ERNW
Enno Rey Netzwerke GmbH

ERNW Newsletter 4 / April 2004

Liebe Partner, liebe Kollegen,

willkommen zur vierten Ausgabe des ERNW-Newsletters, die unter dem Motto steht:

Arbeiten als „Non-Admin“ unter Windows

Das Problem
Das Arbeiten als Administrator bzw. mit einem Account mit Administrator-Rechten unter Windows hat sich in vielen Firmen-Umgebungen und im privaten Bereich weitestgehend eingebürgert.

Windows XP z.B. versieht den ersten Benutzer-Account mit administrativen Rechten und dies hat auch einen guten Grund: Einem normalen Benutzer ist es nicht gestattet Software oder Treiber zu installieren oder die IP Adresse zu ändern – nicht einmal das Ändern der System-Zeit ist zulässig.

Im User-Alltag werden diese Funktionen sehr selten benötigt – für den Office-Einsatz und das Surfen im Internet sind keineswegs Administrator-Rechte erforderlich.

Im Gegenteil – als Administrator zu arbeiten birgt sogar erhebliche Gefahren. Alle Programme, die Sie starten, arbeiten unter dem mächtigsten Benutzer-Account, den Ihr System zu bieten hat. Diesen Programmen ist es gestattet auf Ihrem System beliebige Dateien zu lesen, hinzuzufügen oder zu löschen. Dies schließt natürlich beliebige Registry-Schlüssel, Passwort-Dateien, System-Bibliotheken sowie Email und Internet Funktionalitäten mit ein.

Heutzutage kann man sich auf verschiedenste Art und Weise einen Virus oder Wurm „einfangen“ und es können sich erhebliche Softwarefehler (sog. Buffer Overflows“) in nahezu jeder Standard-Software (z.B. Outlook, Internet Explorer, Macromedia Flash Player, RealAudio Player usw.) einnisten.
All dies kann dazu führen, dass böswilliger Code auf Ihrem System zur Ausführung kommt und dieser Code wird mit den Rechten des aktuell angemeldeten Benutzers ausgeführt.

90% aller Viren wären kläglich gescheitert wenn sie nicht Rechte auf gewisse Systemdateien oder Registry Schlüssel gehabt hätten (z.B. um sich automatisch

startend beim Booten des Systems zu konfigurieren). Das Austauschen von System-Dateien ist ebenfalls nur als Administrator möglich.

Warum sich also dieser Gefahr aussetzen?

Windows bietet hervorragende Möglichkeiten temporär den Sicherheits-Kontext zu ändern, um Aufgaben durchzuführen, die nur Administratoren vorbehalten sind - nämlich die Konfiguration des Systems.

Nachfolgend wird beschrieben, wie man seine Alltags-Aufgaben unter einem geschützten Benutzer-Konto durchführen kann, aber trotzdem komfortabel in den administrativen Kontext wechseln kann.

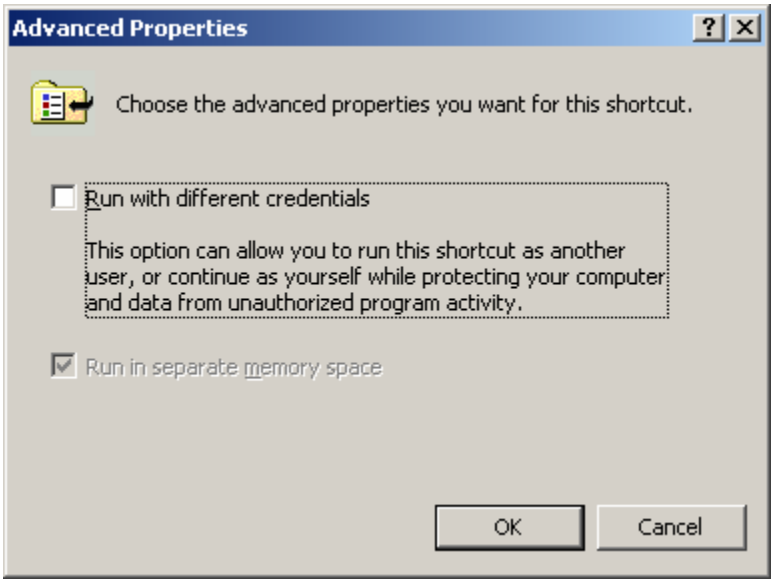
Prinzipiell wäre es schon damit getan, einfach einen neuen Benutzer anzulegen (wenn Sie im Moment den Account ‚Administrator' benutzen) bzw. Ihren Benutzer-Account lediglich der ‚Benutzer' Gruppe zuzuordnen.

