

**INSTITUT FÜR INFORMATIK**  
DER LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN



**Fortgeschrittenenpraktikum**

**Entwicklung einer Methode zur  
effizienten Wartung der Windows Clients im  
CIP-Pool der Informatik**

Andreas Heindel  
Thomas Rickinger

Aufgabensteller: Prof. Dr. H.G. Hegering  
Betreuer: Annette Kosteletzky

# Inhaltsverzeichnis

<b>1. Einleitung</b>	3
<b>2. Allgemeines</b>	3
<b>3. Symantec Ghost AutoInstall (AI)</b>	4
3.1 Erstellen eines Distributionspakets auf dem Modellcomputer.....	5
3.1.1 Allgemeines .....	5
3.1.2 Vorgehensweise .....	5
3.2 Weiterverarbeitung des Distributionspakets.....	12
3.2.1 Allgemeines .....	12
3.2.2 Entfernen der Einträge „\$CurUserDir\$“ und „HKEY_CURRENT_USER“.....	12
3.2.3 Hinzufügen einer Deinstallations-Option.....	17
3.3 Verteilen des AI-Pakets vom Server auf die Clients.....	18
3.3.1 Erstellen eines Installationsvorganges für ein AI-Paket.....	18
3.3.2 Erstellen eines Deinstallationsvorganges für ein AI-Paket.....	25
3.4 Automatische Installation von AI-Paketen mittels Zeitplaner.....	27
3.4.1 Erstellen eines zeitversetzten Installationsvorganges.....	27
3.5. Weitere Hinweise zum Einsatz von Symantec Ghost AutoInstall in der CIP- Umgebung .....	32
<b>4. Microsoft Software Update Service (SUS)</b>	35
4.1 Konfiguration des SUS-Servers .....	35
4.2 Konfiguration der Clientrechner .....	43
4.2.1 Manuelle Konfiguration .....	43
4.2.2 Konfiguration mittels Systemrichtlinie.....	46
<b>5. Schluss</b>	53
<b>6. Quellenverzeichnis</b>	54
<b>7. Anhang</b>	55

## 1. Einleitung

Das Institut für Informatik stellt für Studenten Rechnerarbeitsplätze in sogenannten CIP-Pools zur Verfügung. In diesen Pools können die Studenten begleitende Übungen zu den Vorlesungen sowie anfallende rechnergestützte Arbeiten im Rahmen des Studiums verrichten. Seit dem Wintersemester 02/03 stehen neben den bisherigen Linux Rechnern auch 20 Arbeitsplatzrechner mit Windows 2000 Professional als Betriebssystem zur Verfügung. Für die Wartung der Rechner ist die RBG, eine kleine Gruppe von Personen, mit unter auch studentische Hilfskräfte, verantwortlich.

Mit dieser Anzahl an Rechnern ist bereits eine Größenordnung erreicht, die eine zentrale Lösung unabdingbar macht. Daher soll im Rahmen dieses Praktikums eine Methode entwickelt werden, mittels der die Windows Clients in effizienter Weise gewartet werden können.

Hierzu sollen in einem ersten Schritt bekannte SW Produkte wie zum Beispiel „Ghost“ oder Microsofts „Software Update Service (SUS)“ untersucht werden, in wie weit diese für die Pflege der Clients geeignet sind. Im Anschluss daran soll die entwickelte Methode auf einen zentralen Server umgesetzt und getestet werden.

## 2. Allgemeines

Sowohl bei der „**AI-Funktion**“ von Symantec Ghost als auch bei Microsofts „**System Update Service**“ muss zum Zeitpunkt der geplanten Distribution auf den Zielrechnern Windows 2000 laufen. Läuft in diesem Moment Linux, schlägt die Installation der Softwarepakete fehl.

Einige Softwareprodukte und Systemupdates erfordern im Anschluß an die Installation einen Neustart des Rechners.

Werden mit Symantec Ghost mehrere AI-Pakete gleichzeitig installiert, können gegebenenfalls auch mehrere Neustarts notwendig werden. Es wäre daher empfehlenswert, die Boot-Reihenfolge des LILO-Bootmanagers auf den Clientrechnern so zu verändern, dass Windows 2000 primär gestartet wird. Anderenfalls bootet der PC Linux und die Installation kann erst nach einem manuellen Restart fortgesetzt werden.

### 3. Symantec Ghost AutoInstall (AI)

Zur Softwareverteilung mit Hilfe der AutoInstall-Funktion von Symantec muss zuerst ein **Distributionspaket** auf einem **Modellcomputer** erstellt werden. Anschließend kann das neu erstellte Distributionspaket vom Server aus auf die Clientrechner aufgespielt werden. Der Modellcomputer sollte in seiner Hardware- und Softwarekonfiguration möglichst den späteren Zielrechnern entsprechen.

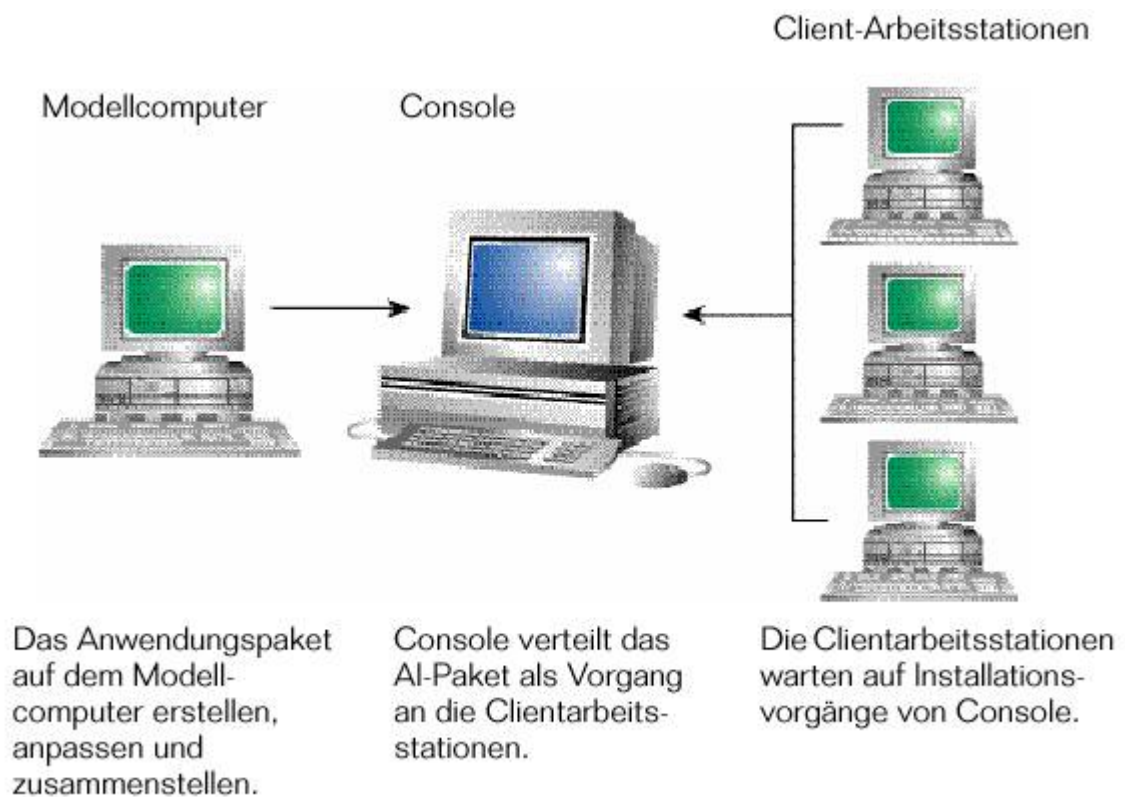


Abb. 1: Funktionsweise der AI-Funktion von Symantec Ghost (Quelle: [SGIh], S. 267).

## 3.1 Erstellen eines Distributionspakets auf dem Modellcomputer

### 3.1.1 Allgemeines

Der Modellcomputer sollte möglichst über die gleiche Hard- und Softwarekonfiguration verfügen. Außerdem empfiehlt es sich, alle im Hintergrund laufenden Anwendungen sowie Autostart-Programme zu deaktivieren, bevor mit „**AI-Snapshot**“ ein Distributionspaket erstellt wird.

### 3.1.2 Vorgehensweise

Zuerst muss auf dem Modellcomputer ein „Schnappschuss“ des aktuellen Systemzustandes erstellt werden. Dies geschieht mit dem Programm „**AI-Snapshot**“ von Symantec Ghost.

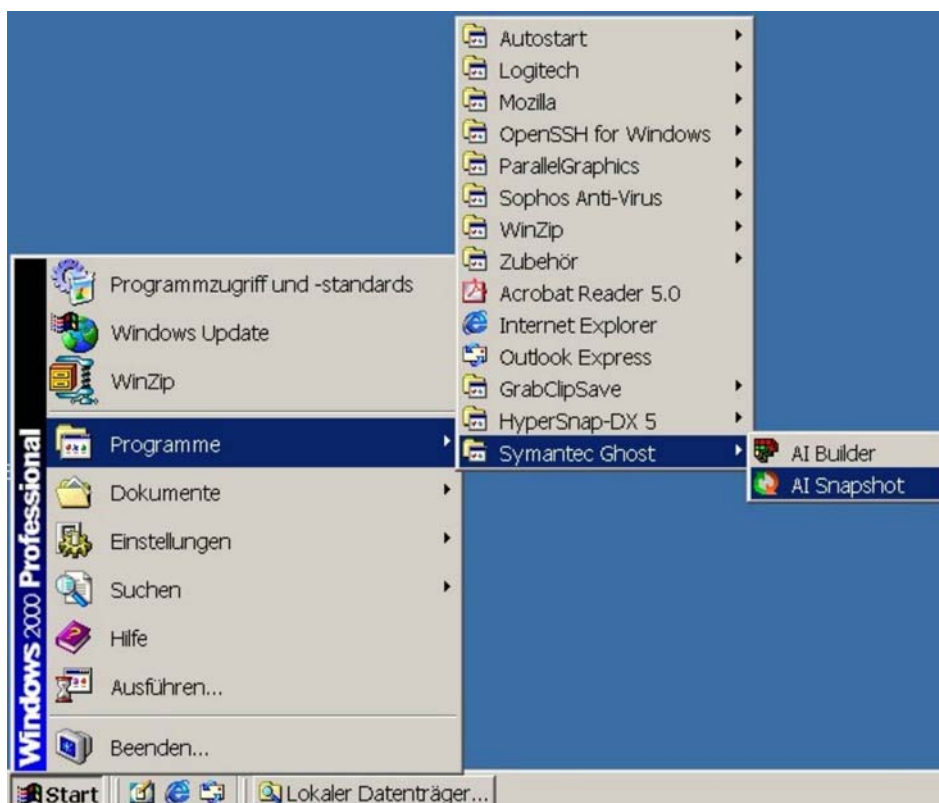


Abb. 2: „AI-Snapshot“ starten.



Abb. 3: Hier klickt man auf „Weiter“. Bei „Optionen“ muss man in der Regel nichts ändern.



Abb. 4: AI-Snapshot erstellt nun ein Abbild des Systemzustandes.

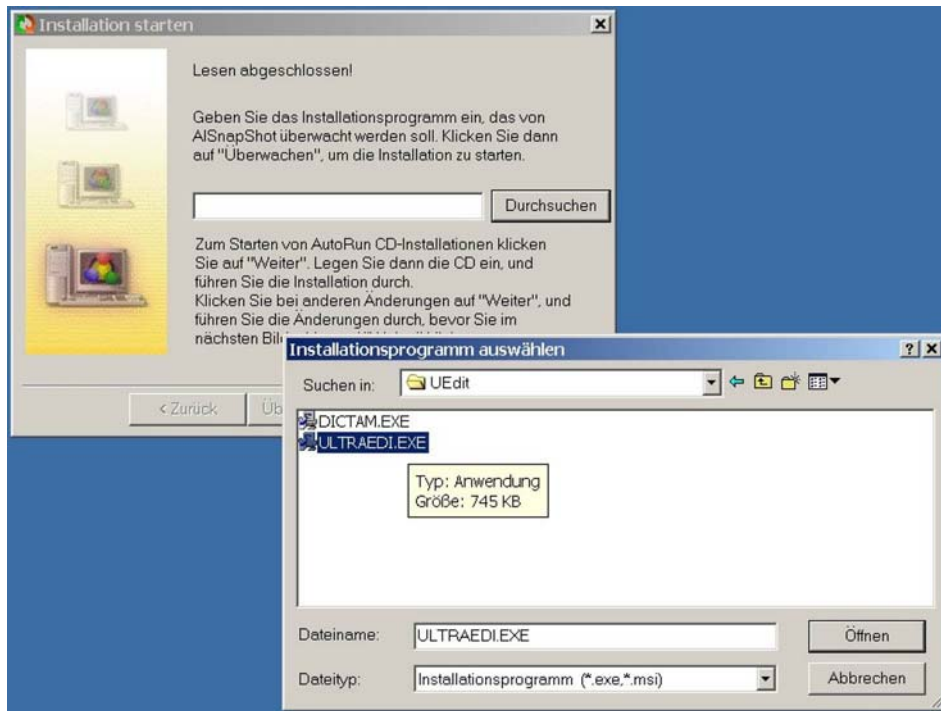


Abb. 5: Sobald der Schnappschuss fertiggestellt wird, muss das Setupprogramm der zu installierenden Anwendung ausgewählt werden. Hierzu klickt man auf „Durchsuchen“ und wählt im neuen Fenster die entsprechende Installationsdatei aus.

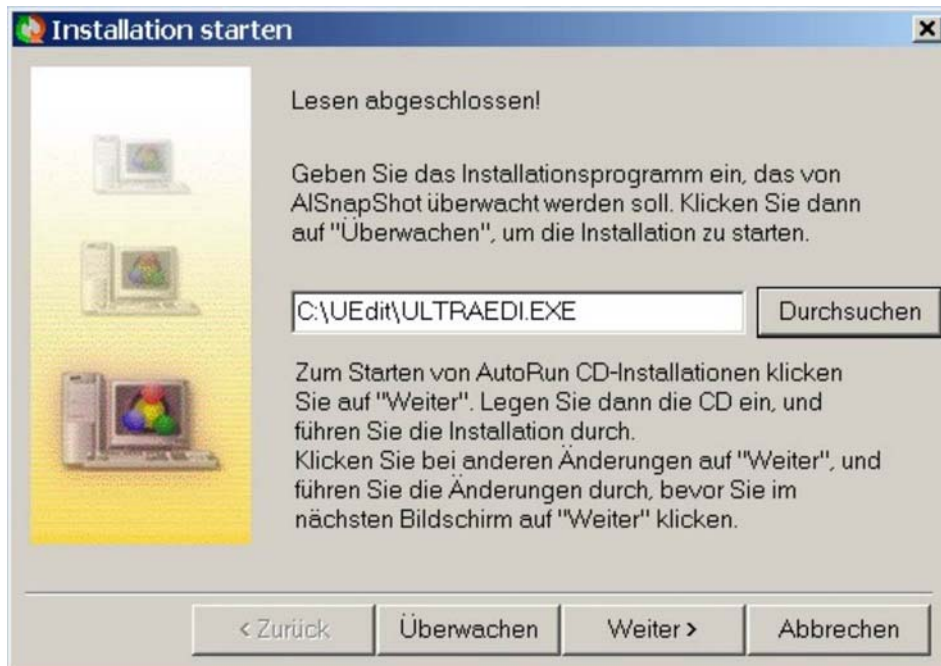


Abb. 6: Anschließend klickt man auf „Überwachen“.

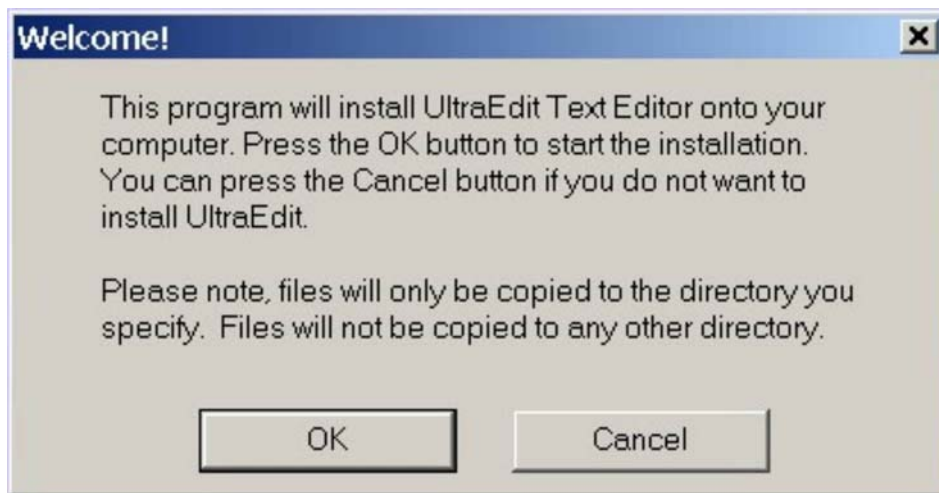


Abb. 7: Jetzt startet das Setup-Programm der Anwendung, von der ein Distributionspaket erzeugt werden soll. Man installiert die Anwendung nun auf die übliche Art und Weise.



Abb. 8: Nach Abschluss der Installation erscheint dieses Fenster. Hier gibt man den gewünschten Namen für das neu erstellte Distributionspaket ein und klickt dann auf „Vergleichen“.

### **Wichtig**

Einige Programme fordern an dieser Stelle zu einem Neustart des Rechners auf. Dies darf man bei Microsoft-Produkten **nicht erlauben**, sondern muss erst das Distributionspaket zusammenstellen lassen (vgl. [SGIh], S. 268). In allen anderen Fällen darf man den Neustart zulassen und das Distributionspaket erst anschließend zusammenstellen lassen.





Abb. 9: Nun erstellt „AI-Snapshot“ einen weiteren Schnappschuss des Systemzustandes.

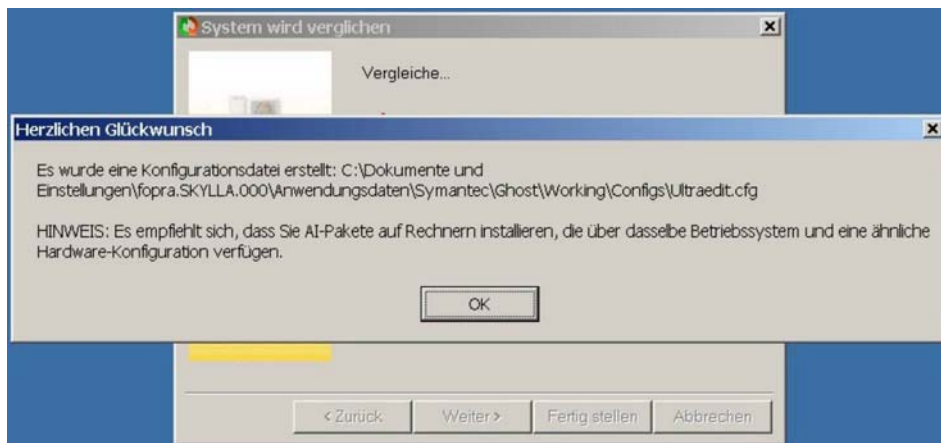


Abb. 10: Aus dem Vergleich zwischen altem und neuem Schnappschuss generiert „AI-Snapshot“ eine Konfigurationsdatei.



Abb. 11: Anschließend kann man das Distributionspaket zusammenstellen lassen. Hierzu klickt man auf „Zusammenstellen“.

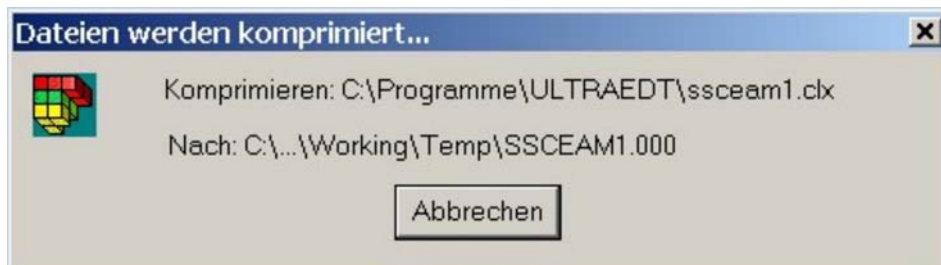


Abb. 12: Nun wird das Distributionspaket zusammengestellt.



