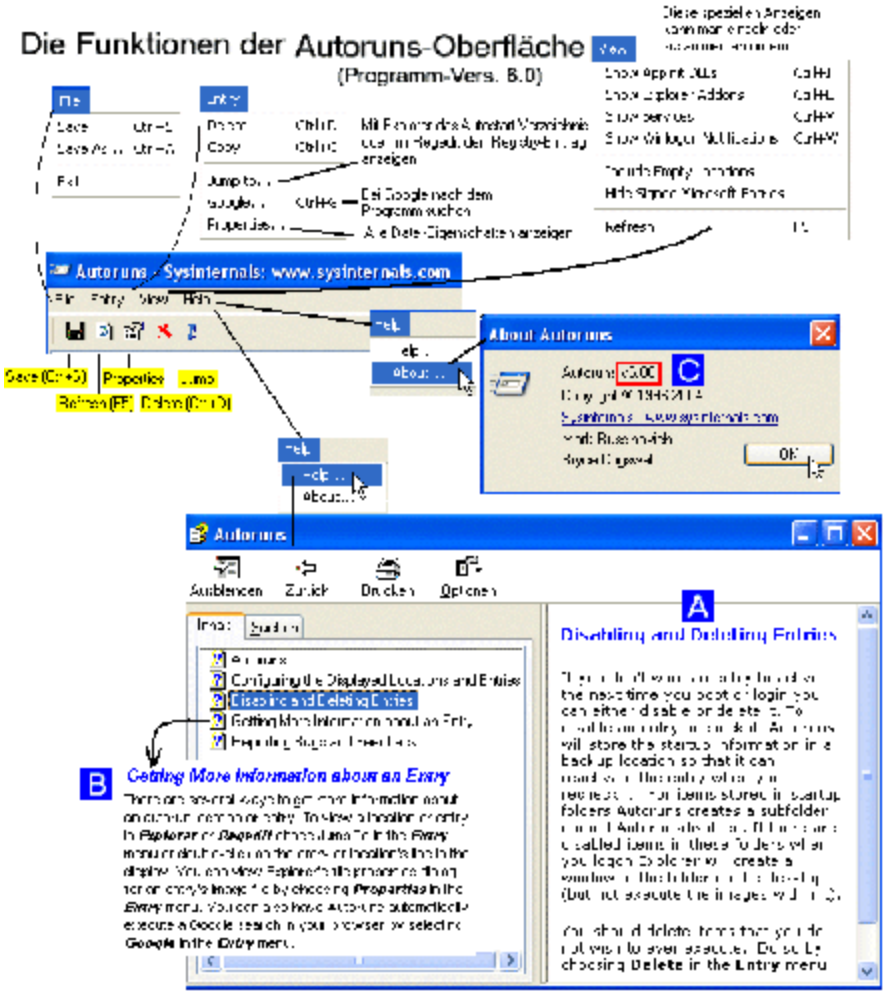

Bild 7.1 Die Pulldown-Menüs und Funktions-Icons von Autoruns, Vers. 6.0

Über das View-Menü kann man sich weitere Informationen anzeigen lassen. Einige Sonderfälle werden weiter unten vorgestellt.

Zusätzlich zu den in der Autoruns-Anzeige schon gemeldeten Information "Description" (Beschreibung) und "Publisher" (Firma) kann man sich zu jedem angeklicktem Programm (1) entweder durch

==> Rechte Maus(Programm) ==> Properties (2)

oder über das

==> Entry-Menü (2a) ==> Properties (2b)

alle Eigenschaften anzeigen lassen:

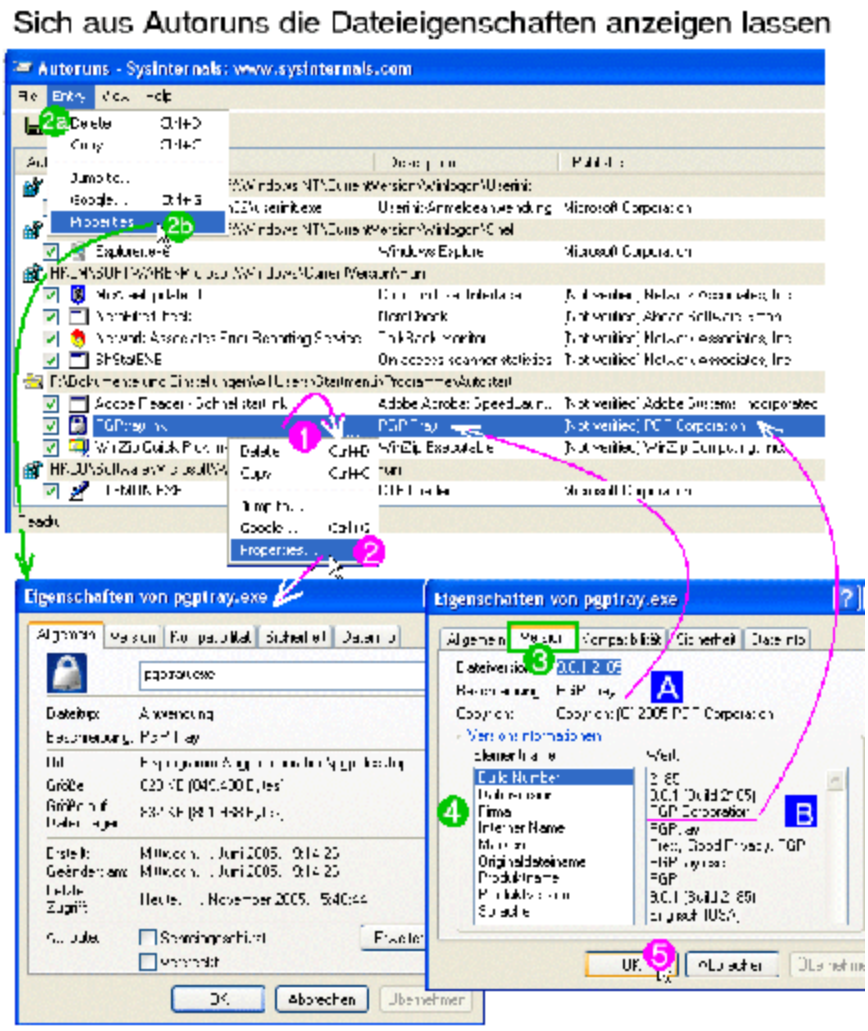

Bild 7.2 Zugriff aus Autoruns auf alle Eigenschafts-Angaben eines Programms

Diese Angaben sind aber nicht überzubewerten, denn um nicht aufzufallen, werden Angreifer versuchen, ihren Programmen harmlos klingende Eigenschaften zu geben.

In den folgenden drei Bilder werden die im Help-Menü im Abschnitt "Getting more Info about an Entry" genannten Möglichkeiten (s. B in Bild 7.1) gezeigt, wie man sich zu einem Eintrag aus dem Autoruns-Programm heraus sehr einfach mehr interne Informationen anzeigen lassen bzw. bei Google eine Nachfrage starten kann.