Alle Programme, die den Windows Logo Guidelines entsprechen (z.B. Office), funktionieren sofort im Benutzer-Kontext.

Möchten Sie jedoch Programme starten, die administrative Rechte benötigen, gibt es mehrere Möglichkeiten.

Sie können jedes beliebige Programm mit der rechten Maustaste (Windows XP/2003) oder Shift-rechte Maustaste (Windows 2000) mit dem Menüpunkt ‚Ausführen Als' starten. Hier können Sie auswählen unter welchem Benutzer-Account das Programm gestartet werden soll.

Sie können auch direkt den Programmverweis konfigurieren, so dass der Passwort-Dialog immer erscheint (Eigenschaften –> Erweitert).



Die Lösung

Die o.g. Lösung ist ein einfacher und gangbarer Weg. Wenn Sie aber erweiterte Funktionalität benötigen, sollten Sie ein paar Modifikationen an Ihrer Arbeits-Umgebung durchführen.

1. Den gewünschten Benutzer-Account anlegen.
2. Eine Gruppe „Trusted Users“ anlegen.
3. Den Benutzer-Account dieser Gruppe hinzufügen
4. Erstellen Sie sich ein Verzeichnis für Ihre privaten Dateien (z.B. d:\etc). Erstellen sie dann unterhalb von etc ein Verzeichnis für Tools, z.B. d:\etc\Tools.
5. Fügen Sie das „Tools“-Verzeichnis Ihrem Pfad hinzu (Arbeitsplatz -> Rechte Maustaste -> Eigenschaften -> Erweitert -> Umgebungsvariablen)
6. Geben Sie der Gruppe ‚Trusted Users’ alle Rechte auf dieses Verzeichnis (und die Unterverzeichnisse) außer ‚Full Control’.
7. Erstellen Sie im „Tools“-Verzeichnis eine Batch-Datei mit Namen ‚su.cmd’ (Angelehnt an den Unix Befehl) mit folgendem Inhalt:

```
@runas /env /user:administrator "cmd.exe /k
d:\etc\tools\admin.bat"
```

8. Erstellen Sie weiterhin eine admin.bat:

```
@cls
@title ADMIN Command Prompt
@color c0
```

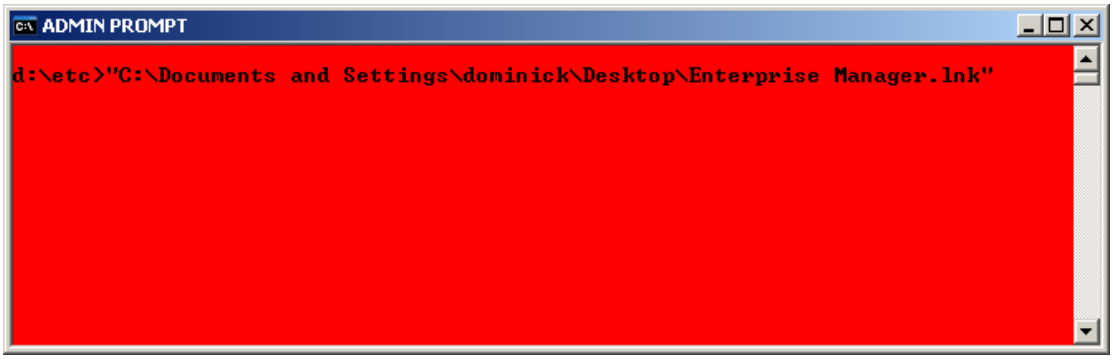
9. Dies bewirkt, dass sie einen Command-Prompt öffnen und Ihr Admin-Passwort eingeben müssen. Danach läuft dieses Eingabe-Fenster als Administrator und sie können in diesem Fenster alle administrativen Tätigkeiten durchführen. Um konstant daran erinnert zu werden mit welchen Rechten dieses Fenster läuft, ist es rot eingefärbt und der Fenster-Titel wurde Dementsprechend modifiziert.

10. Arbeiten Sie gleichzeitig auch in einer Domain-Umgebung, können Sie runas

so modifizieren, dass die Kommandozeile lokal als Administrator und in der Domäne als Benutzer gestartet wird. Modifizieren Sie dafür su.cmd folgendermaßen:

```
runas /u:administrator "runas /netonly /u:domain\user
\"admin.bat\""
```

In dieses neue Admin-Fenster können Sie nun einfach per Drag und Drop jedes beliebige Programm, das Admin-Rechte benötigt (z.B. SQL Server Enterprise Manager, User-Verwaltung etc.) ziehen und mit ‚Enter' starten. Das Programm wird nun mit den benötigten Rechten ausgeführt.
Dies gilt z.B. auch für Installations-Programme.