Abb. 13: Eine mögliche Fehlermeldung. Hier konnte eine Datei nicht gelesen werden, weil sie von einem anderen Programm verwendet wurde. Derartige Fehler können auftreten, wenn man im Hintergrund laufende Anwendungen und Autostart-Programme nicht deaktiviert, bevor man „AI-Snapshot“ ausführt.

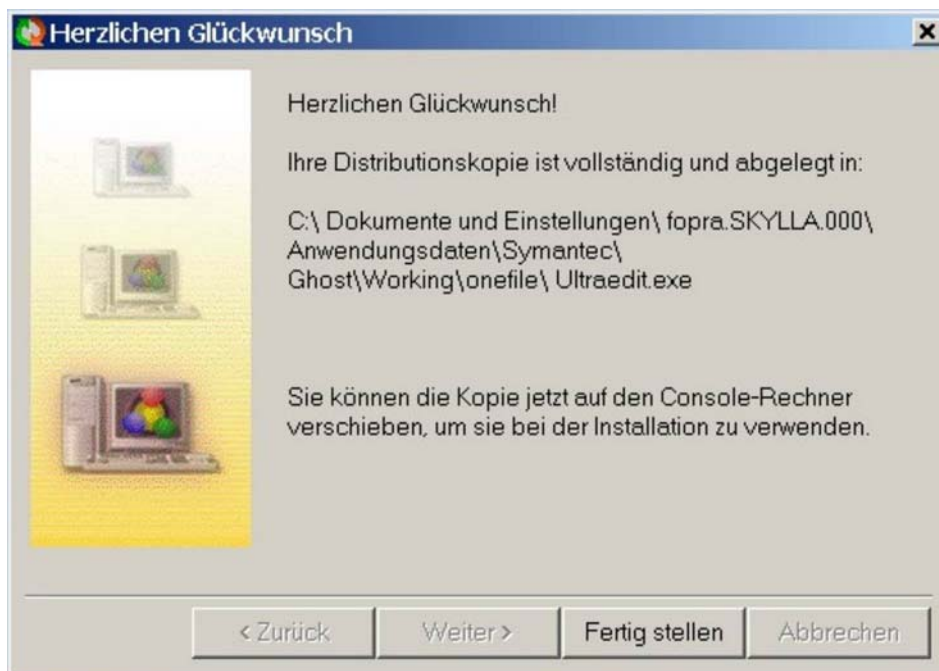


Abb. 14: Wenn alles geklappt hat, kommt diese Meldung. Das Distributionspaket ist nun fertig und mit einem Klick auf „Fertig stellen“ kann „AI-Snapshot“ beendet werden.

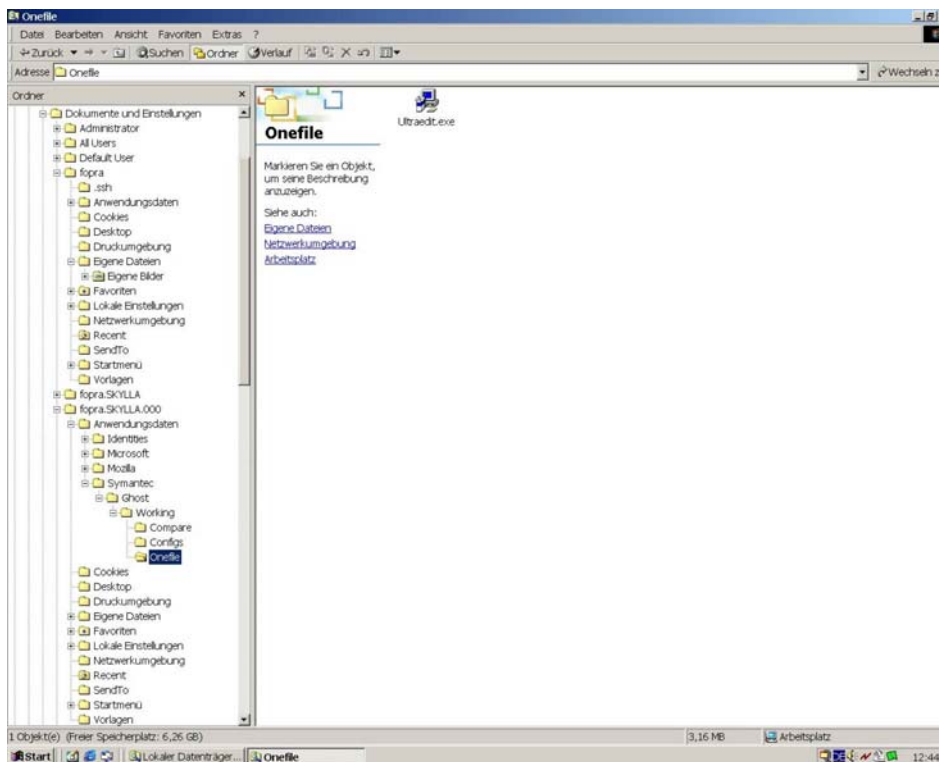


Abb. 15: Das neu erstellte Distributionspaket findet man nun im angegebenen Verzeichnis. Es muss zur weiteren Verwendung noch auf den Server transferiert werden.

## 3.2 Weiterverarbeitung des Distributionspakets

### 3.2.1 Allgemeines

„AI-Snapshot“ erzeugt das Distributionspaket aus dem Vergleich von altem und neuem Systemzustand. Nicht alle Einträge im erzeugten AI-Paket sind deshalb sinnvoll. Während unserer Tests haben die Einträge „\$CurUserDir\$“ und „HKEY\_CURRENT\_USER“ wiederholt Probleme und Fehlermeldungen erzeugt.

Diese Einträge betreffen ausschließlich den aktuell oder zuletzt angemeldeten Benutzer und bewirken, dass das Programm für den betreffenden User praktisch bereits „vorkonfiguriert“ installiert wird. Das ist nicht sinnvoll, weil sich die Anwendung beim ersten Start automatisch konfigurieren sollte. Da der „aktuelle User“ auf dem Modell- und Zielcomputer mit ziemlicher Sicherheit nicht derselbe ist, sind die entsprechenden Einträge auch falsch (ungültige Pfadangaben o.ä.) und erzeugen dann bei dem zuletzt angemeldeten Benutzer Fehlermeldungen beim Programmstart.

Es empfiehlt sich daher, alle derartigen Einträge aus dem AI-Paket herauszulöschen.

### 3.2.2 Entfernen der Einträge „\$CurUserDir\$“ und „HKEY\_CURRENT\_USER“

Zum Ändern des Distributionspakets wird das Programm „AI-Builder“ benötigt. Dieses lässt sich beispielsweise über das Hauptfenster der Symantec Ghost Console starten.

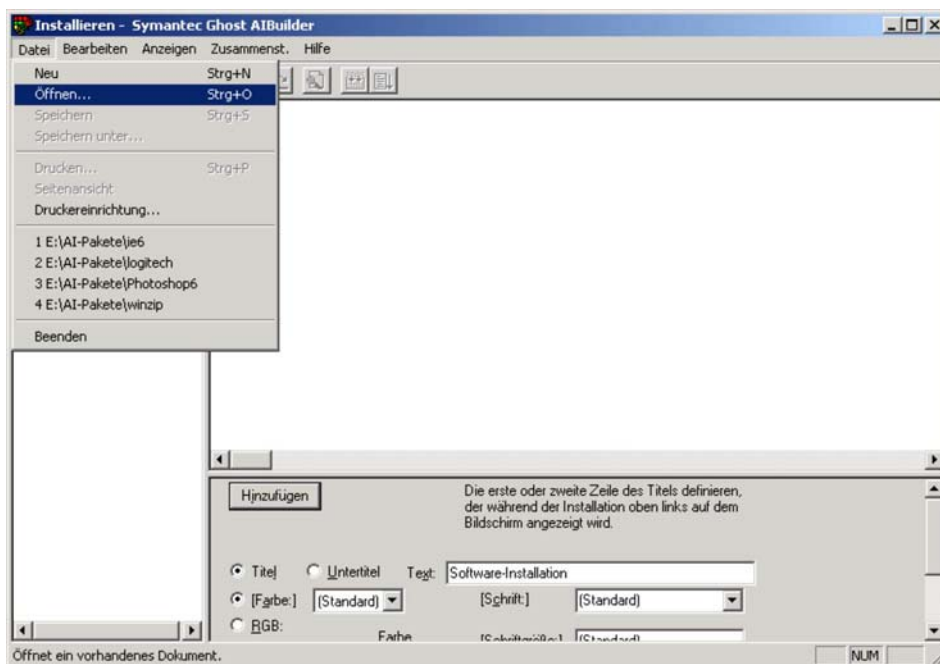


Abb. 16: „AI-Builder“. Das zu bearbeitende Distributionspaket wird über „Datei“, „Öffnen“ geladen.

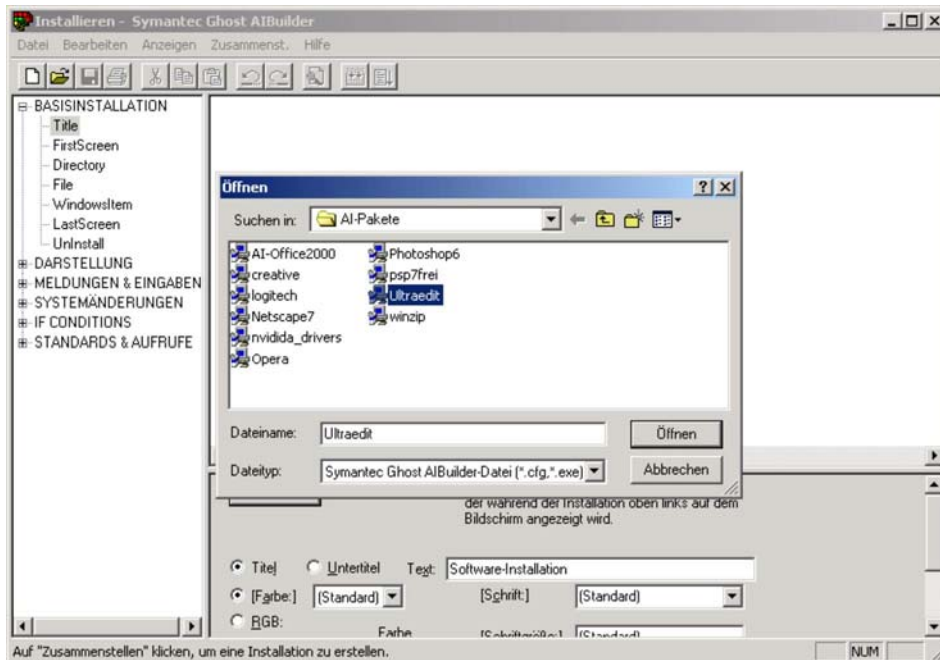


Abb. 17: Hier wählt man nun das Distributionspaket aus, das bearbeitet werden soll.

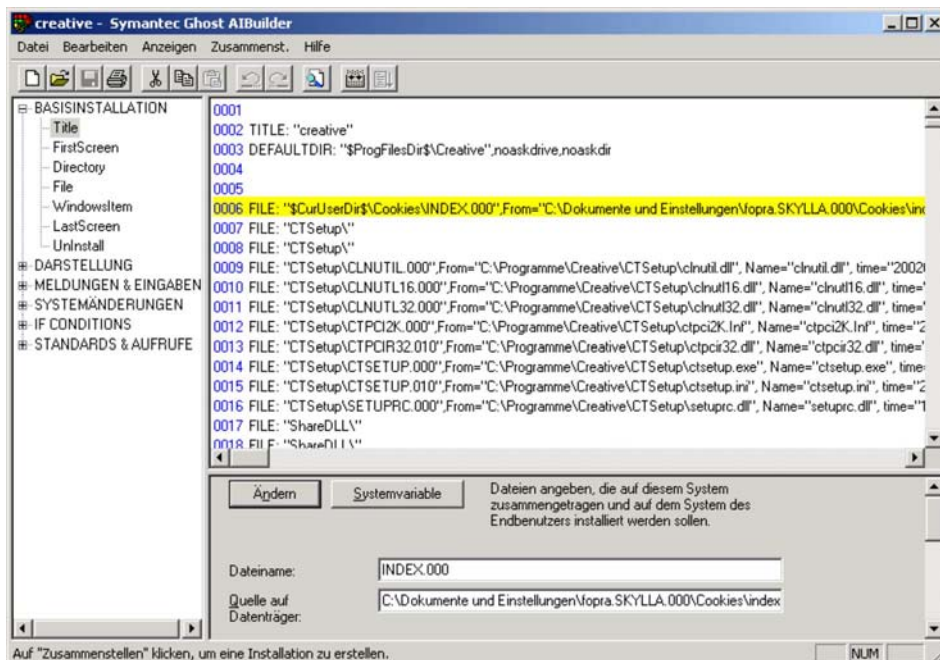


Abb. 18: Nun sucht man alle Einträge, die mit „\$CurUserDir\$“ beginnen und löscht sie mittels der „Entf“-Taste.



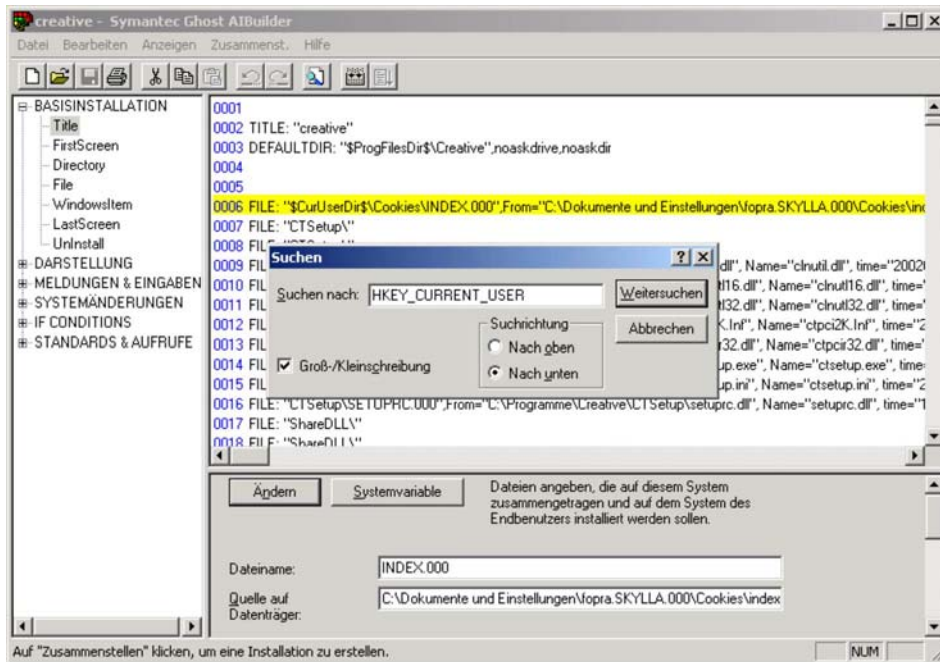


Abb. 19: Entsprechend verfährt man mit den Einträgen „HKEY\_CURRENT\_USER“.

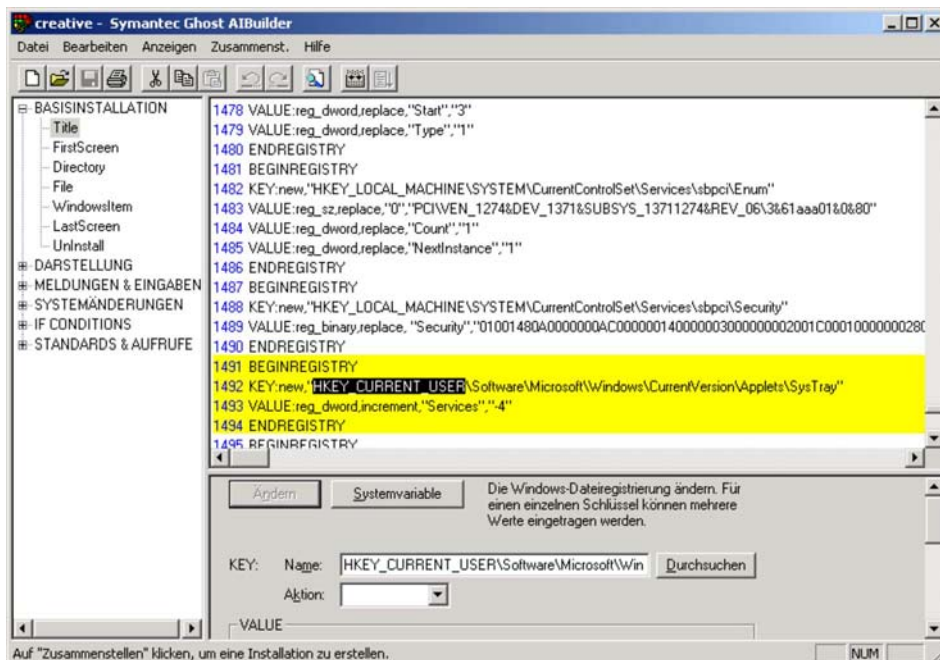


Abb. 20: wie oben.

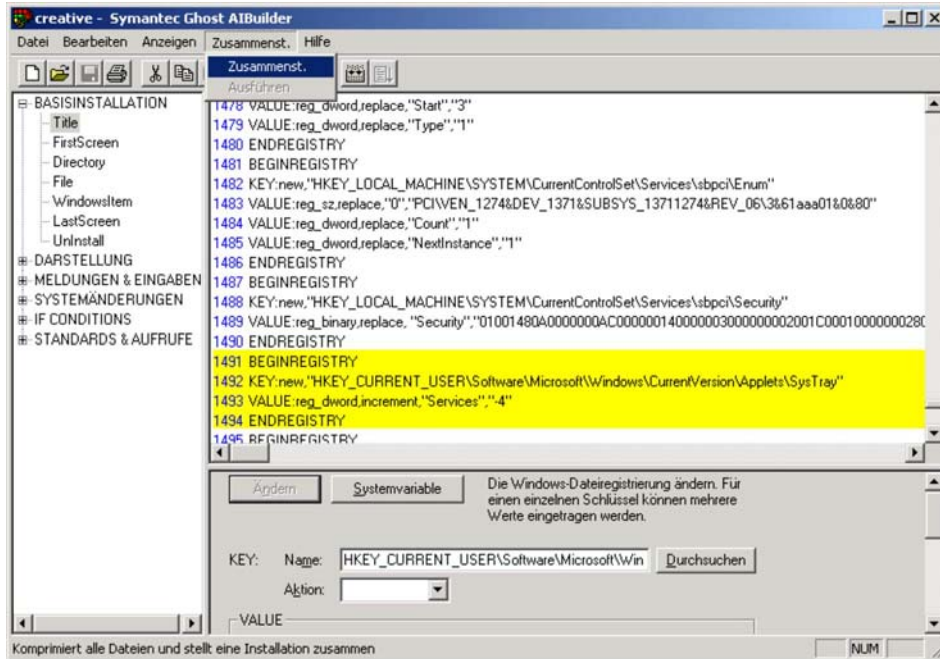


Abb. 21: Sind alle derartigen Einträge entfernt, muss das Paket neu zusammengestellt werden. Hierzu wählt man die Option „Zusammenst.“.