Wenn man z.B. sich zu einem Programm das betreffende Autostart-Verzeichnis ansehen möchte, so genügt es, den betreffenden Eintrag zweimal anzuklicken (Doppel-Klick) (1). Schon wird der Windows Explorer gestartet, das betreffende Autostart-Verzeichnis aufgeklappt und dort das betreffende Programm hervorgehoben.
Sie können den Eintrag aber auch anwählen (anklicken) (1) und dann entweder direkt das **Jump**-Icon (2) oder im Entry-Menü (2a) den "Jump to"-Eintrag (2b) ausführen:

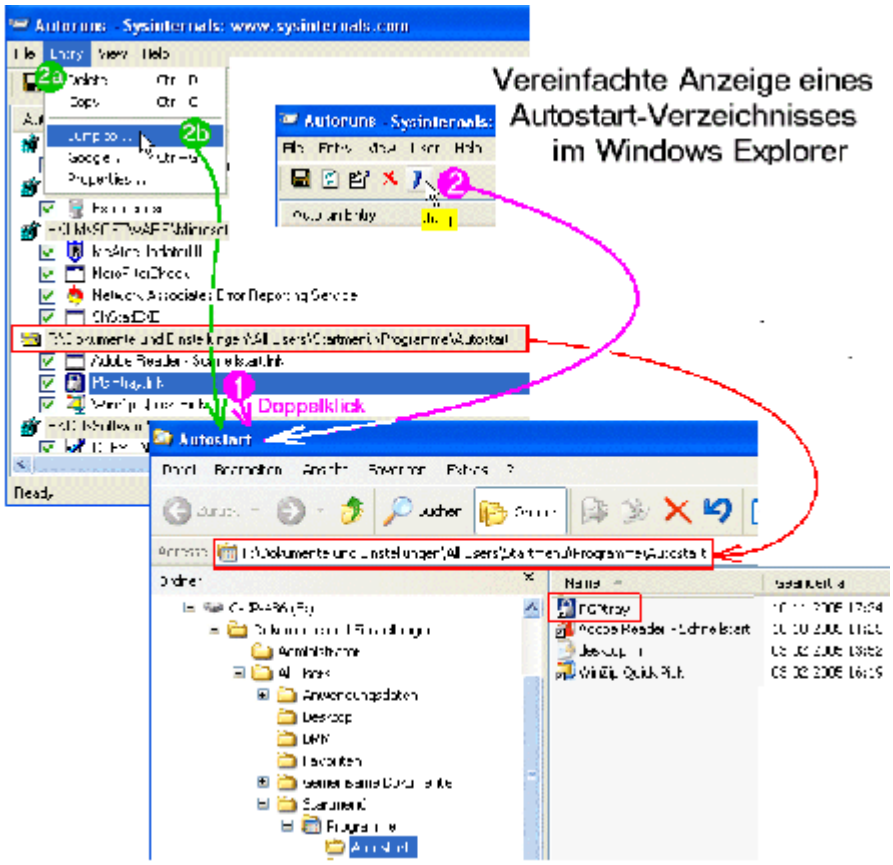

Bild 7.3 Vereinfachte Anzeige eines Autostart-Verzeichnisses mit dem Windows-Explorer

Auch die Anzeige eines Eintrages in der Registry ist mit Autoruns wieder sehr einfach entweder per Doppelklick (1) oder über das Jump-Icon (2) oder wieder im Entry-Menü (2a) über den "Jump to"-Eintrag (2b) anzufordern:

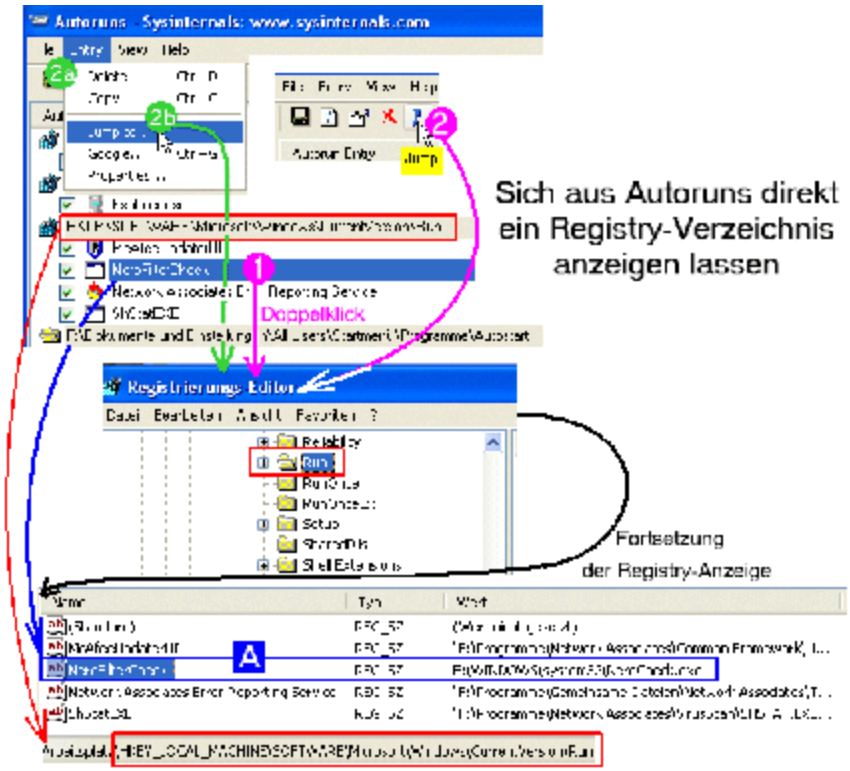

Bild 7.4 Vereinfachte Anzeige eines Registry-Eintrages

Sehr praktisch ist es auch, daß man sich zu einem ausgewählten Programm (1) direkt aus Autoruns weitere Informationen von Google holen kann, entweder über **Strg+G** (2) oder im Entry-Menü (2a) über den Google-Aufruf (2b):

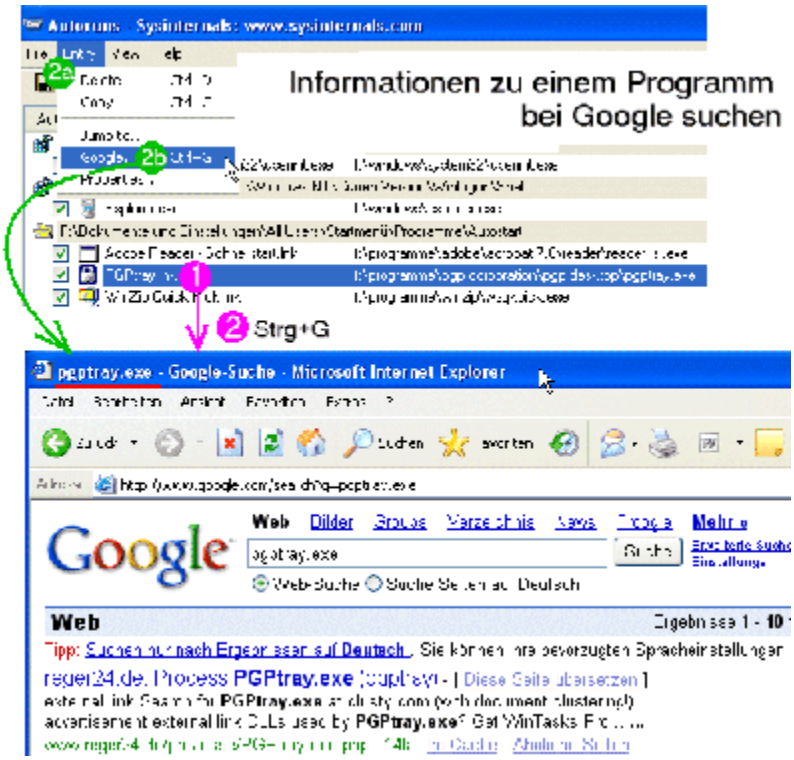

Bild 7.5 Vereinfachter Google-Suchaufruf zu einem Programm

Die Google-Suchantwort wird automatisch mit Ihrem Standard-Browser dargestellt.

