

# **SuRun**

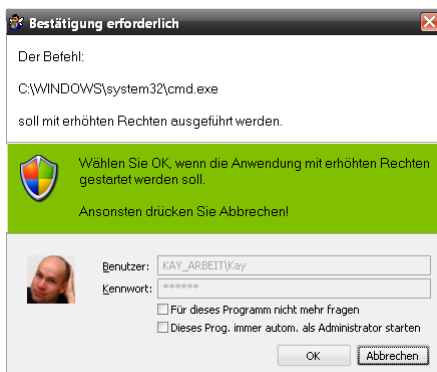
# **„Benutzerhandbuch“**

**(ein Versuch)**

# Inhaltsverzeichnis

Was ist SuRun?.....	3
Warum braucht man SuRun?.....	3
Wie funktioniert SuRun?.....	4
Warum keine Windows Bordmittel?.....	5
Installation.....	8
Deinstallation.....	10
Konfiguration.....	10
SuRun Einstellungen „Allgemein“.....	11
SuRun Einstellungen „SuRunners-Gruppe“.....	15
SuRun Einstellungen „Erweitert“.....	18
Betrieb.....	21
„SuRunner“ werden.....	21
Starte als Administrator.....	22
Automagie und Fragefreiheit.....	23
Das Kontext-Menü der Windows Shell.....	24
Integration in das System-Menü.....	25
Hinweisfenster für automagische Starts.....	26
Hinweisfenster für Administrator-Konten ohne Kennwort.....	26
Taskleistensymbol.....	26
„Ausführen als...“ durch SuRun ersetzen.....	27
Der WatchDog.....	28
Lizenz, Garantie und Haftung.....	29

## Was ist SuRun?



**SuRun** ist eine kostenlose Software, mit frei verfügbaren Quelltexten die das Arbeiten mit eingeschränkten Rechten unter Windows 2000, XP und Server 2003 erleichtert.

SuRun ermöglicht es, bestimmte Programme als Administrator zu starten, ohne ein Administrator-Kennwort preis zu geben, ohne die Registry des Benutzers zu wechseln oder Umgebungsvariablen zu verändern.

SuRun erhebt auf Anfrage den eingeschränkten Benutzer kurzzeitig zum Administrator.

SuRun läuft nicht in Windows 95/98/ME.

Für Windows Vista braucht man SuRun eigentlich nicht. Dort funktioniert es aber, wenn man die User Account Control abschaltet.

## Warum braucht man SuRun?

In Windows NT und dessen Kindern (2000, XP, 2003, Vista...) hat Microsoft eine Rechteverwaltung integriert. Anhand von Zugriffskontrollisten legt Windows fest, ob und wie auf Objekte (z.B. Dateien, Geräte, Registry) zugegriffen werden darf oder nicht.

Jedes Programm wird standardmäßig mit den Rechten des Programms ausgeführt, das es startet. So z.B. *erbt Notepad* üblicher Weise die Rechte von *Explorer*.

Auch schadhafte Software, die ausgeführt wird, hat die Rechte des ausführenden Programms. So würde ein Virus die Rechte des *Internet Explorers* bekommen der die Rechte von *Explorer* bekam der die Rechte des angemeldeten Benutzers hat.

**Wenn man immer als Administrator arbeitet, kann ein Virus den PC unbemerkt komplett übernehmen und das System unbrauchbar machen.**

Durch die integrierte Unterstützung für Virtualisierung in allen aktuellen Prozessoren, kann man sogar das ganze Windows im laufenden Betrieb in eine virtuelle Maschine verbannen. Ein experimentelles Beispiel dafür hat 2007 *Joanna Rutkowska* (<http://InvisibleThings.org>) mit BluePill (<http://bluepillproject.org/>) geliefert. Sie packt das System „zurück in die *Matrix*“ während Windows weiterhin meint die Kontrolle zu haben. Doch auch BluePill braucht Administratoren-Rechte (oder eine Lücke im System). Sonst kann sie sich nicht installieren.

Arbeitet man mit eingeschränkten Rechten, kann ein Virus das System prinzipiell nicht angreifen, da ihm, wie dem angemeldeten Benutzer, die Rechte dazu fehlen.

**In Windows ist es mit Bordmitteln nicht leicht, mit eingeschränkten Rechten zu arbeiten.** Selbst für einfache Sachen, wie das Stellen der Systemuhr oder das Anpassen der Energieverwaltung, braucht Windows einen Administrator. Software darf man normalerweise gar nicht installieren, Hardware auch nicht.

Historisch gewachsene Windows Programme benutzen INI-Dateien im Windows-Verzeichnis um deren Einstellungen zu speichern. All diese Programme laufen nicht mit

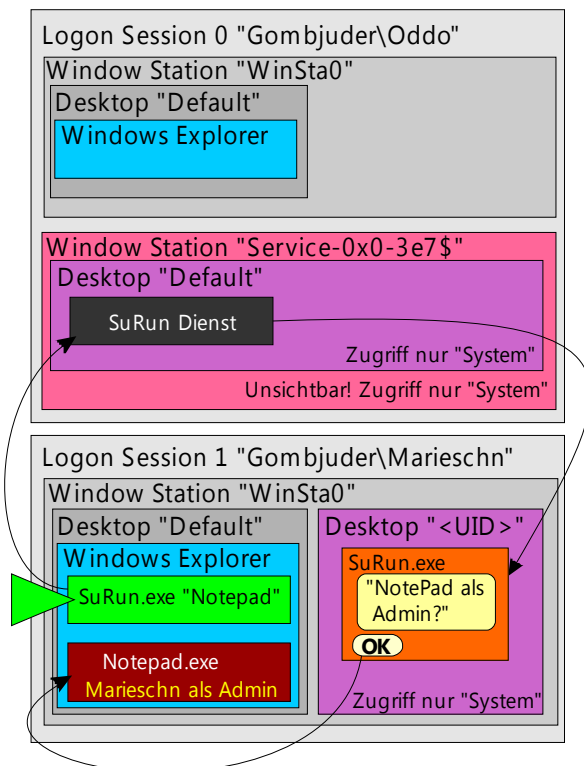
eingeschränkten Rechten. Man muss die Berechtigungen für jede INI-Datei anpassen, damit eingeschränkte Benutzer darin schreiben dürfen.

## Wie funktioniert SuRun?

**SuRun** benutzt einen einfachen Trick um bestimmte Benutzer auf Anfrage eine Anwendung mit administrativen Rechten ausführen zu lassen. Es hat einen eigenen Windows Dienst, der den Benutzer kurz in die lokale Gruppe der „Administratoren“ einträgt, das gewünschte Programm startet und den Benutzer aus der „Administratoren“ Gruppe wieder entfernt. Vorher muss der Benutzer auf einem abgesicherten Desktop den Start der Anwendung bestätigen.

Dadurch kann man **Administrator werden, ohne ein Administratoren-Kennwort zu kennen**.

Das Ganze funktioniert prinzipiell so:



### Informelle Beschreibung:

An Gombuter sind (Dank schneller Benutzerumschaltung) zwei Benutzer angemeldet. Zuerst kam Oddo, der wollte noch schnell ein Spiel spühlen.

Dann kam Marieschn, die noch eine Email schreiben muss.

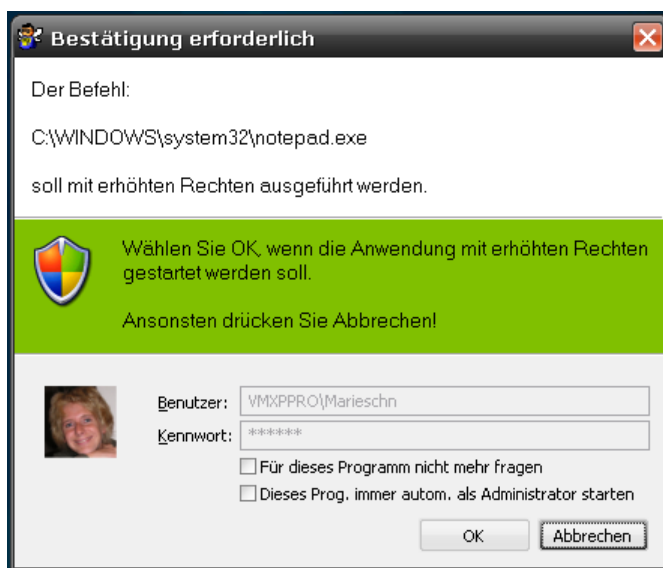
Also drückte Oddo kurz [WIN]+„L“ und ließ Marie sich anmelden und ihre Email schreiben.

Marie will weder Virenschanner noch Viren haben und arbeitet deshalb vorbildlich mit eingeschränkten Rechten.

Das Email Programm “Notepad” verweigert aber den Dienst, weil es noch einige hundert Megabyte Sicherheitsupdates aus dem Internet nachinstallieren muss und dafür administrative Rechte braucht.

Also klickt die Goldmarie mit der rechten Maustaste auf Notepad.exe und dann auf SuRuns Eintrag “Starte als Administrator“. Damit wird “SuRun.exe Notepad.exe” gestartet. SuRun.exe kontaktiert den Dienst und teilt ihm mit, dass die Marie in Logon Session 2 ein Notepad.exe mit administrative Rechten braucht.

Der Dienst ist sich nicht ganz sicher, ob die Marie das wirklich will oder ein Virus in ihrem Namen zu handeln versucht. Also macht er erstmal einen neuen Desktop in Marieschns “Window Station” auf. Auf diesen neuen Desktop dürfen als Programme nur Dienste zugreifen. Dort wird die Marie nochmal gefragt, ob sie wirklich Notepad administrativ ausführen wollte.



Ein Virus könnte hier keinen Klick simulieren, aber die Marie findet leicht den “OK” Knopf und drückt ihn. Das macht den SuRun Dienst nun sicher und er startet “Notepad.exe” als Benutzer “Marieschn” aber mit den Rechten eines Administrators.

Nach ein paar Sekunden hat sich Notepad die Updates einverleibt, Marie kann schnell ihre Email schreiben und Oddo bricht den Streckenrekord im Geschirrspühler.

Alle sind glücklich.

## Warum keine Windows Bordmittel?

Der Windows Explorer hat einen “Ausführen als...” Befehl.