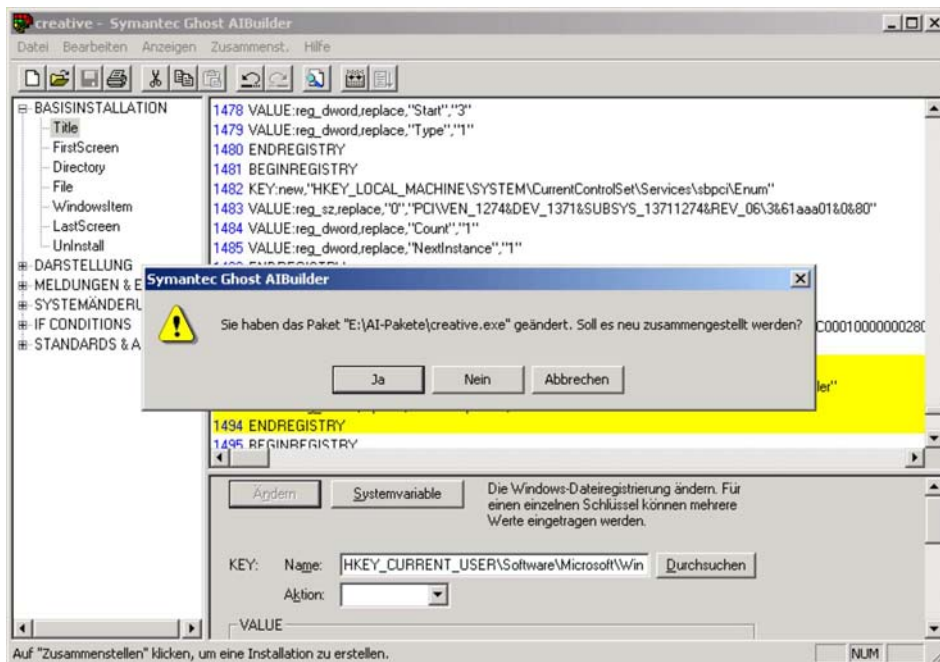


Abb. 22: „AI-Builder“ fragt nun, ob das Paket neu zusammengestellt werden soll. Hier bestätigt man mit „Ja“.

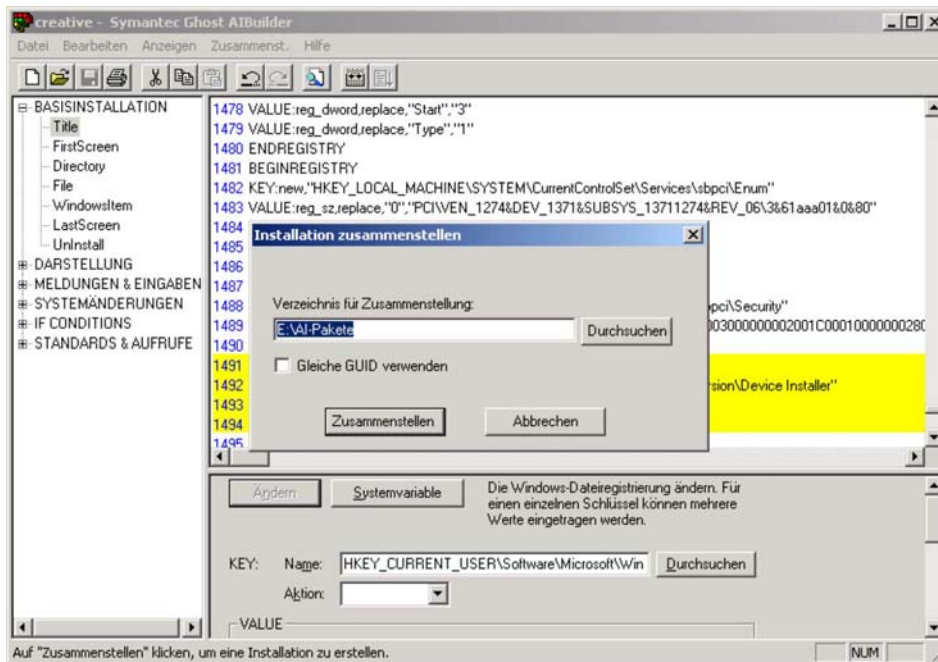


Abb. 23: Nun muss man noch ein Verzeichnis angeben, in dem das neu zusammengestellte Paket abgelegt werden soll.

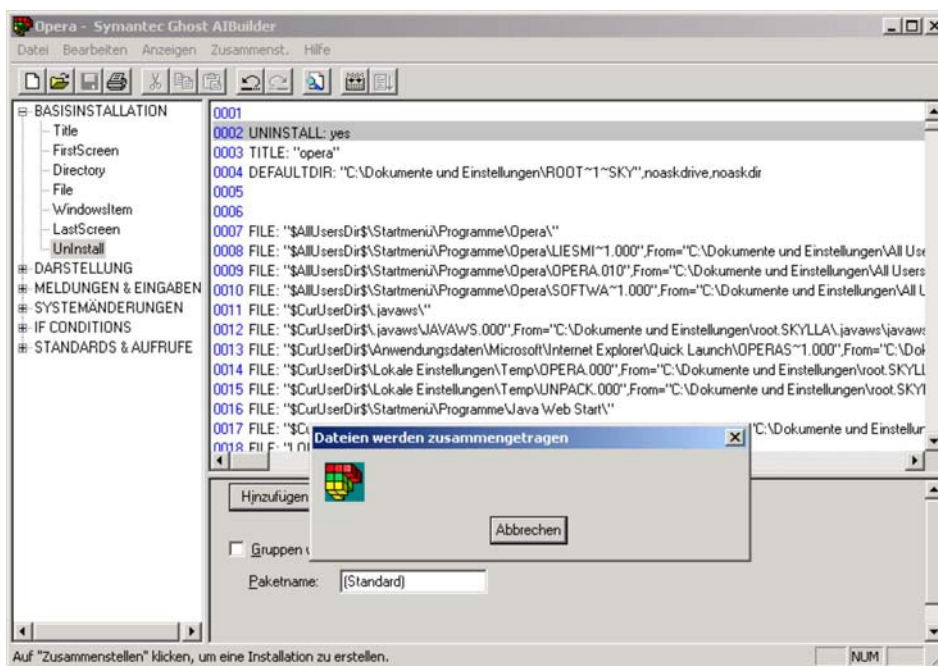


Abb. 24: Das Paket wird nun neu erstellt und im ausgewählten Verzeichnis gespeichert. Anschließend kann man „AI-Builder“ beenden. **Wichtig:** Das alte Distributionspaket muss nun noch durch die veränderte Version ersetzt werden!

### Hinweis:

AI-Builder fragt beim Beenden stets nach, ob das Paket neu zusammengestellt werden soll – auch wenn es bereits vorher neu zusammengestellt und dann nicht mehr geändert wurde. In diesem Fall verneint man die Frage einfach.



### 3.2.3 Hinzufügen einer Deinstallations-Option

Distributionspakete lassen sich mit der AutoInstall-Funktion auch wieder deinstallieren. Hierzu muss dem Paket vorher aber eine Deinstallations-Option hinzugefügt werden.

#### Hinweis:

Bei Microsoft-Produkten ist eine Deinstallation **nicht** möglich (vgl. [SGIh], S. 268).

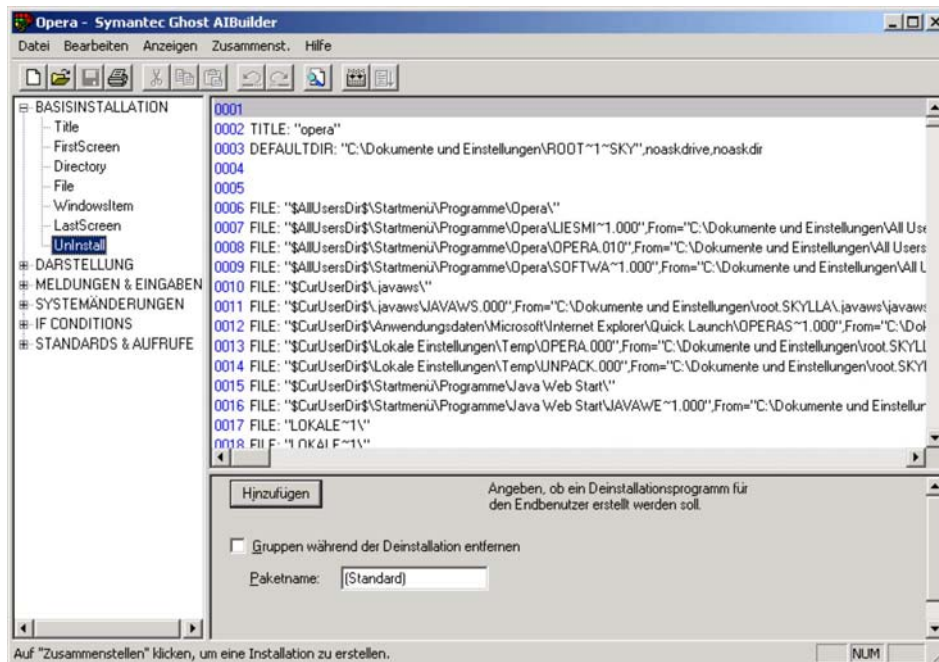


Abb. 25: Zum Hinzufügen eines Deinstallationsbefehls wird das Paket wie unter 3.2.2 beschrieben zuerst im „AI-BUILDER“ geöffnet. Anschließend wechselt man im linken Fenster zur Option „Uninstall“.

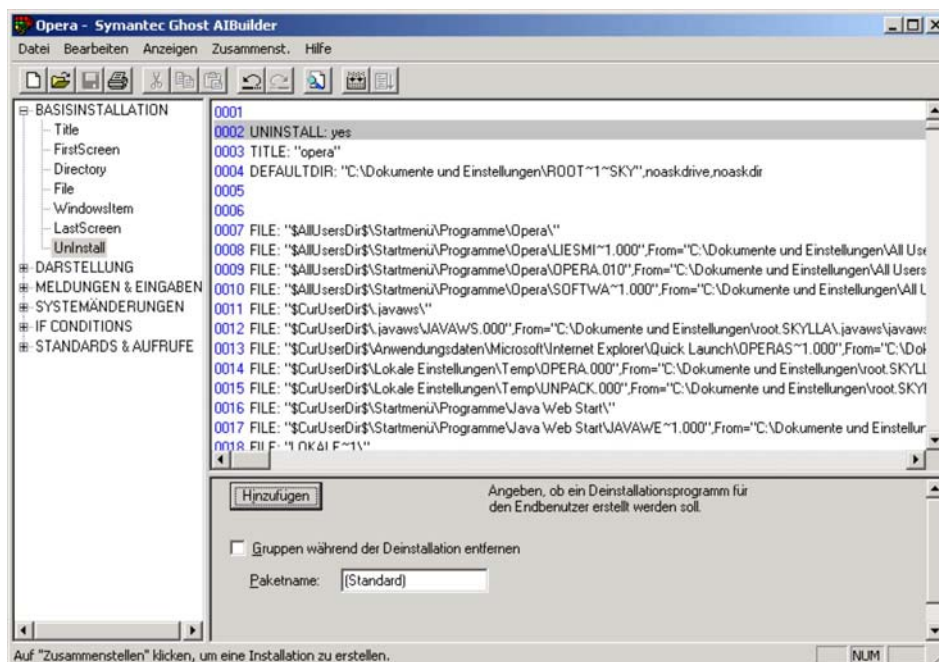


Abb. 26: Durch Klick auf „Hinzufügen“ wird das Paket mit einer Uninstall-Option versehen. Das Distributionspaket muss anschließend neu zusammengestellt werden (vgl. 3.2.2).

### 3.3 Verteilen des AI-Pakets vom Server auf die Clients

Das fertige AI-Distributionspaket kann anschließend vom Server aus auf den jeweiligen Clientrechnern installiert werden.

#### 3.3.1 Erstellen eines Installationsvorganges für ein AI-Paket

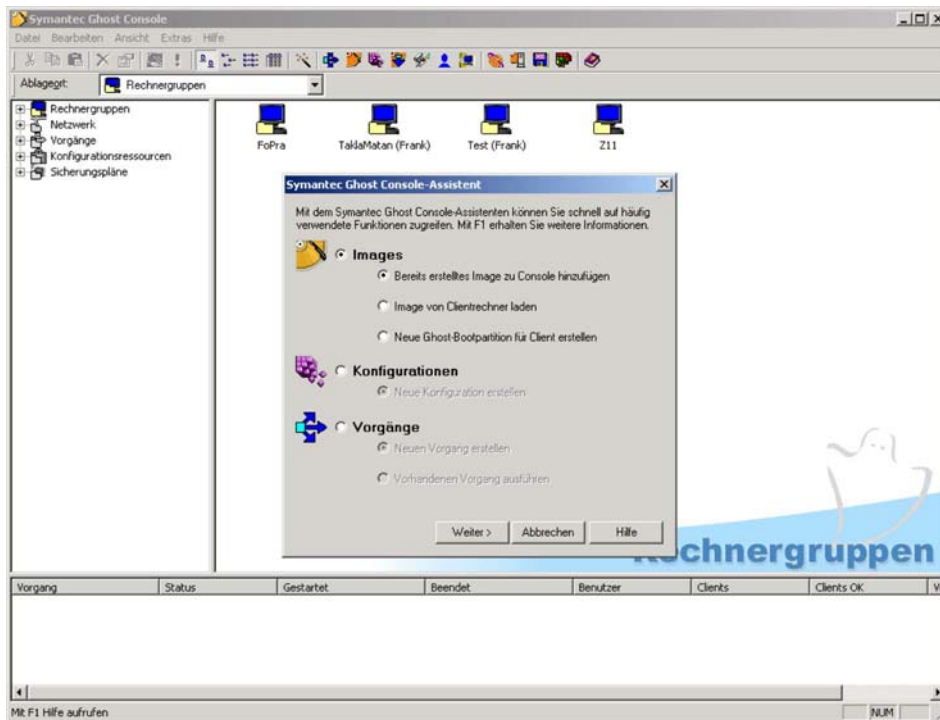


Abb. 27: Ghost Konsole Hauptfenster. Hier wählt man „Vorgänge, Neuen Vorgang erstellen“ aus.

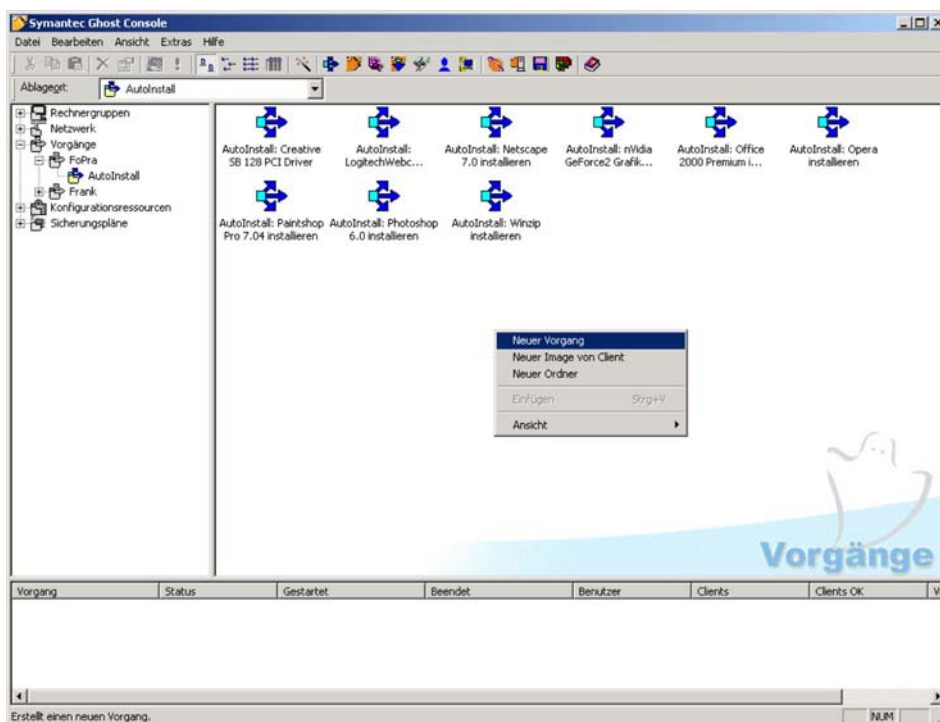


Abb. 28: Alternativ kann man auch im Unterfenster „Vorgänge“ mittels Rechtsklick einen neuen Vorgang erstellen lassen.

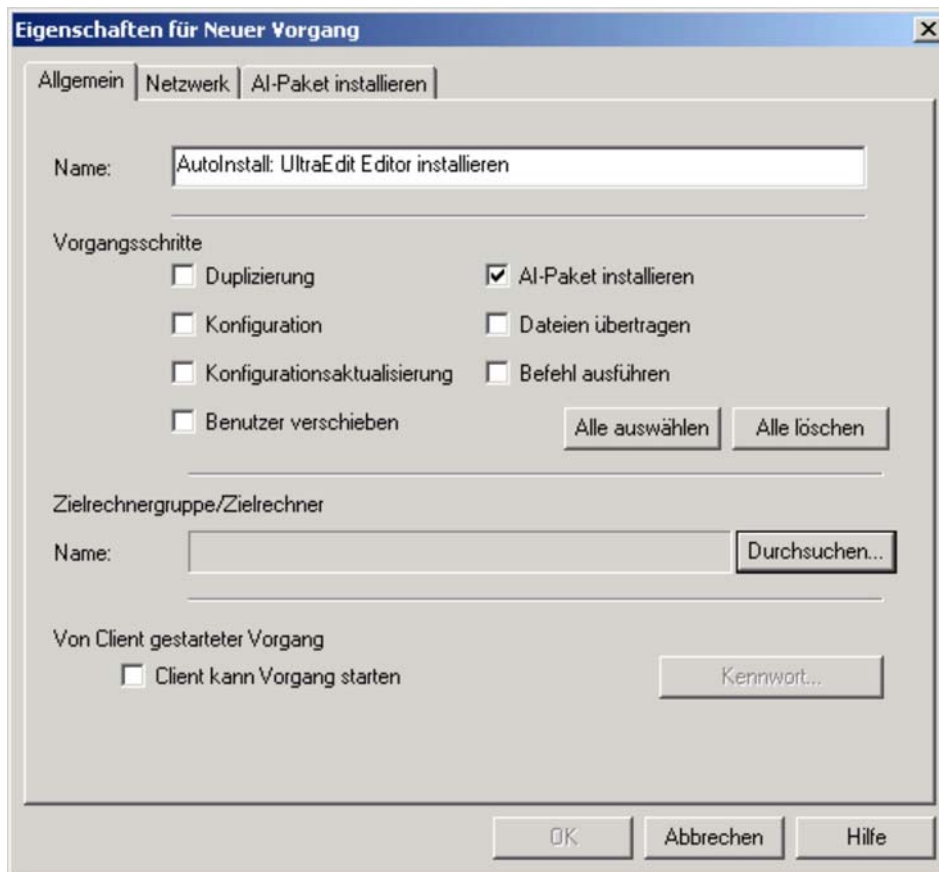


Abb. 29: Bei „Vorgangsschritte“ ist lediglich „AI-Paket installieren“ zu aktivieren. Bei „Zielrechnergruppe/Zielrechner“ klickt man auf „Durchsuchen“.



Abb. 30: Hier wählt man den gewünschten Zielrechner oder die Zielrechnergruppe aus.

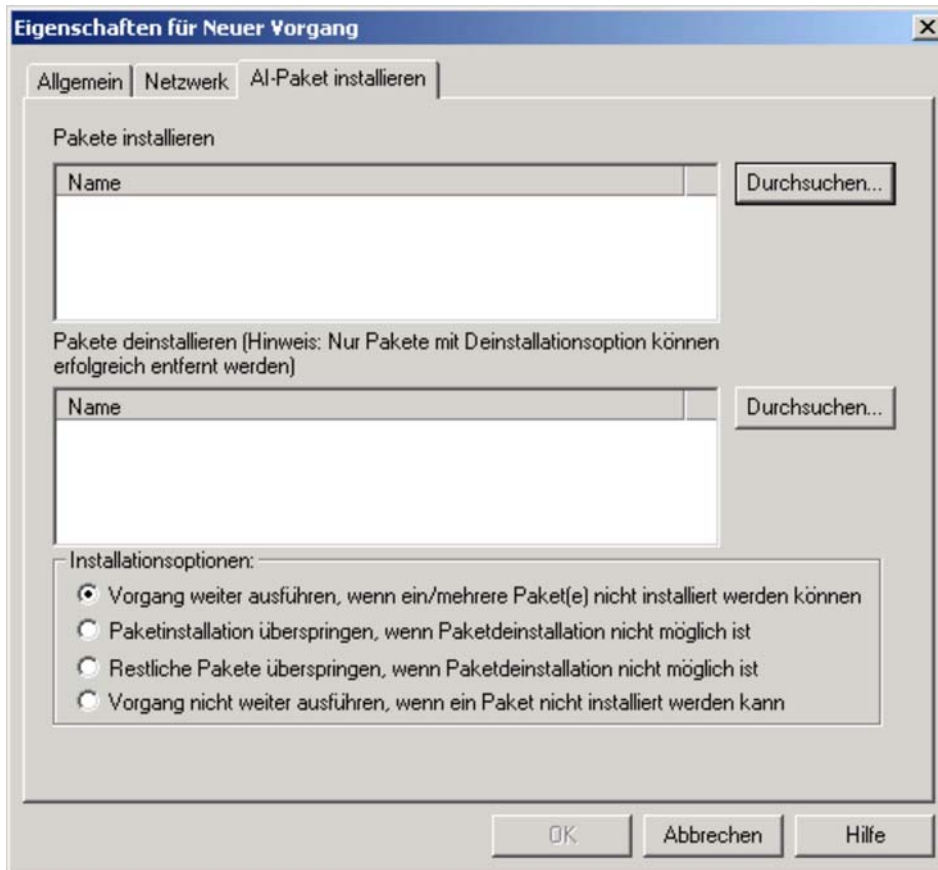


Abb. 31: Beim Untermenü „AI-Paket“ trägt man im oberen Fenster die zu installierenden Pakete ein. Auch das Verhalten für den Fehlerfall lässt sich hier festlegen.

