21 Registry-Absicherung

363 Registry-Zugriff schützen
369 Netzwerkzugriff kontrollieren
374 Abwärtskompatibilität herstellen

Weil die interne Registry-Datenbank der Aufbewahrungsort für viele Sicherheitseinstellungen ist, spielt sie eine entscheidende sicherheitstechnische Rolle. Es muss gewährleistet sein, dass die sensiblen Bereiche der Registry nicht von Unbefugten geändert werden können. Dazu gehört auch, den Netzwerkzugriff auf die Registry zu kontrollieren.

In diesem Kapitel lesen Sie:

- Wie können Registry-Einträge vor unbefugter Veränderung geschützt werden, und wie schützt Windows sensible Registry-Bereiche in den Standardeinstellungen?
- Wie funktionieren Sicherheitsvorlagen, und wie können Sie die Basissicherheit der Registry überprüfen und wiederherstellen?
- Wie wird der Netzwerkzugriff auf die Registry kontrolliert, wofür ist er überhaupt notwendig, und welche Sicherheitslücken sind dabei zu berücksichtigen?

Registry-Zugriff schützen

Jeder Zweig in der Registry kann ganz analog wie Ordner und Dateien im Dateisystem mit Zugriffsberechtigungen versehen werden. Sicherheitseinstellungen können deshalb so konfiguriert werden, dass nur ein Administrator sie setzen kann.

Zugriffsberechtigungen setzen

In älteren Windows-Versionen konnten die Registry-Zugriffsberechtigungen nur über das Werkzeug *REGEDT32.EXE* eingesehen und gesetzt werden. Seit Windows XP ist diese Fähigkeit in *REGEDIT.EXE* integriert.

Um zu bestimmen, welche Benutzer in welcher Weise auf Informationen in der Registry zugreifen können, starten Sie bei Windows 2000 zum Beispiel über *Ausführen* im Startmenü *REGEDT32* und navigiern zum Eintrag oder Schlüssel. Dann wählen Sie *Sicherheit – Berechtigungen*.

Tobias Weltner, Kai Wilke, Björn Schneider: Windows-Sicherheit - Das Praxisbuch: ISBN: 3-86063-686-3. Microsoft Press 2002

Bei Windows XP startet man stattdessen *REGEDIT.EXE* und klickt den Registry-Schlüssel in der linken Spalte mit der rechten Maustaste an. Wählen Sie anschließend aus dem Kontextmenü *Berechtigungen*.

In beiden Fällen öffnet sich ein Dialogfenster, mit dem bestimmt wird, wer welche Zugriffsrechte erhält (Abbildung 21.1). Zur Verfügung stehen Vollzugriff (*Lesen, Ändern, Löschen*) und Lesen.

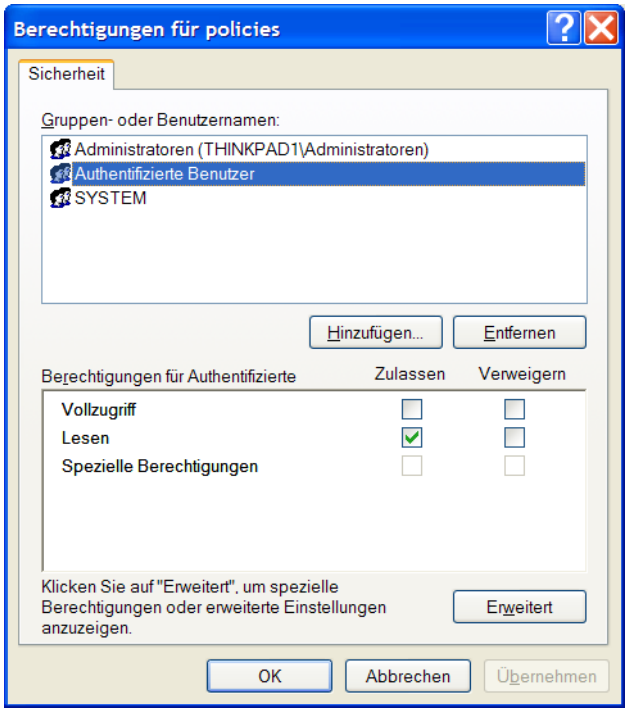

Abbildung 21.1: *Zugriffsberechtigungen für einzelne Registry-Zweige festlegen*

Über die Schaltfläche *Erweitert* stehen alle Basisberechtigungen zur Auswahl. Hier wird auch deutlich, dass Berechtigungen in der Registry ebenso wie im Dateisystem vererbbar sind (Abbildung 21.2). Mit einer einzigen Zugriffsberechtigung lassen sich so ganze Registry-Zweige schützen.

Tobias Weltner, Kai Wilke, Björn Schneider: Windows-Sicherheit - Das Praxisbuch: ISBN: 3-86063-686-3. Microsoft Press 2002