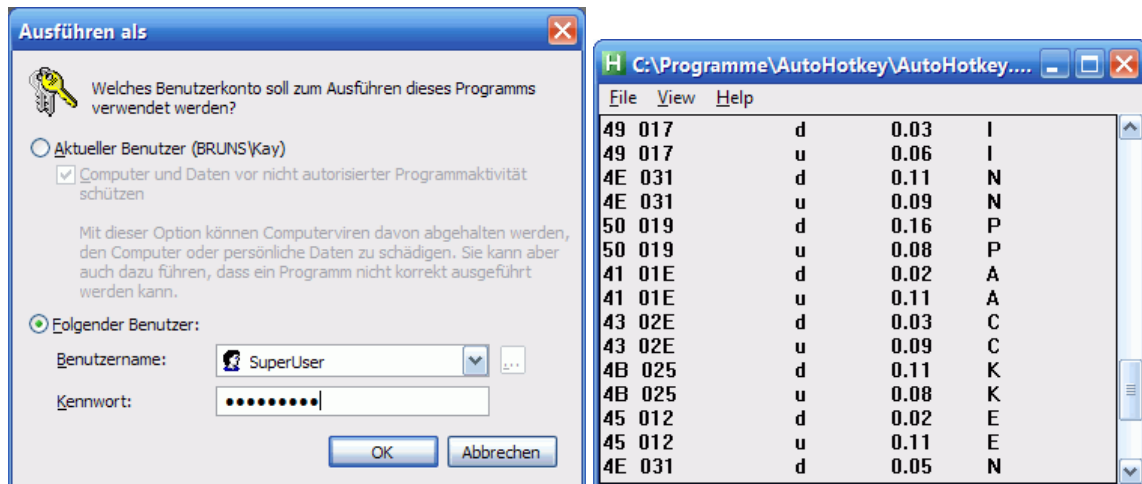
Der hat allerdings zwei entscheidende Nachteile!

**Der erste und fatale Nachteil:** Schadsoftware kann sich durch „Ausführen als...“ mit einfachsten Mitteln ein Administratoren-Kennwort besorgen.

Als Demonstration dafür kann man einfach AutoHotkey benutzen.

## Warum keine Windows Bordmittel?

AutoHotkey schneidet alle Tastendrücke mit und man kann sich das Passwort im LOG ansehen.



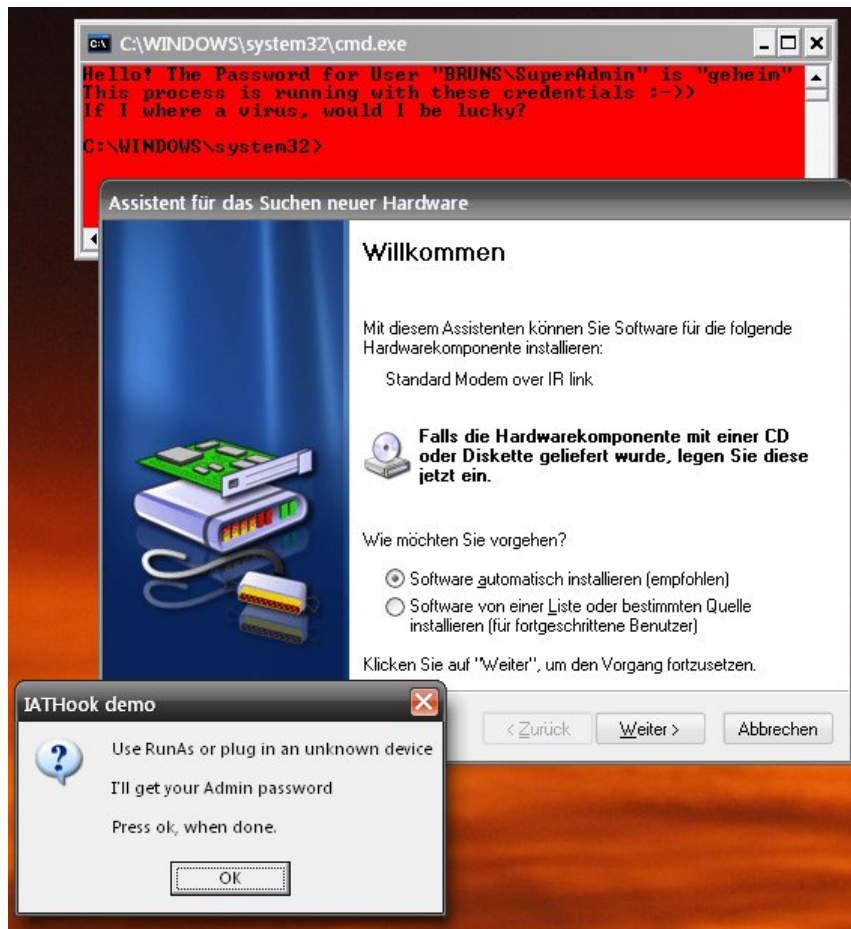
Mit dem Windows Kommandozeilenprogramm „RunAs“, oder dem *MachMichAdmin Script* ist es nicht viel anders. Auch wenn da ein normaler Keylogger nicht reicht, kann man diese Programme missbrauchen, um unbemerkt an ein Administrator-Kennwort zu gelangen.

Wie das geht, demonstriert z.B. meine Demo [„IAT-Hook“](#).

Wenn man, selbst als Gast, die Demo startet, neue Hardware ansteckt oder RunAs benutzt und die Daten eines Administrators eingibt,



startet diese Demo eine cmd-Konsole mit diesen Berechtigungen.



Das Microsoft dieses Thema so nachlässig behandelt hat, ist mir unverständlich. Schon in Windows NT 3.1 hätte man das Sicherheitsloch stopfen können. An der Rechteverwaltung hat sich bis einschließlich Windows XP nichts geändert.

**Das zweite Problem** des „Ausführen als...“ Befehls von Windows ist, dass das gestartete Programm im Kontext eines anderen Benutzers läuft. Das Benutzer-Verzeichnis und HKEY\_CURRENT\_USER in der Registry zeigen auf die Orte des Benutzers, der in „Ausführen als...“ angegeben wurde.

Ein Beispiel:

Ich bin als eingeschränkter Benutzer „Oddo“ angemeldet und will SuperApp installieren.

Das Installationsprogramm meckert, dass es keine ausreichenden Rechte hat. Also benutzt „Oddo“ „Ausführen als...“, um die Software als Administrator „SubberUhser“ zu installieren.

SuperApp ist wahnsinnig teuer, darf nur von einem Benutzer ausgeführt werden und speichert den Lizenzschlüssel und Einstellungen in HKEY\_CURRENT\_USER\Software\SuperApp bzw. dem Benutzerverzeichnis „C:\Dokumente und Einstellungen\SubberUhser“ ab.

Das Dumme ist, das genau diese Orte während der Installation auf den falschen Ort verweisen.

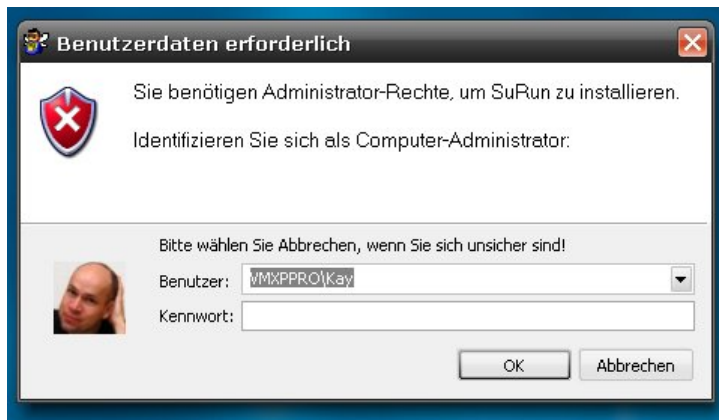
Der Benutzer "Oddo" hat seine Einstellungen in "C:\Dokumente und Einstellungen\Oddo" gespeichert, SuperApp legt den Lizenzschlüssel aber in "C:\Dokumente und Einstellungen\SubberUhser" ab.

Will "Oddo" nun SuperApp benutzen, guckt er in eine "Sie haben keine Lizenz" Meldung, denn "Oddo" darf in "C:\Dokumente und Einstellungen\SubberUhser" Dateien weder lesen noch schreiben. [Mit der Registry ist das analog!]

## Installation

**GANZ WICHTIG!** Behalten Sie immer ein Administrator-Konto, an das Sie sich anmelden können, falls SuRun Unerwartetes tut!

Um SuRun zu installieren muss man einfach das Installations-ZIP in einen Ordner auspacken und "*InstallSuRun.exe*" ausführen. Ist man während der Installation kein Administrator, fragt SuRun nach einem Administrator Passwort.



**WARNUNG:** Das Passwort für die Installation wird in einer nicht gesicherten Umgebung abgefragt. Schon vorhandene Passwortschnüffler würden es herausfinden! Sicher ist, den Netzwerkstecker zu ziehen, sich als Administrator anzumelden und SuRun zu installieren.

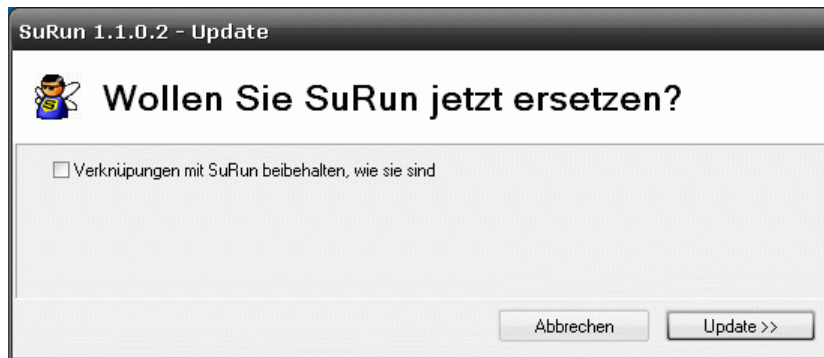


Der Dialog für die Installation beinhaltet zwei Checkboxes.

Sie sollten auf jeden Fall den Haken in **"'Administratoren' statt 'Ersteller' als Standard-Besitzer für von Administratoren erstellte Objekte."** aktiviert lassen!



Ist SuRun bereits installiert, wird „*InstallSuRun.exe*“ ein Update vorschlagen.



SuRuns Einstellungen werden bei einem Update nicht verändert. Lediglich die „**Starte als Administrator...**“-Verknüpfungen werden neu angelegt. Ist jedoch „**Verknüpfungen mit SuRun beibehalten, wie sie sind**“ aktiviert, werden auch diese nicht verändert.

