Inhaltsverzeichnis

Tipp 1.12: Benutzerinformationen auf dem Desktop anzeigen

»Auf meinem Rechner bzw. in unserem Netzwerk gibt es mehrere Benutzer. Oft ist nicht ohne weiteres zu erkennen, wer an einer Maschine angemeldet ist und wie diese Maschine überhaupt heißt. Was kann ich da machen?«

Es gibt eine recht einfache Möglichkeit, auf dem Desktop Informationen über den gerade angemeldeten Benutzer anzuzeigen. Hierfür kann man das Symbol *Arbeitsplatz* dynamisch umbenennen. Voraussetzung dafür ist, dass das Symbol auch angezeigt wird.

Möglich wird dies durch eine Manipulation der Registrierung. Natürlich gelten hierfür alle Warnungen, die immer beim Bearbeiten der Registrierung zutreffen!

Da der Registrierungs-Editor von Windows XP die nötige Änderung nicht ohne weiteres zulässt, können Sie sie über eine vorbereitete *.reg*-Datei durchführen. Erfassen Sie das Listing 1.1 in einem Texteditor, und speichern Sie die Datei mit der Erweiterung *.reg* ab. Nach dem Download der Begleitdateien (siehe ➧ Einleitung) finden Sie die Datei *Username_auf_Desktop.reg* im Ordner *\Kap01*.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}]
"InfoTip"="Zeigt Dateien und Ordner auf dem Computer an."
@=hex(2):25,00,75,00,73,00,65,00,72,00,64,00,6f,00,6d,00,61,00,69,00,6e,00,25,\
  00,5c,00,25,00,75,00,73,00,65,00,72,00,6e,00,61,00,6d,00,65,00,25,00,20,00,\
  61,00,6e,00,20,00,25,00,63,00,6f,00,6d,00,70,00,75,00,74,00,65,00,72,00,6e,\
  00,61,00,6d,00,65,00,25,00,00,00
"LocalizedString1"="@C:\\WINNT\\system32\\shell32.dll,-9216@1031,Arbeitsplatz"
"LocalizedString"=-
```

Listing 1.1: *Eine Manipulation der Registrierung bewirkt, dass das Symbol* Arbeitplatz *den Namen des angemeldeten Benutzers zeigt*

Doppelklicken Sie auf die Datei, und bestätigen Sie die Sicherheitsabfrage. Wenn Sie nun den Desktop anzeigen (und ihn ggf. einmal mit F5 aktualisieren), wird statt der Beschriftung *Arbeitsplatz* der Benutzer- und der Computername angezeigt.

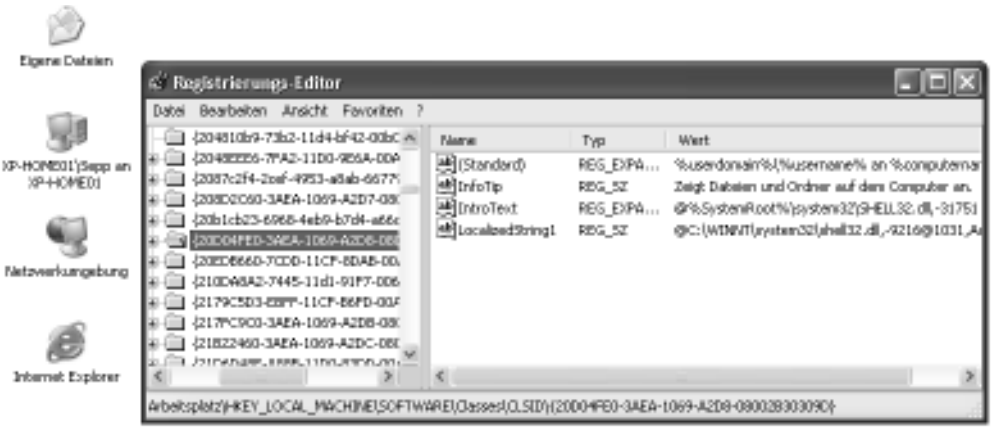

Abbildung 1.10: *Eine Manipulation der Registrierung zeigt Benutzerinformationen auf dem Desktop an*

HINWEIS: Falls Sie das Symbol *Arbeitsplatz* vorher bereits manuell umbenannt hatten, wird auch weiterhin Ihr selbst eingegebener Titel angezeigt. In diesem Fall können Sie das Symbol markieren, F2 drücken und den eigenen Text einfach löschen. Danach sollten die dynamischen Informationen sichtbar sein.

Tipp 1.13: Noch mehr Informationen auf dem Desktop anzeigen

»Benutzername und Computername auf dem Desktop sind ja ganz schön. Ich hätte aber gern noch mehr Informationen auf einen Blick.«

In vielen Situationen ist es nützlich, möglichst viele Systeminformationen auf einen Blick zu erhalten. Eine einfache und sehr praktische Möglichkeit, dies zu erreichen, ist das kostenlose Tool *BGInfo.exe* von Bryce Cogswell, das unter *http://www.sysinternals.com* heruntergeladen werden kann. BGInfo blendet einen Textblock mit frei wählbaren Systeminformationen in den Desktophintergrund ein. Der Textblock kann dabei auch ein vorhandenes Hintergrundbild überlagern.

Die Informationen, die angezeigt werden können, umfassen Basisdaten wie den Computernamen, den Namen des angemeldeten Benutzers oder die IP-Konfiguration, aber auch den freien Platz auf der Festplatte, den Service-Pack-Stand oder die Version des Internet Explorer. Darüber hinaus lassen sich auch eigene Informationen einbinden, die z.B. von einem Skript ermittelt oder aus der Registrierung gelesen werden.

BGInfo lässt sich über Kommandozeilenschalter auch ohne die grafische Oberfläche nutzen. Dadurch eignet es sich, um etwa per *Autostart*-Ordner bei jeder Anmeldung aktualisiert zu werden. Jüngere Versionen können die ermittelten Informationen darüber hinaus in eine zentrale Datenbank schreiben, so dass ein einfaches Basis-Tool für eine Inventarisierung entsteht.

Besonders interessant ist BGInfo, wenn im Netzwerk Tools zur Fernwartung eingesetzt werden, z.B. die Remotedesktopverbindung. Beim Hin- und Herschalten zwischen verschiedenen zu verwaltenden Rechnern herrscht so stets Klarheit, mit welchem System man gerade verbunden ist.

HINWEIS: BGInfo speichert das generierte Hintergrundbild standardmäßig direkt im Systemverzeichnis. Das ist problematisch, weil normale Benutzer hier keine Schreibrechte haben. Das führt dazu, dass BGInfo den Hintergrund bei normalen Benutzern nicht aktualisieren kann und dass u.U. sogar eine Fehlermeldung erscheint.

Zwei Möglichkeiten können hier abhelfen: Einerseits können Sie die NTFS-Berechtigungen der Datei *%systemroot%\BGInfo.bmp* so verändern, dass Benutzer Schreibrechte haben. Andererseits können Sie BGInfo aber auch anweisen, die Bitmap an einer anderen Stelle zu speichern (Menübefehl *Bitmap/Location*).

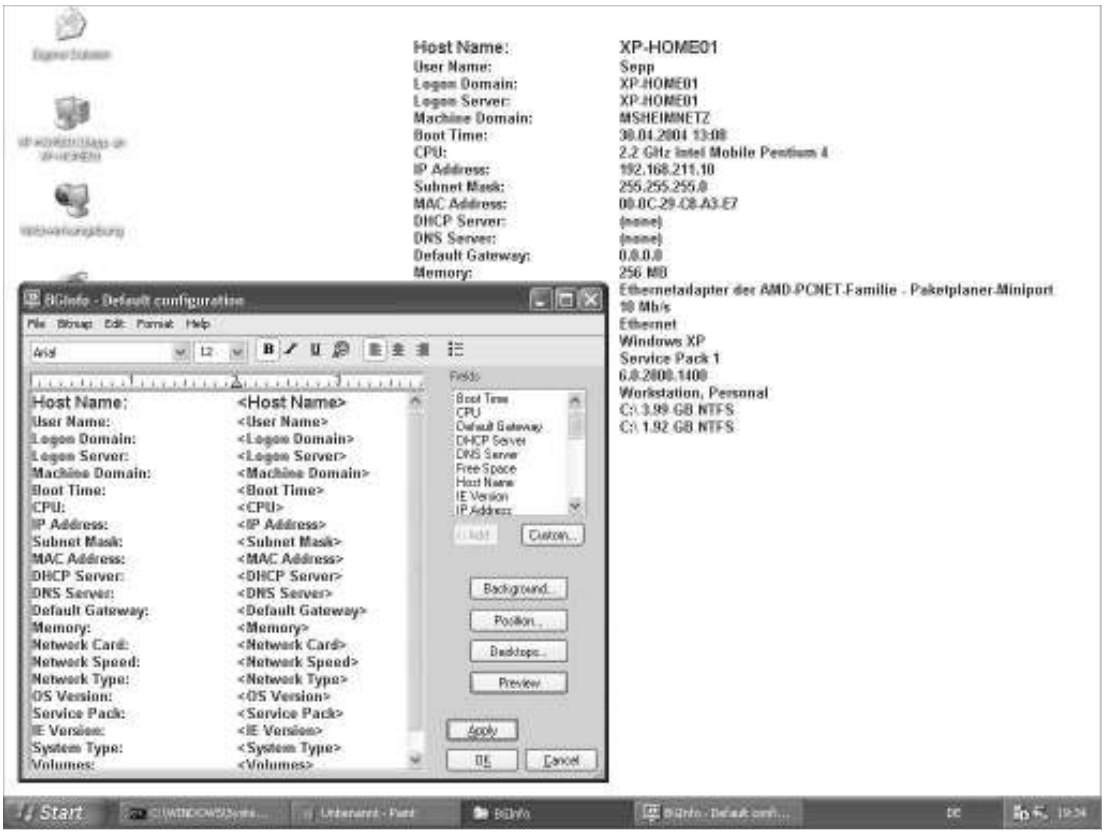

Abbildung 1.11: BGInfo blendet konfigurierbare Systeminformationen in den Desktop-Hintergrund ein

Tipp 1.14: Das System dokumentieren

»Ich möchte mir die Eckdaten zu meinem System übersichtlich anzeigen lassen und sie zu Dokumentationszwecken als Datei speichern. Was brauche ich dazu?«

Eine aussagefähige und aktuelle Systemdokumentation ist in vielen Situationen kritisch, sei es, dass das System nach einem Zusammenbruch möglichst schnell und möglichst vollständig wieder aufgebaut werden muss oder dass Sie ein identisches System auf anderer Hardware aufbauen wollen. Auch für Service und Troubleshooting ist eine umfassende Dokumentation eine wichtige Vorbedingung.

Die Basisdokumentation Ihres Windows-Systems können Sie mit Bordmitteln anfertigen und dies auch automatisieren. Das mitgelieferte Programm Systeminformationen ermittelt zahlreiche Daten über das System und speichert sie auf Wunsch in eine Datei. So geht's:

1. Um das Programm mit seiner grafischen Oberfläche zu starten, drücken Sie am besten Windows+R, tippen dann `msinfo32` ein und drücken Eingabe.

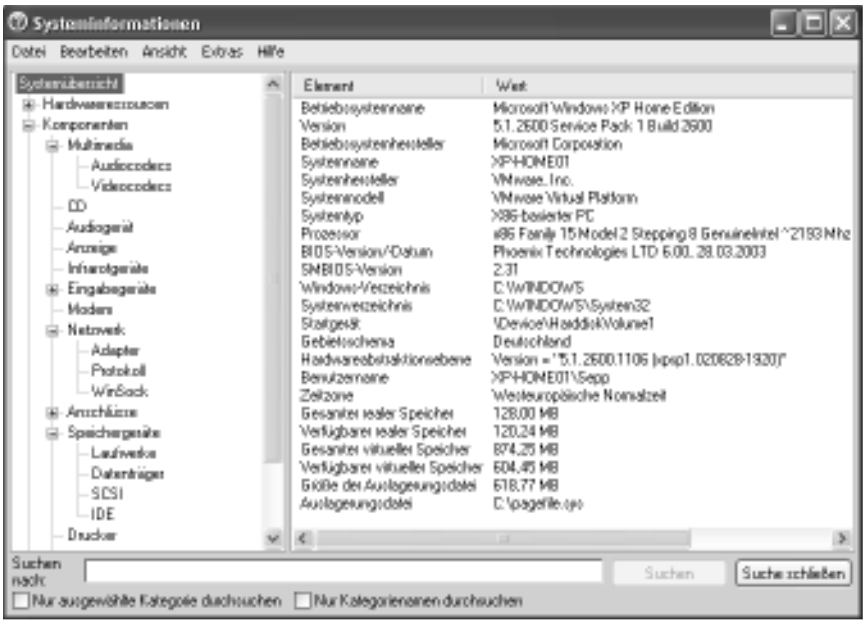

Abbildung 1.12: *Die Systeminformationen bieten eine umfassende Basisdokumentation*

2. Navigieren Sie im Strukturfenster links zu den Informationskategorien, die Sie interessieren.
3. Wenn Sie die Informationen als Bericht abspeichern wollen, wählen Sie den Menübefehl *Datei/Speichern*. Die so erzeugte *.nfo*-Datei können Sie mit dem Windows-Programm »Systeminformationen« (*msinfo32.exe*) wieder öffnen.
4. Wollen Sie einen Bericht in Textform erzeugen, wählen Sie den Menübefehl *Datei/Exportieren*. So können Sie die Daten mit einem beliebigen anderen Programm nutzen.

Um die Systeminformationen automatisiert zu speichern, beispielsweise zeitplangesteuert mit dem Taskplaner einmal wöchentlich, können Sie die Kommandozeilenoptionen nutzen. In einer Batchdatei oder auch im Taskplaner geben Sie z.B. Folgendes an, um die Daten im programmeigenen Format abzulegen (Achtung, die Anführungszeichen sind wichtig, und der ganze Befehl ist eine zusammenhängende Zeile):