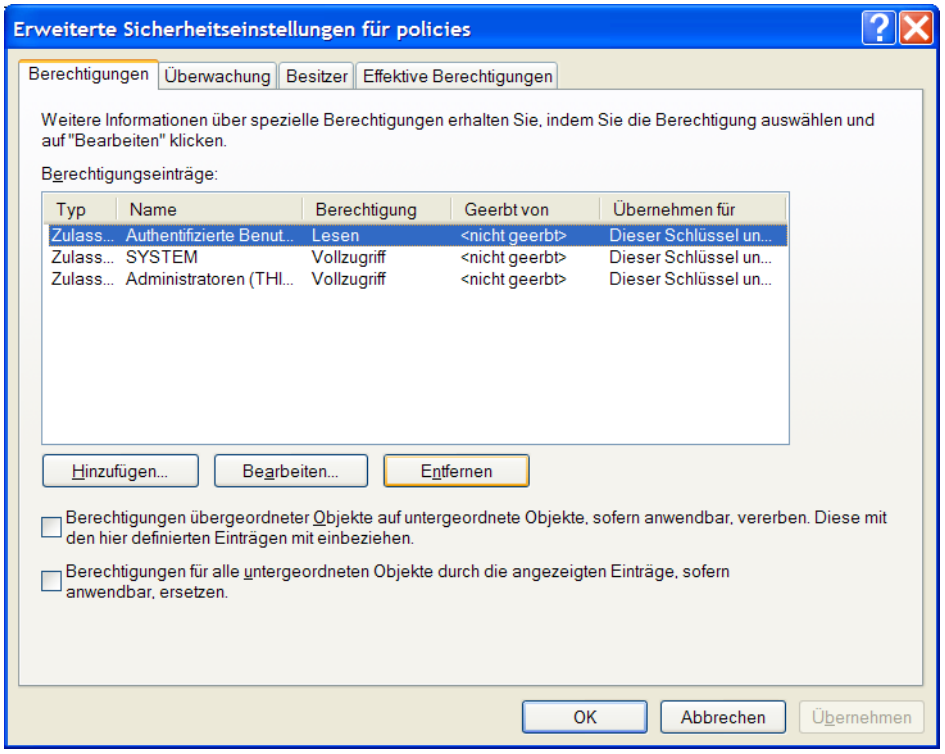

Abbildung 21.2: *Berechtigungen in der Registry sind vererbbar*

Glücklicherweise brauchen sich Administratoren nur in den seltensten Fällen selbst um die Absicherung der Registry-Zweige zu kümmern. Windows 2000 schützt bei der Installation alle systemrelevanten Registry-Zweige automatisch. Welche Berechtigungen dabei typischerweise für die Gruppen *Hauptbenutzer* und *Benutzer* vergeben werden, zeigt Tabelle 21.1. Die Gruppe der *Administratoren* erhält jeweils Vollzugriff.

Handlungsbedarf besteht also nur, wenn weitere eigene Zweige angelegt und geschützt werden sollen oder wenn die Basissicherheit, die Windows 2000 implementiert, als nicht ausreichend angesehen wird.

Registry Objekt	Hauptbenutzer	Benutzer
HKLM\Software	Ändern	Lesen
HKLM\SW\Classes\helpfile	Lesen	Lesen
HKLM\SW\Classes\.hlp	Lesen	Lesen
HKLM\SW\MS\Command Processor	Lesen	Lesen
HKLM\SW\MS\Cryptography	Lesen	Lesen
HKLM\SW\MS\Driver Signing	Lesen	Lesen
HKLM\SW\MS\EnterpriseCertificates	Lesen	Lesen
HKLM\SW\MS\Non-Driver Signing	Lesen	Lesen
HKLM\SW\MS\NetDDE	Keine	Keine ▶

Tobias Weltner, Kai Wilke, Björn Schneider: Windows-Sicherheit - Das Praxisbuch: ISBN: 3-86063-686-3. Microsoft Press 2002

Registry Objekt	Hauptbenutzer	Benutzer
HKLM\SW\MS\Ole	Lesen	Lesen
HKLM\SW\MS\Rpc	Lesen	Lesen
HKLM\SW\MS\Secure	Lesen	Lesen
HKLM\SW\MS\SystemCertificates	Lesen	Lesen
HKLM\SW\MS\Windows\CV\RunOnce	Lesen	Lesen
HKLM\SW\MS\W NT\CV\DiskQuota	Lesen	Lesen
HKLM\SW\MS\W NT\CV\Drivers32	Lesen	Lesen
HKLM\SW\MS\W NT\CV\Font Drivers	Lesen	Lesen
HKLM\SW\MS\W NT\CV\FontMapper	Lesen	Lesen
HKLM\SW\MS\W NT\CV\Image File Execution Options	Lesen	Lesen
HKLM\SW\MS\W NT\CV\IniFileMapping	Lesen	Lesen
HKLM\SW\MS\W NT\CV\Perflib	Lesen (via *INTERAKTIV*)	Lesen (via *INTERAKTIV*)
HKLM\SW\MS\W NT\CV\SecEdit	Lesen	Lesen
HKLM\SW\MS\W NT\CV\Time Zones	Lesen	Lesen
HKLM\SW\MS\W NT\CV\Windows	Lesen	Lesen
HKLM\SW\MS\W NT\CV\AsrCommands	Lesen	Lesen
HKLM\SW\MS\W NT\CV\Winlogon	Lesen	Lesen
HKLM\SW\MS\W NT\CV\Classes	Lesen	Lesen
HKLM\SW\MS\W NT\CV\Console	Lesen	Lesen
HKLM\SW\MS\W NT\CV\ProfileList	Lesen	Lesen
HKLM\SW\MS\W NT\CV\Svchost	Lesen	Lesen
HKLM\SW\Policies	Lesen	Lesen
HKLM\System	Lesen	Lesen
HKLM\SYSTEM\CCS\Control\SecurePipeServers\winreg	Keine	Keine
HKLM\SYSTEM\CCS\Control\Session Manager\Executive	Ändern	Lesen
HKLM\SYSTEM\CCS\Control\TimeZoneInformation	Ändern	Lesen
HKLM\SYSTEM\CCS\Control\WMI\Security	Keine	Keine
HKLM\Hardware	Lesen (via *Jeder*)	Lesen (via *Jeder*)
HKLM\SAM	Lesen (via *Jeder*)	Lesen (via *Jeder*)
HKLM\Security	Keine	Keine
USERS\DEFAULT	Lesen	Lesen
USERS\DEFAULT\SW\MS\NetDDE	Keine	Keine
HKEY_CURRENT_USER	Vollzugriff	Vollzugriff