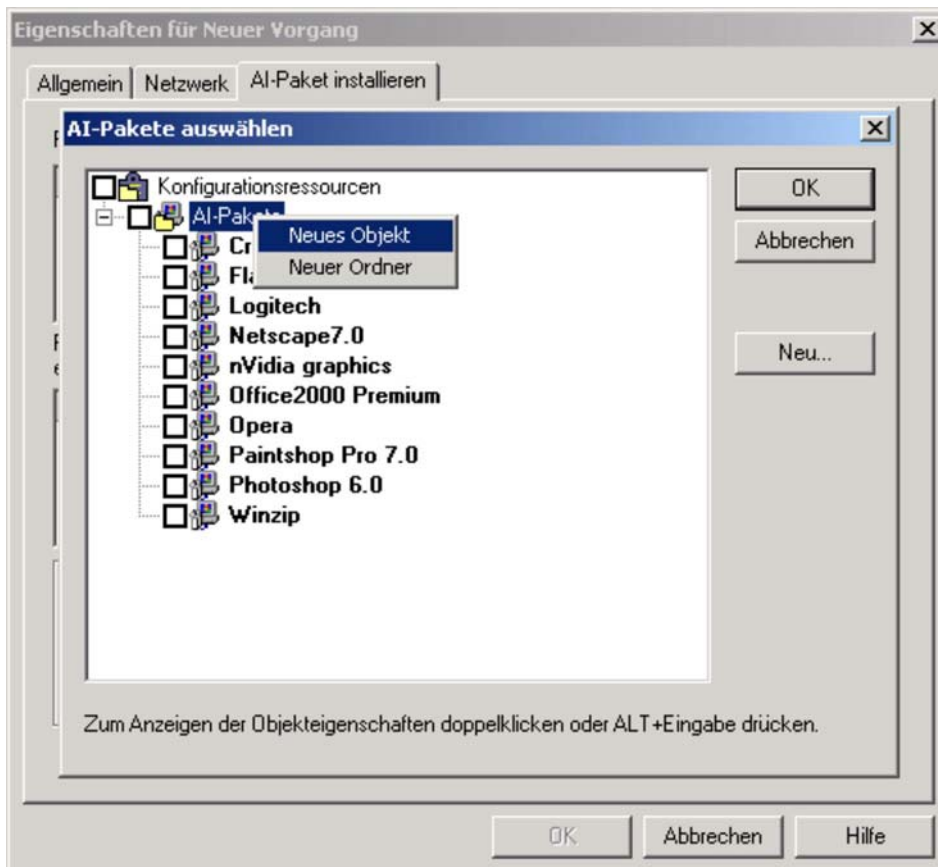


Abb. 32: Damit ein AI-Paket in der Liste der Konfigurationsressourcen erscheint, muss es erst als neues Objekt angelegt werden.

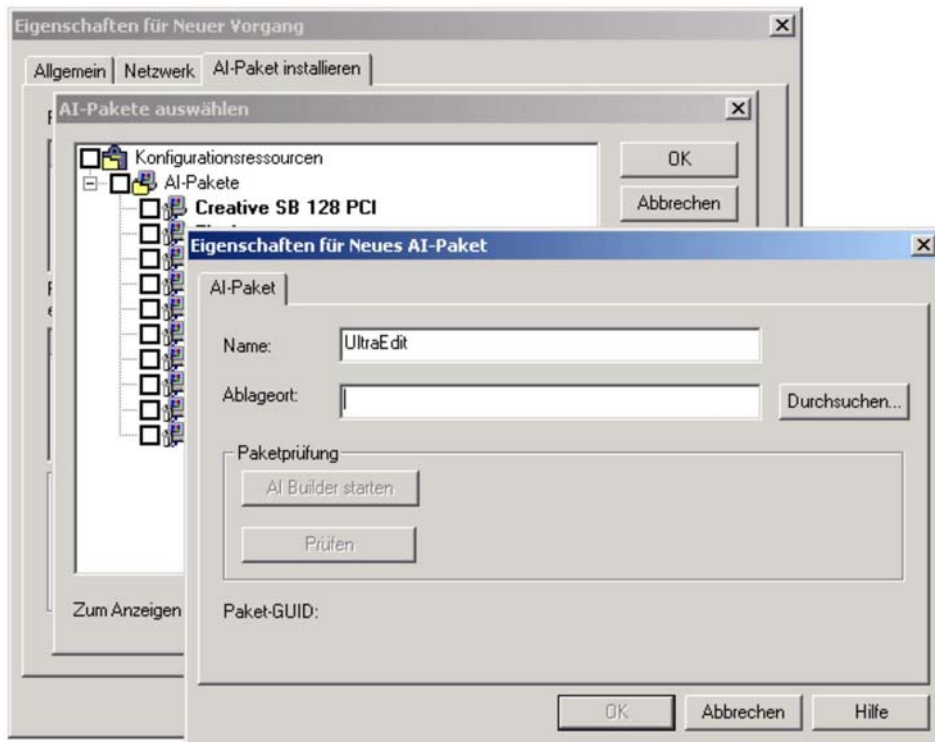


Abb. 33: Hierzu gibt man einen Namen...

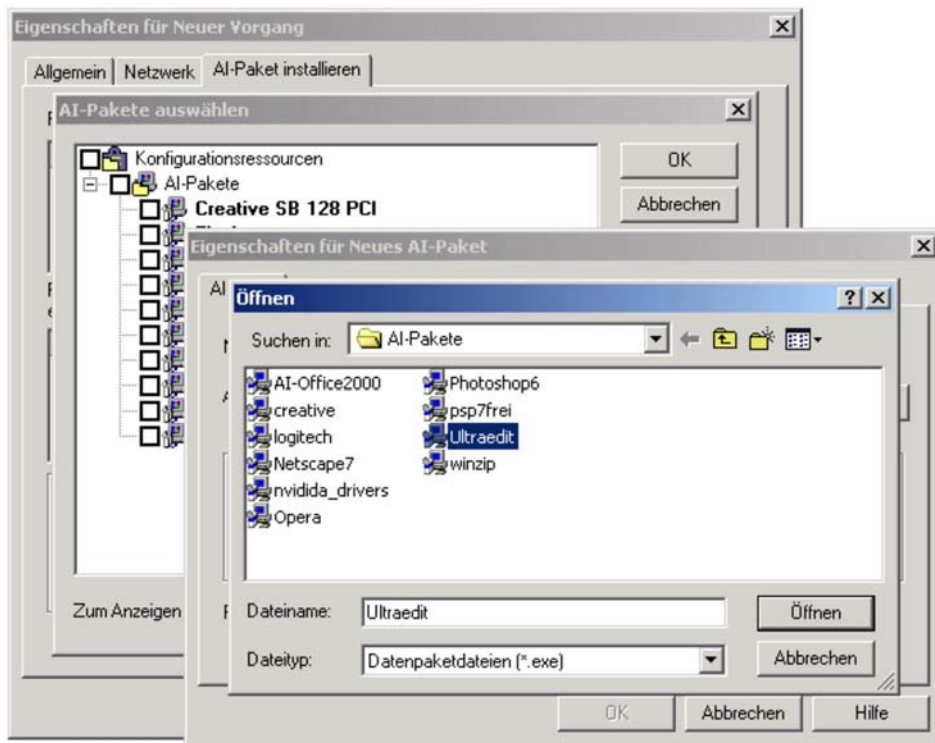


Abb. 34: ...und den Ablageort des Distributionspaketes ein.

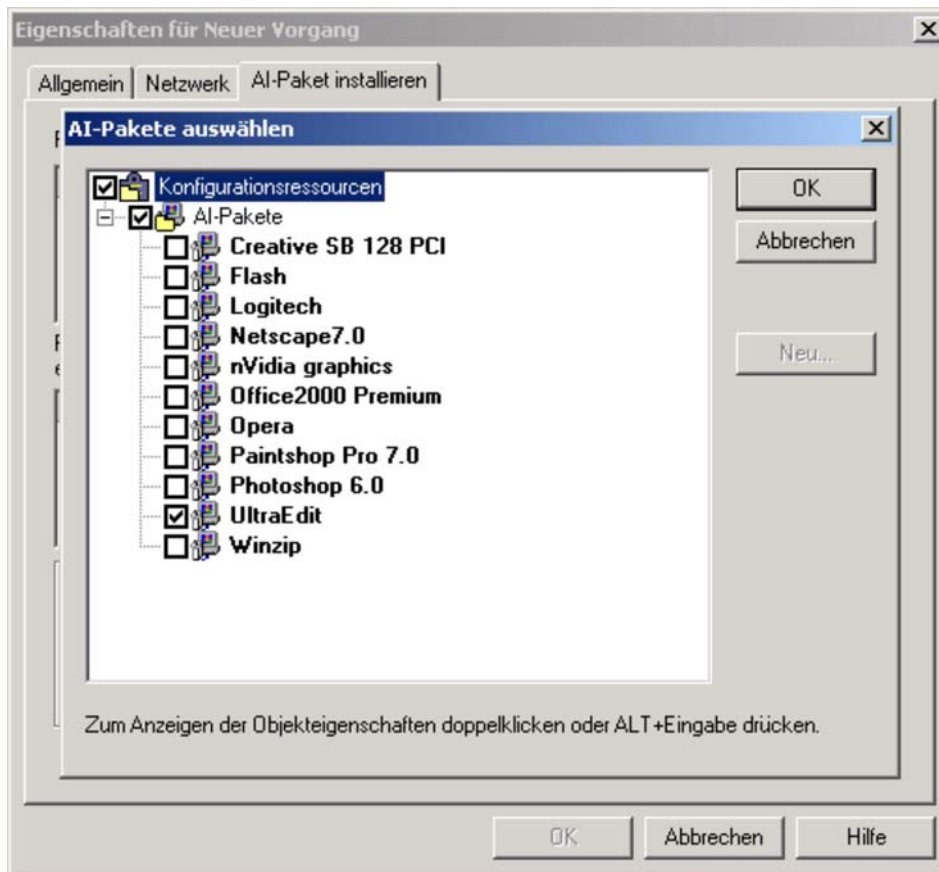


Abb. 35: Nun kann es ausgewählt und mit Klick auf „OK“ zur Liste der zu installierenden Pakete hinzugefügt werden.

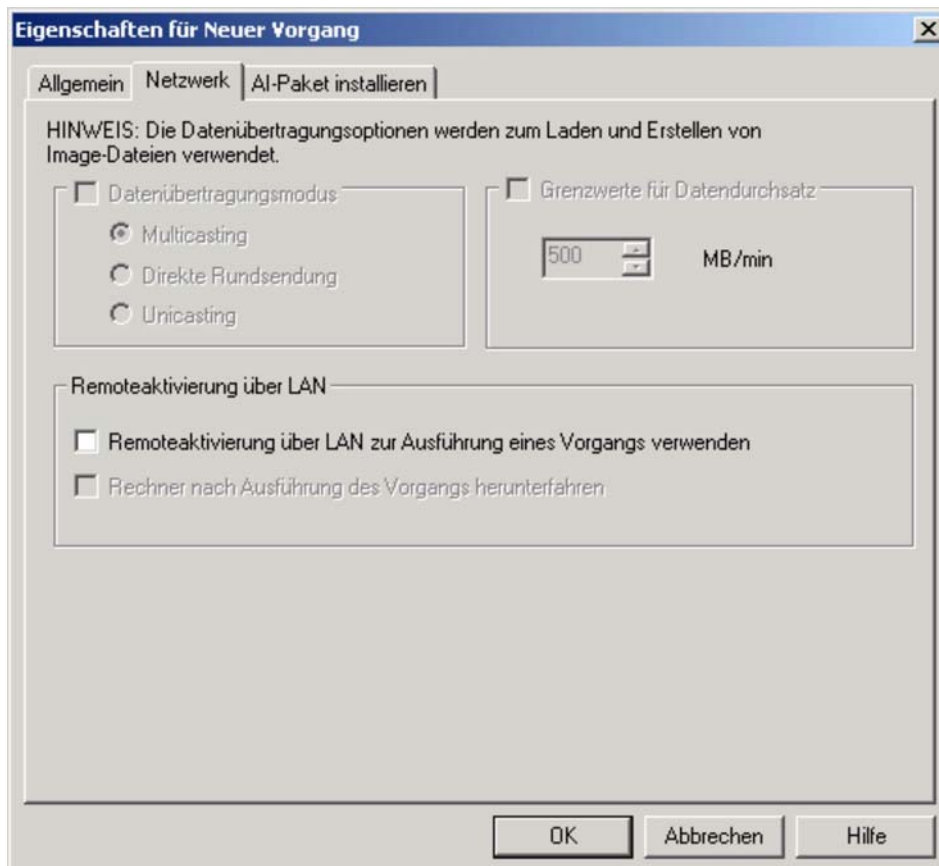


Abb. 36: Unter „Netzwerk“ lassen sich die Datenübertragungsoptionen festlegen. In der Regel sollten die Default-Einstellung passen.



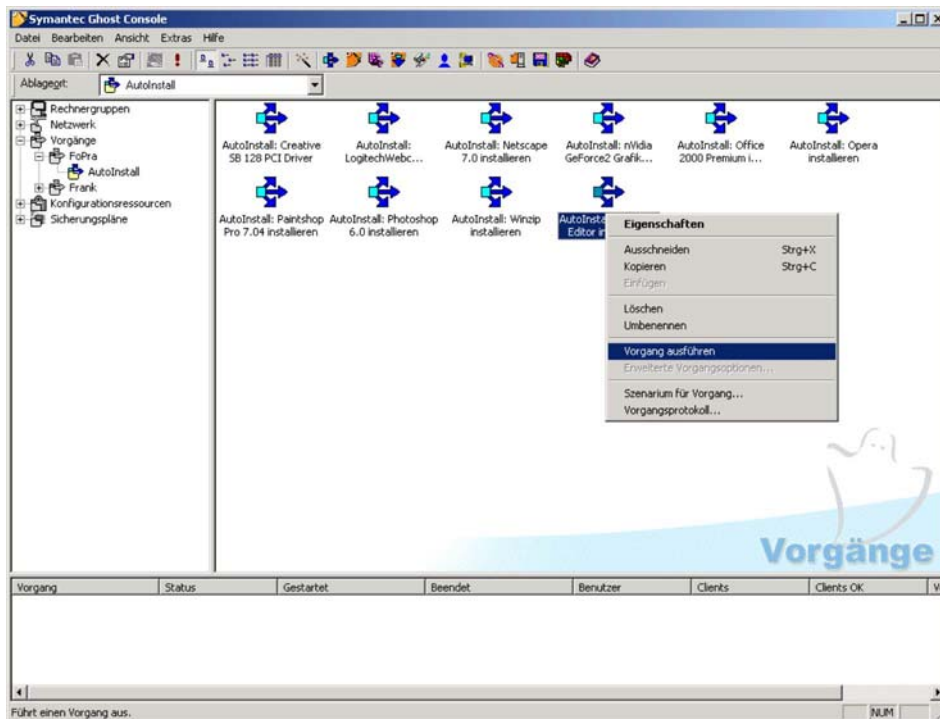


Abb. 37: Der neu erstellte Installationsvorgang kann nun mittels Rechtsklick und anschließender Wahl von „Vorgang ausführen“ gestartet werden.

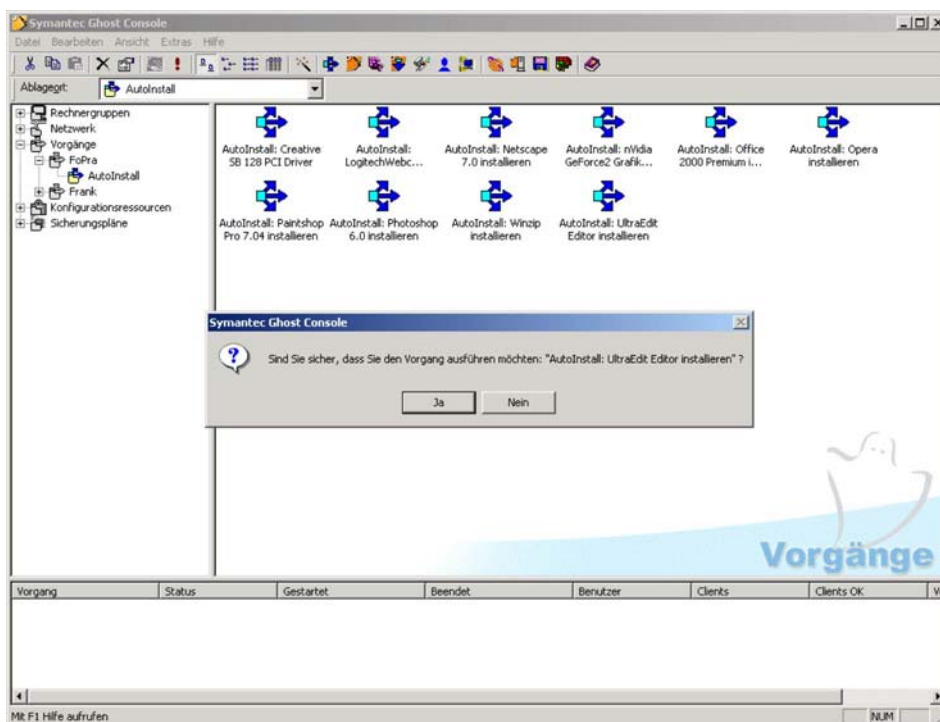


Abb. 38: Bestätigen dieses Warnhinweises startet den Installationsvorgang.

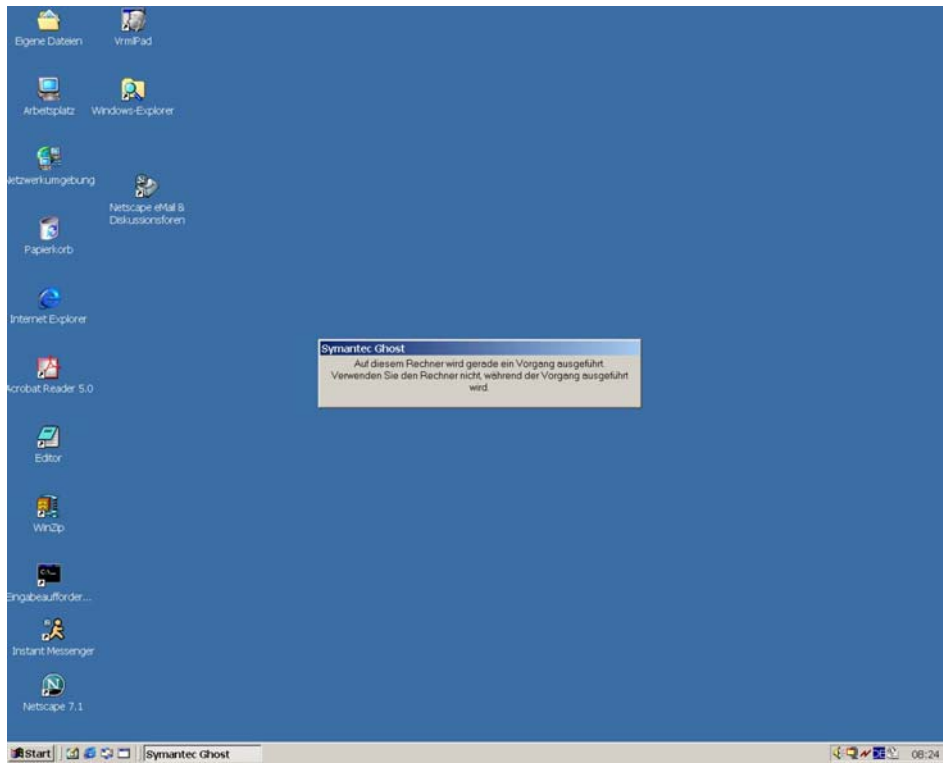


Abb. 39: Falls auf dem Zielrechner ein Benutzer eingeloggt ist, erscheint nun diese Meldung.