Nützliche Kommando-Zeilen Befehle die System-Steuerungs Applets direkt aufzurufen:

Administrative action	Control Panel applet
Accessibility Options	access.cpl
802.11 Monitor	apgui.cpl
Add/Remove Programs	appwiz.cpl
Console	console.cpl
Display	DESK.cpl
SCSI, PCMCIA, and Tape Devices	DEVAPPS.cpl
Add New Hardware Wizard	hdwwiz.cpl
Internet	inetcpl.cpl
Regional Settings	INTL.cpl
Game Controllers	joy.cpl
Mouse, Font, Keyboard, Printers	main.cpl
Multimedia and Sounds	MMSYS.cpl
Modems	MODEM.cpl
Network	ncpa.cpl
Logon Management for XP	nusrmgr.cpl (XP)
ODBC	odbccp32.cpl
Power Options	powercfg.cpl
Ports	PORTS.cpl
Devices, Services, Server	srvmgr.cpl
System	SYSDM.cpl
Telephony	telephon.cpl
Date/Time	TIMEDATE.cpl
UPS	ups.cpl

Und für MMC SnapIns:

Administrative action	Microsoft Management Console file
Current user certificates	certmgr.msc
Certificate authority	certsrv.msc
Certificate templates	certtmpl.msc
Indexing service	ciadv.msc
Computer management	compmgmt.msc
Group policy object editor	dcpol.msc
Device manager	devmgmt.msc
Disk defragmenter	dfrg.msc
Distributed file system	dfsgui.msc
Disk management	diskmgmt.msc
Active directory domains and trust	domain.msc
Default domain security settings	dompol.msc
Active directory users and computers	dsa.msc
Active directory sites and services	dssite.msc
Event viewer	eventvwr.msc
File server	filesvr.msc
Shared folders	fsmgmt.msc
Group policy object editor	gpedit.msc
Internet authentication service	ias.msc
Local users and groups	Lusrmgr.msc
Removable storage	ntmsmgr.msc
Removable storage operator requests	ntmsoprq.msc
Performance	perfmon.msc
Routing and remote access	rrasmgmt.msc
Resultant set of policy	rsop.msc
Local security settings	secpol.msc
Services	services.msc
Telephony	tapimgmt.msc
Terminal services configuration and connections	tscc.msc
Remote desktops	tsmmc.msc
Windows management infrastructure	wmimgmt.msc

Das Computer-Management kann somit folgendermaßen aufgerufen werden:

Wenn Sie ohne eine grafische Oberfläche nicht auskommen…
Es liegt nahe ‚explorer.exe' aus dem Admin Prompt zu starten. Dies funktioniert aber leider nicht. Der Windows Explorer überprüft nämlich ob bereits eine Kopie von sich selbst auf dem System läuft und gibt ein Signal zum öffnen eines neuen Fensters. Mit anderen Worten – Explorer kontaktiert Ihren Desktop (der ja zum Glück als Benutzer läuft), und dieser öffnet ein neues Fenster. Wir haben also nichts gewonnen.