Tabelle 21.1: *Automatisch implementierte Registry-Berechtigungen*

Tobias Weltner, Kai Wilke, Björn Schneider: Windows-Sicherheit - Das Praxisbuch: ISBN: 3-86063-686-3. Microsoft Press 2002

Abkürzungen:

- *HKLM* = HKEY_LOCAL_MACHINE
- *USERS* = HKEY_USERS
- SW = Software
- *MS* = Microsoft
- *CV* = CurrentVersion
- *CCS* = CurrentControlSet
- *W NT* = Windows NT

Überprüfen der Basis-Berechtigungen

Ob die Registry-Zweige (noch) wie in Tabelle 21.1 geschützt sind, kann die Sicherheitsanalyse aufdecken. Sie vergleicht die aktuellen Berechtigungen der Registry mit den Vorgaben aus der entsprechenden Sicherheitsvorlage, die während der Installation auf die Registry angewendet wurde.

Sollten Berechtigungen in der Zwischenzeit geändert worden sein, markiert die Analyse diese Zweige mit einem roten Warnsymbol.

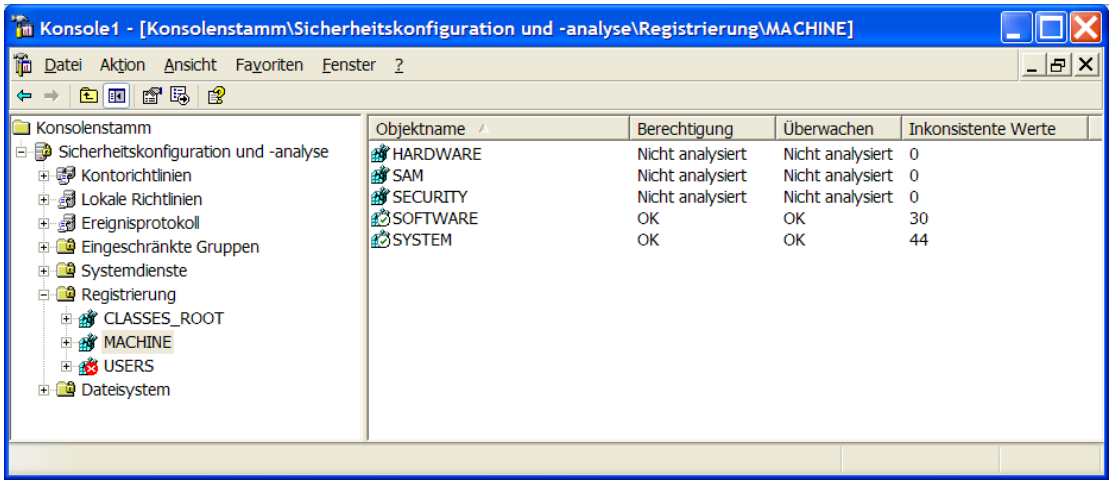

Abbildung 21.3: *Automatische Analyse der Registry-Berechtigungen*

Praxis: Sicherheitsanalyse Registry-Zugriffsberechtigungen

So gehen Sie vor, um die Basissicherung der Registry zu überprüfen:

1. Wählen Sie im Startmenü *Ausführen*, und geben Sie `MMC` ein und drücken Sie anschließend die EINGABETASTE. Eine leere Microsoft Management Console öffnet sich.
2. Drücken Sie STRG+M, um ein neues Snap-In hinzuzufügen, und klicken Sie auf *Hinzufügen*. Wählen Sie das Snap-In *Sicherheitskonfiguration und -analyse* aus, und klicken Sie auf *Schließen*.
3. Klicken Sie auf *OK*. Das Snap-In ist nun einsatzbereit. Klicken Sie in der linken Spalte mit der rechten Maustaste auf *Sicherheitskonfiguration und -analyse*, und wählen Sie *Datenbank öffnen*. Geben Sie einen Namen für die zu erstellende Analysedatenbank an.

4. Geben Sie nun die Sicherheitsvorlage an, gegen die das System geprüft werden soll. Für Windows 2000 Professional wählen Sie *%WINDIR%\Inf\defltwk.inf*, für Windows 2000 Server *defltsv.inf* oder *defltdc.inf* (Domänencontroller).
5. Klicken Sie in der linken Spalte noch einmal auf *Sicherheitskonfiguration und -analyse*, und wählen Sie *Computer jetzt analysieren*. Bestätigen Sie die vorgeschlagene Logdatei. Das System wird überprüft.
6. Öffnen Sie nach der Überprüfung den Zweig *Registrierung* (Abbildung 21.3). Hier sehen Sie alle überprüften Hauptäste der Registry. Klicken Sie auf einen dieser Äste, um in der rechten Spalte zu lesen, ob darin Inkonsistenzen gefunden wurden.

Zwar können Abweichungen von der Sicherheitsvorlage direkt in der MMC nachgeschlagen werden, wesentlich informativer ist aber das während der Analyse angelegte Log. Es meldet kurz und bündig alle Einstellungen, die nicht den Einstellungen der Sicherheitsvorlage entsprachen.