### 3.3.2 Erstellen eines Deinstallationsvorganges für ein AI-Paket

#### Hinweis:

Nur AI-Pakete, die mit einem Deinstallations-Befehl versehen sind, können später wieder deinstalliert werden. Das Hinzufügen eines Deinstallationsbefehls ist unter *Abschnitt 3.2.3* beschrieben.

Ein Deinstallationsvorgang wird praktisch auf die gleiche Art erstellt wie ein Installationsvorgang. Er unterscheiden sich nur in einigen Details:

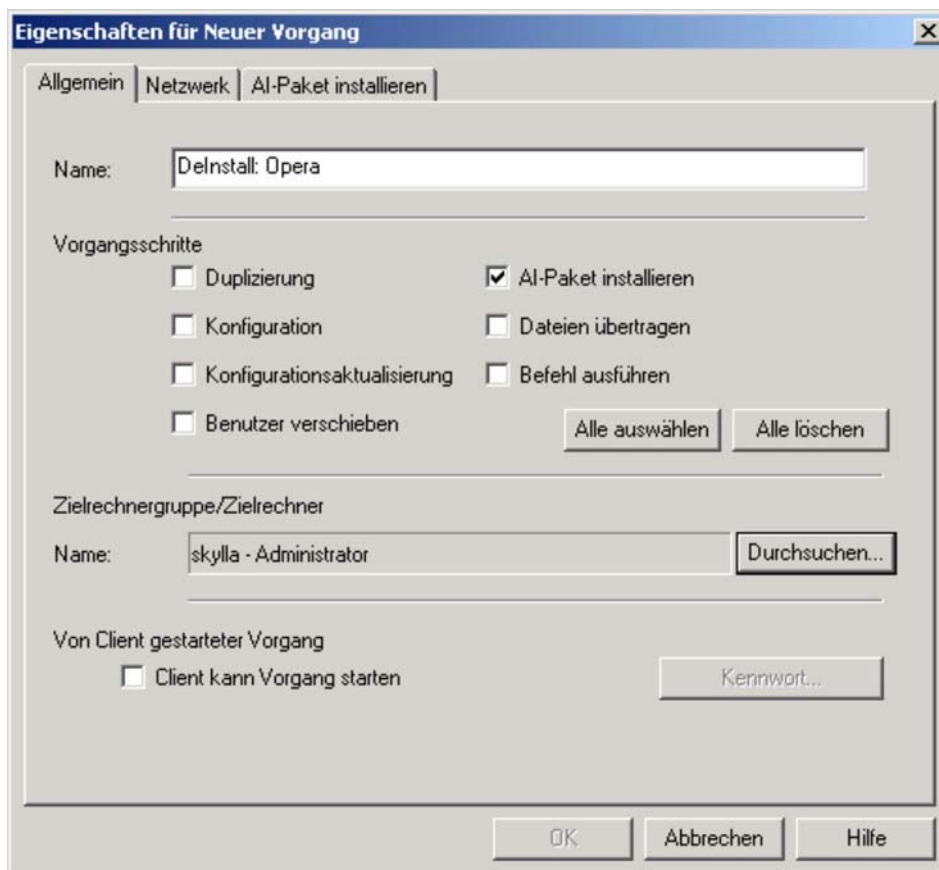


Abb. 40: Erstellen eines Deinstallationsvorganges. Die Vorgehensweise entspricht anfangs der unter *Abschnitt 3.3.1*, *Abb. 27–30* beschriebenen.

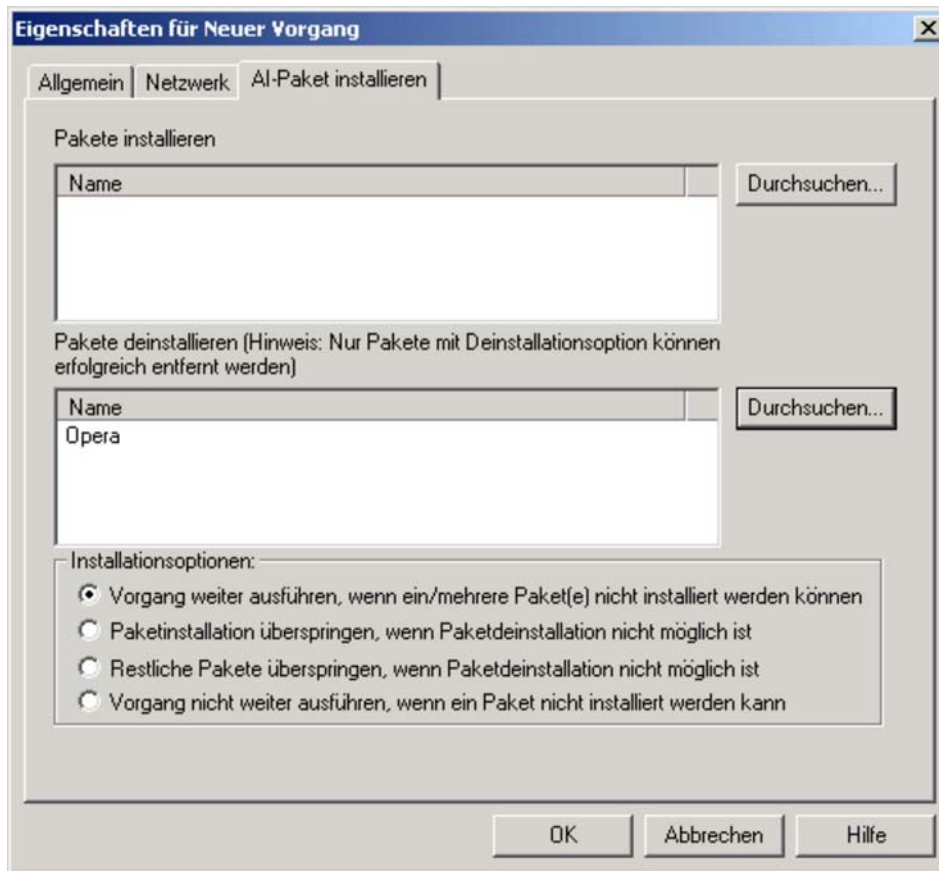


Abb. 41: Mit dem **unteren** „Durchsuchen“-Button wählt man das AI-Paket aus, das deinstalliert werden soll.  
**Wichtig:** Im Gegensatz zu einem Installationsvorgang muss man das gewünschte Distributionspaket im unteren Menüfenster einfügen.

Anschließend kann der neu erstellte Vorgang wie unter *Abschnitt 3.3.1, Abb. 37-38* beschrieben ausgeführt werden.

### 3.4 Automatische Installation von AI-Paketen mittels Zeitplaner

Es bietet sich vermutlich an, die Distributionspakete zeitversetzt und automatisch mittels Zeitplaner zu installieren.

Mit dieser Methode können die gewünschten Anwendungen und Programme beispielsweise über Nacht installiert werden, wenn niemand an den Clientrechnern arbeitet.

Hierzu muss allerdings sichergestellt sein, dass zum Zeitpunkt der Installation auf den Clientrechnern Windows 2000 läuft und dass bei einem etwaigen Neustart nicht zu Linux gebootet wird (siehe auch *Kapitel 2 „Allgemeines“*).

#### 3.4.1 Erstellen eines zeitversetzten Installationsvorganges

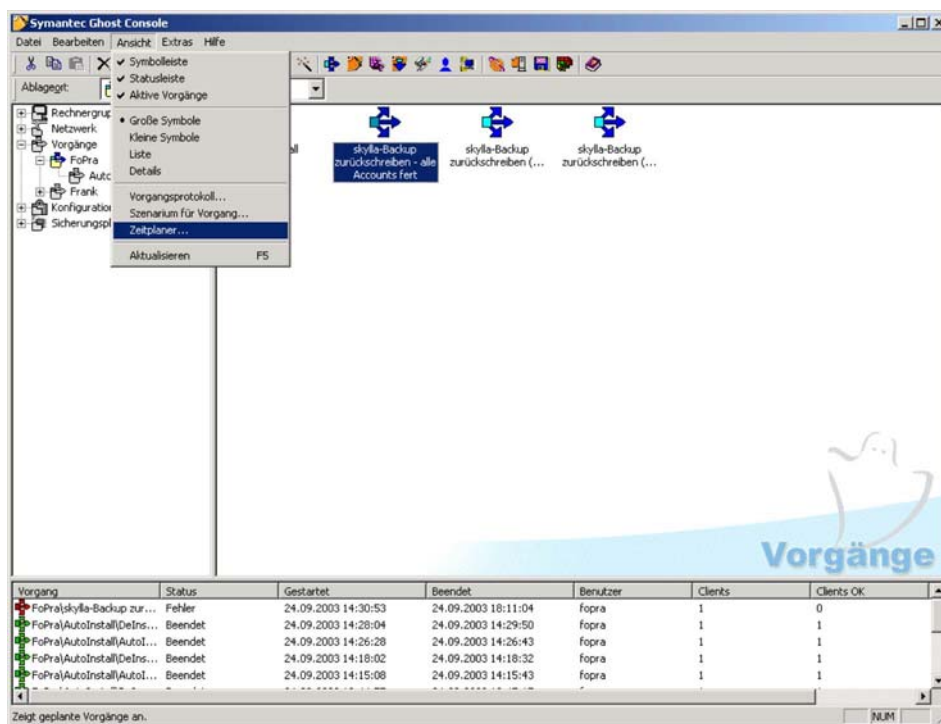


Abb. 42: Im Hauptfenster der Symantec Ghost Konsole wählt man „Ansicht, Zeitplaner“.

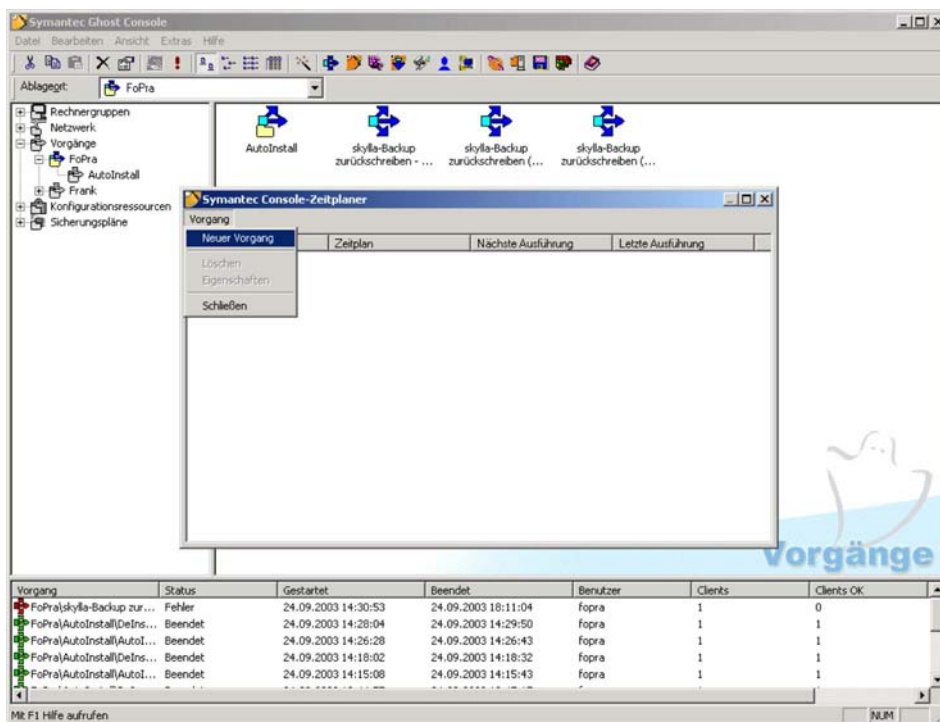


Abb. 43: Im Zeitplanerfenster klickt man auf „Vorgang, Neuer Vorgang“.

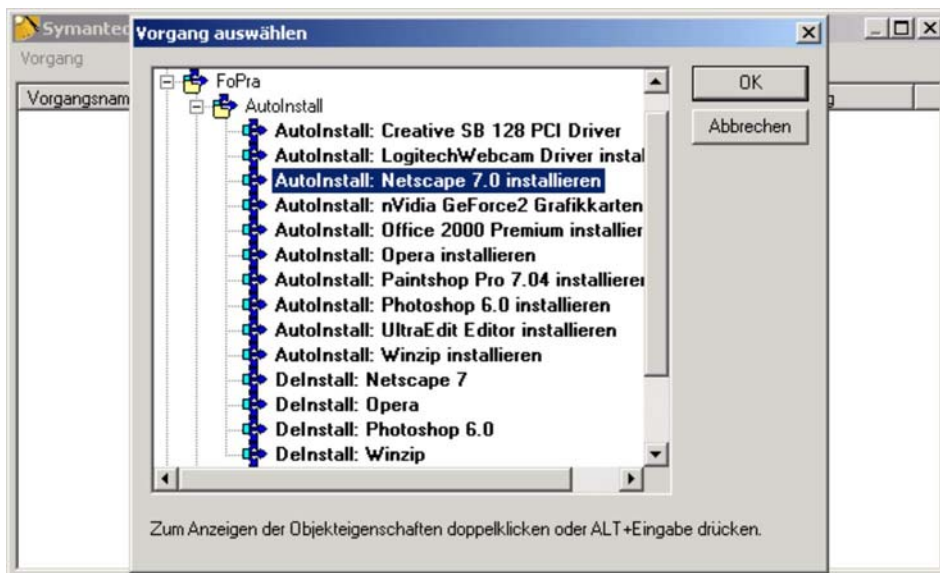


Abb. 44: Nun wählt man den Installations- oder Deinstallationsvorgang aus, der zeitversetzt ausgeführt werden soll. Der entsprechende Vorgang muss zuvor wie unter *Abschnitt 3.3.1 bzw. 3.3.2* beschrieben erstellt werden.

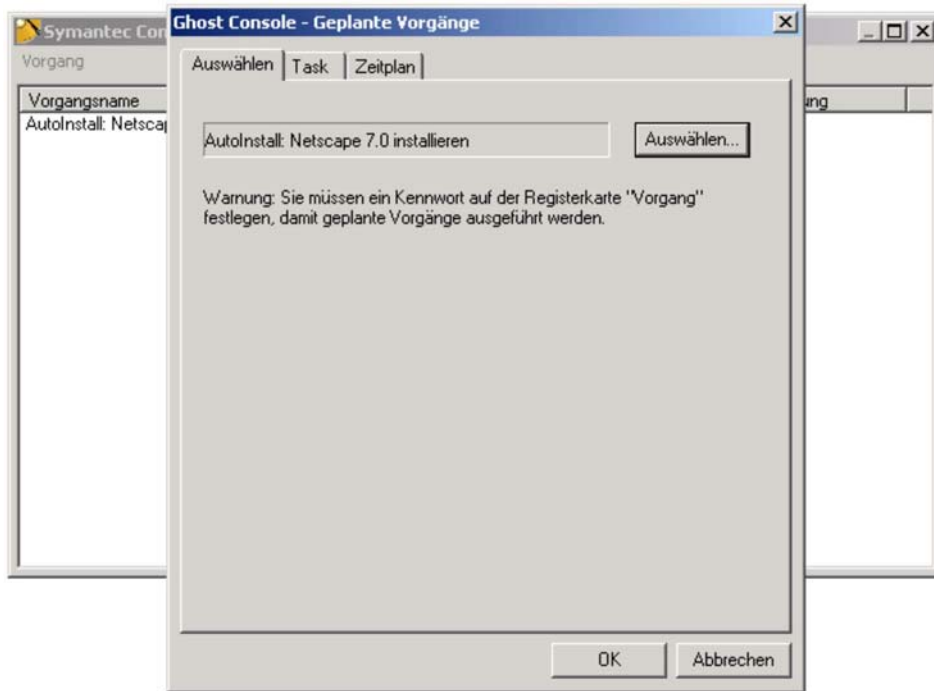


Abb. 45: Anschließend sieht das so aus.

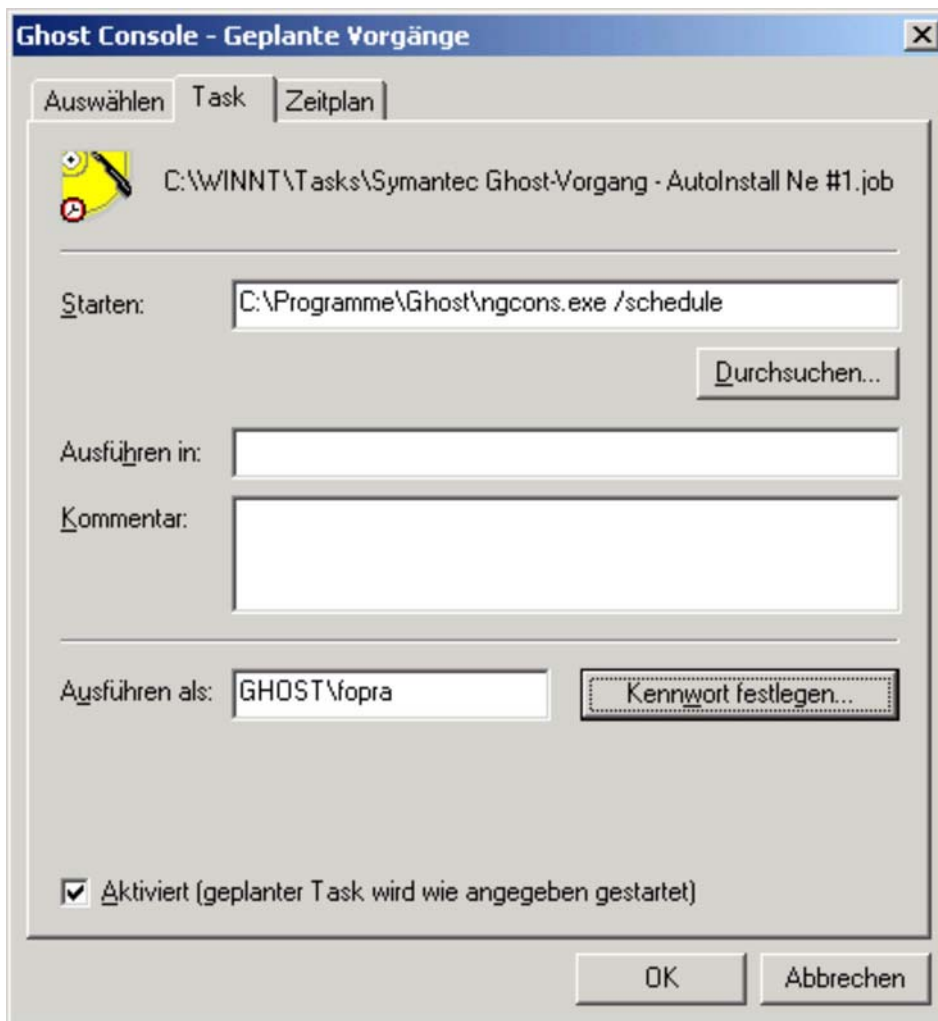


Abb. 46: Im Untermenü „Task“ ist darauf zu achten, dass bei „Aktiviert“ ein Häkchen ist. Unter „Ausführen als:“ muss ein **lokaler Administratoraccount** eingetragen werden. Anschließend klickt man auf „Kennwort festlegen...“.