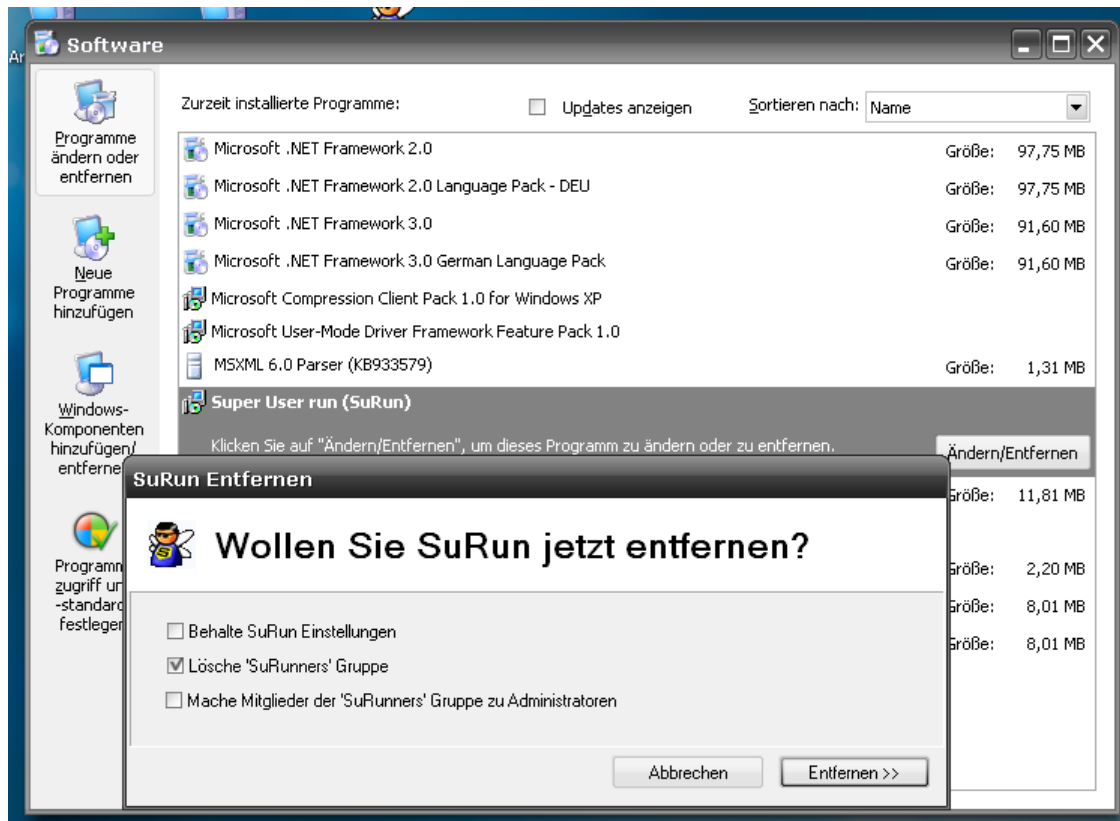
Während der Installation zeigt SuRun durchgeführte Aktionen in einer Liste an.



Um die Installation abzuschließen, **müssen Sie sich von Windows ab-** und wieder **anmelden**.

### Deinstallation

SuRun kann über „Software“ in der Systemsteuerung entfernt werden.



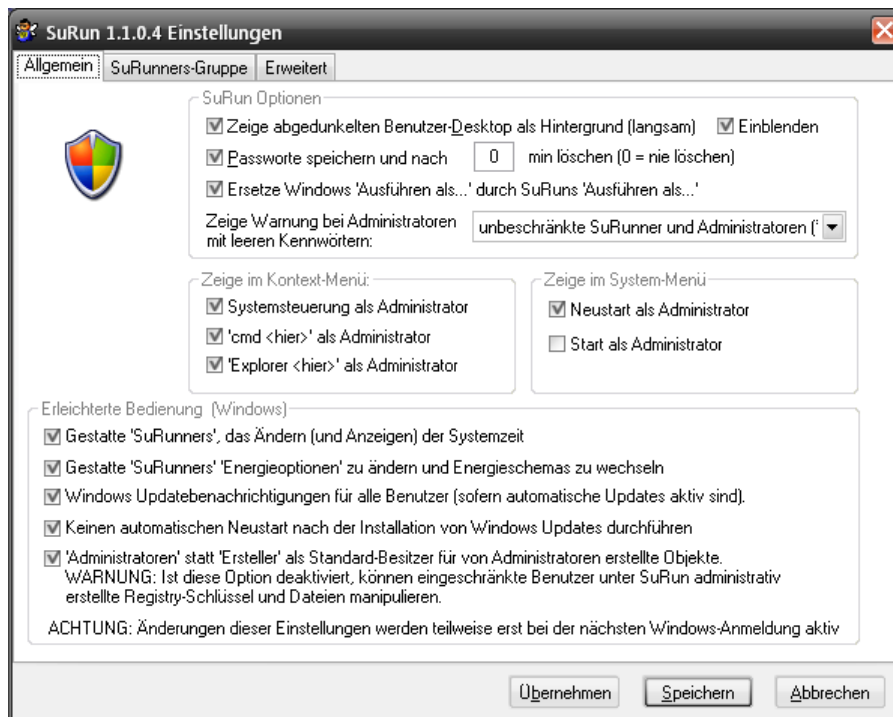
Ist die Option „**Behalte SuRun Einstellungen**“ aktiviert, wird SuRun alle Einstellungen belassen, wie sie sind und die Gruppe „*SuRunners*“ nicht löschen.

Dateien die nicht sofort gelöscht werden können, werden beim nächsten Systemstart gelöscht.

## Konfiguration

Über die Kommandozeile **“surun /setup”** oder „*SuRun Einstellungen*“ in der Systemsteuerung erscheint SuRuns Konfigurationsdialog auf einem abgesicherten Desktop.

### *SuRun Einstellungen „Allgemein“*



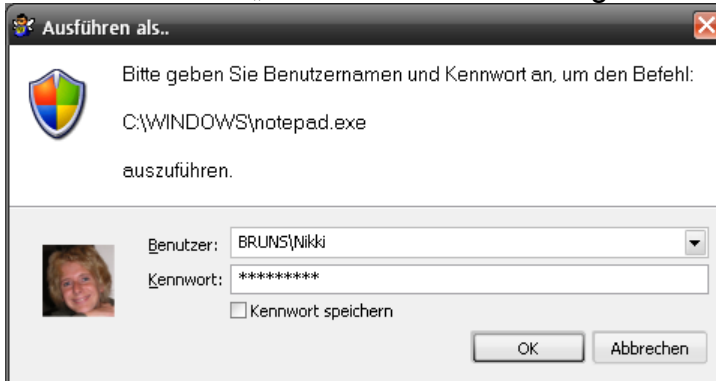
- **"Zeige abgedunkelten Benutzer-Desktop als Hintergrund (langsam)"**  
Ist diese Option aktiviert, wird vor dem Umschalten auf den abgesicherten Desktop ein Schnappschuss des Benutzer-Desktops gemacht, verwaschen und abgedunkelt und dann als Hintergrundbild im abgesicherten Desktop dargestellt. (Das kostet auf meinem System (PIV 3.2GHz, 2800×1050 Pixel) ca. 0.5s, sieht aber schön aus)
- **„Einblenden“**  
Der Hintergrund des abgesicherten Desktops wird ein- und ausgeblendet. Ist diese Option aktiv, werden erhebliche Ressourcen und ein schnelles System benötigt.
- **"Passworte speichern und nach <t> min löschen (0 = nie löschen)"**  
Diese Option schaltet das Speichern eingegebener Passworte in der Registry an oder aus. Die Passworte werden im Zweig HKEY\_LOCAL\_MACHINE\ Security\ SuRun abgelegt, auf den standardmäßig nicht einmal Administratoren Zugriff haben. Die Passworte werden zusätzlich mit Blowfish verschlüsselt.

Ist eine Zeit verschieden von NULL angegeben wird SuRun erneut nach dem Passwort fragen, wenn man SuRun länger als diese Zeit nicht zum starten eines Programm benutzt. Das ist Sinnvoll für Situationen, in denen man häufig Programme als Administrator starten muss aber das Passwort nicht dauerhaft speichern will.

- **„Ersetze Windows 'Ausführen als...' durch SuRuns 'Ausführen als...'“**

Das Benutzen des eingebauten „Ausführen als...“ von Windows ist sehr gefährlich! Selbst Programme mit Gast-Rechten können die eingegebenen Daten abfangen und das System übernehmen.

SuRun kann den „Ausführen als...“-Eintrag des Shell Kontext-Menüs ersetzen:



Das hat den großen Vorteil, dass das Benutzerkennwort auf einem abgesicherten Desktop abgefragt wird und nicht ausgespäht werden kann. Das Kennwort für den Benutzer kann gespeichert werden. Es wird leicht verschlüsselt in der Registry unter „HKEY\_LOCAL\_MACHINE\SECURITY\SuRun\RunAs\<username>\Cache“ gespeichert.

**HINWEIS:** Das Optionsfeld kennt drei Zustände:

Ist der Haken gesetzt, werden alle Windows „Ausführen als...“ Einträge in der Registry durch SuRuns „Ausführen als...“ ersetzt.

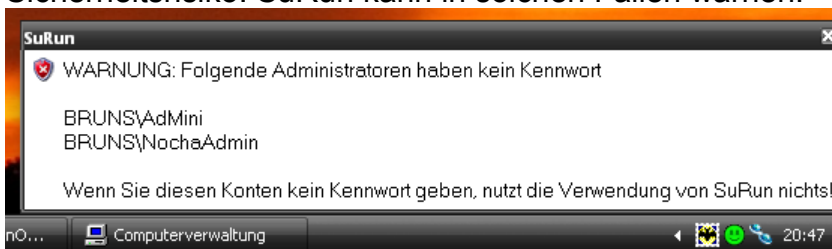
Ist der Haken gelöscht, werden alle SuRun „Ausführen als...“ Einträge in der Registry durch Windows „Ausführen als...“ ersetzt.

Ist der Haken „Intermediate“, wird nichts unternommen.

- **„Zeige Warnung bei Administratoren mit leeren Kennwörtern“**

SuRun kann beim Anmelden eines Benutzers prüfen, ob im System lokale Administratoren existieren, die kein Kennwort haben.

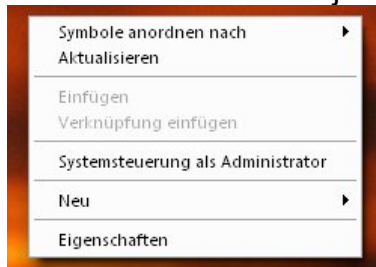
Standardmäßig legt Microsoft bei der Installation genau so ein Konto, den vordefinierten „Administrator“ ohne Kennwort an. Das ist ein erhebliches Sicherheitsrisiko! SuRun kann in solchen Fällen warnen:



Das Hinweisfenster verschwindet nicht von selbst und muss manuell geschlossen werden.