Dasselbe Resultat kann auch über die Kommandozeile mit *SecEdit* erreicht werden. Der Befehl dazu könnte lauten:

```
Secedit /analyze /db c:\sec.sdb /cfg %windir%\inf\defltwk.inf /log c:\log.txt
```

Das Log ist relativ umfangreich, weil jeweils nur die gesamte Sicherheitsvorlage überprüft werden kann. Es enthält deshalb auch Informationen zum Beispiel über inkonsistente Dateisystemberechtigungen (Abbildung 21.4).

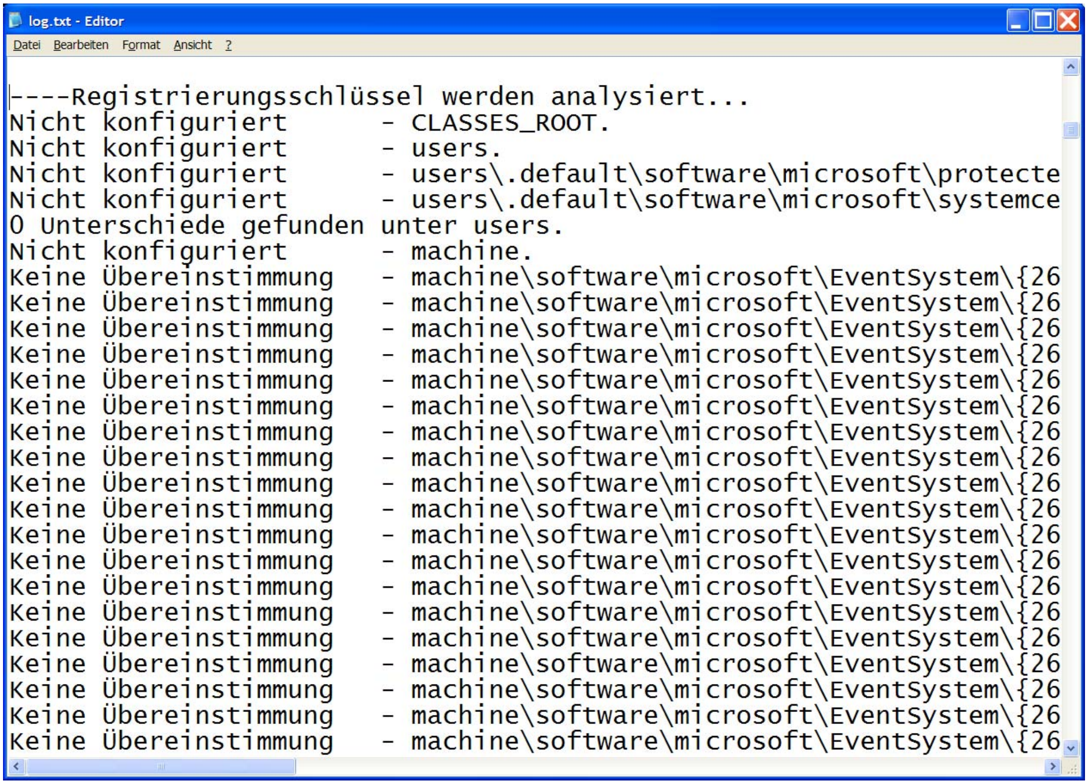

Abbildung 21.4: *Ausführliche Informationen über Inkonsistenzen in der Logdatei*

Tobias Weltner, Kai Wilke, Björn Schneider: Windows-Sicherheit - Das Praxisbuch: ISBN: 3-86063-686-3. Microsoft Press 2002

Inkonsistenzen können sich aus verschiedenen Gründen ergeben, zum Beispiel:

- Die Zugriffsberechtigungen eines Zweiges entsprechen nicht denen der Vorlage.
- Der überprüfte Zweig verwendet eigene Zugriffsberechtigungen, obwohl er laut Vorlage die Berechtigungen des übergeordneten Zweiges erben sollte.

Basis-Sicherheit wiederherstellen

Die Registry-Zugriffsberechtigungen aus der Sicherheitsvorlage können jederzeit erneut auf das System angewendet werden. Dies darf allerdings nur geschehen, wenn Sie sich absolut sicher sind, dass die darin festgelegten Zugriffsberechtigungen für Ihre Einsatzzwecke geeignet sind. Möglicherweise wurden die Zugriffsberechtigungen in der Registry absichtlich angepasst und würden durch das erneute Anwenden der Sicherheitsvorlage in den Ausgangszustand zurückversetzt.

Das *Sicherheitskonfigurations- und -analyse*-Snap-In kann die Sicherheitseinstellungen der Vorlage nur insgesamt auf das System anwenden. Um selektiv nur die darin festgelegten Regsitry-Berechtigungen zu setzen, wenden Sie den Konsolenbefehl *SECEDIT* an. Für Windows 2000 Professional könnte der Befehl so aussehen:

```
Secedit /configure /db %temp%\sec.sdb /cfg %windir%\inf\defltwk.inf /areas
regkeys /log c:\log.txt /overwrite
```

Eine anschließende erneute Analyse zeigt, ob die Änderungen wie gewünscht umgesetzt wurden.

Bevor Sie die mitgelieferten Sicherheitsvorlagen auf Produktivsystemen anwenden, informieren Sie sich zuerst in ▶ Teil F: »Dateisystemsicherheit« über alle Vorlagen, die zur Verfügung stehen, und testen Sie die Auswirkungen dieser Vorlagen auf speziellen Testsystemen.