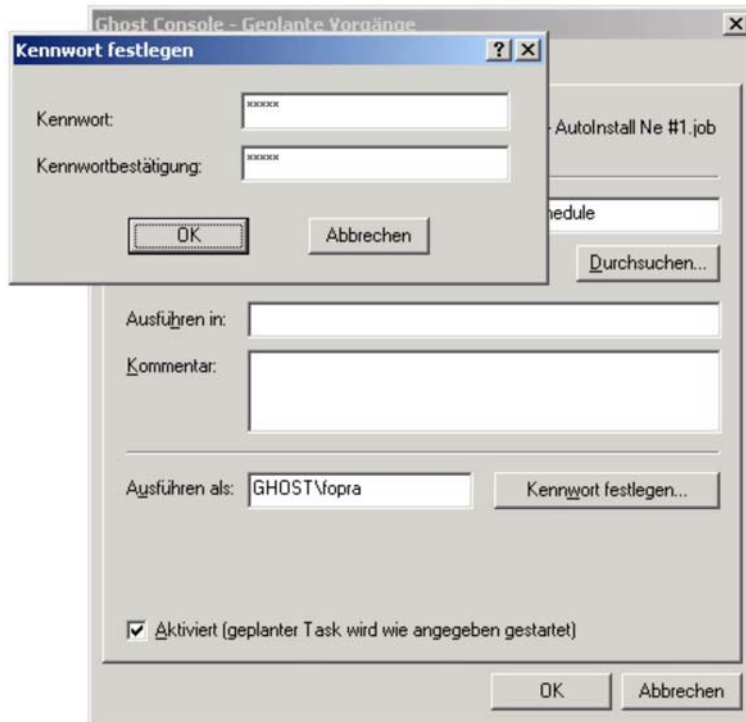



Abb. 47: Hier trägt man nun das Passwort des entsprechenden lokalen Administratoraccounts ein (in unserem Beispiel „GHOST\fopra“).



Abb. 48: Im Untermenü „Zeitplan“ legt man nun fest, wann der Task ausgeführt werden soll. Auch mehrfache Termine sind möglich, falls beim ersten Termin die Installation fehlschlägt (beispielsweise weil der Clientrechner ausgeschaltet ist).



The screenshot shows a window titled "Symantec Console-Zeitplaner". Below the title bar, the word "Vorgang" is displayed. A table with four columns is shown: "Vorgangname", "Zeitplan", "Nächste Ausführung", and "Letzte Ausführung". The first row of the table contains the following data: "Autolnstell: Netscape 7.0 i...", "Um 23:00 am 01.10.2003", "01.10.2003 23:00:00", and "Nie".

Vorgangname	Zeitplan	Nächste Ausführung	Letzte Ausführung
Autolnstell: Netscape 7.0 i...	Um 23:00 am 01.10.2003	01.10.2003 23:00:00	Nie

Abb. 49: Im Symantec Consolen-Zeitplaner erscheint nun der neu erstellte Task.

### 3.5. Weitere Hinweise zum Einsatz von Symantec Ghost AutoInstall in der CIP-Umgebung

Während unseres Praktikums haben wir folgende Softwareprodukte mit den vorstehend beschriebenen Vorgangsweisen erfolgreich auf einem zu Testzwecken eingerichteten Clientrechner getestet:

- Microsoft Office 2000 Premium
- Adobe Photoshop 6.0
- Jasc Paintshop Pro 7.04
- Netscape Navigator 7.0
- Opera 7.20
- WinZip 8.1 SR-1
- UltraEdit32

Lediglich bei Paintshop Pro 7.04 mussten wir auf dem Clientrechnern noch manuell nachbessern.

Hier hatten normale Benutzer keinen Zugriff auf des Arbeitsverzeichnis des Programmes, C:\Programme\Jasc Software Inc\Paint Shop Pro 7\Tubes.

Abhilfe ließ sich schaffen, indem wir normalen Benutzern Zugriffsrechte auf das entsprechende Verzeichnis gaben.

Dies ist anscheinend aber ein generelles Problem von Paint Shop Pro und kein von der AI-Funktion hervorgerufener Effekt.

Laut dem Symantec Ghost-Handbuch kann es aufgrund des Systemdateischutzes (SFP) bei neueren Microsoft-Betriebssystemen zu Problemen kommen, wenn Softwareprodukte mittels AI dupliziert und verteilt werden, die Betriebssystem-Dateien verändern, z.B. Gerätetreiber und Systemupdates (vgl. [SGIh], S. 270 – dort findet sich auch eine Liste der entsprechenden Produkte).

Wir konnten bei unseren Test trotzdem folgende Software mit AI fehlerfrei installieren:

- Creative Labs Soundblaster 128 PCI Driver (finale Releaseversion)
- nVidia GeForce2 MX/MX 400 Driver Version 4.5.2.3
- Logitech Quickcam Version 7.0.0.1221
- Microsoft Mediaplayer 9
- Empfohlenes Update KB822831 für Windows 2000 Professional

Keinen Erfolg hatten wir trotz mehrfacher Bemühungen mit dem neuesten Internet Explorer 6 SP-1. Hier schlug der SFP stets gnadenlos zu. In diesem Fall bietet sich als Ausweg entweder eine manuelle Installation oder die Distribution eines entsprechenden Imagefiles von einem Modellcomputer an.

#### **Wichtig:**

Grundsätzlich sollte jedes neu erstellte Distributionspaket nach Möglichkeit zuerst einmal auf Herz und Nieren geprüft werden, bevor es auf die Clientrechner ausgebracht wird. Unerlässlich ist dies bei Software, die Betriebssystemdateien austauscht und damit möglicherweise Probleme mit dem Windows-Dateischutz (SFP) erzeugt.



## Bekannte Probleme

### Defekte Profile

Während unserer Tests hat wir einige Fälle, bei denen das auf dem Samba-Server gespeicherte Benutzerprofil defekt war (vgl. Abb. 50). Hierbei hat der jeweilige Benutzer keine Schreibrechte auf seinen in der Datei ntuser.dat gespeicherten Registry-Subtree. Die Konsequenz ist, dass die installierten Programme keine Einträge hinzufügen können und dadurch Fehlermeldungen erzeugen bzw. gar nicht laufen. Defekte Profile lassen sich erkennen, indem man die entsprechende ntuser.dat-Datei mit dem Registry-Editor regedt32.exe öffnet und die Berechtigungen für HKEY\_CURRENT\_USER vergleicht.

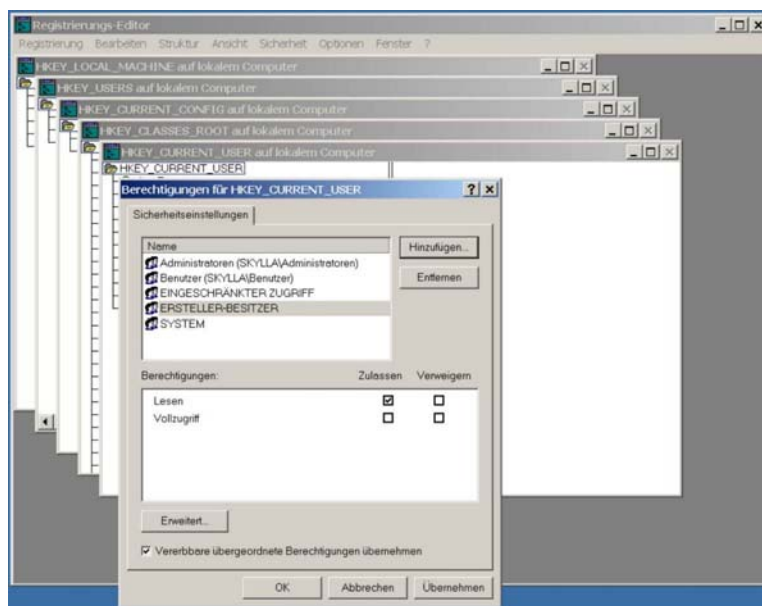


Abb. 50: Defektes Profil. Es fehlt der Besitzer, statt dessen erscheinen die beiden Einträge „Benutzer“ und „ERSTELLER-BESITZER“, die lediglich Leserechte haben.

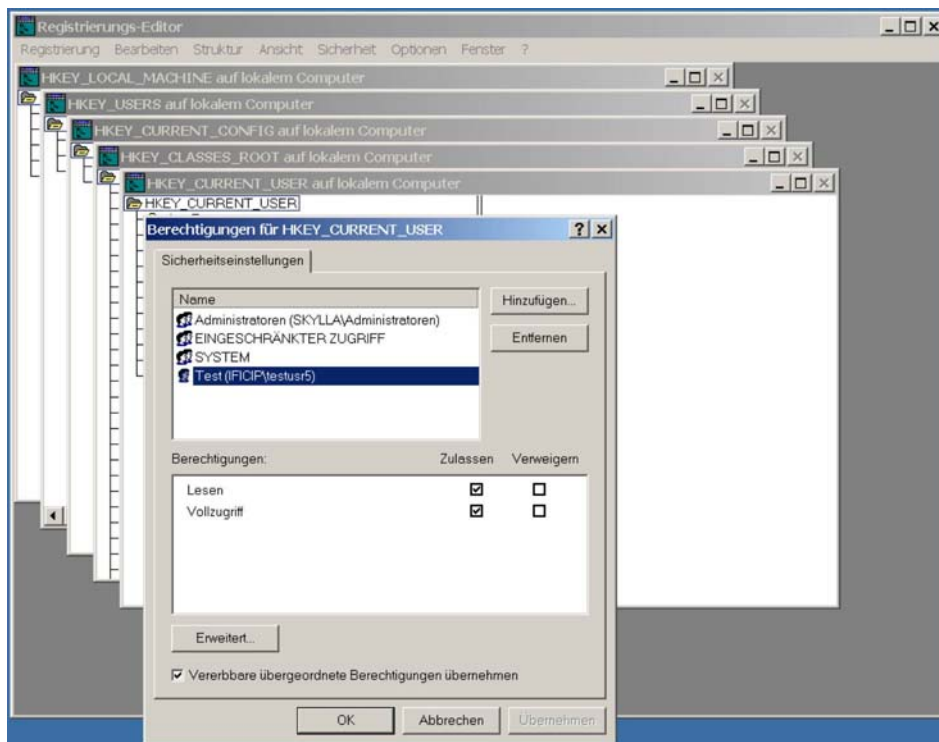


Abb. 51: Profil mit korrekt gesetzten Berechtigungen. Der Besitzer des Profils ist in der Liste aufgeführt und hat Vollzugriff auf den Registry-Subtree „HKEY\_CURRENT\_USER“.

Abhilfe lässt sich schaffen, indem das entsprechende Benutzerprofil auf dem Samba-Server gelöscht wird. Windows 2000 legt anschließend automatisch ein neues Profil mit Default-einstellungen an. Vermutlich genügt es auch, nur die betroffene ntuser.dat zu löschen.

## Outlook.pst

Ein weiteres Problem tritt im Zusammenhang mit Outlook 2000 auf. Outlook speichert alle Mails, Kalenderdaten, Termine etc. in der Datei outlook.pst, die defaultmäßig im Ordner C:\Dokumente und Einstellungen\Benutzername\Lokale Einstellungen\Anwendungsdaten\Microsoft\Outlook abgelegt wird. Die Dateien in diesem Verzeichnis werden nach dem Logout des Benutzers nicht auf den Samba-Server zurückkopiert. Beim nächsten Login findet Outlook nun diese Datei nicht mehr. Es sollte daher der Samba-Server entsprechend konfiguriert werden, dass diese Datei zurückkopiert wird, falls ein Einsatz von Outlook 2000 auf den Clients geplant ist.

## Weitere Hinweise – Microsoft Office XP

Bei der Installation von Office XP sind einige Besonderheiten zu beachten. Die Vorgehensweise ist in [SGIh], S. 269 im Detail beschrieben.

## 4. Microsoft Software Update Service (SUS)

Mit dem Microsoft Software Update Service (SUS) lassen sich „Wichtige Updates“ (Critical Updates) und seit kurzem auch „Service Packs“ von einem Server aus auf Clientrechnern installieren. SUS unterstützt im Moment die Microsoft Betriebssysteme Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advanced Server, Windows XP Professional und Windows XP Home Edition.

Software aus der Kategorie „Empfohlene Updates“ (d.h. Updates, die von Microsoft nicht als kritisch eingestuft werden), installiert SUS im Moment nicht. Dies gilt auch für diverse MS-Anwendungen wie Mediaplayer 9 oder Java Virtual Machine, die zwar auf der Microsoft Windows Update-Website [WU] liegen, aber nicht mittels SUS distribuiert werden können. In der Regel lässt sich derartige Software aber mit der in Kapitel 3 beschriebenen Symantec Ghost AI-Funktion installieren.

Laut Microsoft ist auch eine Erweiterung der Funktionalität von SUS in Planung.

### **Hinweis:**

Die Hardwareanforderungen an den Server, auf dem SUS laufen soll, sind laut Microsoft:

*The minimum configuration for a server running Software Update Services is:*

- *Pentium III 700 MHz or higher processor.*
- *512 megabytes of RAM.*
- *6 gigabytes (GB) of free hard disk space for setup and security packages.*

*This configuration will support approximately 15000 clients using one server running Software Update Services.*

Quelle: [SUS01], S. 7

Der im CIP-Pool verwendete Server erfüllt diese Requirements teilweise nicht. SUS lief bei unseren Test zwar spürbar langsam, aber fehlerfrei. Wohlgermerkt mit einem einzigen Client als Testrechner – bei Verwendung mehrerer Clients könnte ggf. eine Aufrüstung der Hardware unumgänglich werden.

### 4.1 Konfiguration des SUS-Servers

Der Server sollte vor der Installation auf den neuesten Patchstand gebracht werden. Weiterhin muss Internet Information Services (IIS) 5.0 oder höher installiert sein.

SUS Server liegt unter [SUS02] zum Download bereit.

Nach der Installation startet man den Software Update Service über das Startmenü.

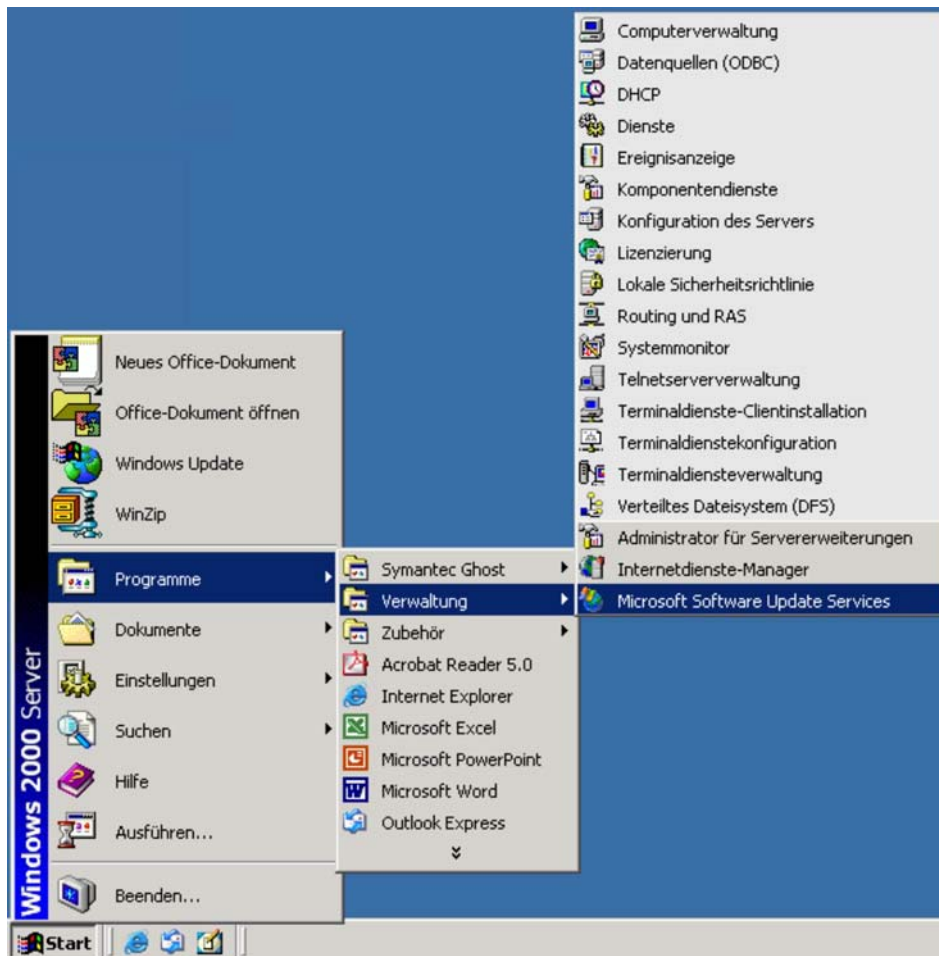


Abb. 52: Nach der Installation von SUS Server findet man im Startmenü unter „Verwaltung“ einen neuen Eintrag: „Microsoft Software Update Services“.

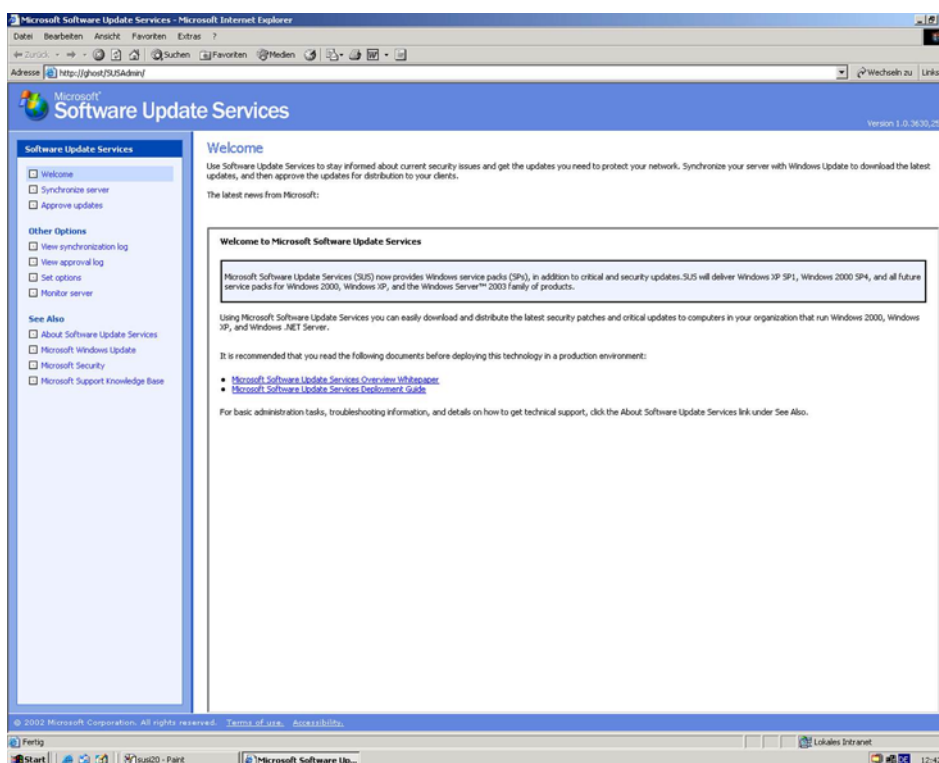


Abb. 53: „Microsoft Software Update Services“ Hauptfenster.

Zuerst muss der SUS Server entsprechend konfiguriert werden. Dies erfolgt im Untermenü „Set Options“ (vgl. Abb. 54).

Die Bedeutungen der einzelnen Optionen sind in [SUS01] erläutert.

Wir haben die folgenden Einstellungen verwendet:

- Bei „**Select a proxy server configuration**“ ist „**Use a proxy server**“ und „**Automatically detect proxy server settings**“ zu aktivieren
- Bei „**Specify the name your clients use to locate this update server**“ ist der NetBIOS Name des Servers oder alternativ der DNS Name bzw. die IP-Adresse einzugeben. Wir haben hier „Ghost“ eingetragen.
- Bei „**Select which server to synchronize content from**“ sollte direkt von den Microsoft Servern synchronisiert werden.
- Bei „**Select how you want to handle new versions of previously approved updates**“ kann eingestellt werden, ob neue Versionen von bereits freigegebenen Updates automatisch freigegeben werden sollen oder ob dies manuell geschieht. Wir haben bei unseren Tests die manuelle Methode verwendet.
- Bei „**Select where you want to store updates**“ sollte als Speicherort „lokales Verzeichnis“ (local folder) gewählt werden. Außerdem genügt es, SUS auf englisch- und deutschsprachige Updates zu beschränken.