Über das View-Menü 

kann man den Umfang der von Autoruns angezeigten Informationen definieren. Mit der Option "Include Empty Locations" (E) z.B. zeigt Autoruns auch diejenigen Verzeichnisse an, wo es keinen Entrag findet. Man sieht dann aber, was Autoruns alles überprüft:

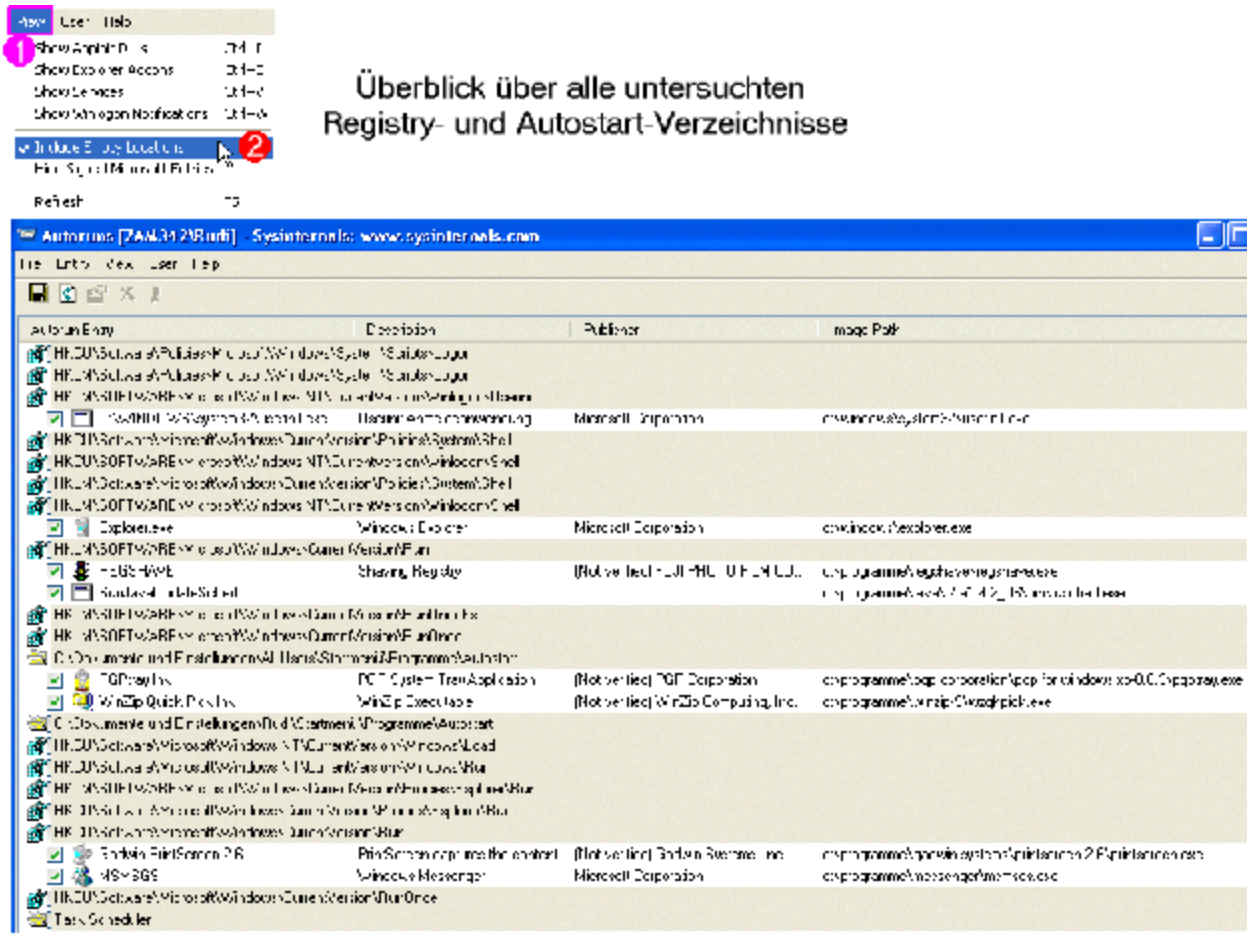

Bild 7.6 Überblick über alle von Autoruns untersuchten Registry- und Autostart-Verzeichnisse

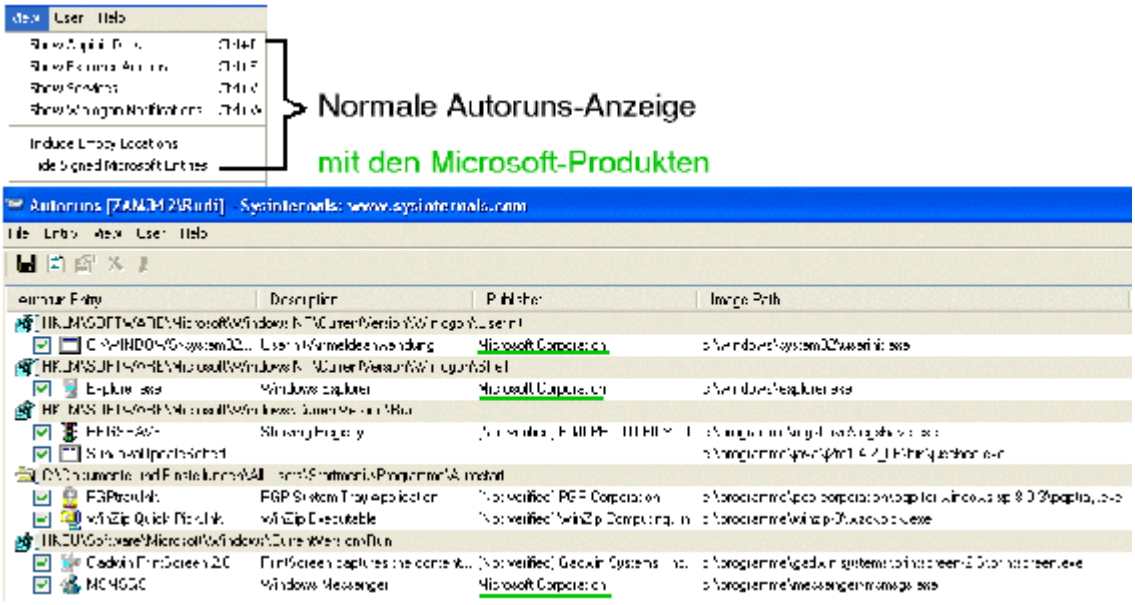

Bild 7.7 Normale Autoruns-Anzeige, also mit den Microsoft-Produkten

Durch die Option "Hide Signed Microsoft Entries" (F) werden nur noch die Aufrufe von solchen Programmen angezeigt, die nicht von Microsoft stammen. Das sind aber gerade diejenigen Programme, die man im Verdacht hat, daß sie ungewollt gestartet werden.