Netzwerkzugriff kontrollieren

Der allgemeine Zugriff auf die Registry wird über die Zugriffsberechtigungen der einzelnen Zweige und Einträge wie oben beschrieben kontrolliert und erfordert meist keine weiteren Eingriffe. Die Basisabsicherung schützt automatisch alle sicherheitsrelevanten Bereiche.

Ein ganz anderes Risiko betrifft die Anwendergruppe, die sich Zugriff auf die Registry-Informationen verschaffen kann. Die meisten Informationen in der Registry werden nämlich nur in Hinblick auf Schreibberechtigungen geschützt, damit sichergestellt ist, dass reguläre Anwender nicht etwa zentral konfigurierte Sicherheitseinstellungen ihrer Rechner von Hand außer Kraft setzen.

Lesezugriff auf die Registry ist dagegen allen *Authentifizierten Benutzern* gestattet. Da die Registry vielfältige Detailinformationen über das System enthält, müssen diese Informationen insbesondere vor unbefugtem Netzwerkzugriff geschützt werden.

Als Standard gewährt Windows 2000 allen Benutzern Netzwerkzugriff auf die Registry, die in den Gruppen *Administratoren* oder *Sicherungs-Operatoren* Mitglied sind.

Tobias Weltner, Kai Wilke, Björn Schneider: Windows-Sicherheit - Das Praxisbuch: ISBN: 3-86063-686-3. Microsoft Press 2002

Netzwerkzugriff testen

Der Netzwerkzugriff auf die Registry ist auf vielfältigem Wege möglich.

Praxis: Netzwerkzugriff auf die Registry eines anderen Systems

So können Sie den Netzwerkzugriff selbst testen:

1. Wählen Sie im Startmenü *Ausführen*, geben Sie REGEDIT ein und drücken Sie anschließend die EINGABETASTE. Der Registrierungseditor startet.
2. Wählen Sie *Datei – Mit Netzwerkregistrierung verbinden*, und geben Sie den Rechnernamen an, mit dem Sie sich verbinden wollen. Melden Sie sich mit einem lokalen Administrator-Konto und Kennwort an.
3. Der Registrierungseditor verbindet sich über das Netzwerk mit der fremden Registry und zeigt deren Inhalt an.

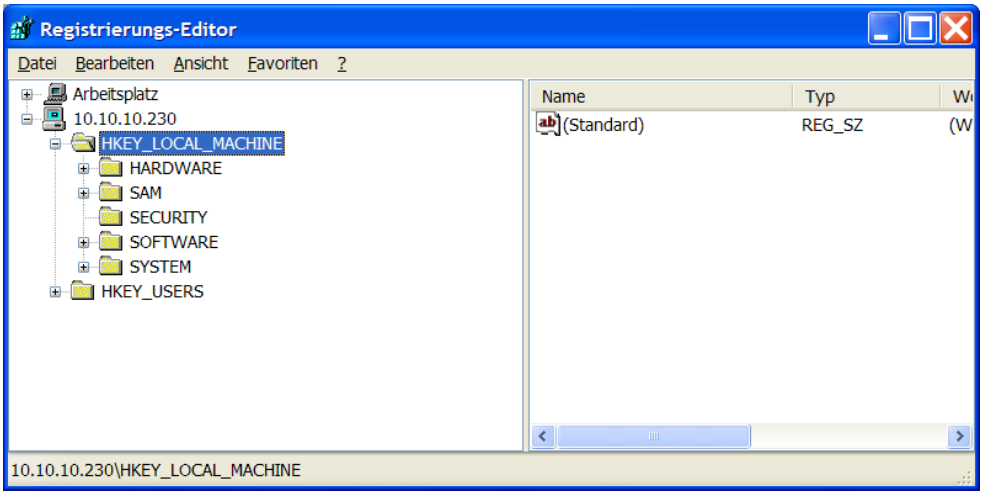

Abbildung 21.5: *Ferngesteuert auf eine fremde Registry zugreifen*

Netzwerkzugriff unterbinden

Der Netzwerkzugriff auf die Registry wird über einen Registry-Eintrag kontrolliert. Jeder Benutzer, der Zugriffsberechtigungen auf den Schlüssel *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg* besitzt, ist berechtigt, die Registry abzufragen. Als Standard wird dieser Zugriff nur der Gruppe der *Administratoren* und der *Sicherungs-Operatoren* gewährt.

Um den Netzwerkzugriff auf die Registry zu kontrollieren, setzen Sie die Berechtigungen auf diesen Schlüssel. Dazu wird bei Windows 2000 *REGEDT32.EXE* eingesetzt, bei Windows XP *REGEDIT.EXE*.

Daneben können die Berechtigungen auch zentral über Gruppenrichtlinien zugewiesen werden.

Praxis: Netzwerkzugriff auf Registry beschränken (Windows 2000)

1. Wählen Sie im Startmenü *Ausführen*, und geben Sie REGEDT32 ein. Drücken Sie anschließend die EINGABETASTE. Der Registrierungseditor startet.