```
"%CommonProgramFiles%\Microsoft Shared\MSInfo\msinfo32.exe"
/nfo C:\daten\sysinfo.nfo
```

Wenn Sie die Daten im Textformat ablegen wollen, ändern Sie die Kommandozeile in:

```
"%CommonProgramFiles%\Microsoft Shared\MSInfo\msinfo32.exe"
/report C:\daten\sysinfo.txt
```

Eine Übersicht über die Kommandozeilenoptionen zeigt Ihnen folgender Befehl:

```
"%CommonProgramFiles%\Microsoft Shared\MSInfo\msinfo32.exe" /?
```

HINWEIS: Einige Anwendungen mögen es gar nicht, wenn sie keinen virtuellen Arbeitsspeicher finden. Daher sollte diesen auf einem der vorhandenen Laufwerke auch bei großzügig bemessenem RAM ein kleiner Bereich als Auslagerungsdatei eingeräumt werden. Wenn Sie mit solch einer Situation konfrontiert werden, empfiehlt es sich, im Dialogfeld *Virtueller Arbeitsspeicher* einen Wert für die *Benutzerdefinierte Größe* einzugeben. Dieser sollte für die Einträge *Anfangsgröße* und *Maximale Größe* identisch sein, um das Risiko einer späteren Fragmentierung der Auslagerungsdatei zu verringern.

Tipp 4.15: NTFS auf allen Partitionen benutzen

»Windows XP unterstützt das Dateisystem NTFS. Dieses soll langsamer sein als FAT32 und im Fall von Bootproblemen ist die Datenrettung schwerer, weil man von einer DOS-Bootdiskette nicht darauf zugreifen kann. Warum sollte ich dann umsteigen?«

Gerade auf Rechnern, die von Windows 9x oder Millennium Edition auf Windows XP aktualisiert wurden oder auf denen Windows XP zum Testen zunächst als zweites Betriebssystem installiert wurde, existieren oft immer noch FAT32-Partitionen. Diese bieten keine Sicherheit auf Dateisystemebene und lassen somit das System weit geöffnet für verschiedenste Angriffe sowohl lokal als auch über das Netzwerk. Das NTFS-Dateisystem hingegen ist nicht nur sicherer, indem es erlaubt, Berechtigungen bis hin zur Dateiebene zu setzen, sondern bietet auch weitere Vorteile durch höhere Performance und eine erheblich verbesserte Robustheit im Fall von Systemabstürzen. Verschiedene Windows XP-Funktionen können ebenfalls nur auf NTFS-Partitionen zum Einsatz kommen.

Sobald auf alte Windows-Versionen verzichtet werden kann, sollten daher auch die letzten verbliebenen FAT-Partitionen zu NTFS konvertiert werden. Über die Datenträgerverwaltung, die unter Windows XP Bestandteil der Computerverwaltung ist, kann schnell das Dateisystem jeder einzelnen Partition ermittelt werden. Befinden sich nun noch Partitionen darunter, die einer Umwandlung auf das NTFS-Dateisystem bedürfen, kann das mit dem in Windows XP enthaltenen Befehlszeilenprogramm *convert.exe* – erklärt in . Kapitel 3 – erreicht werden, ohne dabei Daten zu verlieren.

Selbst wenn ältere Windows-Versionen noch beibehalten werden sollen, können all jene Partitionen, auf die diese Versionen nicht zugreifen müssen, zu NTFS konvertiert werden. In der Folge bleiben die konvertierten Partitionen für die alten Betriebssysteme unsichtbar, während aber von Windows XP aus ohne weiteres Dateien und Verzeichnisse auf diejenigen Betriebssystempartitionen kopiert oder verschoben werden können, die die älteren Windows-Versionen noch lesen können.

Im Schadensfall gibt Ihnen die Reparaturkonsole von Windows XP die Werkzeuge an die Hand, um in aller Regel wieder Zugriff zu Ihrem System und Ihren Daten zu bekommen.

Nach durchgeführter Konvertierung empfiehlt sich auf jeden Fall eine Optimierung der Datenstrukturen durch Defragmentierung des Laufwerkes.

ACHTUNG: Die Konvertierung einer Partition von FAT zu NTFS bedeutet nicht gleichzeitig, dass danach auch alle NTFS-Berechtigungen sicherheitskonform gesetzt sind. Hier müssen Sie gegebenenfalls noch selbst Hand anlegen, beispielsweise durch die Nutzung von Sicherheitsvorlagen.

Tipp 4.16: Dateien und Ordner schützen

»Ich möchte die Sicherheitsfunktionen des Dateisystems NTFS nutzen, das Windows XP mitbringt. Wie stelle ich das am besten an?«

Windows XP umfasst einige Funktionen, mit denen sich die Sicherheit für Dateien und Ordner erhöhen lässt. Die wichtigsten umfassen die Verwaltung von Berechtigungen und die Verschlüsselung von Dateien.

An dieser Stelle unterscheiden sich Windows XP Home Edition und Windows XP Professional sehr deutlich. Während Windows XP Professional grafische Hilfsmittel und Kommandozeilenbefehle zur Verwaltung der Sicherheitsfunktionen mitbringt, fehlen die grafischen Werkzeuge unter Windows XP Home Edition im Normalbetrieb vollständig. Die Verschlüsselungsfunktion steht in der Home-Version überhaupt nicht zur Verfügung.

Das empfohlene Dateisystem für beide Varianten von Windows XP ist NTFS. Hier haben Sie die Möglichkeit, exakt festzulegen, wer was mit welchen Daten anstellen kann. Aber Vorsicht: Die Berechtigungen greifen nur, solange das Betriebssystem ausgeführt wird, von dem aus die Berechtigungen festgelegt wurden. Wenn ein Benutzer Gelegenheit hat, den Computer mit einem anderen Betriebssystem zu starten, kann er u. U. auf alle Daten zugreifen. Sie sollten also ggf. mit einem BIOS-Kennwort oder anderen Methoden verhindern, dass Benutzer ein anderes Betriebssystem booten können.

Grundsätzlich gilt: Sie sollten Berechtigungen nur auf Ordnerebene erteilen. Obwohl Sie mit NTFS auch einzelne Dateien mit differenzierten Zugriffsrechten ausstatten können, ist dies nur im Ausnahmefall sinnvoll. Die Wahrscheinlichkeit, dass der Überblick (und damit die Sicherheit) verloren geht, ist zu groß. Weiterhin sollten Sie vorzugsweise Gruppen mit Zugriffsrechten ausstatten und nicht einzelne Benutzer. Nähere Hinweise hierzu finden Sie in ➧ Kapitel 4.

Wenn Sie Berechtigungen verwalten, gehen Sie stets vom geringsten Recht aus: Welcher Zugriff ist wirklich nötig, um eine Aufgabe auszuführen? Nur diese Berechtigung wird dann auch erteilt. Grundsätzlich gehen Sie dabei folgendermaßen vor:

1. Identifizieren Sie, wer auf die Daten zugreifen soll und welche Rechte dazu benötigt werden.
2. Stellen Sie fest, ob adäquate Gruppen existieren, um diese Zugriffsrechte abzubilden. Falls nicht, erstellen Sie neue Gruppen und versehen Sie diese mit den entsprechenden Mitgliedern. Anweisungen dazu finden Sie in ➧ Kapitel 4.
3. Weisen Sie dann die Berechtigungen zu.

Zum Zuweisen der Berechtigungen haben Sie zwei Möglichkeiten: Sie nutzen die Kommandozeile oder die grafischen Werkzeuge. Die Textbefehle der Kommandozeile stehen Ihnen sowohl unter Windows XP Home Edition als auch unter Windows XP Professional zur Verfügung. Für nähere Informationen zur Kommandozeile und dem Befehl *cacls.exe* lesen Sie in ➧ Kapitel 3 nach.