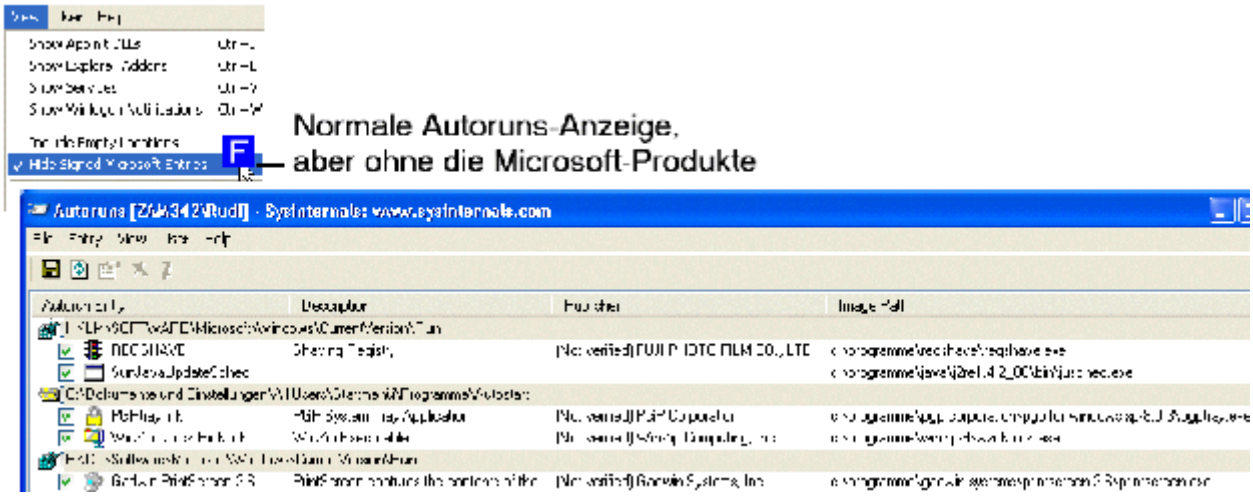

Bild 7.8 Normale Autoruns-Anzeige jedoch **ohne** die verifizierten Microsoft-Produkte

Explorer-Erweiterungen können gefährlich sein:

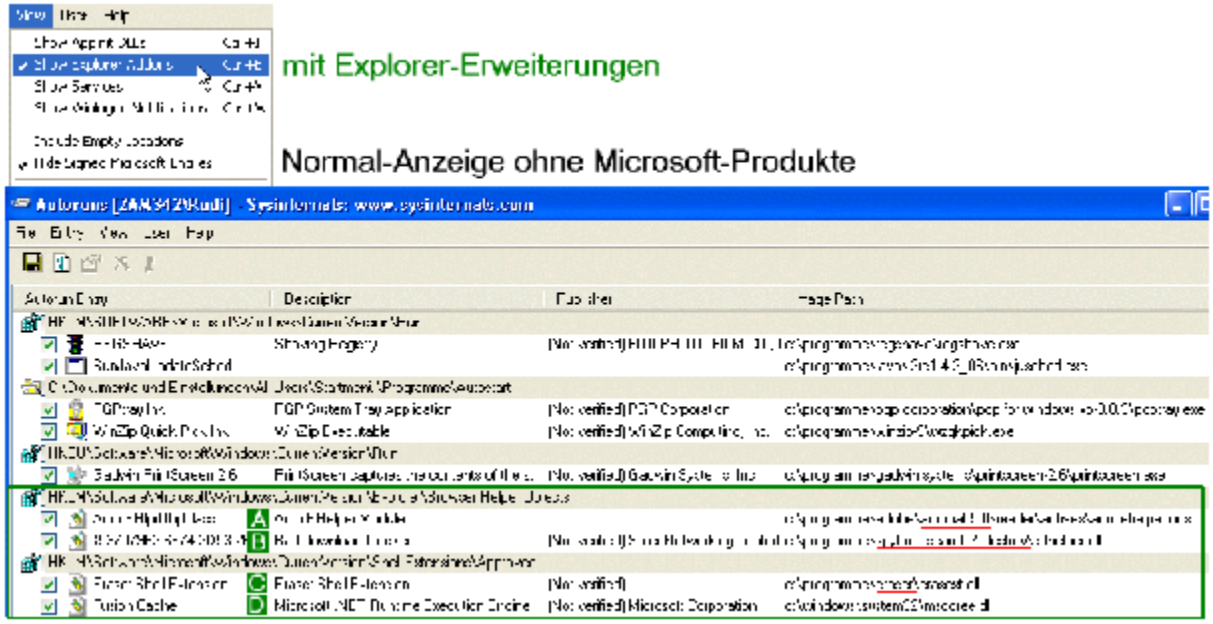

Bild 7.9 Anzeige der Explorer-Erweiterungen
zusätzlich zu den normalen Autoruns-Anzeige (ohne die verifizierten Microsoft-Produkte)

Der letzte Eintrag (Fusion Cache (s. D)) wird doch angezeigt, obwohl Microsoft-Produkte unterdrückt werden, weil dieses Produkt nicht signiert ist.
Die anderen drei Programme (A bis C) sind mir bekannt, also keine unbeabsichtigt installierte Programme (Entwarnung).

Interessant zur Aufdeckung ungewollt installierter Programme sind weiterhin die Dienste:

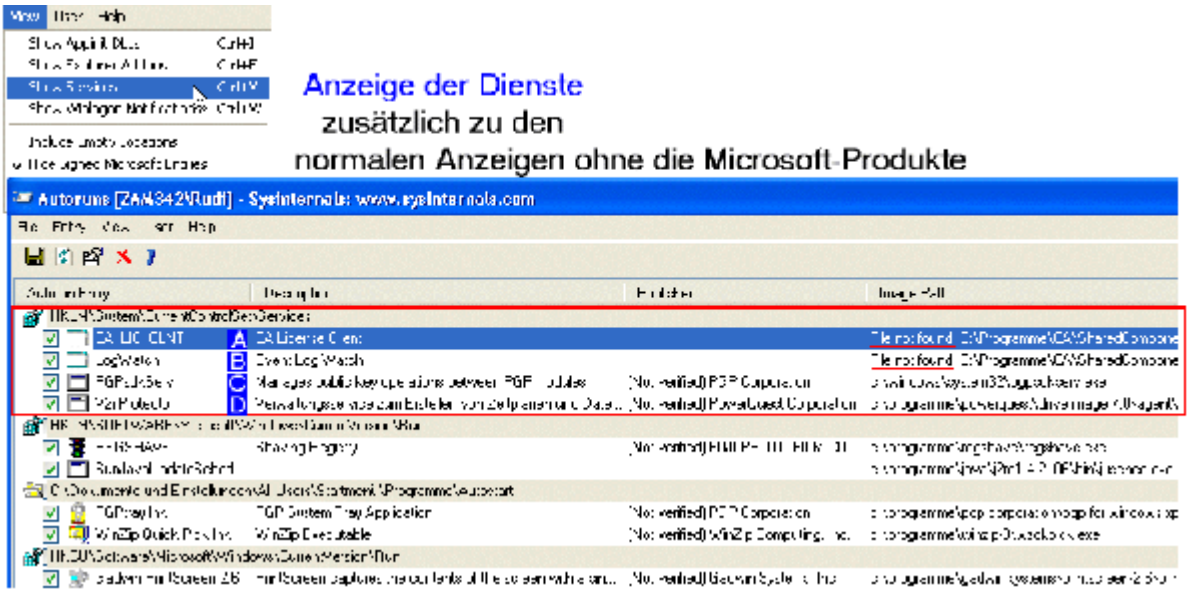

Bild 7.10 Anzeige der Dienste
zusätzlich zu den normalen Autoruns-Anzeige (ohne die verifizierten Microsoft-Produkte)

Für mich waren die beiden ersten Dienste (s. A und B) interessant, weil deren Programme gar nicht mehr existierten. Aus deren Pfad-Namen ist unschwer zu erkennen, daß diese zu einer CA-Software gehörte, die ich de-installiert hat, deren Uninstall-Programm aber nicht alle Einträge in der Registry sauber entfernt hat. Bevor ich diese Dienste entgültig gelöscht habe, habe ich mir per Doppelklick (s. 1 im folgenden Bild) die betreffenden Einträge in der Registry zeigen lassen, um zu prüfen, ob es dort weitere CA-Einträge gibt:

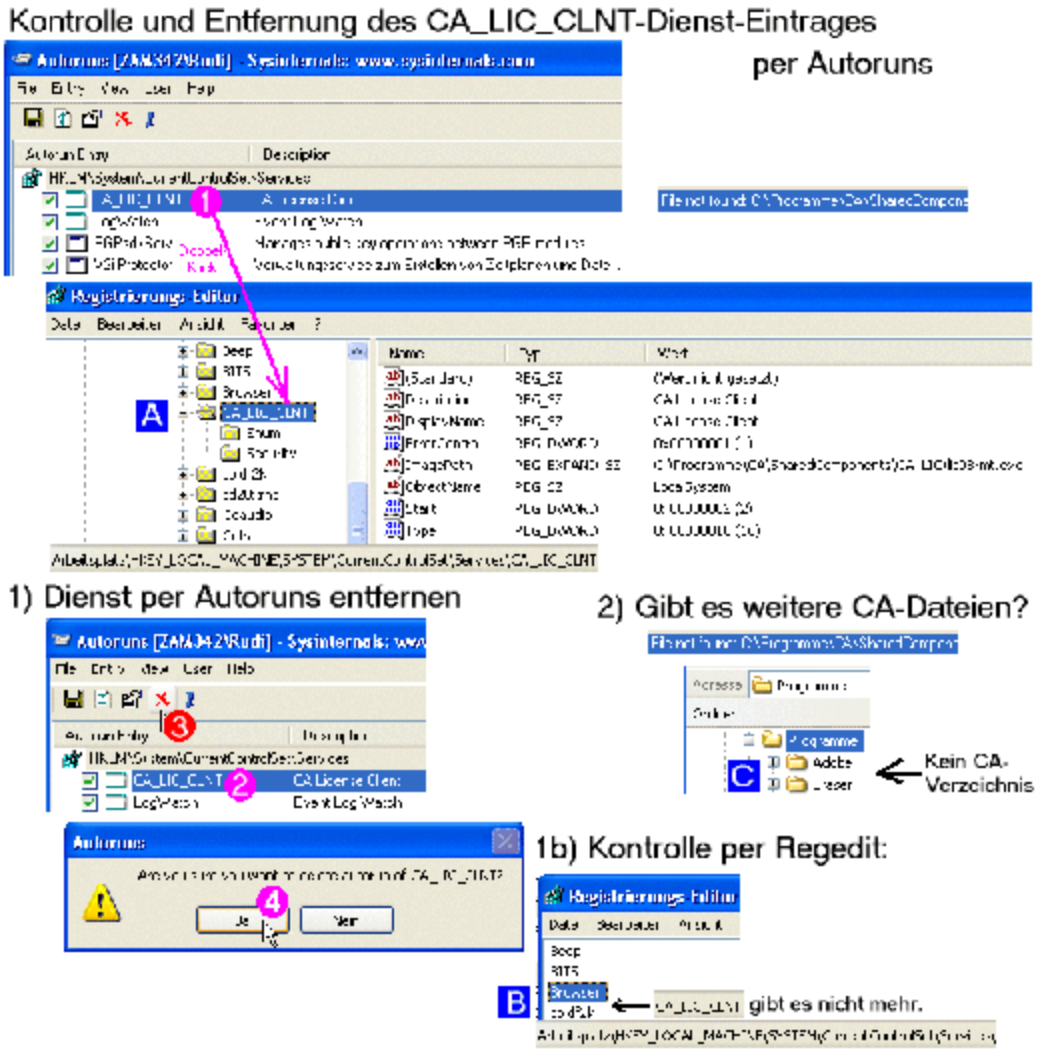

Bild 7.11 Kontrolle und Entfernung des CA_LIC-CLNT-Dienstes

In der Registry gab dort ein Verzeichnis mit zwei Unterverzeichnissen (s. A).
Mit Hilfe des Delete-Icons (3) habe ich diesen Dienst gelöscht. Die Löschung mußte bestätigt werden (4).
Wie die Kontrolle mit dem Registry-Editor zeigte (s. B), hat Autoruns den unerwünschten Dienst mit all seinen Unterverzeichnissen aus der Registry gelöscht.
Vorsichtshalber habe ich noch geprüft, ob es noch das C:\Programme\CA\-Verzeichnis gab. Das war aber früher schon korrekt gelöscht worden (C).

Analog wurde auch der unerwünschte LogWatch-Dienst mit Hilfe von Autoruns kontrolliert und gelöscht.

8. Ein erster Blick auf die Bedienung-Oberfläche der Autoruns-Version 8.31

Die Autoren Mark Russinovich und Bryce Cogswell habe das Programm gegenüber der in den vorherigen Kapiteln dokumentierten Programm-Version 6.0 weiterentwickelt. Anfang November 2005 war bereits die Version 8.31 aktuell.

Nun kann ich nicht bei jeder neuen Version alle bisherigen Bilder neu erstellen. Die Bedienung der Grundaufgabe, nämlich den Start von Programmen entweder vorübergehend durch Verschiebung eines Eintrages in ein parallel erstelltes AutorunsDisabled-Verzeichnis oder permante durch Löschen eines Start-Eintrages zu verhindern, hat sich ja auch nicht geändert.

Das folgende Bild zeigt die Bedien-Oberfläche von Autoruns Programm-Version 8.31 bei der Darstellung aller Ereignisse (allerdings ohne die verifizierten Microsoft-Ereignisse), die Autoruns kontrolliert. Dabei wird wiederum der gleiche PC betrachtete mit der gleichen Software-Umgebung, die auch in den Bildern 7.7 bis 7.10 vorgestellt wurde.