Als Standard werden Administratoren und nicht eingeschränkte Mitglieder der Gruppe SuRunners gewarnt, es gibt jedoch fünf Optionen, welche Benutzer gewarnt werden: „Alle Benutzer“, „SuRunner und Administratoren“, „unbeschränkte SuRunner und Administratoren“, „Administratoren“ und „Niemanden“.

**"Zeige im Kontext-Menü:"** Ein Kontext-Menü für ein Objekt erscheint, wenn man mit der rechten Maustaste auf ein Objekt klickt bzw. die Menü-Taste drückt.



- **"Systemsteuerung als Administrator"**  
...wird im Kontext-Menü des Desktops eingeblendet.  
Klickt man auf den Befehl, wird die Systemsteuerung mit erhöhten Rechten gestartet.
- **"cmd <hier>' als Administrator"**  
...wird im Kontext-Menü für Ordner eingeblendet.  
Klickt man auf den Befehl, wird die Eingabeaufforderung (cmd) im gewählten Ordner mit erhöhten Rechten gestartet.
- **"Explorer <hier>' als Administrator"**  
...wird im Kontext-Menü für Ordner eingeblendet.  
Klickt man auf den Befehl, wird Explorer im gewählten Ordner mit erhöhten Rechten gestartet.

**"Zeige im System-Menü"** Das System-Menü erscheint, wenn man auf das Symbol in der Titelleiste einer Anwendung klickt, wenn man auf die Titelleiste der Anwendung mit der rechten Maustaste klickt oder wenn man [ALT]+[Leerzeichen] drückt:



- **"Neustart als Administrator"**  
Beendet das laufende Programm brutal und startet es erneut als Administrator.  
**Vorsicht:** Wenn man das mit Explorer macht, läuft danach die Windows Shell mit Administrator-Rechten.
- **"Start als Administrator"**  
Startet das laufende Programm noch mal, aber mit Administrator-Rechten.

Mit Einstellungen im Feld **"Erleichterte Bedienung (Windows)"** kann man einige Unannehmlichkeiten umgehen. Die Änderungen dieser Einstellungen werden erst bei der nächsten Windows-Anmeldung bzw. einem Windows Neustart wirksam.

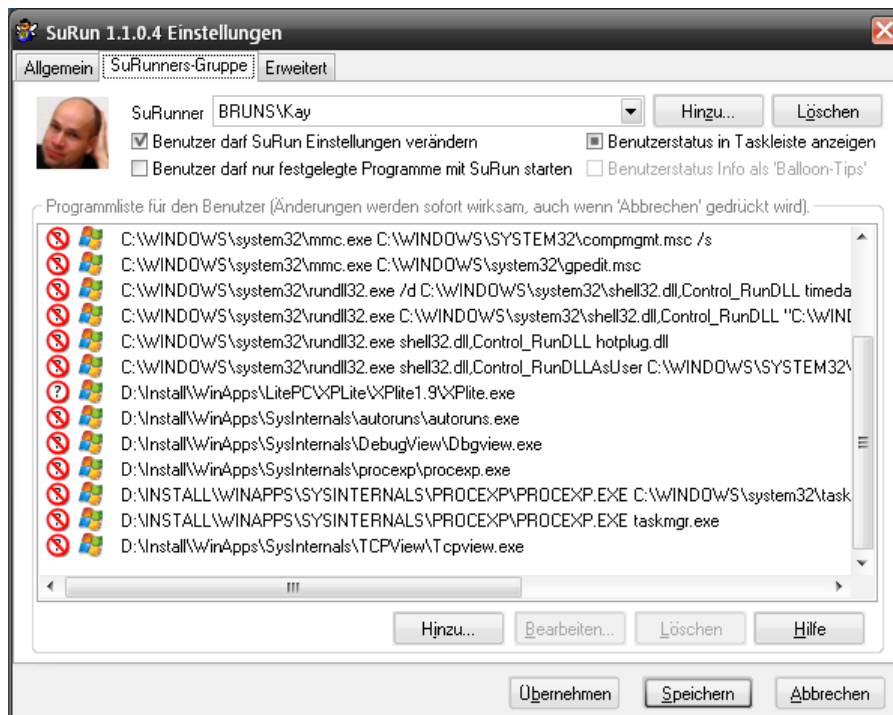
- **"Gestatte 'SuRunners', das Ändern (und Anzeigen) der Systemzeit"**  
Eingeschränkte Benutzer dürfen in Windows NT die Uhrzeit des Systems **nicht** verändern. Das mag sinnvoll sein, wenn der Rechner Domänenmitglied ist, aber für die meisten Heimsysteme nervt das nur. Wenn man auf die Uhrzeit im Infobereich der Taskleiste doppelklickt, meckert Windows, dass einem die Rechte zum stellen der Uhr fehlen, auch wenn man nur sehen will, wann der Dritte des vorigen Monats war.  
Aktivieren Sie diese Option, bekommen Mitglieder der Gruppe SuRunners das Privileg **"SeSystemtimePrivilege"** und dürfen ab der nächsten Anmeldung die Systemzeit verändern.
- **"Gestatte 'SuRunners' 'Energieoptionen' zu ändern und Energieschemas zu wechseln"**  
Seit ich SuRunner bin, darf ich auf meinem Notebook nicht mehr per Linksklick auf das Akku-Symbol in der Taskleiste einstellen, ob ich Energie oder Zeit sparen möchte. Das liegt daran, dass eingeschränkte Benutzer keinen Schreibzugriff auf die Energie-Einstellungen in der Registry (HKLM\Software\Microsoft\Windows\CurrentVersion\Controls Folder\PowerCfg) haben.  
Aktivieren Sie diese Option, wird den Berechtigungen für den Registry-Zweig Vollzugriff für die SuRunners gesetzt. Wenn Sie die Option deaktivieren, werden die SuRunners wieder aus den Registry-Berechtigungen entfernt.
- **"Windows Updatebenachrichtigungen für alle Benutzer (sofern automatische Updates aktiv sind)."**  
Eingeschränkte Benutzer werden standardmäßig nicht über Updates informiert. In Windows XP Professional kann man das mit dem Gruppenrichtlinien-Editor ändern. In Windows XP Home geht das mit Windows-Mitteln nicht zu ändern.  
Aktivieren Sie diese Option um die gewohnten Balloon-Tips und Schild-Symbole des Windows Update Clients in der Taskleiste zu sehen.
- **"Keinen automatischen Neustart nach der Installation von Windows Updates durchführen"**  
Sind automatische Updates aktiviert und ein eingeschränkter Benutzer angemeldet, werden Updates installiert und der PC dann neu gestartet. Ob ein nicht gespeichertes Dokument offen ist, oder nicht. Auch das kann man nicht mit Bordmitteln von Windows XP Home verändern.  
Aktivieren Sie diese Option, können Sie wählen, ob Sie *nach einem Update jetzt* oder *später* den PC neu starten wollen.
- **"Administratoren' statt 'Ersteller' als Standard-Besitzer für von Administratoren erstellte Objekte."**  
Standardmäßig ist der Ersteller eines Objektes, z.B. einer Datei, eines Ordners oder eines Registry Schlüssels, dann auch dessen Besitzer. Besitzer von Objekten dürfen sich darauf Vollzugriff verschaffen. Wenn zum Beispiel ein mit SuRun gestarteter, als Administrator laufender Prozess, einen Registry Schlüssel unter HKEY\_LOCAL\_MACHINE anlegt, kann der eingeschränkte Benutzer, der SuRun benutzt hat, diesen Registry Schlüssel jederzeit manipulieren, indem er sich mit

Vollzugriff in die Zugriffskontrollliste des Registry Schlüssels einträgt und dann damit macht, was er will. Das Gleiche geht mit Dateien.

Ist diese Option aktiviert, sind Objekte, die ein Administrator erstellt im Besitz der Gruppe "Administratoren" und **nicht** im Besitz des Benutzers. Das verhindert, dass diese Objekte später von dem selben aber dann eingeschränkten Benutzer manipuliert werden können.

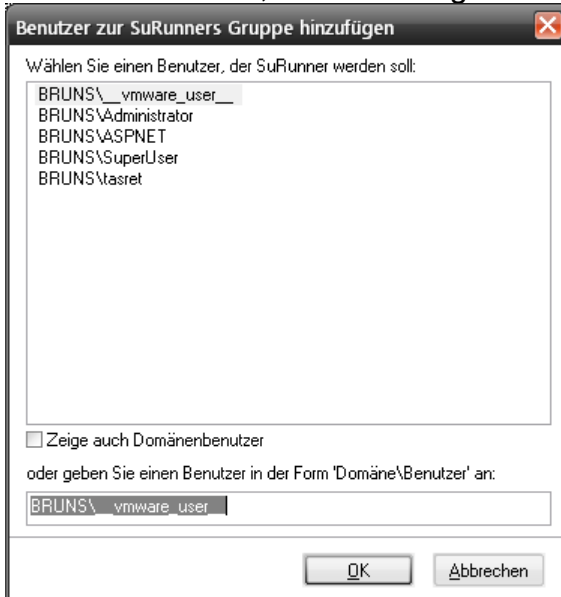
**HINWEIS: Diese Option sollte unbedingt aktiviert sein!**

## SuRun Einstellungen „SuRunners-Gruppe“



- **SuRunner <Name>, Hinzu, Löschen**

In der Liste stehen alle Mitglieder der lokalen Benutzergruppe „SuRunners“. Die Optionen des ausgewählten Benutzers werden auf dieser Seite dargestellt. Wählen Sie Hinzu, erscheint folgender Dialog:



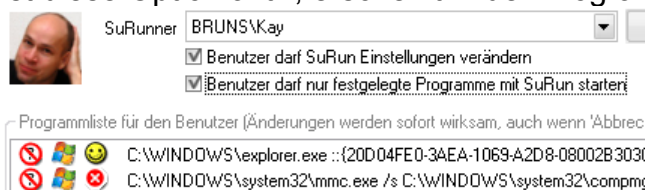
Hier können Sie einen Benutzer, der nicht Mitglied der lokalen Benutzergruppe „SuRunners“ ist, in die Gemeinde der SuRunners aufnehmen. Administratoren werden dabei automatisch zu normalen Benutzern degradiert. Mit „Löschen“ können Sie einen SuRunner aus der Gemeinde verbannen. Wenn Sie das tun wird SuRun fragen, ob der verbannte zum Administrator gemacht werden soll.