Tobias Weltner, Kai Wilke, Björn Schneider: Windows-Sicherheit - Das Praxisbuch: ISBN: 3-86063-686-3. Microsoft Press 2002

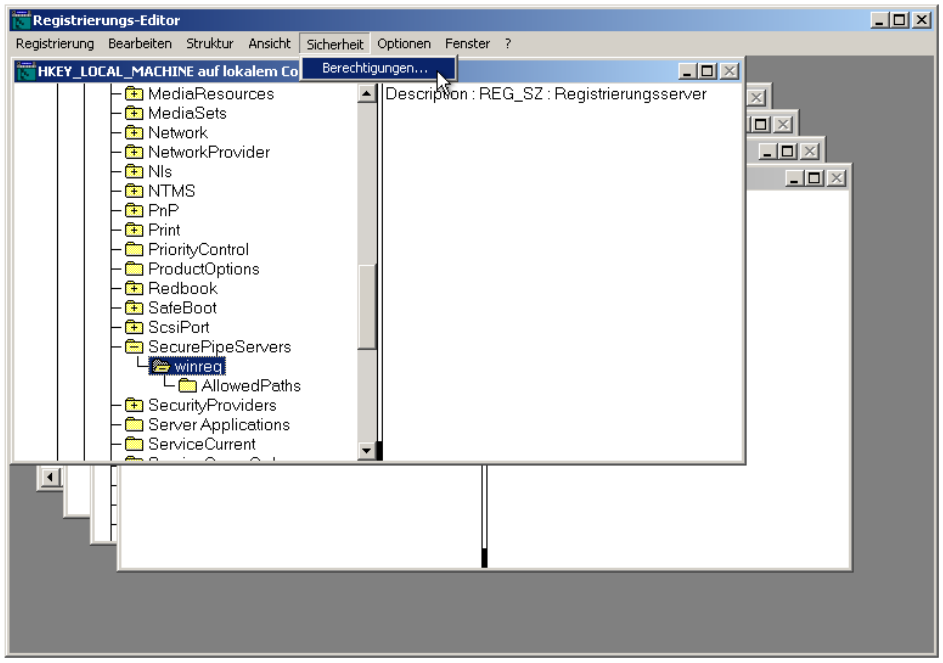

Abbildung 21.6: *Mit REGEDT32.EXE den Netzwerkzugriff auf die Registry verbieten*

2. Wählen Sie das Fenster *HKEY_LOCAL_MACHINE*, und navigieren Sie zum Eintrag *SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg*. Markieren Sie den Schlüssel *winreg*, und wählen Sie *Sicherheit – Berechtigungen*.
3. Ein Dialogfenster erscheint, mit dem Sie die Zugriffsberechtigungen auf diesen Schlüssel festlegen. Ändern Sie die Vorgabe, wenn Sie selbst den Netzwerkzugriff auf die Registry kontrollieren wollen.

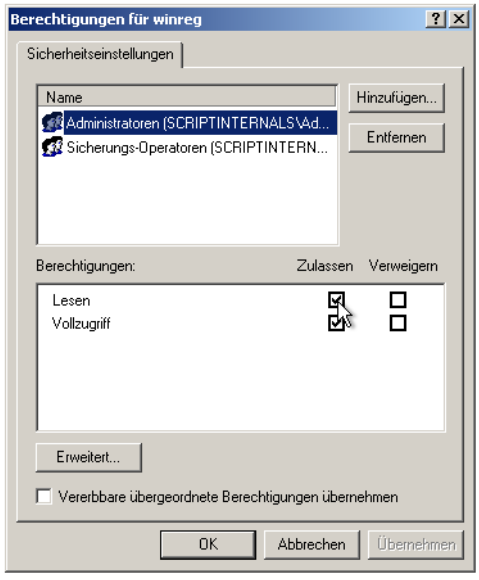

Abbildung 21.7: *Bestimmen Sie, welche Personen Netzwerkzugriff auf die Registry haben*

Tobias Weltner, Kai Wilke, Björn Schneider: Windows-Sicherheit - Das Praxisbuch: ISBN: 3-86063-686-3. Microsoft Press 2002

Windows XP

Bei Windows XP funktioniert die Einstellung prinzipiell gleich, jedoch wird hier *REGEDIT* gestartet. Klicken Sie dann den Schlüssel *WinReg* mit der rechten Maustaste an, und wählen Sie im Kontextmenü Berechtigungen.

Ausnahmen für den Netzwerkzugriff erlauben

Wenn Sie den Netzwerkzugriff auf die Registry unterbinden, dann denken Sie daran, dass einige Dienste diesen Zugriff brauchen, um ordnungsgemäß arbeiten zu können. Dazu zählen zum Beispiel der *Directory Replicator* Dienst und auch der Druckspooler, wenn auf Drucker über das Netzwerk zugegriffen wird.

Entweder fügt man die dafür notwendigen Berechtigungen direkt in den *winreg*-Schlüssel ein. Der Dienst erhält so uneingeschränkten Zugriff auf die Registry. Oder aber man formuliert Ausnahmen.

Registry-Schlüssel, die als Ausnahmen in den Untereintrag *AllowedPaths* eingetragen werden, fallen nicht unter die Netzwerkbeschränkungen und stehen allen Benutzern offen. Dies ist die Vorgabe.

Um sich zu informieren, welche Schlüssel von der Netzwerkbeschränkung nicht betroffen sind, öffnen Sie den *AllowedPath*-Eintrag. Dies ist ein *MultiString*-Eintrag, der erst beim Öffnen den gesamten Inhalt anzeigt.