Die grafischen Werkzeuge können Sie unter Windows XP Professional immer nutzen. Unter Windows XP Home Edition hingegen müssen Sie dazu erst in den *Abgesicherten Modus* starten:

1. Starten Sie Ihren Computer neu. Drücken Sie die Taste F8, wenn die BIOS-Meldungen beendet sind.
2. Im folgenden Textmenü wählen Sie die Option *Abgesicherter Modus*.
3. Wenn der Anmeldebildschirm erscheint, wählen Sie ein Konto mit Administratorrechten zur Anmeldung.
4. Bestätigen Sie den Hinweis auf den abgesicherten Modus.

Die Verwaltung von Berechtigungen geschieht am effizientesten über den Windows-Explorer. Folgendermaßen gehen Sie dazu vor:

1. Navigieren Sie zu den Daten, deren Berechtigungen Sie bearbeiten wollen.
2. Klicken Sie dann mit der rechten Maustaste auf die Daten, deren Sicherheitseinstellungen Sie bearbeiten wollen. Wählen Sie im Kontextmenü den Befehl *Eigenschaften*.
3. Aktivieren Sie im Dialogfeld *Eigenschaften von <Datei-/Ordnername>* die Registerkarte *Sicherheit*.
4. Nun können Sie die Berechtigungen verändern, indem Sie Gruppen oder Benutzer hinzufügen bzw. entfernen oder die Zugriffsrechte für vorhandene Konten bearbeiten.

Die Berechtigungsverwaltung folgt einem Vererbungsprinzip: Die Berechtigungen, die für einen übergeordneten Ordner erteilt wurden, werden standardmäßig auf die untergeordneten Ordner und Dateien übertragen. Dies ermöglicht die effiziente Verwaltung von Zugriffsrechten. Außerdem können Sie so von oben nach unten mit immer spezielleren Rechten arbeiten: Erteilen Sie auf einer hohen Ordnerebene nur »allgemeine« Berechtigungen, und fügen Sie auf tieferen Ebenen weitere Einschränkungen hinzu. Ob eine bestimmte Berechtigung auf das aktuelle Objekt vererbt wurde oder ob sie direkt zugewiesen ist, können Sie am Erscheinungsbild festmachen: Ererbte Berechtigungen sind abgeblendet dargestellt. Diese können Sie nicht direkt bearbeiten, sondern Sie müssten zunächst die Vererbung abschalten.

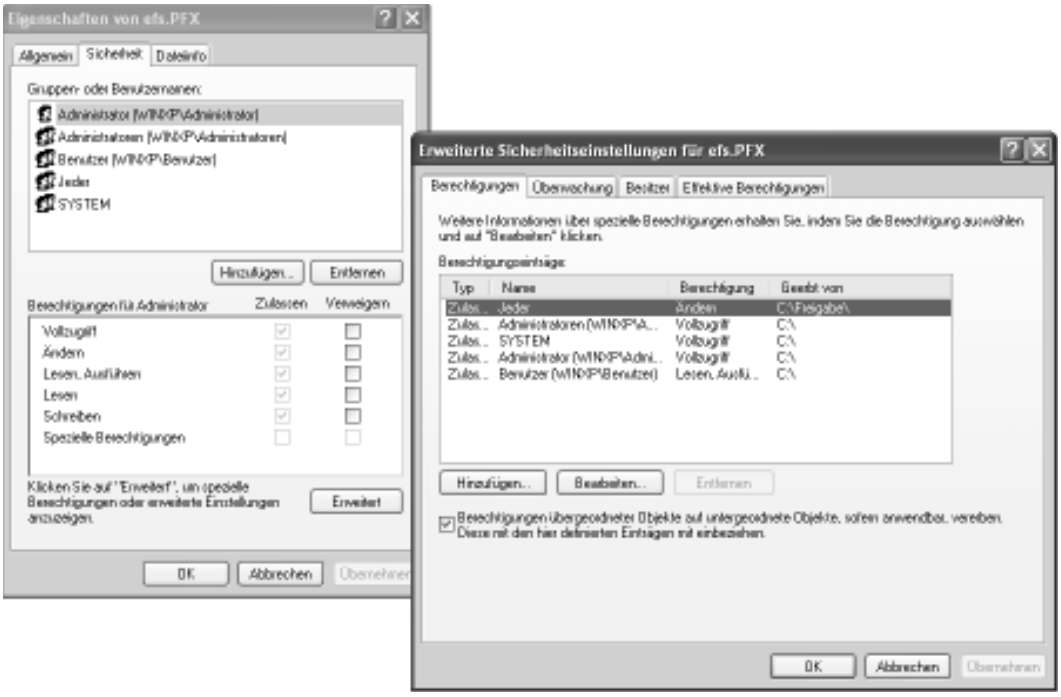

Abbildung 4.8: *Vererbung abschalten über* Erweiterte Sicherheitseinstellungen

Wenn Sie die Vererbung abschalten wollen, wählen Sie dafür auf der Registerkarte *Sicherheit* die Schaltfläche *Erweitert*. Im folgenden Dialogfeld *Erweiterte Sicherheitseinstellungen für <Datei-/Ordnername>* deaktivieren Sie dann das Kontrollkästchen *Berechtigungen übergeordneter Objekte auf untergeordnete Objekte, sofern anwendbar, vererben*. Danach können Sie im Dialogfeld *Sicherheit* auswählen, ob Sie die vorhandenen Rechte als Vorlage nutzen (Schaltfläche *Kopieren*) oder völlig neue Berechtigungen aufbauen wollen (Schaltfläche *Entfernen*).

Eine Besonderheit der Berechtigungsverwaltung sind die Besitzerrechte. Windows setzt stets denjenigen Benutzer als Besitzer einer Datei oder eines Ordners ein, der das Objekt angelegt hat. Der Besitzer hat immer die Möglichkeit, die Berechtigungen einer Datei zu bearbeiten – damit ist der Besitz eine wichtige Eigenschaft. Nachträglich können Sie den Besitz mit »Bordmitteln« nur dann übernehmen, wenn Sie das nötige Recht haben. In diesem Fall tun Sie dies über die Registerkarte *Besitzer* des Dialogfelds *Erweiterte Sicherheitseinstellungen*. Falls es nötig sein sollte, den Besitz an eine dritte Person zu übertragen, können Sie dazu das Werkzeug *SubInACL* aus dem Resource Kit nutzen (zum Resource Kit siehe . Kapitel 6).

Abbildung 4.9: *Besitz übernehmen mit dem Explorer*

Eine Leitlinie bei der Berechtigungsverwaltung sollte sein, möglichst wenige unterschiedliche Berechtigungen zu vergeben. Zusätzlich sollten Sie den jeweils aktuellen Stand der Rechtezuweisung dokumentieren. Hinweise hierzu finden Sie in . Kapitel 1.

Tipp 4.17: Geschützte Dateien kopieren

»Ich habe meine Daten von D: nach E: verschoben. Jetzt sind alle Berechtigungen weg! Was ist denn hier los?«

Wenn Sie Dateien oder Ordner kopieren oder verschieben, werden die Berechtigungen nicht unbedingt auf die Zieldaten übertragen. Als Faustregel gilt: Nur wenn Sie Daten innerhalb derselben Partition verschieben, bleiben die Berechtigungen erhalten. In allen anderen Fällen werden die Berechtigungen des Zielordners übernommen – jedenfalls solange Sie den Windows-Explorer für diese Aktion nutzen.

Der Hintergrund ist relativ einfach: NTFS legt die Berechtigungen als Dateiattribute ab. Wenn Sie nun Dateien kopieren, werden immer neue Dateien am Zielort geschrieben. Diese übernehmen die Berechtigungsattribute des Ordners. Auch beim Verschieben von Daten von einer Partition auf die andere handelt es sich in Wirklichkeit um einen Kopiervorgang (dem dann automatisch ein Löschvorgang im Quellordner folgt). Nur wenn Sie Daten innerhalb derselben Partition verschieben, geschieht etwas anderes: In diesem Fall ändert Windows nur den Pointer innerhalb des Inhaltsverzeichnisses, der auf die tatsächlichen Daten zeigt. Dadurch werden die Attribute nicht verändert, und die Berechtigungen bleiben erhalten.

Mit einem kleinen Trick können Sie diesem Verhalten eine obskure Folge entlocken. Legen Sie einen Ordner *Ordner_1* an und in diesem einen Unterordner *Ordner_2*. Entfernen Sie für *Ordner_1* die vorhandenen Berechtigungen, indem Sie die Vererbung abschalten, und berechtigen Sie die Gruppe *Jeder* mit Vollzugriff (auch wenn man das eigentlich nicht tun soll). Entfernen Sie auch für *Ordner_2* die vorhandenen Berechtigungen, und erteilen Sie der Gruppe *Benutzer* Vollzugriff auf *Ordner_2*.

Legen Sie nun eine Datei in *Ordner_2* an, und kontrollieren Sie deren Zugriffsrechte. Sie sollte für die Gruppe *Benutzer* Vollzugriff ausweisen; durch die Schattierung ist erkennbar, dass die Berechtigungen vom Ordner ererbt sind. Verschieben Sie nun die Datei in *Ordner_1*. Sehen Sie sich jetzt die Berechtigungen an: Immer noch ist der Vollzugriff für die *Benutzer* (angeblich) vom Ordner ererbt. Das kann aber gar nicht sein – für den übergeordneten *Ordner_1* hat ja *Jeder* Vollzugriff …

Um sicher zu gehen, dass die Berechtigungen in jedem Fall erhalten bleiben, sollten Sie solche Kopier- und Verschiebevorgänge auf der Kommandozeile mit dem Befehl *xcopy* ausführen (zum Verschieben fügen Sie dann im zweiten Schritt ein *del* an). Mit Hilfe des Optionsschalters */O* weisen Sie den Befehl an, die Berechtigungen des Originals auf die Kopie zu übertragen. Beispiel:

```
xcopy C:\geheim\umsatz.xls d:\vorstand\umsatz_2004.xls /O
```

Näheres zu *xcopy* erfahren Sie in . Kapitel 3.

Tipp 4.18: Dateien sicher verschlüsseln

»Welche Möglichkeiten gibt es denn außer den NTFS-Berechtigungen, wenn ich sensible Daten schützen möchte?«

Jede Berechtigungsvergabe steht unter einer gravierenden Einschränkung: Wenn der Computer mit einem anderen Betriebssystem gestartet wird, kann ein Benutzer u. U. sämtliche Zugriffsrechte umgehen. Das ist keine Schwäche von Windows, sondern trifft auf jedes Betriebssystem zu – die Sicherheitsmechanismen greifen nur so lange, wie das Betriebssystem sie kontrollieren kann.

Um für solche Fälle wenigstens zu verhindern, dass geschützte Inhalte gelesen werden, können Daten auf der Festplatte verschlüsselt werden. Seit Windows 2000 ist eine Dateiverschlüsselung ins System eingebaut. Sie nennt sich »Verschlüsselndes Dateisystem« (im Original: Encrypting File System, EFS) und funktioniert auf allen NTFS-Partitionen unter Windows 2000, Windows Server 2003 und Windows XP Professional. Unter Windows XP Home Edition steht dieses Feature leider nicht zur Verfügung.

Die Funktionsweise des EFS ist recht komplex; trotzdem soll an dieser Stelle ein kurzer Überblick ausreichen. EFS verschlüsselt Dateien direkt auf der Festplatte nach einem zweistufigen Konzept. Die eigentlichen Daten werden mit einem sog. »symmetrischen Schlüssel« verschlüsselt, d. h. zum Verschlüsseln kommt derselbe Schlüssel zum Einsatz wie zum Entschlüsseln. Dieses Verfahren ist relativ schnell. Der genutzte Schlüssel, der sog. »Dateiverschlüsselungsschlüssel« (im Original: File Encryption Key, FEK), wird in der Datei selbst abgelegt – aber natürlich wird er seinerseits auch verschlüsselt, in diesem Fall nach dem Public-Key-Verfahren, das auch als »asymmetrische Verschlüsselung« bezeichnet wird. Zum Verschlüsseln und zum Entschlüsseln werden hierbei unterschiedliche, zusammengehörige Schlüssel genutzt. Dieses Verfahren ist besonders sicher, aber auch relativ langsam, daher wird es nur zum Codieren des Schlüssels genutzt, nicht für die eigentlichen Daten.

Da der FEK mit dem sog. »Öffentlichen Schlüssel« des Anwenders codiert wird, der die Datei verschlüsselt hat, ist sichergestellt, dass nur dieser Anwender die Datei auch wieder entschlüsseln kann. Hierzu benötigt er seinen sog. »Privaten Schlüssel«, auf den nur er selbst Zugriff hat. EFS ist als Dateisystem eingerichtet und nicht als Anwendung, d. h. es funktioniert mit jedem beliebigen Programm, weil es sozusagen auf einer tieferen Ebene stattfindet.

Beschreibung können Sie in »Vordefiniertes Konto für die Verwaltung des Computers bzw. der Domäne« ändern. Solange die Rechte dieses Benutzerkontos sehr gering gehalten werden – beachten Sie insbesondere auch die Zugriffsrechte auf das Dateisystem – und das Kennwort nicht zu erraten und von hoher Komplexität ist, können von diesem Konto keine Gefahren ausgehen. Dafür kann es Ihnen als wertvolle Informationsquelle über etwaige Angriffe auf die betreffenden Rechner dienen, wenn die Überwachung für Anmeldeversuche und Anmeldeereignisse aktiviert ist.

Tipp 5.18: Gefahren durch Selbstbeschränkung eindämmen

»Immer wieder werde ich gewarnt, ich solle nicht mit dem Administrator-Konto arbeiten. Warum eigentlich nicht?«

Neben der Orientierung auf Benutzer und Gruppen bringt Windows ein weiteres Grundprinzip mit, das es mit allen anderen modernen Betriebssystemen teilt. Es ist das Prinzip des geringsten Privilegs (»least privilege«): Ein Benutzer sollte immer nur das dürfen, was er für seine Aufgaben zwingend benötigt.

Dieses Prinzip ist nicht immer bequem, aber es ist das einzige, mit dem Sie Ihren Computer sichern können. Es ist nicht übertrieben, zu behaupten, dass es wesentlich weniger Sicherheitsprobleme in der Informationstechnologie gäbe, wenn dieser Grundsatz auch nur halbwegs konsequent befolgt würde.

Da Sie vermutlich niemals Ihre EC-Karte nach Eingabe der PIN im Automaten belassen und dann die Bank verlassen würden, sollten Sie auch auf Ihrem PC nur jene Zugriffe erlauben, die Sie im jeweiligen Moment wirklich brauchen. Wenn Sie etwa Büroarbeit erledigen, brauchen Sie weder Administratoren-, noch Hauptbenutzerrechte. Installieren Sie gerade einen Treiber, benötigen Sie sicher keinen Zugriff auf Ihre TAN-Liste fürs Homebanking.

Bedenken Sie: Ihre Anmeldung entscheidet über Ihre Zugriffsrechte. Jedes Programm, das Sie aufrufen, läuft in Ihrem Benutzerkontext und hat damit Ihre Berechtigungen. Das gilt natürlich auch für Code, den Sie gar nicht bewusst aufrufen – sei es Schadcode (Viren, Trojanische Pferde usw.) oder nur eine Funktion, die nicht das tut, was sie soll. Wenn nun Ihre Benutzerrechte bestimmte Zugriffe etwa auf Systemkomponenten oder kritische Daten gar nicht zulassen, wird der mögliche Schaden von vornherein begrenzt oder sogar verhindert.

Tipp 5.19: Höhere Rechte gezielt einsetzen

»Okay, ich habe verstanden. Nun habe ich mein Benutzerkonto eingeschränkt, d.h. es ist nur noch in der Gruppe Benutzer, nicht mehr in der Administratoren-Gruppe. Jetzt kann ich aber viele Dinge nicht mehr tun – z.B. keine Programme installieren. Und jetzt?«

Windows XP macht Ihnen die Beschränkung auf das Nötigste einfach. Sie können Ihre Alltagsarbeit mit einem eingeschränkten Benutzerkonto erledigen (am besten als Mitglied der Gruppe *Benutzer*) und dann, wenn es nötig ist, gezielt mit höheren Rechten arbeiten. Dazu nutzen Sie die Funktion *Ausführen als* oder das Kommando runas. Hinter beiden verbirgt sich der Dienst *Sekundäre Anmeldung*, der es Ihnen erlaubt, zusätzlich zu dem Benutzerkonto, mit dem Sie sich an Windows angemeldet haben, ein weiteres Konto zu nutzen, mit dem Sie nur eine bestimmte Anwendung ausführen. Der Gedanke ist: Wenn Sie nur für eine Anwendung die Administratorrechte benötigen, warum sollten Sie dann für alle Aufgaben mit diesen Rechten arbeiten?

So nutzen Sie *Ausführen als*:

- Klicken Sie mit der rechten Maustaste auf das Programmsymbol, das Sie starten wollen. Wenn der Menübefehl *Ausführen als* nicht zur Auswahl steht, müssen sie die Taste Umschalt gedrückt halten, während Sie die rechte Maustaste drücken.

1. Wählen Sie im Kontextmenü den Befehl *Ausführen als*.

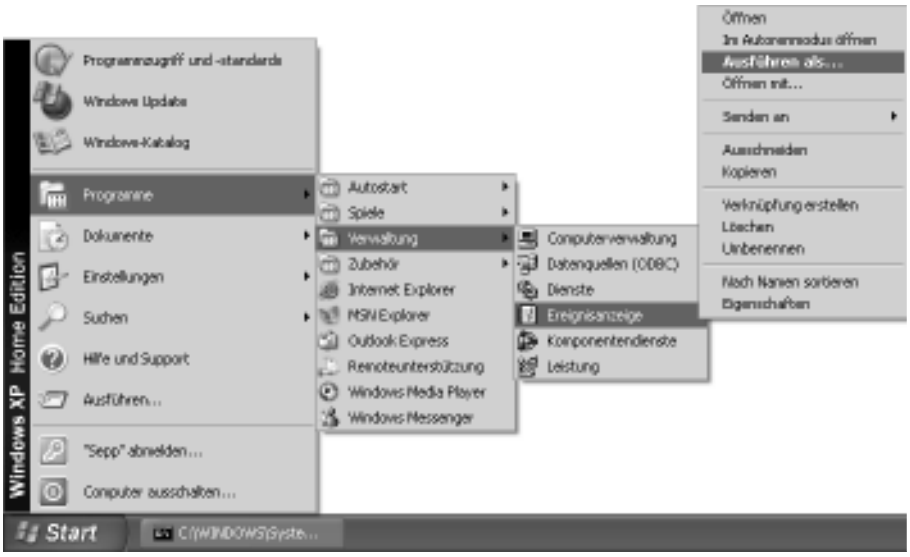

Abbildung 5.17: *Den Befehl* Ausführen als *zum Aufrufen einer Anwendung nutzen*

2. Wählen Sie im Dialogfeld *Ausführen als* die Option *Folgender Benutzer.* Tragen Sie den Benutzernamen und das Kennwort ein.
3. Bestätigen Sie mit der Schaltfläche *OK*. Windows wird nun versuchen, die Anwendung in dem gewählten Benutzerkontext auszuführen.

So nutzen Sie das Kommando runas:

1. Öffnen Sie die Eingabeaufforderung (Windows+R `cmd` Eingabe).
2. Um etwa die Ereignisanzeige (*eventvwr.exe*) als Administrator auszuführen, tippen Sie ein:

```
runas /user:Administrator eventvwr.exe
```

3. Sie werden nun nach dem Kennwort für das gewählte Benutzerkonto gefragt. Tippen Sie es ein, und drücken Sie Eingabe. Windows wird nun versuchen, die Anwendung in dem gewählten Benutzerkontext auszuführen.

Wenn Sie die Funktion *Ausführen als* häufiger nutzen, dann haben Sie verschiedene Möglichkeiten, sich dies etwas bequemer zu machen. Zum einen können Sie die Verknüpfung verändern, die das Programm aufruft:

1. Klicken Sie mit der rechten Maustaste auf das Symbol, mit dem Sie das betreffende Programm starten. Wählen Sie im Kontextmenü den Befehl *Eigenschaften*.
2. Klicken Sie im Dialogfeld *Eigenschaften von (Programmname)* auf die Schaltfläche *Erweitert.*

3. Wählen Sie im Dialogfeld *Erweiterte Eigenschaften* das Kontrollkästchen *Unter anderen Anmeldeinformationen ausführen*.

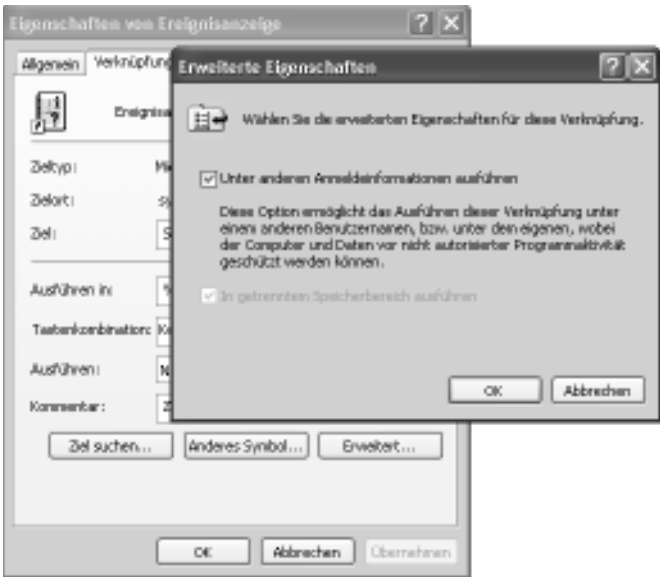

Abbildung 5.18: *Eine Verknüpfung konfigurieren, um die Anwendung in einem anderen Benutzerkontext zu starten.*

4. Von nun an werden Sie bei jedem Aufruf des Symbols nach dem Konto gefragt, dessen Berechtigungen Sie nutzen wollen.

Falls Sie die Funktion *Ausführen als* oft zum Aufruf verschiedener Programme unter einem bestimmten Benutzerkonto nutzen, können Sie die entsprechende runas-Kommandozeile in einer kleinen Batchdatei kapseln. Dieser Batchdatei übergeben Sie dann nur noch den Namen des auszuführenden Programms und geben das entsprechende Kennwort an. Keine Angst, das ist einfacher, als es klingt.

Die Batchdatei sieht folgendermaßen aus. Erfassen Sie den Text in einem Editor, und speichern Sie die Datei unter einem kurzen, prägnanten Namen (beispielsweise *as.bat* für *AdminStart*) an einem Speicherort, der vom System gefunden wird (z.B. *C:\windows*).

IM INTERNET: Nach dem Download der Begleitdateien (siehe Einleitung) finden Sie die Datei *as.txt* im Ordner *\Kap05*. Aus Sicherheitsgründen liegt die Datei als *txt*-Datei vor. Vor einer Ausführung der Batchdatei muss sie in *as.bat* umbenannt werden.