- **"Benutzer darf SuRun Einstellungen verändern"**

Entfernt man den Haken, kann der gewählte Benutzer zukünftig die SuRun Einstellungen weder sehen noch ändern.

- **"Benutzer darf nur festgelegte Programme mit SuRun starten"**


Ist diese Option aktiv, erscheint in der Programmliste für den Benutzer eine Spalte:






Klickt man auf die Spalte, wird das Kreuz zum Smiley und umgekehrt. Ein Smiley bedeutet, dass der beschränkte SuRunner das Programm administrativ starten darf. Bei Programmen, die nicht in der Liste stehen oder keinen Smiley haben, verweigert SuRun den administrativen Start für diesen Benutzer.

- **„Benutzerstatus in Taskleiste anzeigen“**

SuRun kann im Infobereich der Taskleiste ein Symbol einblenden, das anzeigt, welche Rechte das aktive Fenster hat. Fünf verschiedene Symbole werden dargestellt:

-  Aktives Fenster hat Standard-Rechte, Explorer auch
-  Aktives Programm wurde von SuRun mit gehobenen Rechten gestartet

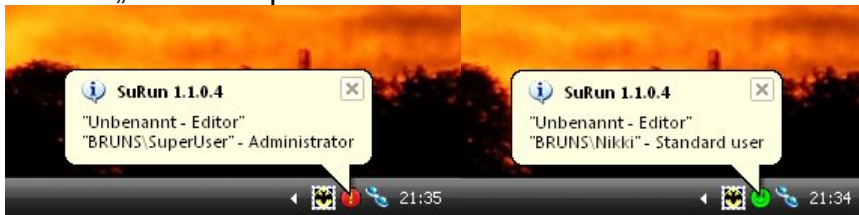


-  Kein aktives Fenster
-  Explorer läuft als Administrator, das aktive Fenster auch
-  Aktives Fenster läuft als Administrator, Explorer nicht

Mit dieser Option kann man für jeden SuRunner getrennt festlegen, ob er das Symbol sehen soll (Haken gesetzt), ob er es nicht sehen soll (Haken gelöscht) oder ob für ihn die Standard-Einstellungen für das Symbol auf der Seite „**Erweitert**“ der SuRun Einstellungen gelten (Haken „Intermediate“).

- **„Benutzerstatus Info als 'Balloon-Tips“**

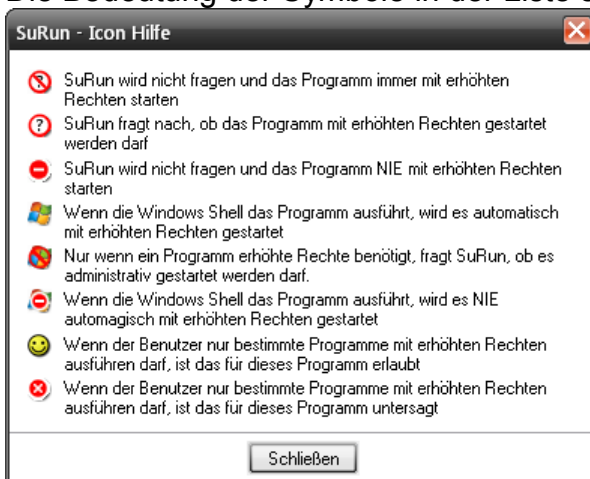
Hat das aktive Fenster einen anderen Benutzer als den angemeldeten, kann SuRun das als „Balloon-Tip“ in der Taskleiste darstellen:



- **Programmliste für den Benutzer, Hinzu, Bearbeiten, Löschen, Hilfe**

In dieser Liste stehen alle Programme, die SuRun besonders behandelt.

Die Bedeutung der Symbole in der Liste sieht man, wenn man „Hilfe“ drückt:



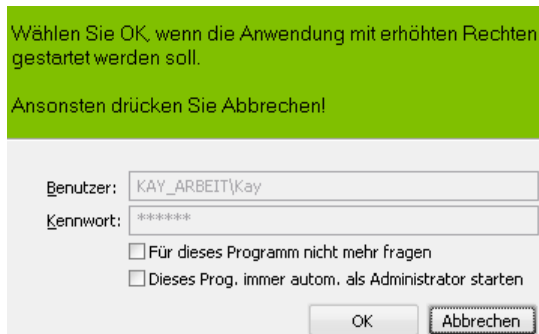
Die Symbole für den automatischen Start sind nur aktiv, wenn SuRun **"Versuche bestimmte Programme AUTOMAGISCH mit gehobenen Rechten zu starten"** auf der Seite „**Erweitert**“ der SuRun Einstellungen aktiviert ist.

Das Smiley- bzw. Kreuzsymbol sieht man nur, wenn der gewählte Benutzer ein eingeschränkter SuRunner ist.

Die Bedeutung der Knöpfe ist selbsterklärend.

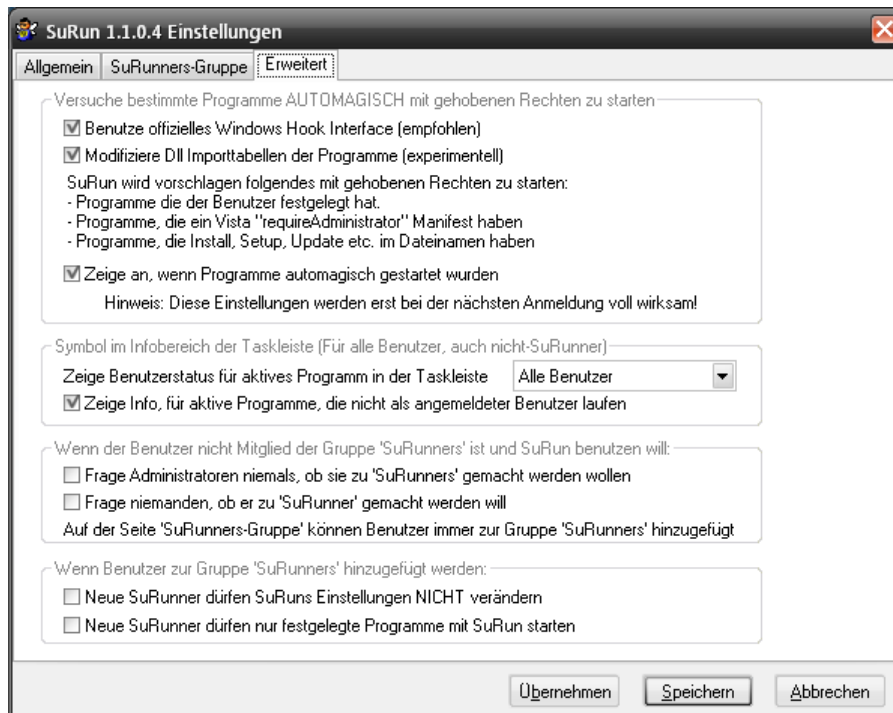
Alle Programme dieser Liste müssen exakt mit allen Parametern eingegeben werden! Leerzeichen im Befehl bzw. Parametern müssen in Anführungszeichen eingeschlossen werden.

Die Programmliste füllt sich selbständig, wenn Sie in SuRuns Bestätigungsdialog:



"Für dieses Programm nicht mehr fragen" oder "Dieses Prog. immer autom. als Administrator starten" aktiviert haben.

### SuRun Einstellungen, „Erweitert“



- **Versuche bestimmte Programme AUTOMAGISCH mit gehobenen Rechten zu starten**

SuRun kann versuchen, das Ausführen von Programmen abzufangen. Wenn ein Programm mit administrativen Rechten ausgeführt werden muss, schlägt SuRun vor, dieses Programm gleich mit erhöhten Rechten zu starten.

So kann man auch ohne Eingabe einer „SuRun <Programm>“ Befehlszeile und ohne „Starte als Administrator“, Programme automatisch administrativ ausführen lassen.

*Unter Windows kann man Programme auf verschiedene Weise in den Speicher Laden und ausführen.*

*Eine Methode ist z.B. die Funktion "CreateProcess", die hat aber für viele den Nachteil, dass man damit wirklich nur EXE-Dateien ausführen kann.*

*Eine zweite Funktion ist "ShellExecute(Ex)".*

*Damit kann man Dateien und Verknüpfungen "ausführen", Drucken und vieles mehr.*

So z.B. startet Explorer -die Windows Shell- bei mir, wenn ich auf ein JPG-File Doppelklicke mit *ShellExecute(Ex)* IrfanView.

Weil das so schön geht, benutzen fast alle Programme ShellExecute, wenn sie etwas ausführen müssen.

In Windows 2000/2003/XP/Vista kann man sich in diese Funktion einklinken.

Das macht man mittels eines COM-Interfaces Namens "*IShellExecuteHook*".

Wenn Sie **"Benutze offizielles Windows Hook Interface"** aktiviert haben, implementiert SuRun dieses Interface und bekommt so mit, wenn ein Programm „*ShellExecute(Ex)*“ aufruft.

Das hat aber auch Nachteile.

Wenn ein Programm nicht „*ShellExecute(Ex)*“, sondern *CreateProcess* benutzt, bekommt SuRun das nicht mit und kann das Programm nicht starten. Falls ein anderes Programm vor SuRun in der Liste der „*IShellExecuteHook*“-Programme aufgerufen wird, bekommt SuRun das auch nicht mit.

Der Explorer von Windows Vista führt z.B. fast nichts per „*ShellExecute(Ex)*“ aus. Deshalb wird ein aktives **"Benutze offizielles Windows Hook Interface"** in Vista nicht sehr Erfolgreich sein.

Die zweite, am häufigsten benutzte Windows Funktion um ein Programm zu starten ist „*CreateProcess*“. Selbst „*ShellExecute(Ex)*“ benutzt meistens „*CreateProcess*“, um ein Programm zu starten.

Dumm nur, dass es keine offizielle Möglichkeit gibt, sich in „*CreateProcess*“ einzuhängen.

Wenn die Option **"Modifiziere Dll Importtabellen der Programme"** aktiviert ist, benutzt SuRun eine nicht offizielle, aber gebräuchliche Methode, um unter anderen „*Createprocess*“ abzufangen.

*Innerhalb eines Windows Prozesses werden Aufrufe von Funktionen, die in DLLs implementiert sind (Importe) über Tabellen gehandhabt. Die jeweilige DLL wird in den Speicher des Prozesses geladen. Dann werden die Tabellen mit den Importierten Funktionen des Moduls auf die geladene DLL "verbogen" und alles läuft prima. Es gibt also Tabellen mit den Adressen importierter DLL Funktionen, kurz Import Address Tabellen oder IAT.*

Wenn man die IAT aller geladenen Module so modifiziert, dass anstatt „*CreateProcess*“ eine eigene Funktion aufgerufen wird, kann man so kontrollieren, was wie gestartet wird.