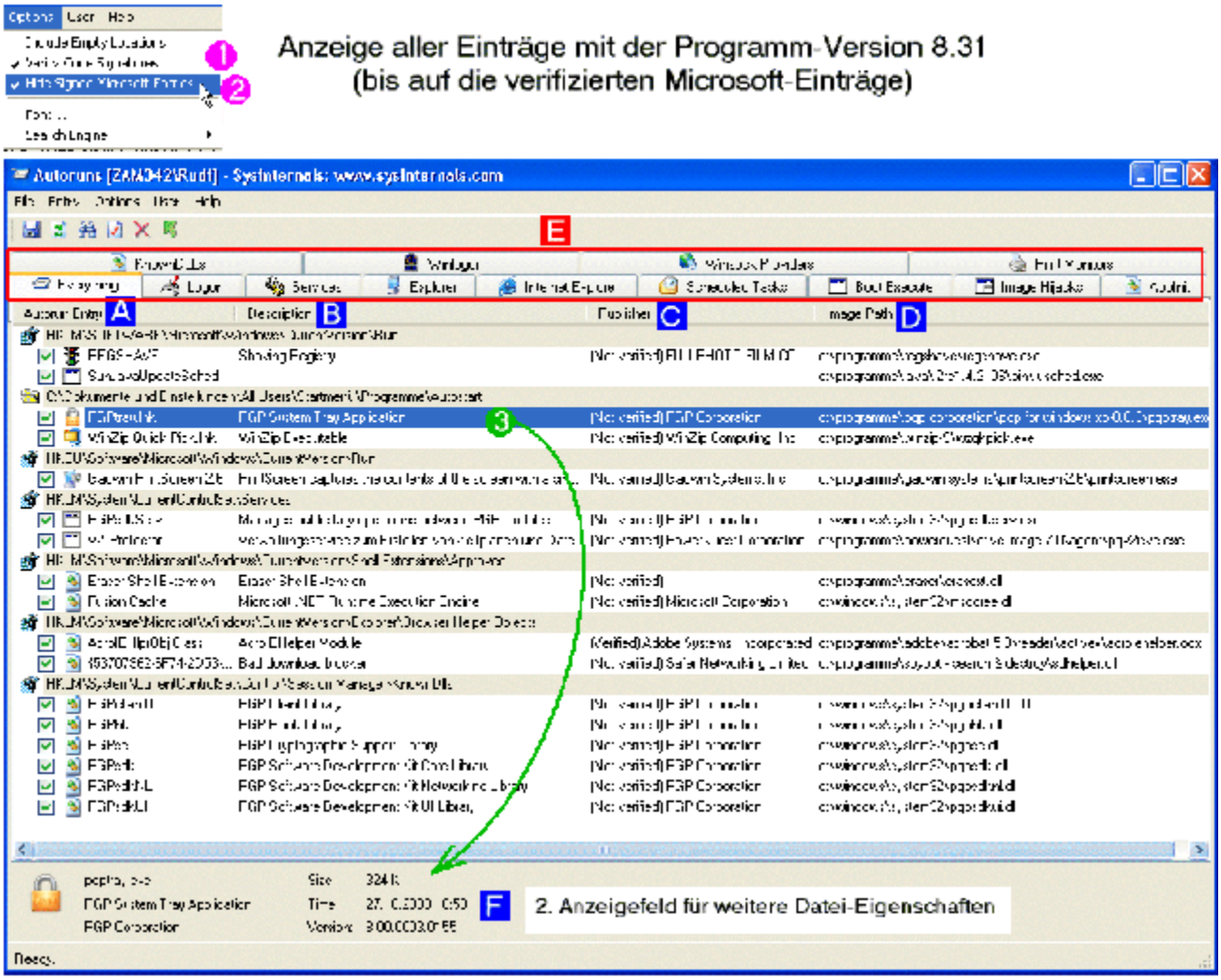

Bild 8.1 Autoruns-Anzeige in der Programm-Version 8.31

Im folgenden Bild sieht man zum einen die Menü-Einträge. Zum andern sind die verschiedenen Elemente der Autoruns-Anzeige getrennt dargestellt:

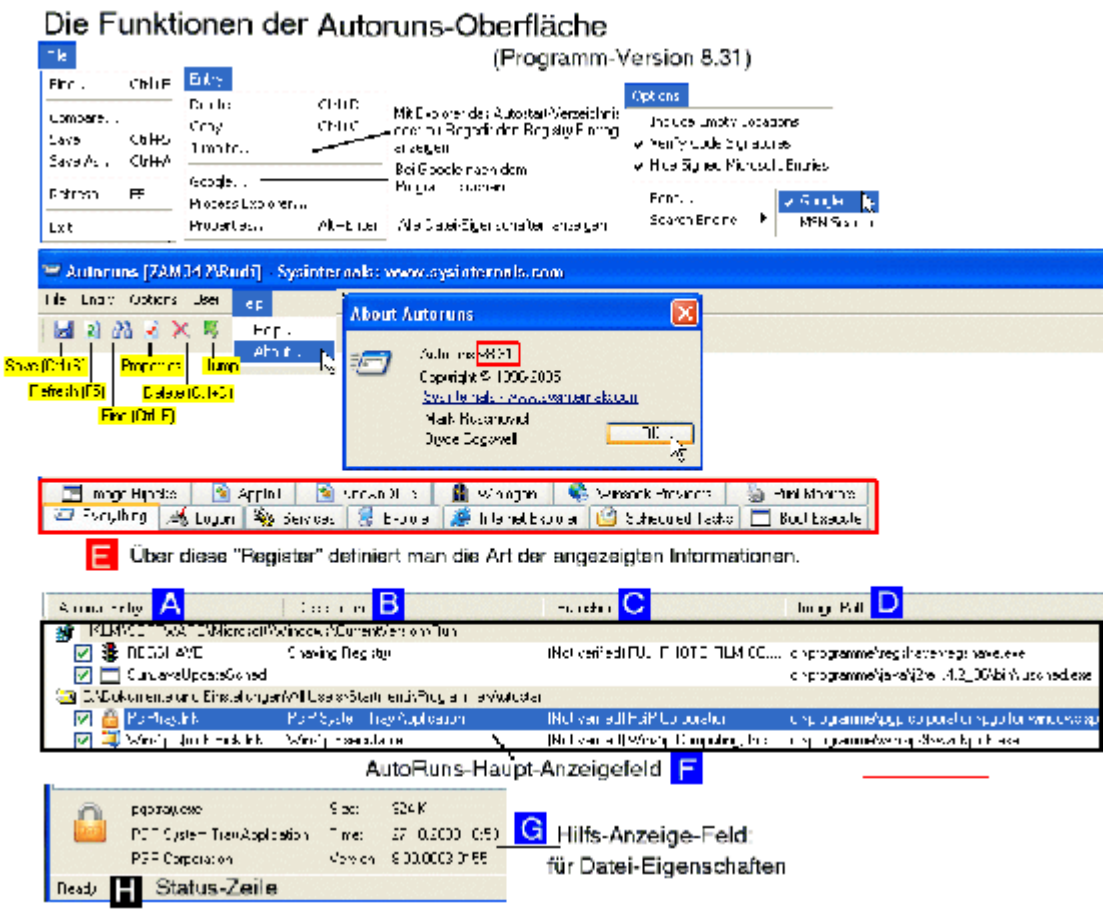

Bild 8.2 Die Autoruns-Bedien-Elemente in der Programm-Version 8.31

Die Autoruns-Bedienoberfläche hat also eine Vielzahl von Register-Einträgen bekommen (s. E), über die man viel besser als bisher definieren kann, was Autoruns wirklich anzeigen soll. Die Funktionen dieser Register sind in der Help-Datei wie folgt beschrieben:

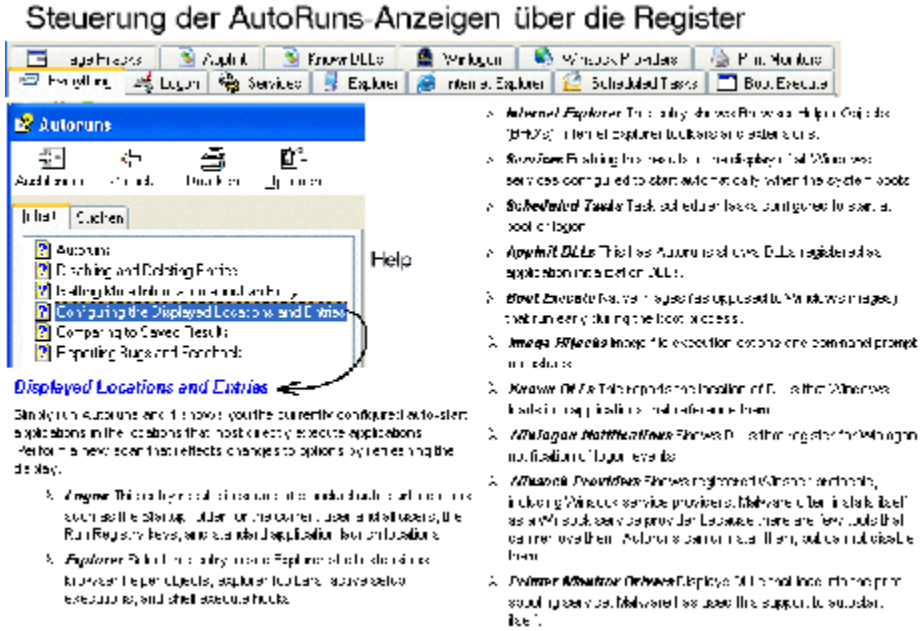

Bild 8.3 Help-Informationen zur Steuerung der Autoruns-Anzeige über die Register

Weiterhin kann man die Anzeige über die Einstellungen im Options-Menü konfigurieren:

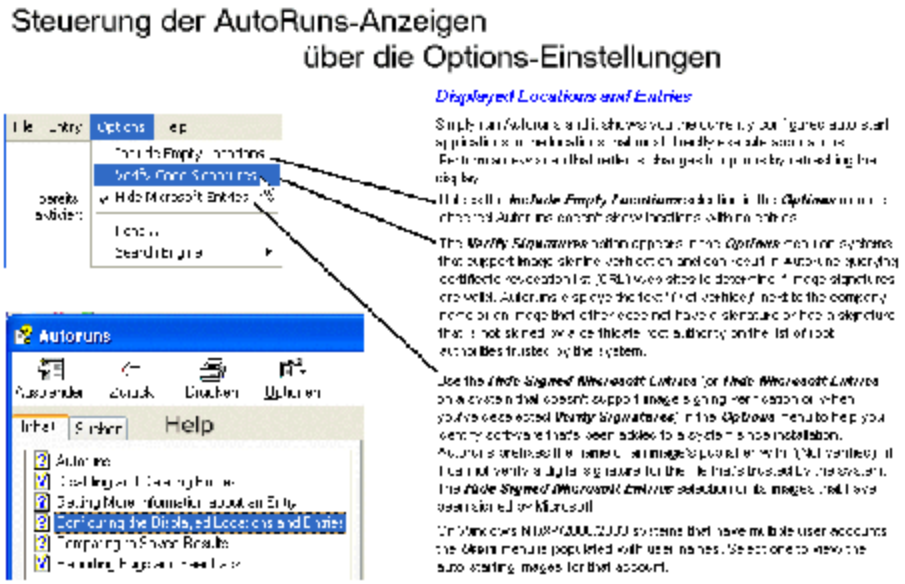

Bild 8.4 Help-Informationen zur Steuerung der Autoruns-Anzeige über die Einstellungen im Options-Menü

Zum anderen ist bei der Version 8.31 die Möglichkeit hinzugekommen, das Ergebnis einer Autoruns-Prüfung abzuspeichern und später mit dem aktuellen Ergebnis vergleichen zu lassen. Dazu heißt es in der Help-Datei:

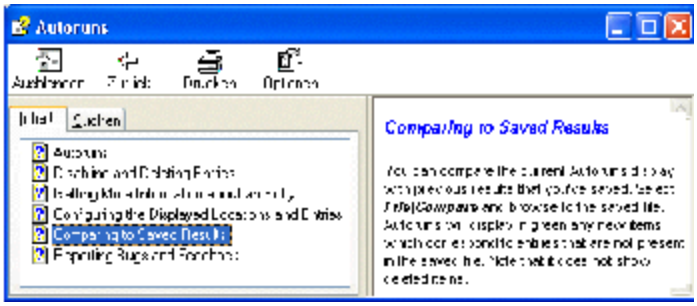

Bild 8.5 Help-Information zum Vergleich mit früher ermittelten Autoruns-Informationen

Um die Vergleichsmöglichkeit zu zeigen, muß man ein abgespeichertes Autoruns-Ergebnisse haben:

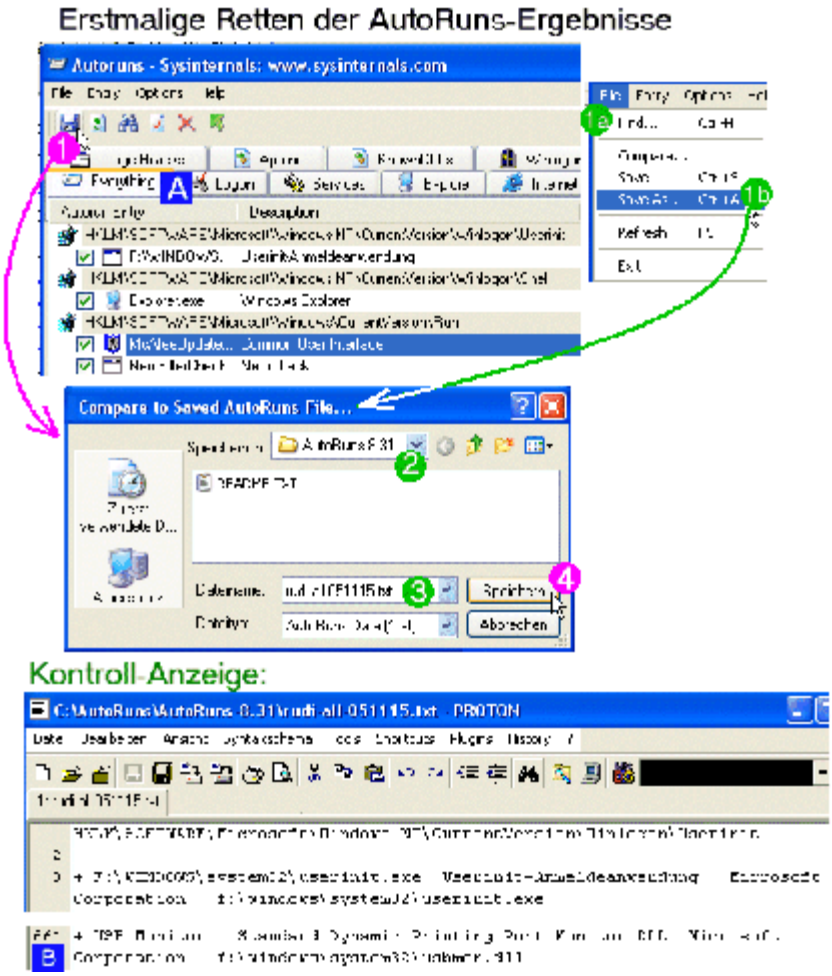

Bild 8.6 Abspeichern der Autoruns-Ergebnisse

Die Kontroll-Anzeige zeigt, daß Autoruns dann, wenn man wie bei diesem Beispiel alles kontrolliert haben will (Everything, s. A), mehrere hunderte Ereignisse erfaßt (B).

Wenn man nun unmittelbar danach den Vergleich durchführt, hat sich natürlich noch nicht viel geändert:

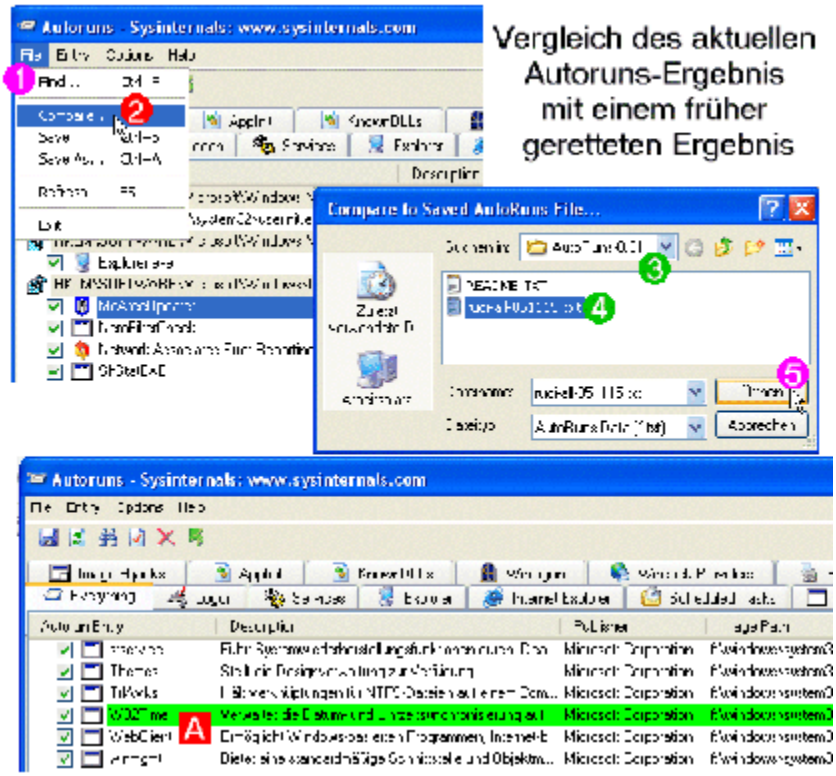

Bild 8.7 Vergleich des aktuellen Autoruns-Ergebnisses mit einem früher geretteten

Das Bild demonstriert aber, wie Autoruns geänderte Einträge hervorhebt, nämlich grün hinterlegt. Autoruns markiert aber inzwischen gelöschte Einträge nicht.

Diese Vergleichsmöglichkeit kann sehr hilfreich sein, um nachträglich installierte, unerwünschte Programme aufzudecken. Sie steht und fällt aber damit, daß man den Status des korrekten Systems erfaßt haben muß.

9. autorunsc.exe, die Kommando-Version von Autoruns

autorunsc.exe ist die Kommando-Version von Autoruns. Sein Syntax ist:

```
 Prompt>autorunsc.exe /?

Autoruns v8.31 - Autostart program viewer
Copyright (C) 2002-2005 Mark Russinovich and Bryce Cogswell
Sysinternals - www.sysinternals.com

Autorunsc shows programs configured to autostart during boot.

Usage: autorunsc [-a] | [-c] [-b] [-d] [-e] [-h] [-i] [-l] [-m] [-p] [-s] [-v] [-w] [user]
     -a         Show all entries.
     -b         Boot execute.
     -c         Print output as CSV.
     -d         Appinit DLLs.
     -e         Explorer addons.
     -h         Image hijacks.
     -i         Internet Explorer addons.
     -l         Logon startups (this is the default).
     -m         Hide signed Microsoft entries.
     -n         Winsock protocol providers.
     -p         Printer monitor DLLs.
     -s         Autostart services.
     -t         Scheduled tasks.
     -v         Verify digital signatures.
     -w         Winlogon entries.
     user       Specifies the name of the user account for which
                autorun items will be shown.
```

10. README.TXT

```
AutoRuns
Copyright (C) 2000-2004 Bryce Cogswell and Mark Russinovich
Sysinternals - www.sysinternals.com

Terms of Use
------------

This software is provided "as is", without any guarantee made
as to its suitability or fitness for any particular use. It may
contain bugs, so use of this tool is at your own risk. We take
no responsilbity for any damage that may unintentionally be caused
through its use.

You may not use the source to Autoruns, or distribute AutoRuns in any form,
without express written permission of Mark Russinovich or Bryce Cogswell.
```

```
Reporting Problems
------------------

If you encounter problems, please visit http://www.sysinternals.com
and download the latest version to see if the issue has been resolved.
If not, please send a bug report to:

        mark@sysinternals.com
```

11. Externe Links

[1] SysInternals:

- Homepage (www.sysinternals.com)
- Freeware von SysInternals (http://www.sysinternals.com/SystemInformationUtilities.html)
- Autoruns-Seite (http://www.sysinternals.com/Utilities/Autoruns.html)
- Autoruns-Beschreibung (in Windows IT Pro Magazine, Ausgabe November 2004:
  Autoruns: Hunt down autostart programs wherever they hide
  Mark Russinovich InstantDoc #44089 November 2004 (http://www.windowsitpro.com/Articles/Print.cfm?ArticleID=44089)
- Aktuelle Autoruns-Version holen (als ZIP-Datei von http://www.sysinternals.com/Files/Autoruns.zip)

[2] Bekannte Restart-Methoden und Verbreitungswege von Viren und Trojaner (Zusammengestellt von Rudi Theisen; http://www.fz-juelich.de/zam/sicherheit/docs/antivir/viren-restart.txt)
Diese Zusammenstellung erhebt keinen Anspruch auf Vollständigkeit.