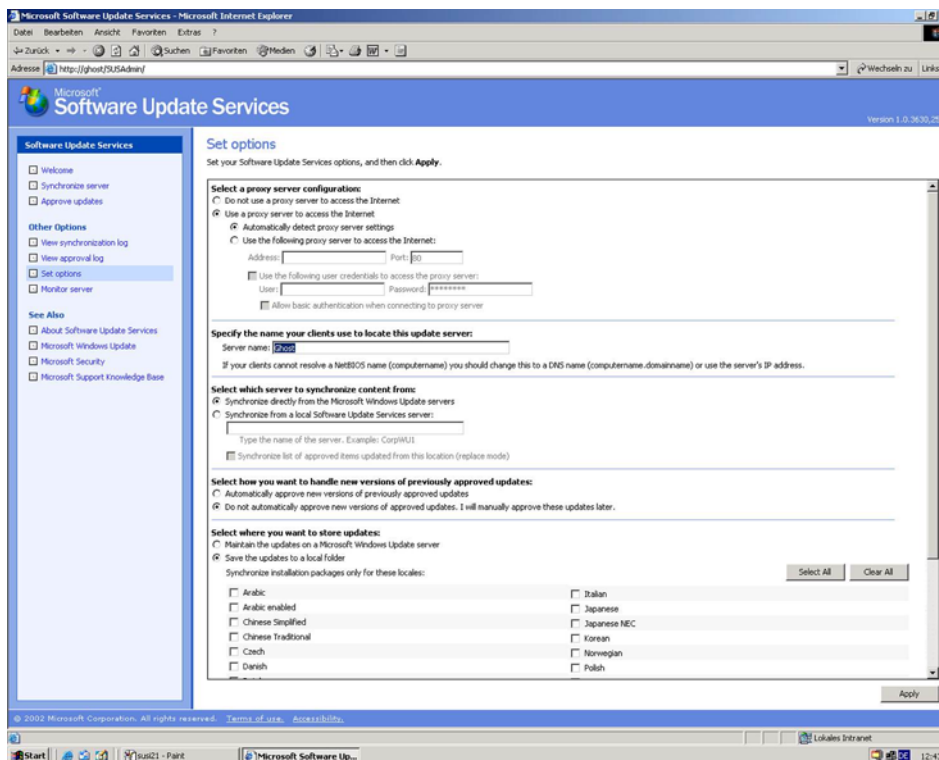


Abb. 54: „Set Options“.

Anschließend muss der SUS Server zuerst einmal mit dem Microsoft Windows Update – Server synchronisiert werden. Dabei werden die benötigten Updates herunter geladen und lokal gespeichert.

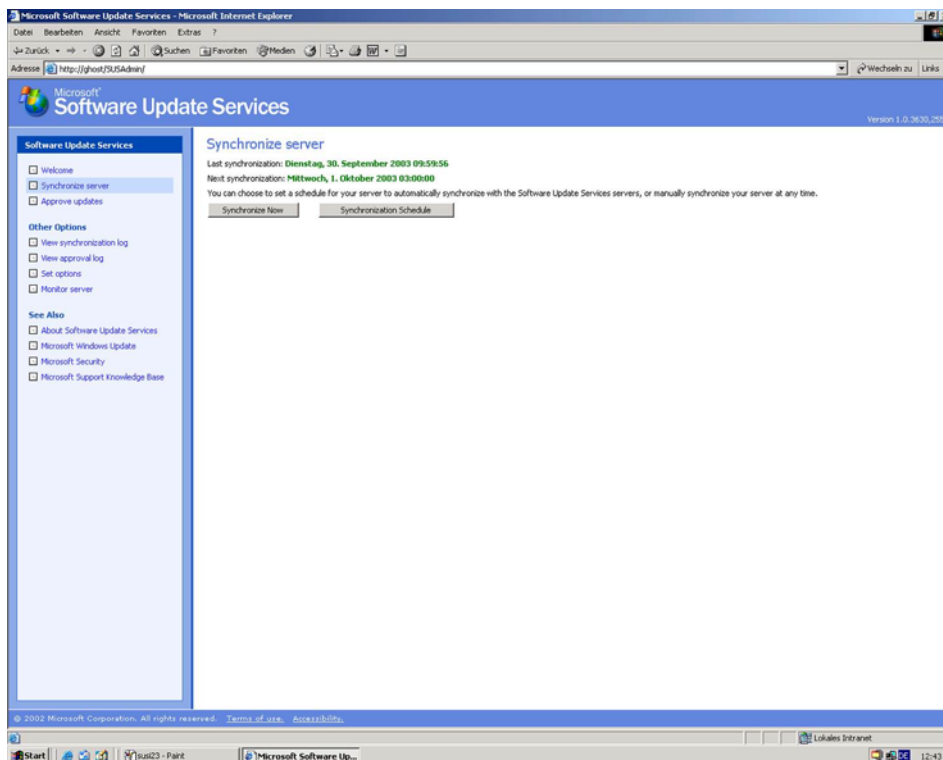


Abb. 55: Das „Synchronize Server“ Menü. Ein Klick auf „Synchronize Now“ startet den Synchronisationsvorgang.

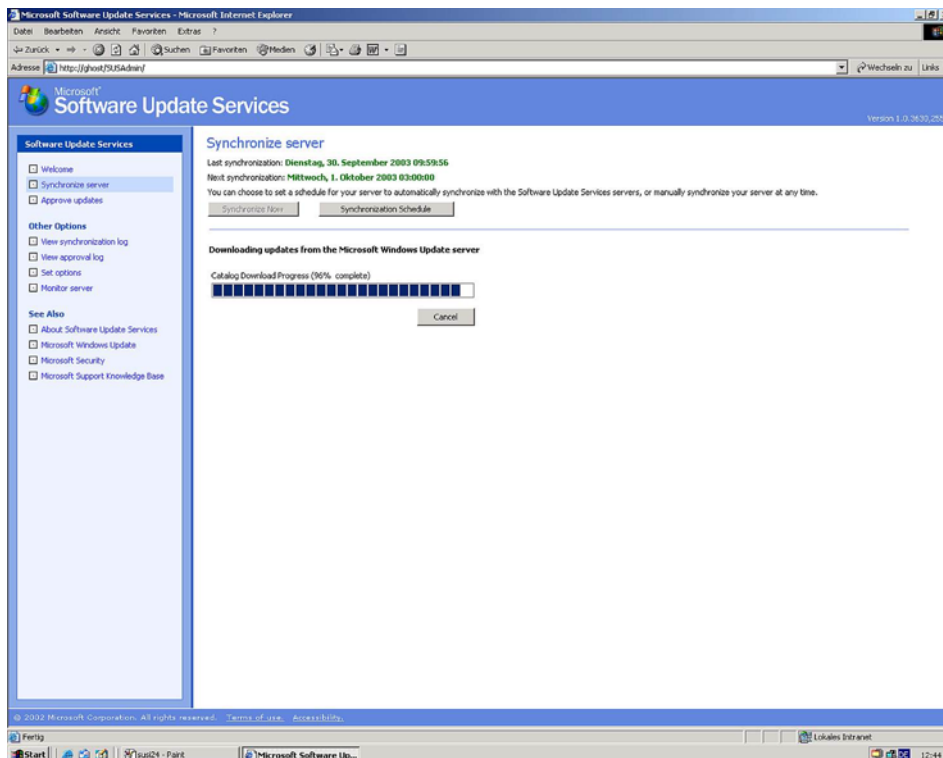


Abb. 56: Der SUS Server wird nun synchronisiert.

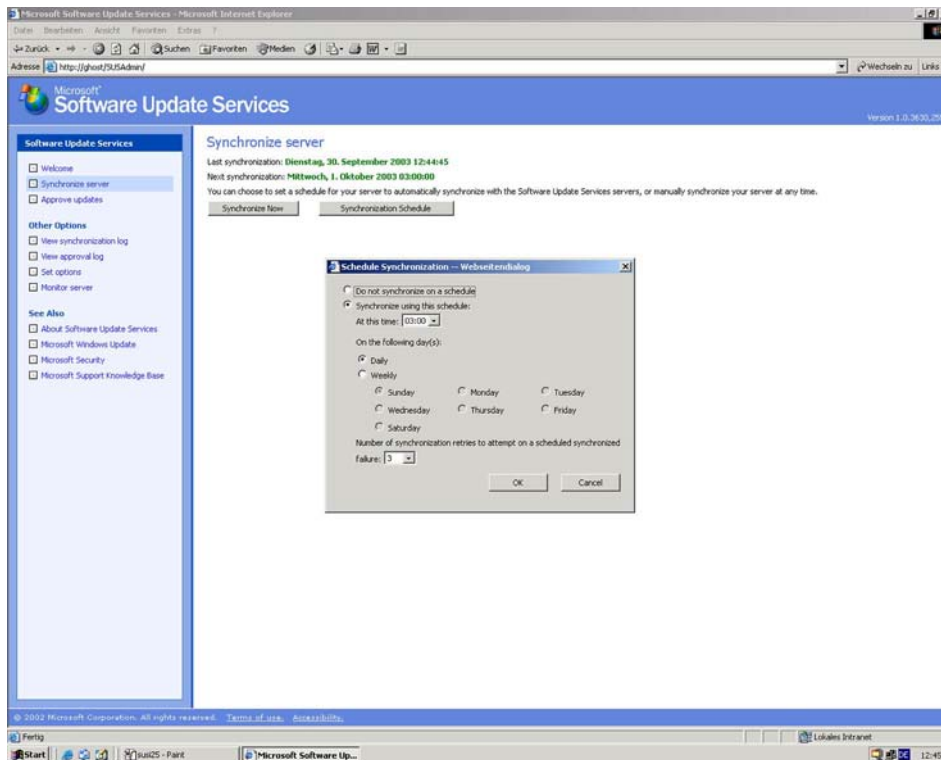


Abb. 57.: Der Synchronisationsprozess lässt sich auch automatisieren. Mittels „Synchronization Schedule“ kann man einen Zeitplan erstellen. Die Synchronisation wird dann regelmäßig zum angegebenen Zeitpunkt durchgeführt.

Nach dem Synchronisationsvorgang müssen die neu heruntergeladenen Updates zuerst freigegeben („approved“) werden. Das geschieht im Menü „**Approve updates**“.

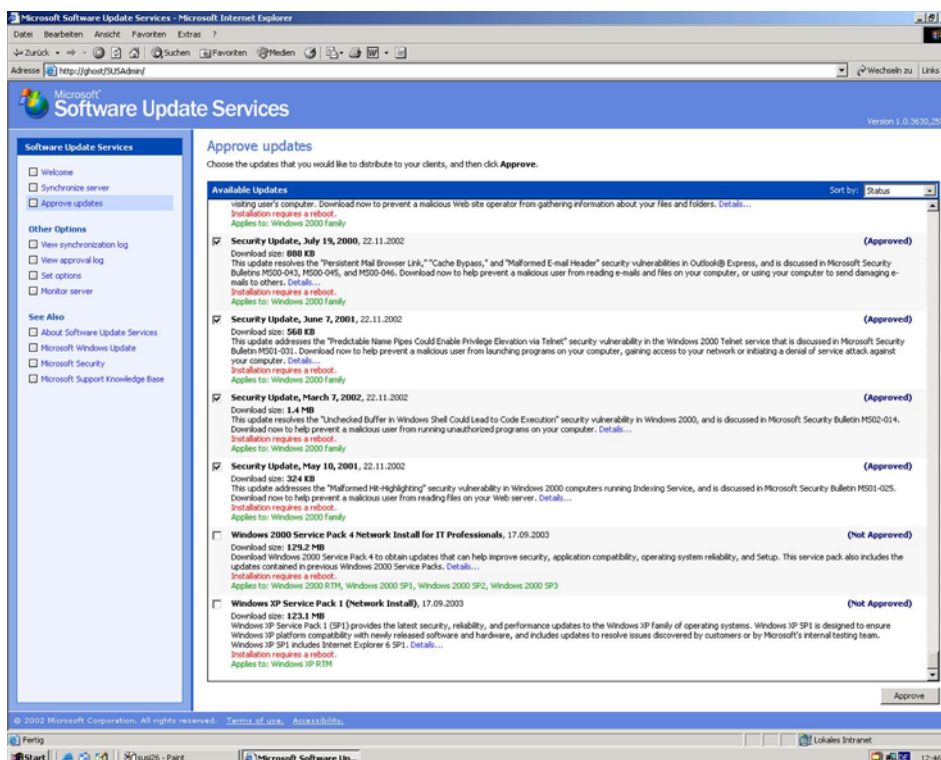


Abb. 58: Das „Approve updates“ Menü. Durch das Setzen des Häkchens und Klick auf den „Approve“-Button lassen sich Updates einzeln freigeben.



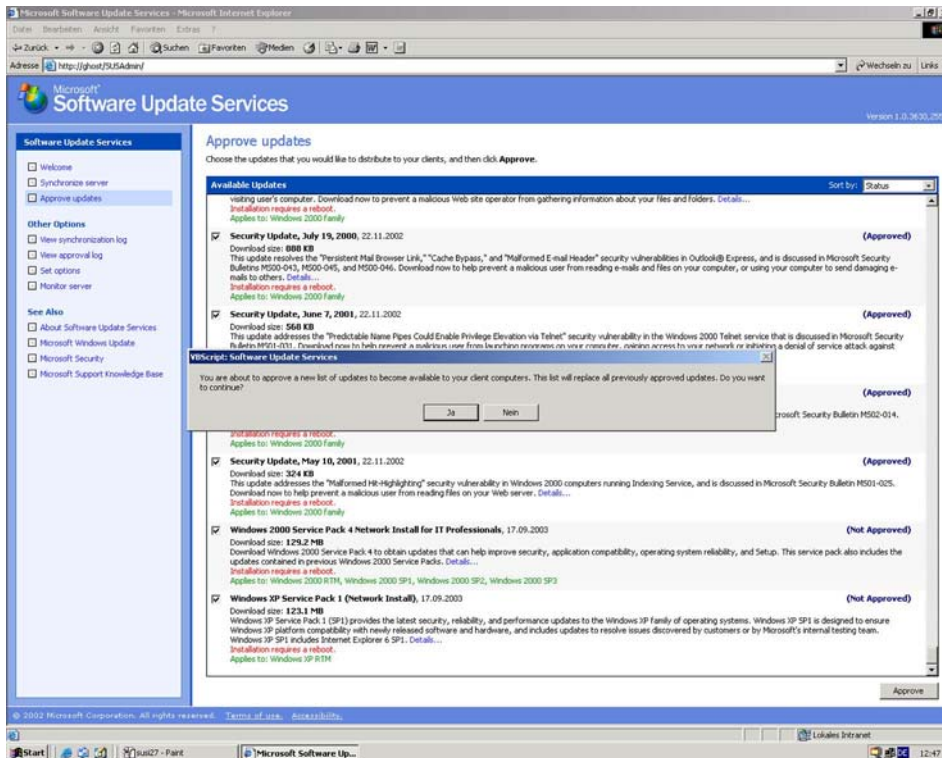


Abb. 59: Um die neuen Updates freizugeben, muss man hier bestätigen...

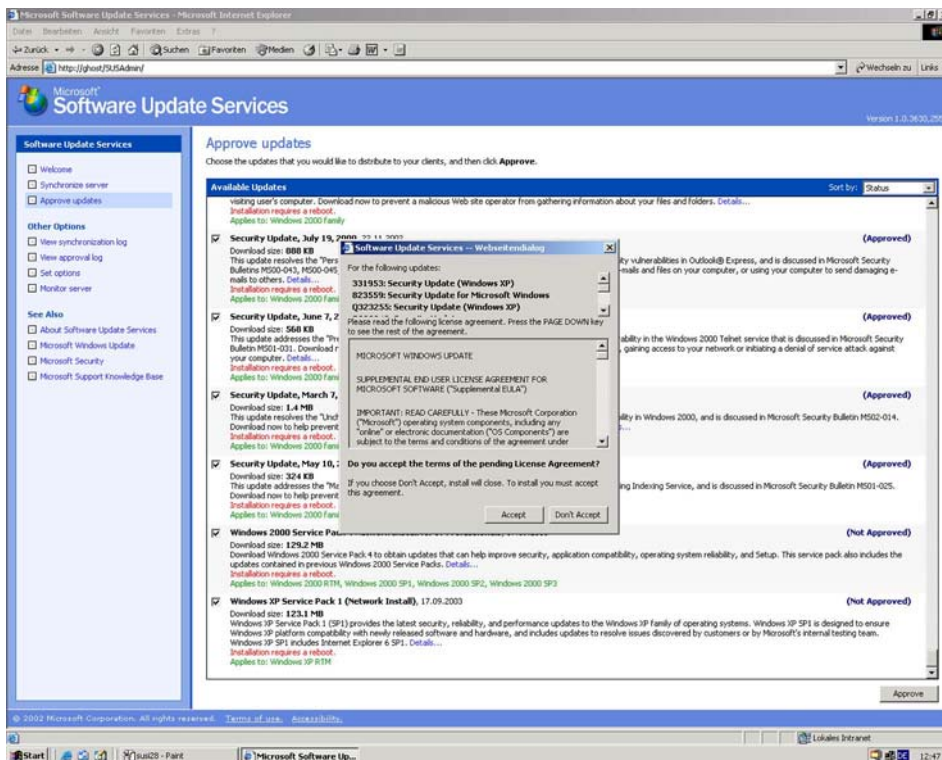


Abb. 60: ... und das End User License Agreement akzeptieren.



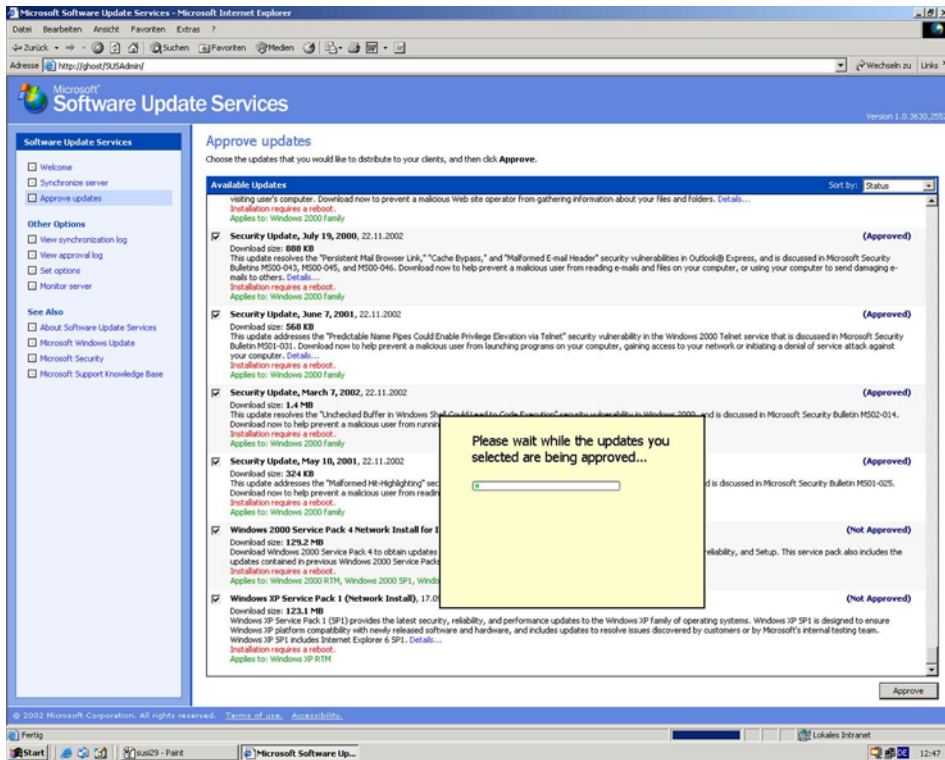


Abb. 61: Anschließend werden die Updates freigegeben...