```
@echo off
runas /user:Administrator "%*"
```

Listing 5.2: *Mit* as.bat *kapseln Sie den Aufruf von* runas.

Wenn Sie nun künftig ein Programm als Administrator starten wollen, z. B. *eventvwr.exe*, so öffnen Sie das Startmenü, wählen *Ausführen* (dies lässt sich übrigens abkürzen mit der Tastenkombination Windows+R) und tippen in das Eingabefeld ein:

```
as eventvwr
```

Die Eingabeaufforderung erscheint und fordert Sie zur Eingabe des Kennworts auf. Einen Moment später wird dann die Ereignisanzeige im Kontext des Administrators geöffnet.

HINWEIS: Sie können bei dem Befehl *runas* auch mit gespeicherten Anmeldeinformationen arbeiten, um zu vermeiden, dass Sie das Kennwort jedes Mal eingeben müssen. Wie das geht, wird im Tipp 5.11 beschrieben.

Tipp 5.20: Administratoren entlarven

»Es gibt eine Reihe von Benutzern auf meinem Computer bzw. in unserem Netzwerk. Wie kann ich feststellen, welcher dieser Benutzer lokale Administratorrechte hat?«

Grundsätzlich hat ein Benutzer genau dann lokale Administratorrechte auf einem Computer, wenn er auf diesem System der lokalen Gruppe *Administratoren* angehört. Es reicht also prinzipiell aus, die Mitglieder dieser Gruppe auszugeben, um festzustellen, wer lokaler Administrator ist. So können Sie dies tun:

1. Öffnen Sie die Eingabeaufforderung (Windows+R `cmd` Eingabe drücken).
2. Geben Sie ein: `net localgroup Administratoren`, und drücken Sie Eingabe.

Dieses Verfahren hat aber zwei Schönheitsfehler: Es zeigt Ihnen zum einen nur die »direkten« Gruppenmitglieder. Wenn ein Benutzer Mitglied einer anderen Gruppe ist, die ihrerseits Mitglied der *Administratoren*-Gruppe ist, so taucht er in der Liste nicht auf – er hat aber trotzdem Administratorrechte. Zum anderen könnte es sein, dass die Administratorengruppe gar nicht *Administratoren* heißt – auf einem englischen System beispielsweise nennt sie sich *Administrators*.

Ein anderes Verfahren geht also direkt über den Benutzer, indem es sein Access Token ausliest. Dieses Token enthält die SIDs aller Gruppen, denen der Benutzer angehört, auch durch »verschachtelte« Mitgliedschaften. Näheres zum Access Token lesen Sie im Tipp 5.22.

Das Access Token können Sie mit dem Tool *whoami.exe* analysieren. Es gehört zu den freien Tools aus dem Resource Kit zu Windows 2000. Unter Windows Server 2003 ist es direkt vorhanden. Nachteil dieses Verfahrens: Es kann nur den aktuell angemeldeten Benutzer analysieren. In einem Netzwerk könnten Sie es aber beispielsweise ins Anmeldeskript integrieren und die Ausgabe in einer Textdatei auf einem Server sammeln.

Das Verfahren nutzt *whoami.exe*, um die Gruppen auszugeben, in denen der aktuelle Benutzer Mitglied ist. In dieser Gruppenliste wird nach der SID *S-1-5-32-544* gesucht, die auf jedem Windows-System sprachunabhängig für die lokale Administratorengruppe steht. Falls die SID vorhanden ist, muss der Benutzer Mitglied dieser Gruppe sein, und es wird eine Meldung ausgegeben.

IM INTERNET: Nach dem Download der Begleitdateien (siehe Einleitung) finden Sie die Datei *BinIchAdmin.txt* im Ordner *\Kap05*. Aus Sicherheitsgründen liegt die Datei als *txt*-Datei vor. Vor einer Ausführung der Batchdatei muss sie in *BinIchAdmin.bat* umbenannt werden.