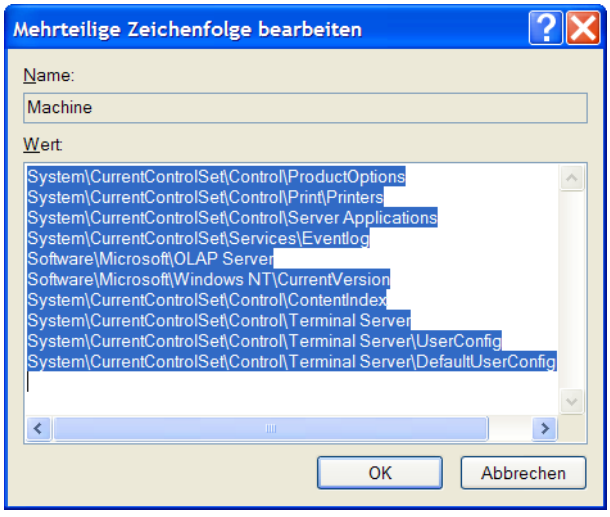

Abbildung 21.8: *Standardmäßig von der Netzwerksicherheit ausgenommene Schlüssel*

Lücken in der Netzwerksicherheit

Es gibt viele Wege nach Rom. Trotz der Netzwerkzugriffsbeschränkungen können Anwender unter Umständen nach wie vor auch über das Netzwerk auf die Registry von Remoterechnern zugreifen.

Dazu verbinden sich die Benutzer zuerst mit einem lokalen Fernverwaltungsdienst auf der betreffenden Maschine wie zum Beispiel WMI. Anschließend wird die lokale WMI des Zielrechners beauftragt, die Registry abzufragen und das Ergebnis über das Netzwerk an den Aufrufer zurückzuliefern. Weil es hierbei nicht zu einem direkten Netzwerkzugriff auf die Registry kommt, bleiben die Berechtigungen des *winreg*-Schlüssels ohne Bedeutung.

Tobias Weltner, Kai Wilke, Björn Schneider: Windows-Sicherheit - Das Praxisbuch: ISBN: 3-86063-686-3. Microsoft Press 2002

Das folgende Skript zeigt den technischen Ansatz. Dazu erfragt das Skript zunächst den Namen des Computers, dessen Registry abgefragt werden soll, sowie das Benutzerkonto und das zugehörige Kennwort, mit dem der Netzwerkzugriff getestet werden soll.