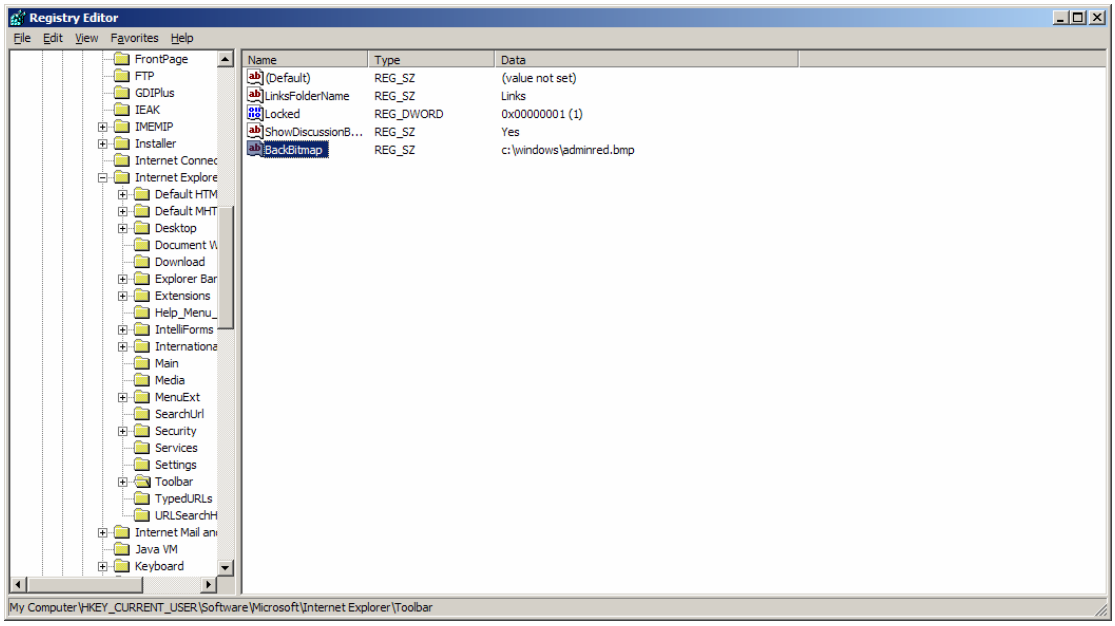
Anders verhält sich der Internet Explorer. Dieser startet einen neuen Prozess mit den aktuellen Rechten, nämlich Admin.
Leider ist der IE nicht im aktuellen Suchpfad. Aus diesem Grund erstellen wir einfach eine IE.cmd in unserem Tools-Verzeichnis, die den IE startet, z.B.

```
@start c:\program" files\internet explorer\iexplore.exe"
```

Sie haben nun einen Internet Explorer mit vollen administrativen Rechten. Natürlich können Sie diesen IE auch nutzen um lokale Verzeichnisse oder die System-Steuerung aufzurufen.
Ähnlich wie bei der Admin Kommandozeile ist es sinnvoll diesem IE-Fenster ein Erkennungsmerkmal zu geben, damit man immer weiß mit welchen Rechten man gerade Programme ausführt.

Um dies zu erreichen, kann man den IE „skinnen“, ihm also ein anderes Erscheinungsbild geben:

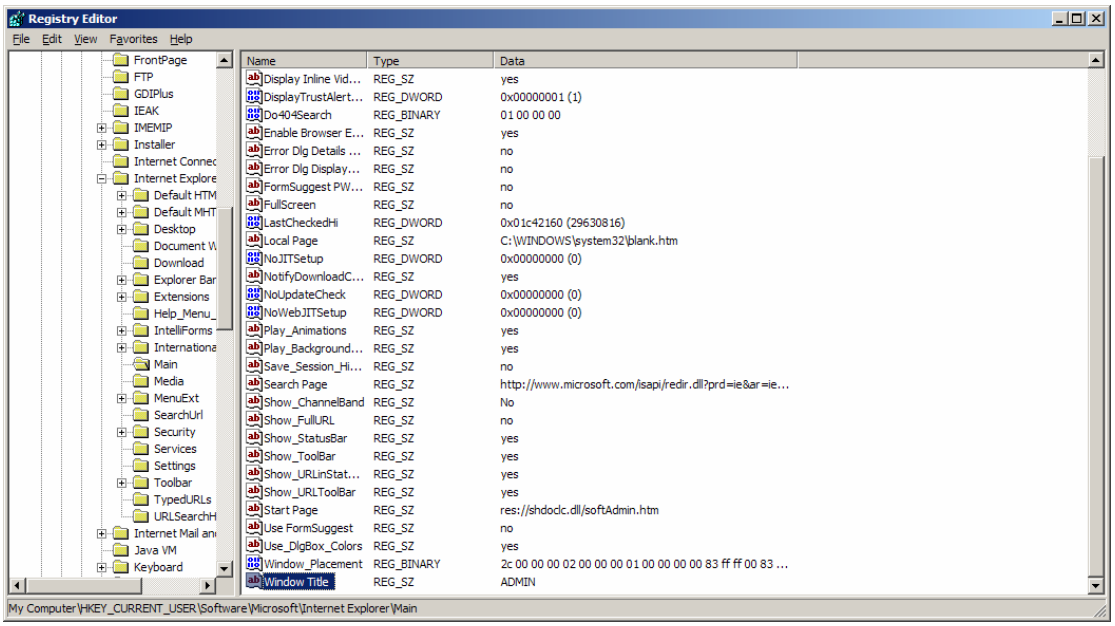
1. Rufen Sie ‚regedit.exe’ aus dem Admin-Prompt auf.
2. Fügen Sie unter HKEY_CURRENT_USER\Software\Microsoft\ Internet Explorer\Toolbar einen neuen String Schlüssel mit dem Namen „BackBitmap“ hinzu. Dieser Schlüssel bestimmt den Hintergrund des Toolbar. Man kann hier einfach den Pfad zu einem 32x32 Bitmap in Rot hinterlegen. Von nun an ist die Hintergrund-Farbe des Toolbar Rot.