```
@echo off
rem Speicherpfad von whoami.exe angeben
set whoamipfad=C:\Tools\Resource_Kit

rem Zu suchende SID angeben (Administratoren: S-1-5-32-544)
set suchsid=S-1-5-32-544

%whoamipfad%\whoami /groups | find "%suchsid%" > nul
if errorlevel 1 goto ende
echo Benutzer %username% ist lokaler Administrator.

:ende
```

Listing 5.3: *Mit* BinIchAdmin.bat *herausfinden, ob der aktuelle Benutzer Administratorrechte hat*

Tipp 5.21: Interne Ausweise (SID) sichtbar machen

»In vielen Artikeln zur Sicherheit unter Windows ist von einer SID die Rede. Was ist das und was nützt es mir?«

Der Windows-Benutzername wird eigentlich nur zur Anmeldung verwendet – und dann, wenn ein Administrator die Benutzerkonten verwaltet. Intern nutzt Windows einen abstrakten Zahlencode, um die verschiedenen Benutzerkonten (oder besser: »Sicherheitsprinzipale«, denn in Wirklichkeit geht es nicht nur um Benutzer) auseinander zu halten. Dieser Code wird als »Security Identifier« bezeichnet – kurz: SID. Er besteht aus mehreren Teilen und ist stets eindeutig. Dies wird dadurch erreicht, dass jede SID nur ein einziges Mal zugeordnet wird: Wenn ein Benutzerkonto etwa gelöscht wird, verfällt die zugehörige SID und wird nie wieder neu verwendet. Außerdem ist ein Teil der SID computerspezifisch, d. h. auch auf verschiedenen Rechnern kann es nie zwei identische SIDs geben.

Die SID ist immer nach demselben Schema aufgebaut. Sehen Sie sich dies anhand eines Beispiels an:

```
S-1-5-21-3013843177-969149449-1252591305-1008
```

1. Seit Windows NT beginnen SIDs immer mit der Zeichenfolge »S-1«. Hätte sich der SID-Aufbau einmal verändert, so wäre die 1 als SID-Versionsnummer hochgezählt worden.
2. Die »5« danach gibt an, dass es sich um eine SID des eigenen Rechners handelt. Es ist die sog. »Autorität«, die diese SID definiert hat. Andere Autoritäten haben andere Nummern, z. B. 1 für vordefinierte Gruppen.
3. Der größte Teil der oben abgebildeten SID besteht aus der sog. »Sub-Autorität«: es ist die Zahlenkolonne »21-3013843177-969149449-1252591305«. Dahinter verbirgt sich nichts anderes als eine eindeutige Kennung des eigenen Rechners. Dieser Teil ist auf jedem Rechner und in jeder Domäne unterschiedlich. An ihm lässt sich unterscheiden, wohin ein Konto gehört (im Falle einiger spezieller SIDs fehlt dieser Abschnitt, z. B. bei der Gruppe *Jeder*).
4. Der letzte Teil nach dem letzten Bindestrich (hier: »1008«) ist der »Relative Identifier« oder »RID«. Er ist für jedes Objekt eindeutig, das von einer Sub-Autorität gekennzeichnet wurde. Die RID »500« übrigens ist stets für das vordefinierte Administrator-Konto reserviert. RIDs sind wie Einwegflaschen, sie werden immer nur einmal verwendet (ein Dosenpfand fällt aber nicht an).

Sie können die SIDs auf Ihrem System selbst erkunden. Wenn Sie als Mitglied der Administratoren-Gruppe an Windows XP Professional angemeldet sind, tippen Sie in einem Eingabeaufforderung ein:

```
WMIC PATH Win32_Account WHERE Name="Ute" GET Sid
```

Als Nicht-Administrator bzw. unter Windows XP Home Edition nutzen Sie das folgende Skript. Haben Sie bei der Benutzung beider Möglichkeiten ein wenig Geduld, denn es dauert einige Sekunden, bis nach der Eingabe eines Namens die Antwort erscheint, weil Windows versucht, auch im Netzwerk nach Namen zu suchen.

IM INTERNET: Nach dem Download der Begleitdateien (siehe . Einleitung) finden Sie die Datei *getSIDbyName.txt* im Ordner *\Kap05*. Aus Sicherheitsgründen liegt die Datei als *txt*-Datei vor. Vor einer Ausführung des Skripts muss sie in *getSIDbyName.vbs* umbenannt werden.

```
strSearch = InputBox("Zu welchem Namen wird die SID gesucht?")

Set objWMI = GetObject("winmgmts:")
strWQL = "select SID from win32_account where Name='" & strSearch & "'"
Set objResult = objWMI.ExecQuery(strWQL)