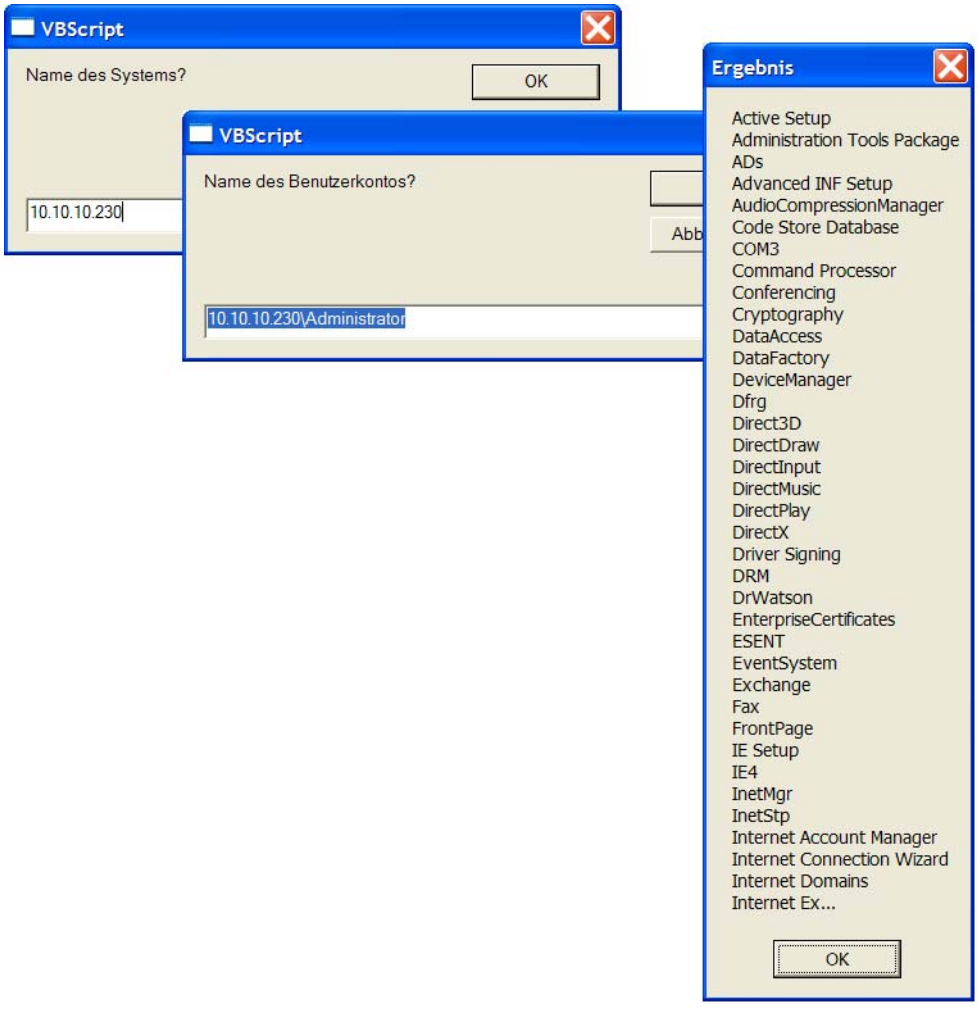

Abbildung 21.9: *Fernabfrage der Registry per Skript testen*

Anschließend wird versucht, die Registry des gewünschten Systems zu kontaktieren. Voraussetzung dafür sind lediglich Administrator-Berechtigungen, und der Zugriff gelingt selbst dann, wenn der Registry-Schlüssel *winreg* eigentlich niemandem Zugriffsberechtigungen erteilt.

```
' ************************************************
' *
' * Fernzugriff auf die Registry
' *
' ************************************************

' Registry-Wurzel
```

```
Const HKEY_LOCAL_MACHINE = &h80000002
' abzufragender Key
Const KEY = "Software\Microsoft"

' Kontaktdaten erfragen
SERVER = InputBox("Name des Systems?")
USER = InputBox("Name des Benutzerkontos?",,SERVER & "\Administrator")
PWD = InputBox("Kennwort?")

' mit System fernverbinden
Set locator = CreateObject("WbemScripting.SWbemLocator")

On Error Resume Next
Set wmi = locator.ConnectServer(SERVER, "root\default", USER, PWD)
errcode = Hex(err.number)
If errcode = "800706BA" then
   ' nicht erfolgreich, Server nicht gefunden
   MsgBox "Server nicht gefunden."
   WScript.Quit
ElseIf not err.number=0 then
   ' nicht erfolgreich, anderer Grund
   MsgBox "Zugriff nicht möglich. Fehler &h" & errcode
   WScript.Quit
End If
On Error Goto 0

' WMI-Registry-Fernabfragefunktionen einbinden
Set instance = wmi.Get("StdRegProv")

' Unterschlüssel des Keys abfragen
retval = instance.EnumKey(HKEY_LOCAL_MACHINE,KEY,ergebnis)

' erfolgreich?
If retval = 0 then
   ' ja, Feld in Text umwandeln und erste 500 Zeichen ausgeben
   MsgBox Left(Join(ergebnis, vbNewLine),500) & "...",,"Ergebnis"
Else
   ' nein
   MsgBox "Zugriff nicht möglich. Fehler-Code " & retval,vbExclamation + vbSystemModal
End If
```

Listing 21.1: *Skript zur Fernabfrage der Registry*

Abwärtskompatibilität herstellen

Eines der größten Praxisprobleme bei der Umstellung auf Windows 2000 ist die Abwärtskompatibilität zu älterer Software. Ältere Software speichert nicht selten Informationen in Registry-Zweigen, die für normale Benutzer gesperrt sind bzw. in denen normale Benutzer keine Schreibberechtigungen haben.

Tobias Weltner, Kai Wilke, Björn Schneider: Windows-Sicherheit - Das Praxisbuch: ISBN: 3-86063-686-3. Microsoft Press 2002

Sicherheitsberechtigungen lockern

Der Grund dafür ist das geänderte Sicherheitsmodell von Windows 2000: Normale Benutzer haben bei Windows 2000 nicht mehr dieselben Berechtigungen wie Windows NT-Benutzer. Stattdessen wird der Zugriff auf alle Ordner und Registry-Schlüssel verweigert, die Einfluss auf andere Benutzer haben und also nicht im Benutzerprofil bzw. der Registry-Hive *HKEY_CURRENT_USER* liegen.

Es existieren zwei offizielle und ein inoffizielles Workaround. Dies sind die beiden Workarounds, die Microsoft offiziell empfiehlt:

- Benutzer, die Probleme mit älterer Anwendungssoftware haben, können zum Mitglied in der Gruppe der *Hauptbenutzer* gemacht werden. Hauptbenutzer verfügen über die Berechtigungen, die NT-Benutzer hatten. Allerdings sind Hauptbenutzer mit einer Fülle weiterer Privilegien ausgestattet, so dass dieser Weg zwar schnell und bequem einzurichten ist, die Sicherheit aber in weiten Bereichen aushebelt. Hauptbenutzer haben zum Beispiel das Recht, neue Benutzerkonten anzulegen – sicher keine Sache, die man regulären Benutzern zustehen möchte.
- Über die Sicherheitsvorlage *COMPATWS.INF* können die Berechtigungen für bestimmte Ordner und Registry-Zweige auf NT 4.0-Niveau gelockert werden. Auf diese Weise erhalten einfache Benutzer ebenfalls die für ältere Software notwendigen höheren Berechtigungen zurück.

In beiden Fällen wird die Systemsicherheit generell abgesenkt, wenn auch in unterschiedlich starkem Maße.

Maßgeschneiderte Abwärtskompatibilität

Häufig sind im Unternehmen nur ganz wenige ältere Anwendungen unersetzlich. Spielt Sicherheit eine große Rolle – und das sollte sie fast immer – dann kann man von den allgemeinen Sicherheitslockerungen auch absehen und stattdessen mit Tools wie *FILEMON* und *REGMON* (kostenlos bei *http://www.sysinternals.com* beziehbar) die Berechtigungen maßgeschneidert nur in den unumgänglichen Bereichen absenken.

FILEMON protokolliert in Echtzeit Dateisystemzugriffe, *REGMON* tut dasselbe für Registry-Zugriffe. Damit kann ein Administrator die ältere problematische Software installieren und testweise einsetzen. Die von *REGMON* und *FILEMON* dabei generierten Protokolle zeigen sofort, auf welche Ordner und Registry-Zweige das Programm tatsächlich zugreift.

Der Administrator legt darauf hin eine neue Gruppe an und weist dieser Gruppe Zugriffsberechtigungen auf die ermittelten Bereiche zu. Anschließend können die Benutzerkonten, die die ältere Software einsetzen müssen, zum Mitglied in dieser Gruppe gemacht werden.

Tobias Weltner, Kai Wilke, Björn Schneider: Windows-Sicherheit - Das Praxisbuch: ISBN: 3-86063-686-3. Microsoft Press 2002

Tobias Weltner, Kai Wilke, Björn Schneider: Windows-Sicherheit - Das Praxisbuch: ISBN: 3-86063-686-3. Microsoft Press 2002