Aber auch das hat Nachteile! Da IAT-Hooking nicht offiziell unterstützt ist, kann es sein, das das irgendwann nicht mehr funktioniert. Bisher geht es allerdings prima, selbst in Windows Vista und Vista x64.

Der zweite Nachteil: Wenn z.B. ein Systemsteuerungs-Modul (wie *ncpa.cpl*) gestartet werden soll, wird zwar der „*IShellExecuteHook*“ aber nicht „*CreateProcess*“ aufgerufen, denn Explorer handhabt das selbst.

Es sollten also beide Optionen aktiviert werden, damit möglichst kein administrativ zu startender Prozess von SuRun verpasst wird.

- **„Benutzerstatus in Taskleiste anzeigen“**

SuRun kann im Infobereich der Taskleiste ein Symbol einblenden, dass anzeigt, welche Rechte das aktive Fenster hat. Fünf verschiedene Symbole werden dargestellt:

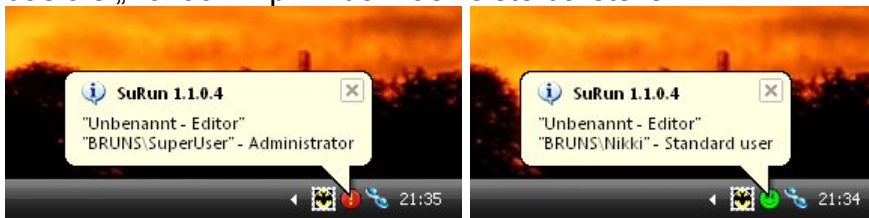
- : Aktives Fenster hat Standard-Rechte, Explorer auch
- : Aktives Programm wurde von SuRun mit gehobenen Rechten gestartet
- : Kein aktives Fenster
- : Explorer läuft als Administrator, das aktive Fenster auch
- : Aktives Fenster läuft als Administrator, Explorer nicht

Mit dieser Option kann man festlegen, welchen Benutzern des PC das Symbol gezeigt werden soll („Administratoren“, „allen Benutzern“, „Niemanden“). Standardmäßig ist das Symbol abgeschaltet.

Für Mitglieder der SuRunners-Gruppe kann diese Option auf der Seite **„SuRunners-Gruppe“** der SuRun-Einstellungen überschrieben werden.

- **„Benutzerstatus Info als 'Balloon-Tips'“**

Hat das aktive Fenster einen anderen Benutzer als den angemeldeten, kann SuRun das als „Balloon-Tip“ in der Taskleiste darstellen:



- **"Frage Administratoren niemals, ob sie zu 'SuRunners' gemacht werden wollen"**

Falls Sie SuRun als Administrator benutzen aber kein Mitglied der lokalen Benutzergruppe „SuRunners“ sind, wird SuRun das Programm einfach starten und nicht versuchen Sie in die „SuRunners“ Gemeinde aufzunehmen.

Da Sie bereits Administrator sind, ist es kein Risiko, das Programm zu starten. So kann man z.B. SuRun-Verknüpfungen für alle Benutzer des PC anlegen und wird als Administrator nicht genervt.

- **"Frage niemanden, ob er zu 'SuRunner' gemacht werden will"**

Falls Sie SuRun benutzen aber kein Mitglied der lokalen Benutzergruppe „SuRunners“ sind, wird SuRun einen Fehler zurückgeben und nicht versuchen Sie in die „SuRunners“ Gemeinde aufzunehmen.

- **"Neue SuRunner dürfen SuRuns Einstellungen NICHT verändern"**

Der Haken in "Benutzer darf SuRun Einstellungen verändern" auf der Seite „SuRunners-Gruppe“ der SuRun Einstellungen wird standardmäßig nicht gesetzt.

- **"Neue SuRunner dürfen nur festgelegte Programme mit SuRun starten"**

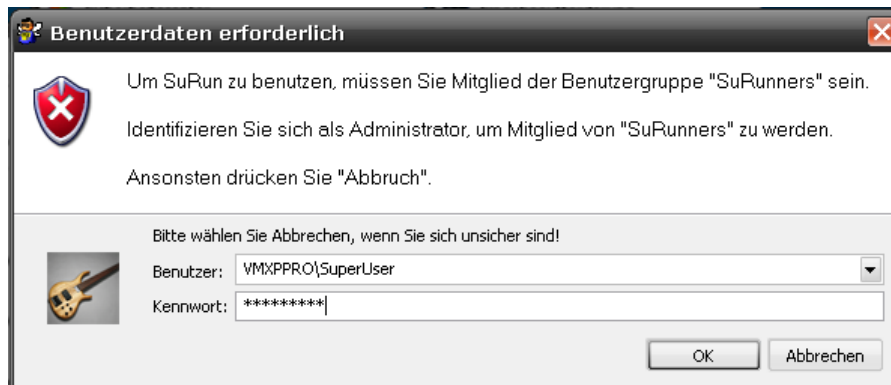
Der Haken in "Benutzer darf nur festgelegte Programme mit SuRun starten" auf der Seite „SuRunners-Gruppe“ der SuRun Einstellungen wird standardmäßig gesetzt.

## Betrieb

### „SuRunner“ werden

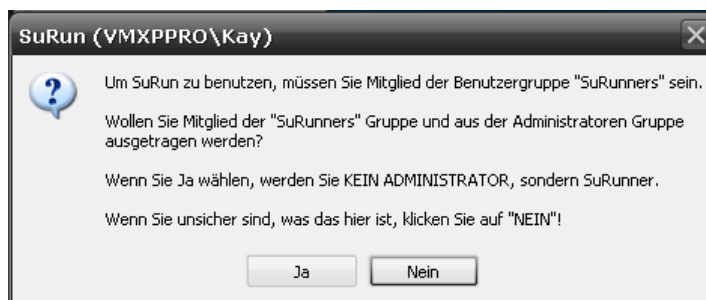
Sind Sie kein Mitglied, der Benutzergruppe **“SuRunners”** und versuchen ein Programm als Administrator zu starten oder die „SuRun Einstellungen“ aufzurufen, bietet Ihnen SuRun an, beizutreten.

Sind sie kein Administrator müssen Sie durch Eingabe des Passwortes eines Administrators als berechtigt ausweisen, damit SuRun Sie in die **“SuRunners”** aufnimmt.



(Das Passwort wird in einer gesicherten Umgebung abgefragt und kann nach meiner Kenntnis nicht erhascht werden.)

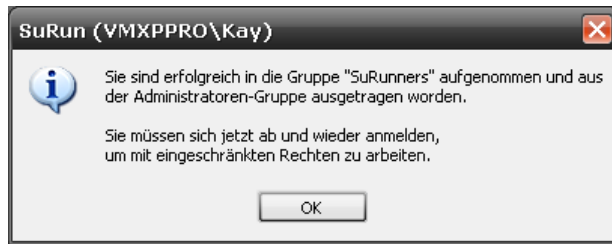
Sind Sie ein Administrator, wird SuRun Sie bei der ersten Benutzung fragen, ob Sie Mitglied der Benutzergruppe **“SuRunners”** und Ex-Mitglied der **“Administratoren”** werden wollen.



Sie müssen sich danach von Windows ab- und wieder anmelden.

(Ist in den SuRun Einstellungen **“Frage niemanden, ob er zu 'SuRunner' gemacht werden will”** bzw. **“Frage Administratoren niemals, ob sie zu 'SuRunners' gemacht werden wollen”** aktiviert, wird SuRun Sie natürlich nicht nerven und Sie „dürfen“ sich selbst in die SuRunners Gruppe ein- und aus der Administratoren-Gruppe austragen.)

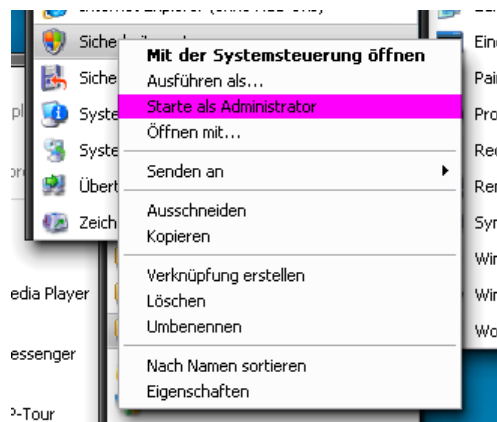




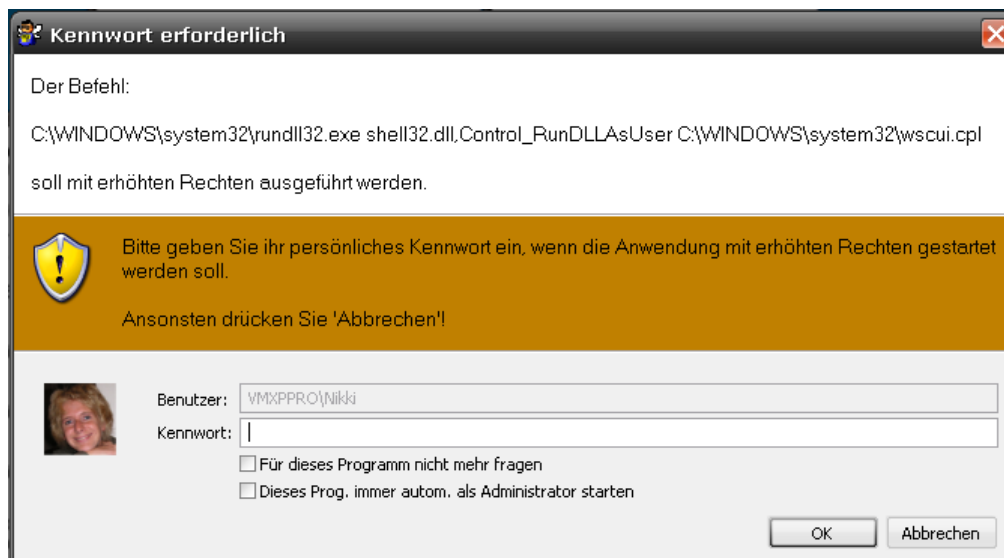
Jetzt sind Sie SuRunner und dürfen komfortabel eingeschränkt arbeiten.

### **Starte als Administrator**

Wenn Sie ein Programm mit erhöhten Rechten starten müssen. Klicken Sie mit der Rechten Maustaste darauf und wählen Sie „*Starte als Administrator*“ im Kontextmenü.