For Each objAcc In objResult
      strResult = objAcc.SID
Next

InputBox "Die SID von " & strSearch & " lautet: ", , strResult
```

Listing 5.4: *Die SID zu einem Namen ermitteln Sie mit* getSIDbyName.vbs.

Eine solche SID wird jedem Objekt zugeordnet, dem Windows Berechtigungen zuweisen kann. Bei einem Einzelrechner können dies zwei Sorten von Objekten sein (so genannte »Objektklassen«): Benutzerkonten und Gruppenkonten. Im Falle eines Windows-Netzwerks mit zentraler Verwaltung, also einer Domäne, kommt als dritte relevante Objektklasse noch das Computerkonto hinzu (gewissermaßen ein Benutzerkonto für einen bestimmten PC).

Wenn Sie als Administrator (oder als kundiger Benutzer) Berechtigungen etwa für einen Ordner oder eine Datei erteilen, speichert Windows intern immer die SID des Benutzer- oder Gruppenkontos, das Sie ausgewählt haben. Daraus erwächst der Vorteil, dass Sie Benutzer und Gruppen auch problemlos umbenennen können, ohne dass sie ihre Zugriffsrechte verlieren: die SID ändert sich ja nicht.

Tipp 5.22: Berechtigungen wirksam machen

»Ich habe einen Benutzer in eine Gruppe aufgenommen, damit er auf bestimmte Daten zugreifen kann. Wenn er nun aber den Zugriff versucht, meldet das System: Zugriff verweigert. Aber die Berechtigungen sind richtig. Was mache ich falsch?«

Das Windows-Sicherheitssystem (die »Local Security Authority« oder »LSA«) stellt dem Benutzer, wenn er erfolgreich authentifiziert wurde, einen Ausweis aus, das sog. »Access Token«. In diesem ist der Benutzer beschrieben, und zwar anhand seiner SID und der SIDs aller Gruppen, denen er angehört. Damit kann künftig schnell entschieden werden, was er darf, denn Windows muss nur das Token kontrollieren und nicht die gesamte Kontendatenbank. Auf diese Weise kann effizient geprüft werden, ob ein Benutzer wirklich berechtigt ist, zu tun, was er anfordert. Das Token wird intern von Windows verwaltet und ist so lange in Benutzung, wie der Benutzer arbeitet. Sobald er sich von Windows abmeldet und damit seine Sitzung beendet, verfällt auch das Token.

Da aber das Access Token nur im Moment der Anmeldung eines Benutzers generiert wird, kann es in ungünstigen Umständen vorkommen, dass seine realen Berechtigungen nicht den Wünschen des Administrators entsprechen. Denn die »effektiven« Gruppenmitgliedschaften werden immer bei der Anmeldung festgelegt und dann nicht mehr geändert. Ändert der Administrator die Mitgliedschaft in einer Gruppe, um einem Benutzer bestimmte Zugriffe zu ermöglichen oder zu verwehren, wird diese Änderung erst dann wirksam, wenn der Benutzer sich das nächste Mal anmeldet.

TIPP: Den Umstand, dass veränderte Gruppenmitgliedschaften sich erst bei der nächsten Anmeldung auswirken, übersehen auch gestandene Netzwerkprofis immer wieder. Manchmal sitzt man Stunden kopfschüttelnd vor einem Problem und stellt hinterher fest, dass man sich nur hätte neu anmelden müssen. Sie sollten daher die Maßnahme »Abmelden und wieder anmelden« in das feste Repertoire Ihrer Fehlerbehebungsversuche aufnehmen.

Tipp 7.14: Reparaturinstallation durchführen

»Ich habe auf mehreren Wegen versucht, mein Windows XP wieder zu ordnungsgemäßer Funktion zu bringen. Leider hat es noch nicht geklappt. Muss ich jetzt ein altes Image zurückspielen, oder habe ich noch eine andere Möglichkeit?«

Wenn die verschiedenen Reparaturmethoden nicht fruchten, bringt Windows XP noch eine weitere Möglichkeit mit, eine Neuinstallation oder den Weg zurück auf ein altes Image zu vermeiden. Es handelt sich um die »Reparaturinstallation«, die ein störrisches Windows wieder auf den Pfad der Tugend bringen soll.

Bei dieser Methode wird das Setup-Programm von Windows XP angewiesen, sämtliche Systemdateien mit dem Original von der Installations-CD zu überschreiben, die Daten des Benutzers sowie die installierten Applikationen aber so zu belassen, wie sie sind. In vielen Fällen führt dies wieder zu einem Windows, wie es sein soll: Die Umgebung ist vertraut, aber unter der Haube ist alles wie neu. Aber Achtung, diese Methode ist in einigen anderen Fällen machtlos, beispielsweise dann, wenn installierte Fremd-Treiber oder »verkonfigurierte« Anwendungen die Probleme verursachen.

Der Weg zur Reparaturinstallation flößt dem, der dies nur selten tut, durchaus Respekt ein: Man bootet seinen Rechner mit der Installations-CD von Windows XP, als wolle man das Betriebssystem auf einem neuen Computer einrichten. Nach der üblichen Hardware-Untersuchung bietet Setup dann die drei Möglichkeiten, Windows XP zu installieren, die Wiederherstellungskonsole zu starten oder doch lieber alles bleiben zu lassen. Hier heißt es selbstbewusst zu sein und alle Scheu hinter sich zu lassen: Die erste Option der kompletten Installation ist die richtige Wahl.

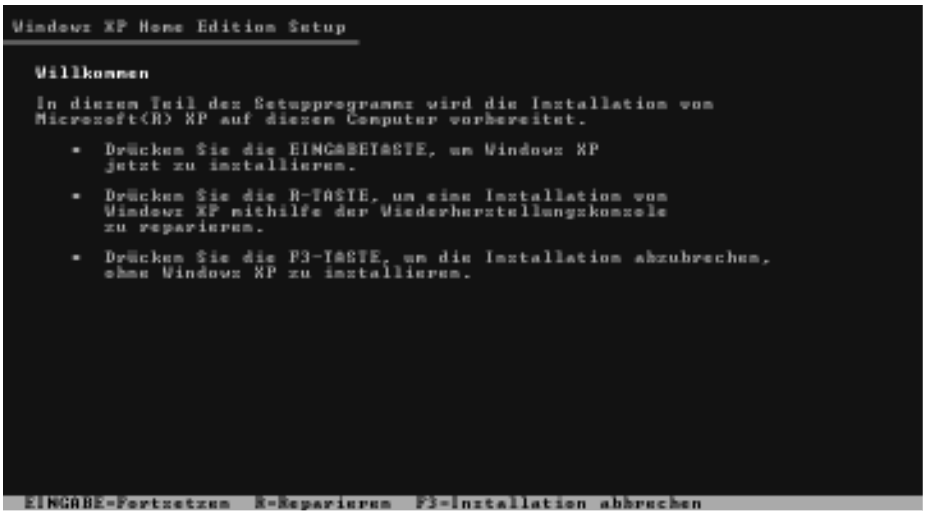

Abbildung 7.20: *Die Reparaturinstallation beginnt wie eine Neuinstallation.*

Erst wenn man nun (erneut) den elektronischen Lizenzvertrag bestätigt hat, schaut Setup nach, ob es nicht doch ein vorhandenes Windows findet. Und nun sollte es die zu reparierende Installation finden und endlich anbieten, die Reparatur auszuführen: Mit der Taste `R` geht es los.

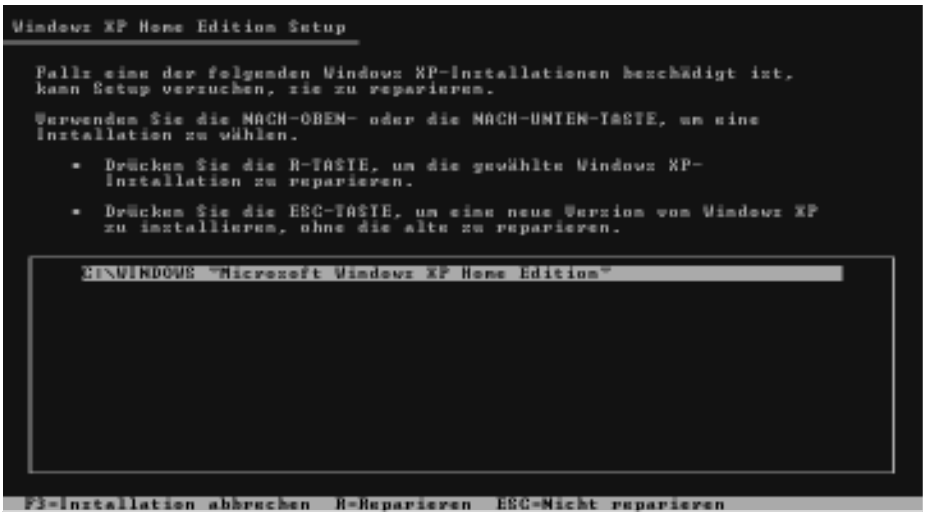

Abbildung 7.21: *Setup hat die zu reparierende Installation gefunden.*

Zum Dank jagt Setup dem leidenden Benutzer nun aber noch mal einen richtigen Schreck ein, denn es löscht kühn alle Systemdateien. Danach aber läuft das Setup praktisch wie gewohnt ab (das betrifft auch die Abfrage der Seriennummer, die man zur Hand haben sollte!), und nach einigen Minuten des bangen Wartens sollte ein gesundetes Windows XP den Benutzer begrüßen.

Zu guter Letzt sollten Sie tun, was Pflicht nach jeder Installation von Windows XP ist: Installieren Sie das aktuelle Service-Pack und bringen Sie Ihr System mit der Update-Funktion auf den aktuellen Patchlevel.