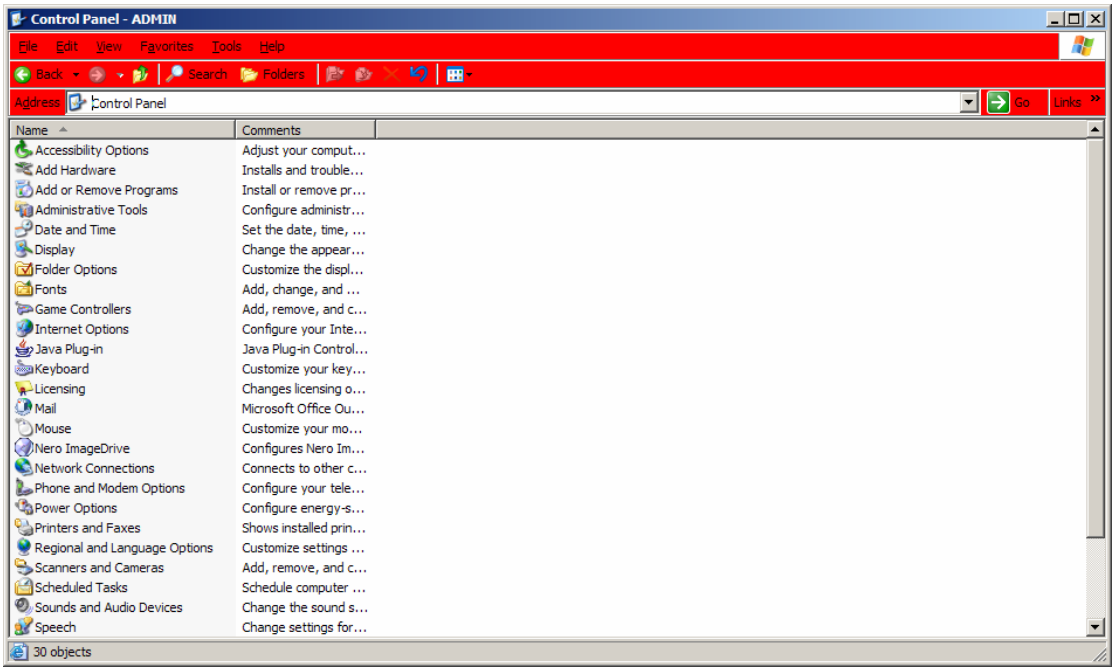
3. Fügen Sie unter

   HKEY_CURRENT_USER\Software\Microsoft\InternetExplorer\Main

   einen neuen String-Schlüssel mit dem Namen „Window Title“ hinzu. Diese Zeichenkette modifiziert die Titel-Leiste des IE Fensters. Benutzen Sie z.B. den Wert „IE ADMIN“.



4. Sie verfügen nun über einen Internet Explorer mit Admin-Rechten, der Ihnen auch ganz deutlich zeigt, dass er als Admin gestartet wurde.



Wo stehen wir?
Wir haben nun ein System, das zu 90% als Benutzer bedient wird. Die alltäglichen Aufgaben wie Surfen, Emails schreiben oder Office-Programme werden im geschützten Benutzer-Kontext aufgerufen.
Wenn Sie Programme, die Admin-Rechte benötigen, aufrufen müssen, können Sie dies über einen der beschriebenen Wege bewerkstelligen.
Der einfachste Weg ist, den Admin-Prompt zu starten und diese Programme von diesem Prompt aus zu öffnen.

Das farbliche Markieren hat den Vorteil, das man immer sofort sieht mit welchen Rechten ein Programm gestartet wird. Das Überschreiten der Benutzer/Admin-Linie geschieht bewusster.

Falls Sie Fragen, Anregungen oder Tips haben zögern Sie bitte nicht mich zu kontaktieren.

Dominick Baier (dbaier@ernw.de)

Es grüssen Sie herzlich

Enno Rey & das Team von ERNW

ERNW Enno Rey Netzwerke GmbH - Zaehringerstr. 46 - 69115 Heidelberg Tel. +49 6221 480390 - Fax 6221 419008 - Mobil +49 173 6745902 www.ernw.de