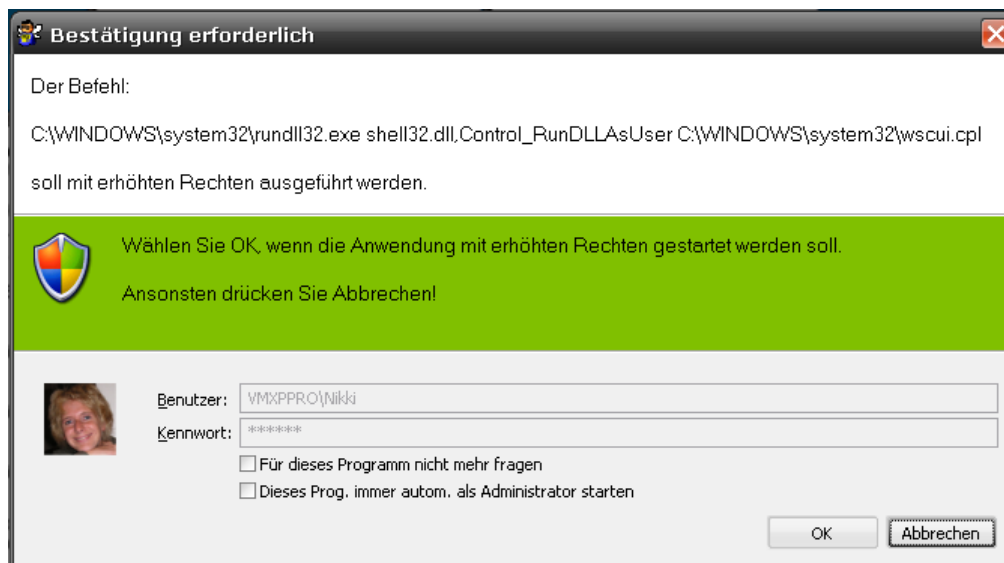
SuRun benötigt (normalerweise) einmalig das persönliche Passwort des angemeldeten Benutzers.



Das ist notwendig, weil SuRun der Benutzer erneut am System anmelden muss, während er in der Administratoren-Gruppe ist.

Das Passwort wird leicht verschlüsselt und in einem gesicherten Zweig in der Registry des Systems gespeichert.

Danach fragt SuRun nur noch nach Bestätigung:



## Automagie und Fragefreiheit

Aktivieren Sie das Kästchen **„Für dieses Programm nicht mehr fragen“**, so wird SuRun für dieses Programm bei allen folgenden Aufrufen mit SuRun automatisch die von Ihnen gewählte „Antwort geben“.

Im obigen Beispiel würde SuRun nicht mehr fragen, ob das Sicherheitscenter mit erhöhten Rechten gestartet werden darf. Klicken Sie „OK“, wird der es ohne Nachfragen gestartet. Klicken Sie „Abbrechen“, wird SuRun das Sicherheitscenter auch in Zukunft automatisch nicht starten.

Diese Option ist sinnvoll, um z.B. Windows-Autostart Programme zu starten, die administrative Rechte benötigen.

Es ist auch möglich, das SuRun fälschlicher Weise ein Programm administrativ starten will. Ein Fiktives Programm „PlinseTupper.exe“ z.B. beinhaltet „setUp“. Deshalb wird SuRun fragen, ob das Programm als Administrator gestartet werden soll. Aktivieren Sie das Kästchen **„Für dieses Programm nicht mehr fragen“** und drücken Sie „Abbrechen“, um die Nerverei zu beenden.

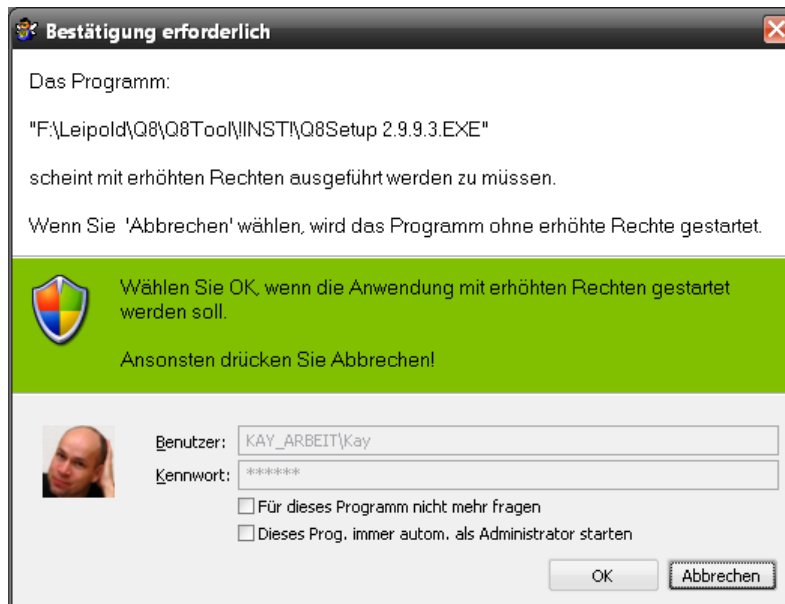
Ist **„Dieses Prog. immer autom. als Administrator starten“** aktiv, wird SuRun versuchen dieses Programm auch ohne **„Starte als Administrator“** immer mit erhöhten Rechten zu starten.

Scheint ein Programm gehobene Rechte zu benötigen, wird SuRun fragen, ob es damit gestartet werden soll. Dass ein Programm gehobene Rechte braucht, erkennt SuRun so:

- Das Programm steht als **„immer mit gehobenen Rechten starten“** in der Programmliste des Benutzers
- Das Programm hat als Endung exe, cmd, lnk, com, pif, bat und der Dateiname enthält eine der Zeichenfolgen „install“, „setup“ oder „update“
- Das Programm hat eine Manifest Ressource oder eine externe Manifest Datei die `<*trustInfo>-> <*security>-> <*requestedPrivileges>-> <*requestedExecutionLevel`

level="requireAdministrator"> enthält

Soll ein Programm ausgeführt werden und eine der Bedingungen ist erfüllt, wird SuRun folgendes fragen:

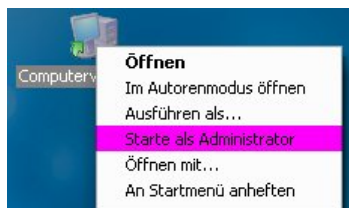


Wie SuRun versucht, den Start eines Programms in Windows abzufangen um es selbst eventuell automagisch mit gehobenen Rechten zu starten, steht [hier](#).

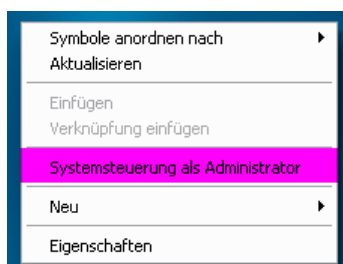
## Das Kontext-Menü der Windows Shell

Zum erleichterten Ausführen von Programmen integriert sich SuRun in das Kontextmenü des Windows Explorers.

Es fügt dem Kontextmenü von Dateien mit der Endung bat, cmd, cpl, exe, lnk und msi einen **“Starte als Administrator”** Befehl hinzu.



Dem Kontextmenü für den Desktop-Hintergrund fügt SuRun (wie auch [SuDown](#)) einen **“Systemsteuerung als Administrator”** Befehl hinzu.

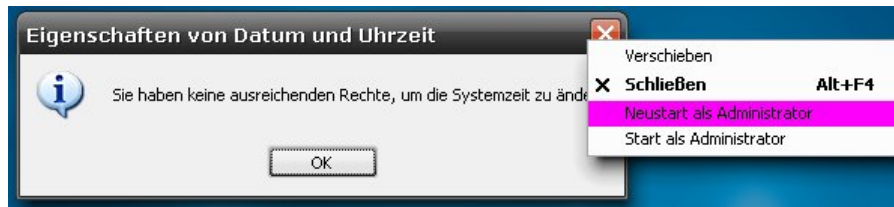




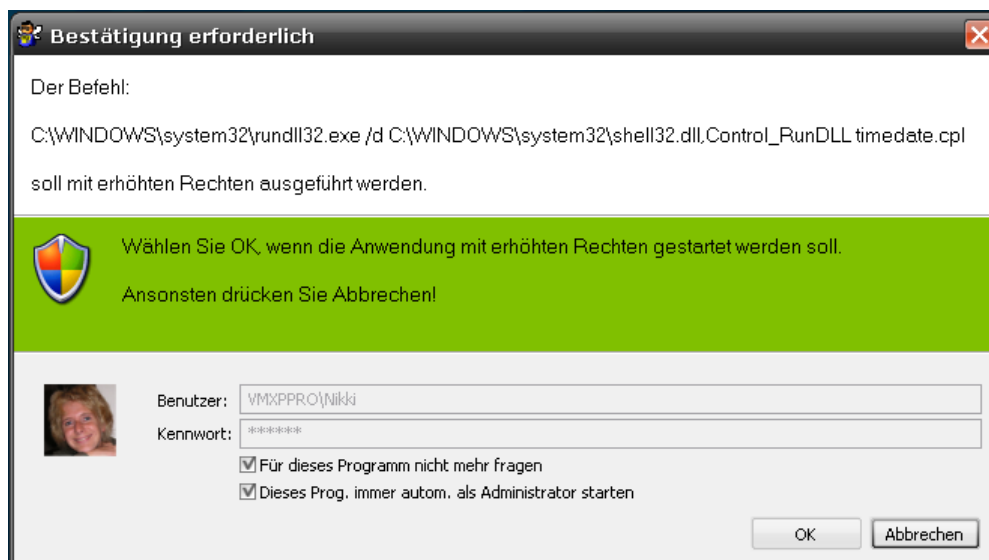
## Integration in das System-Menü

Manche Programme erfordern administrative Rechte, z.B. um installiert zu werden, erzählen davon aber erst, wenn sie sich beenden. Wie genau die Befehlszeile für solch ein Programm aussieht, ist nur schwer zu erraten.

Um diese Programme komfortabel nutzen zu können, integriert sich SuRun in das Windows-Systemmenü:

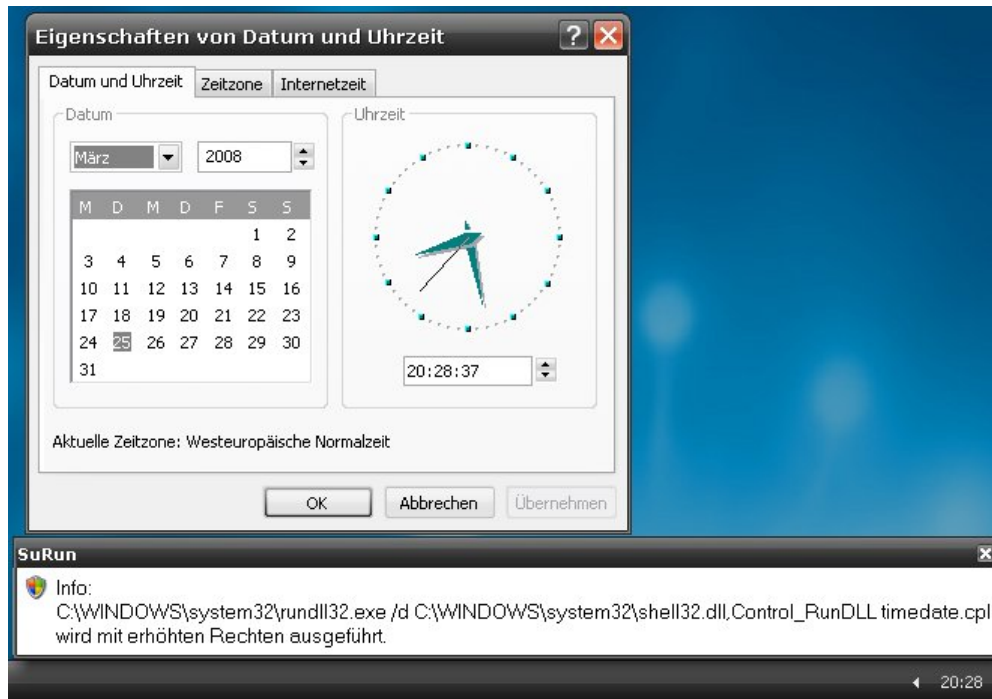


Mit einem Klick mit der rechten Maustaste auf die Titelleiste eines Fensters und den Befehlen **„Neustart als Administrator“** oder **„Start als Administrator“** kann man so des Problemchens Herr werden.



Falls Sie in obigem Beispiel (Doppelklick auf die Uhrzeit im „Tray“) beide Optionen aktivieren und „OK“ drücken, werden beim nächsten Doppelklick darauf die **„Eigenschaften von Datum und Uhrzeit“** als Administrator gestartet.

## Hinweisfenster für automatische Starts



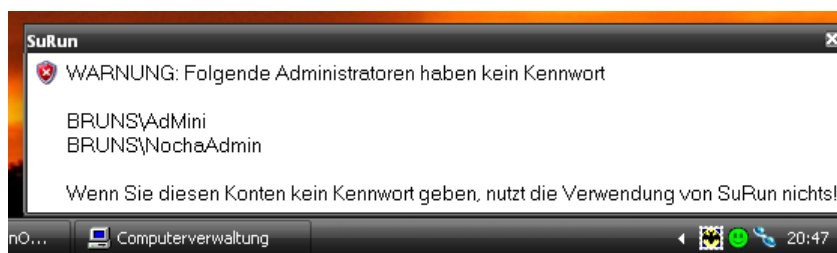
Bei solchen automatischen administrativen Starts zeigt SuRun das optional in einem kleinen Fenster 20 Sekunden lang an.

## Hinweisfenster für Administrator-Konten ohne Kennwort

Standardmäßig legt Microsoft bei der Installation genau so ein Konto, den vordefinierten „Administrator“ ohne Kennwort an.

Das ist ein erhebliches Sicherheitsrisiko!

SuRun kann beim Anmelden eines Benutzers prüfen, ob im System lokale Administratoren existieren, die kein Kennwort haben und dann folgendes zeigen:








Das Hinweisfenster verschwindet nicht von selbst und muss manuell geschlossen werden. Als Standard werden Administratoren und nicht eingeschränkte Mitglieder der Gruppe SuRunners gewarnt, es gibt jedoch fünf Optionen, welche Benutzer gewarnt werden: „Alle Benutzer“, „SuRunner und Administratoren“, „unbeschränkte SuRunner und Administratoren“, „Administratoren“ und „Niemanden“.

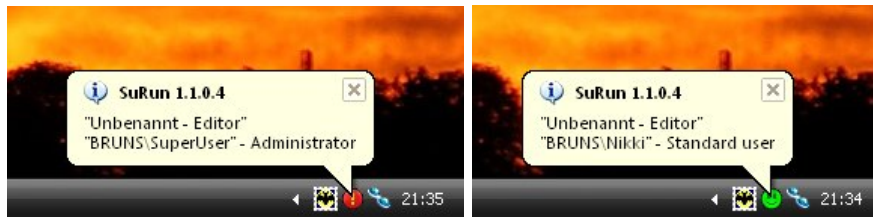
## Taskleistensymbol

SuRun kann im Infobereich der Taskleiste ein Symbol einblenden, dass anzeigt, welche

Rechte das aktive Fenster hat. Fünf verschiedene Symbole werden dargestellt:

-  Aktives Fenster hat Standard-Rechte, Explorer auch
-  Aktives Programm wurde von SuRun mit gehobenen Rechten gestartet
-  Kein aktives Fenster
-  Explorer läuft als Administrator, das aktive Fenster auch
-  Aktives Fenster läuft als Administrator, Explorer nicht

Hat das aktive Fenster einen anderen Benutzer als den angemeldeten, kann SuRun das optional als „Balloon-Tip“ in der Taskleiste darstellen:



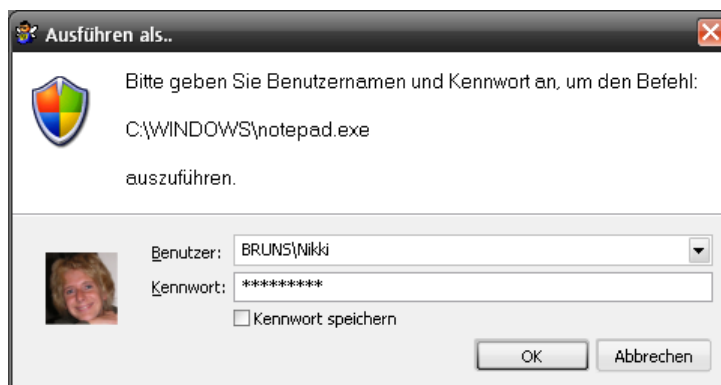
Die Darstellung des Symbols kann für alle Benutzer des Systems festgelegt und für jeden SuRunner einzeln überschrieben werden.

### „Ausführen als...“ durch SuRun ersetzen

Das Benutzen des eingebauten „Ausführen als...“ von Windows ist sehr gefährlich!

Selbst Programme mit Gast-Rechten können die eingegebenen Daten abfangen und das System übernehmen.

SuRun kann den „Ausführen als...“-Eintrag des Shell Kontext-Menüs ersetzen:



Das hat den großen Vorteil, dass das Benutzerkennwort auf einem abgesicherten Desktop abgefragt wird und nicht ausgespäht werden kann.

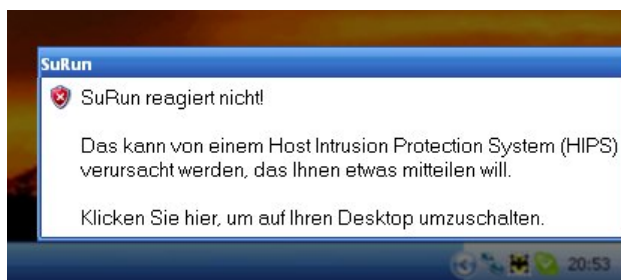
Für jeden Benutzer von „Ausführen als...“ können die eingegebenen Kennworte gespeichert werden. Sie werden leicht verschlüsselt in der Registry unter „HKEY\_LOCAL\_MACHINE\SECURITY\SuRun\RunAs<username>\Cache“ gespeichert. Auf diesen Registry-Zweig haben normalerweise nur Dienste Zugriff. Die Speicherung erfolgt **getrennt** für jeden Benutzer der „Ausführen als...“ benutzt! Wenn also ein Benutzer Kennworte für „Ausführen als...“ speichert, kann kein anderer Benutzer (leicht) darauf zugreifen.

## ***Der WatchDog***

Falls auf dem System ein HIPS (Host Intrusion Protection System) installiert ist -Das ist Software die ungewöhnliches Verhalten von Programmen analysiert und den Benutzer warnt-, kann es sein, dass es Aktionen von SuRun als ungewöhnlich einstuft. Versucht das HIPS dann den Benutzer zu warnen, funktioniert das nicht, denn der sichere Desktop von SuRun ist aktiv. Das ergibt eine typische Patt-Situation:

- SuRun ist durch das HIPS Blockiert und kann keine Eingaben verarbeiten
- Das HIPS kann keine Eingaben empfangen, weil SuRuns Desktop aktiv ist

Mit SuRun 1.1.0.6 wurde deshalb ein „WatchDog“ eingeführt. Setzt SuRun für länger als zwei Sekunden ein Signal nicht, ist es scheinbar blockiert. Dann zeigt der WatchDog ein Fenster auf dem Benutzbildschirm an:



Klickt man auf das Fenster, wird auf den Benutzer-Desktop umgeschaltet. Hier kann man jetzt die Fragen des HIPS beantworten.

Auf dem Benutzer-Desktop wird vom WatchDog ein Fenster eingeblendet:



Klickt man darauf, kann man mit SuRun weiter arbeiten.

## Lizenz, Garantie und Haftung

...gibt es nicht! Dieses Kapitel hilft hoffentlich, mir ökonomisch orientierte Rechtsverdreher vom Hals zu halten. SuRun hat mit Geld nichts zu tun!

Ich habe SuRun in der verfügbaren Zeit so gut ich konnte programmiert. Ziel war ursprünglich, selbst nicht mehr als Administrator zu arbeiten ohne die üblichen Unannehmlichkeiten in Kauf nehmen oder das System unsicherer machen zu müssen.

Das ist mir meiner Meinung nach gelungen.

Ich setze SuRun selbst auf all meinen PC ohne Probleme ein.

Sollte SuRun jedoch für Schäden irgendwelcher Art verantwortlich gemacht werden, übernehme ich dafür keine Haftung.

Schauen Sie in die Quelltexte bevor Sie SuRun installieren.

Nutzt Ihnen das nichts, und Sie sind sich nicht sicher, ob SuRun Ihnen schadet, benutzen Sie es einfach nicht!

Die Quelltexte sind wie die Software frei verfügbar. Jeder darf damit machen, was er will. Baut jemand SuRun oder Teile davon in sein eigenes Produkt ein und verschweigt die Herkunft, so ist das gestattet, wenn auch nicht erwünscht.