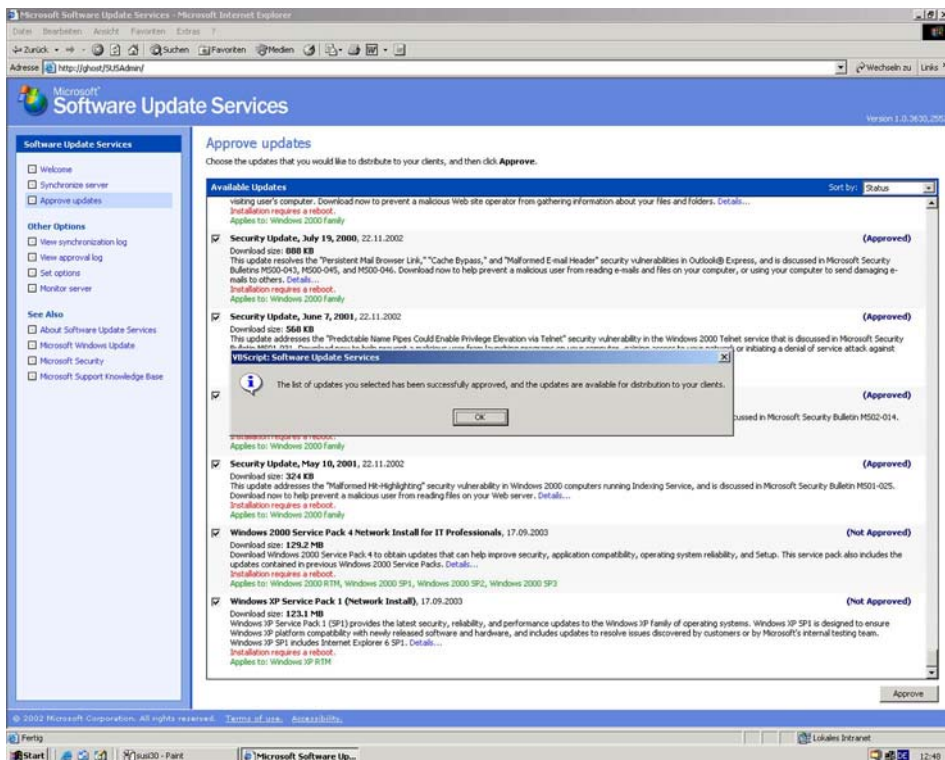


Abb. 62: ... und man erhält diese Bestätigung.

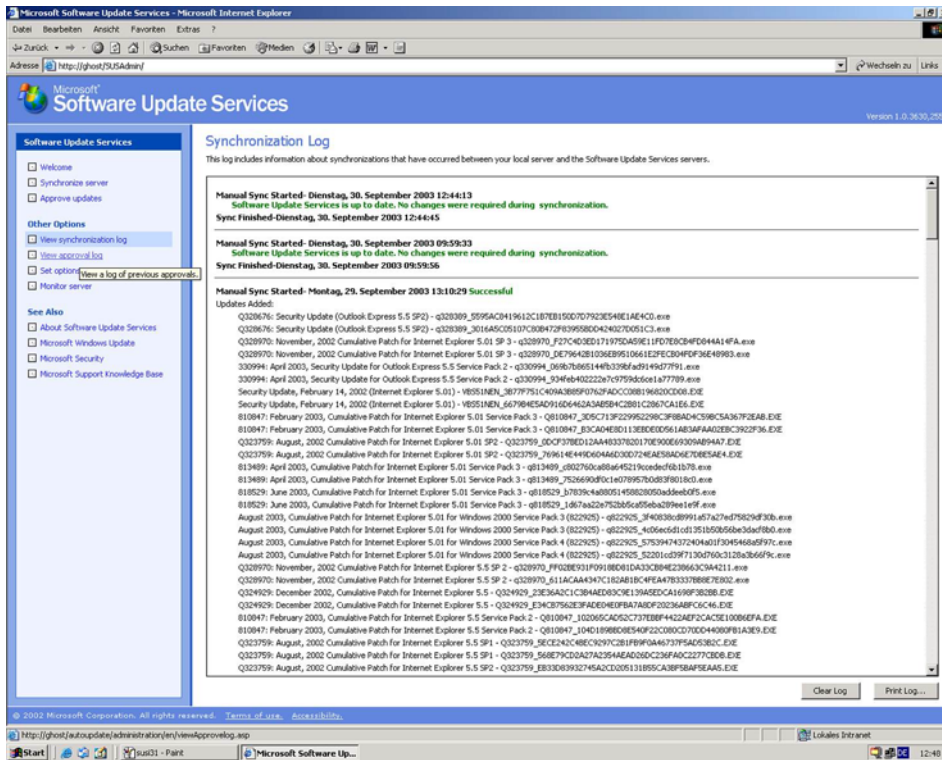


Abb. 63: Das „Synchronisation Log“. Hier kann man sehen, ob die Synchronisation geklappt hat und welche Updates heruntergeladen wurden.

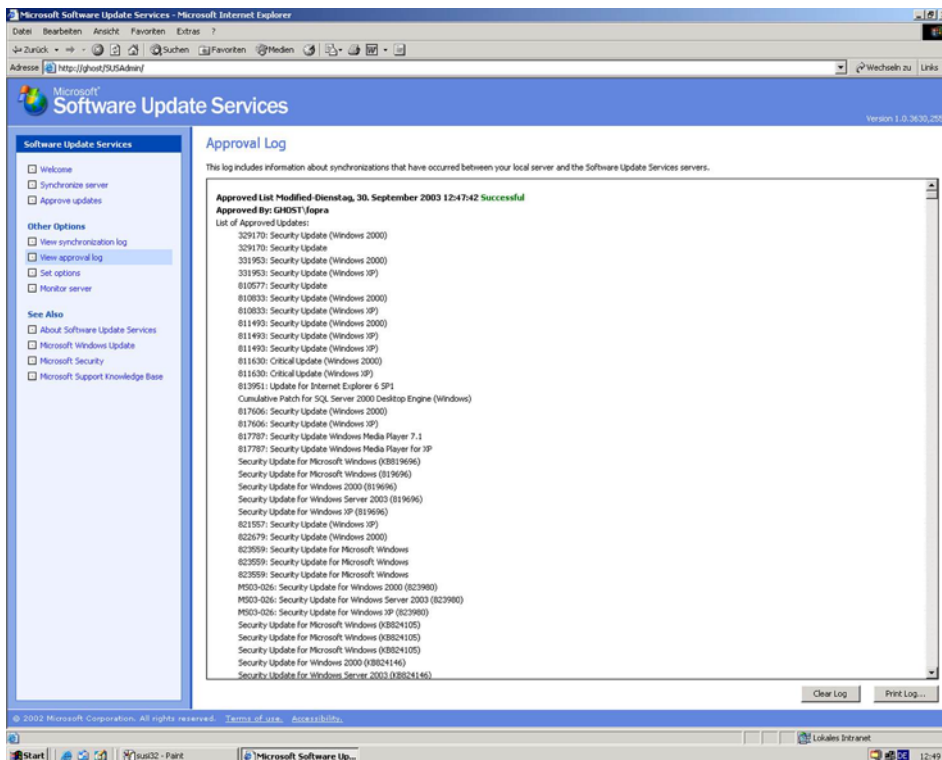


Abb. 64: Das „Approval-Log“ gibt einen Überblick über alle freigegebenen Updates.

## 4.2 Konfiguration der Clientrechner

### Hinweis:

Bei folgenden Betriebssystem-Versionen muss zuerst die neueste „**Automatic Update**“ Version installiert werden:

- Windows 2000 Professional mit Service Pack (SP) 2
- Windows 2000 Server mit SP2
- Windows 2000 Advanced Server mit SP2
- Windows XP Professional
- Windows XP Home Edition

Auf unserem Testrechner war allerdings bereits Service Pack 3 aufgespielt, eine zusätzliche Installation der neuesten „**Automatic Update**“ Version war daher nicht mehr nötig. Die aktuelle „**Automatic Update**“ Version gibt es unter [SUS03] zum Download.

Die „**Automatische Updates**“-Funktion lässt sich auf dem Clientrechner sowohl manuell als auch über Systemrichtlinien konfigurieren. Wir empfehlen die Konfiguration mittels Systemrichtlinie, da sich diese vom Benutzer nicht mehr verändern lässt. Der Vollständigkeit halber seien beide Methoden hier erklärt.

### 4.2.1 Manuelle Konfiguration

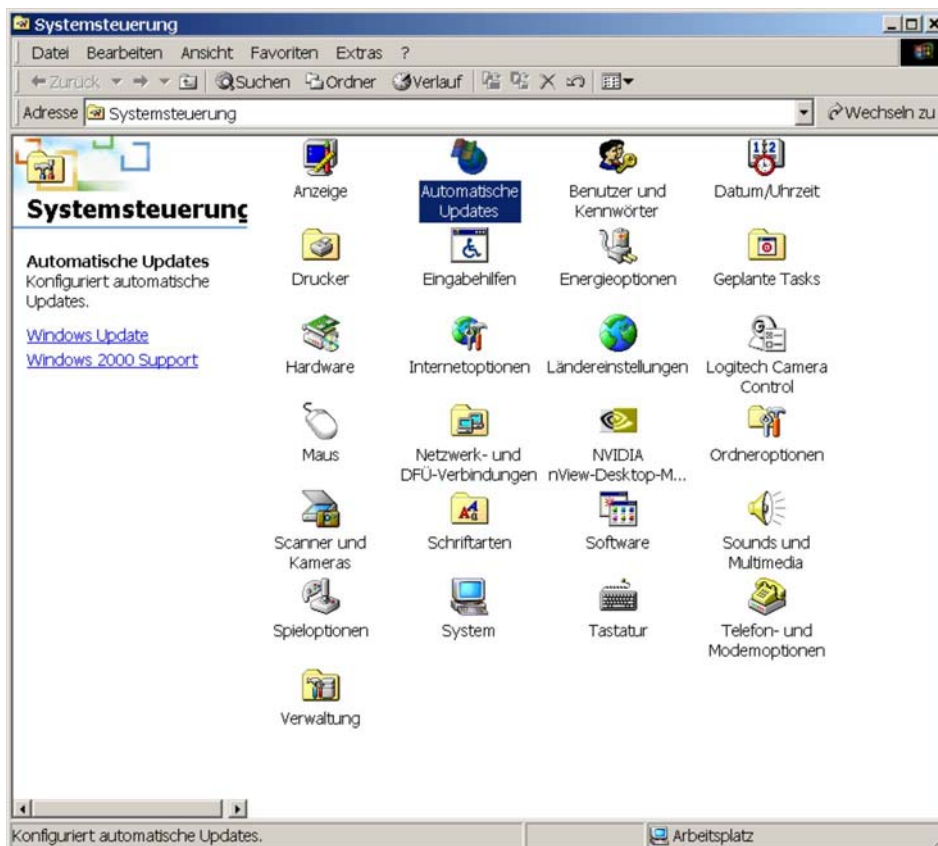


Abb. 65: Die „Automatische Updates“-Funktion findet man in der Systemsteuerung.

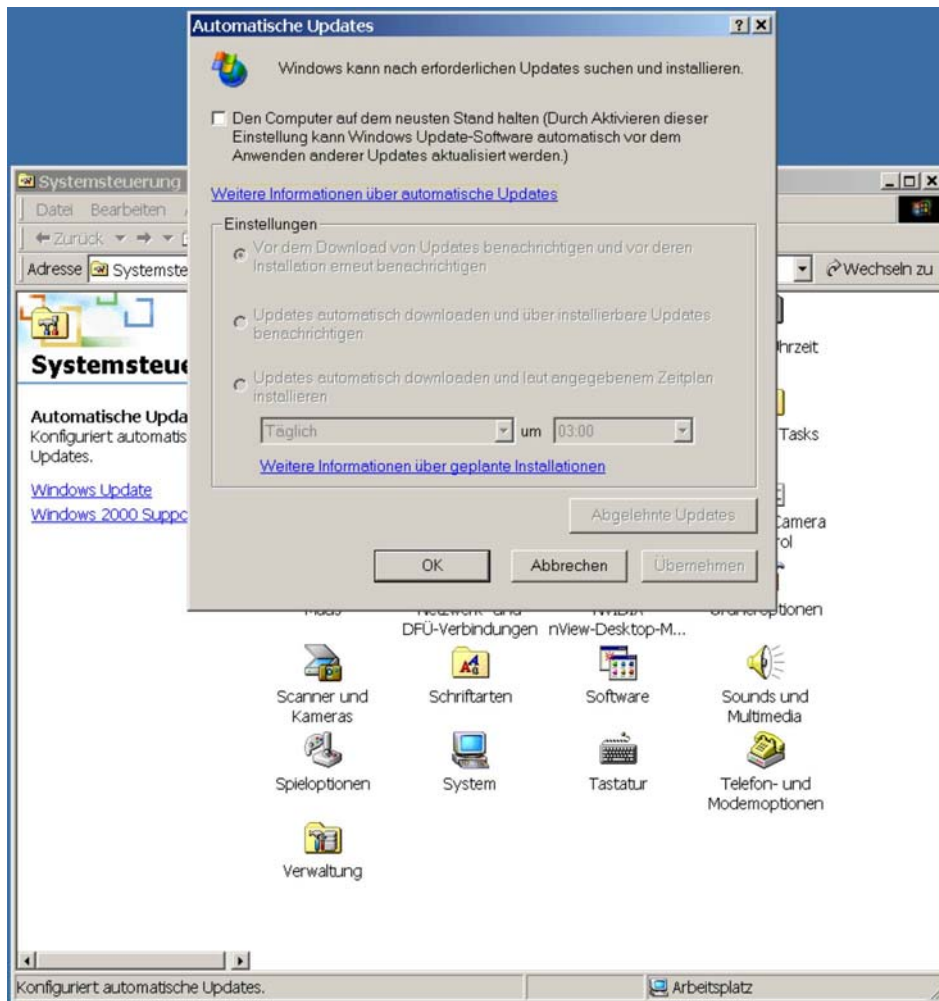


Abb. 66: Beim Öffnen erscheint obiges Menü.

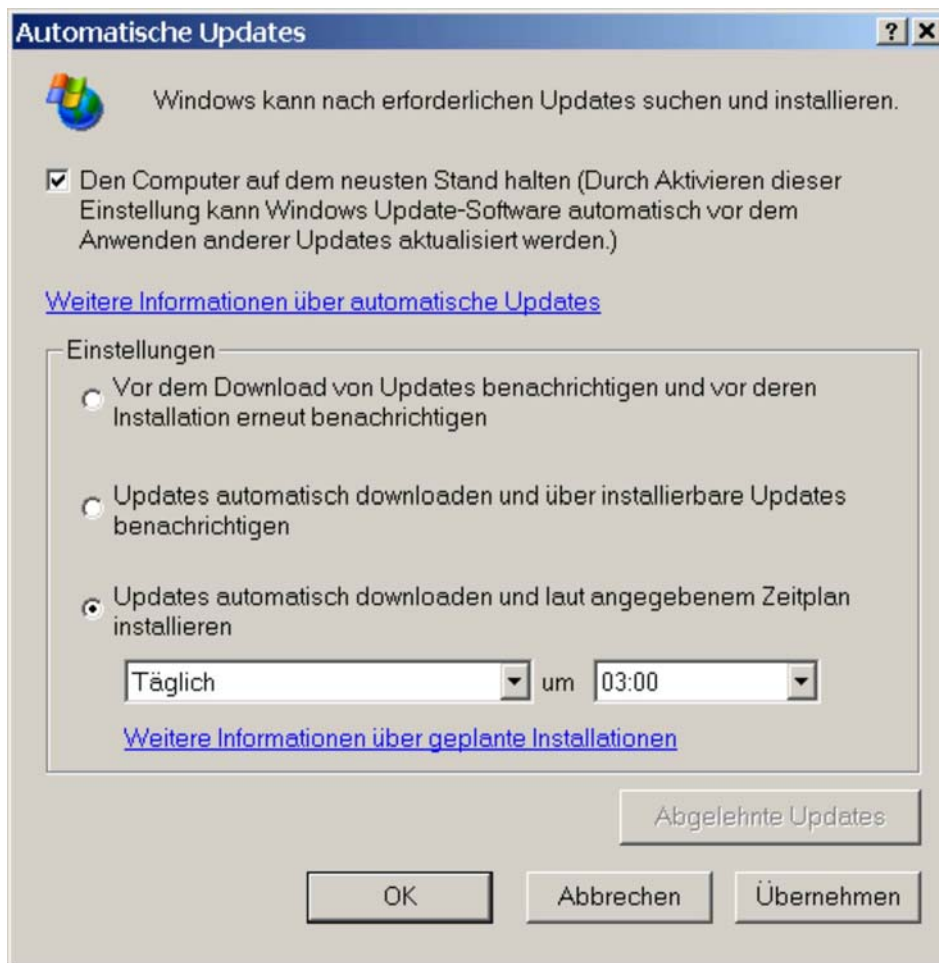


Abb. 67: Nun aktiviert man die Funktion, indem man ein Häkchen bei „Den Computer auf dem neuesten Stand halten“ setzt. Außerdem muss man eine der drei Optionen wählen. Bei der letzten Option erfolgt Download und Installation automatisch zu einem vorgegebenen Zeitpunkt.

Anschließend muss man noch mit regedt32 die Registry editieren und folgende Schlüssel hinzufügen:

Im Zweig

HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU

die Schlüssel

**RescheduleWaitTime**

Typ: REG\_DWORD

Wert: 10

**NoAutoRebootWithLoggedOnUsers**

Typ: REG\_DWORD

Wert: 1

**UseWUserver**

Typ: REG\_DWORD

Wert: 1

sowie im Zweig  
HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate

die Schlüssel

**WUserver**

Typ: REG\_SZ

Wert: http://Ghost (bzw. den korrekten Servernamen)

**WUstatusServer**

Typ: REG\_SZ

Wert: http://Ghost (bzw. den korrekten Servernamen)

Eine detaillierte Erklärung findet sich in [SUS01].

#### 4.2.2 Konfiguration mittels Systemrichtlinie

Einfacher und bequemer geht die Konfiguration mittels Systemrichtlinie. Hierzu lädt man unter [Wuau] die entsprechende ADM Datei herunter.

Die Datei sollte nun zweckmäßigerweise zusammen mit den anderen ADM Dateien im Verzeichnis C:\WINNT\INF abgespeichert werden.

Anschließend startet man den Gruppenrichtlinien-Editor gpedit.msc

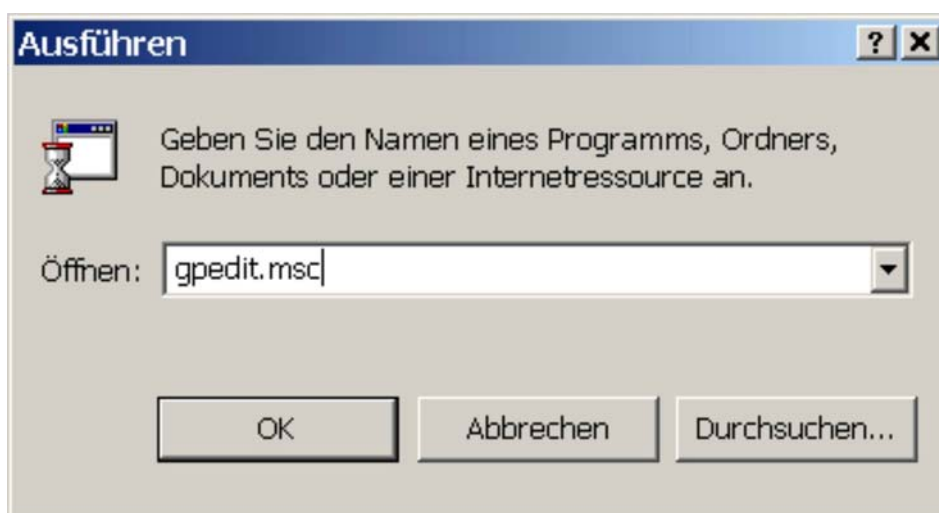


Abb. 68: „Start“, „Ausführen“ und Eingabe von „gpedit.msc“ startet den Gruppenrichtlinien-Editor.



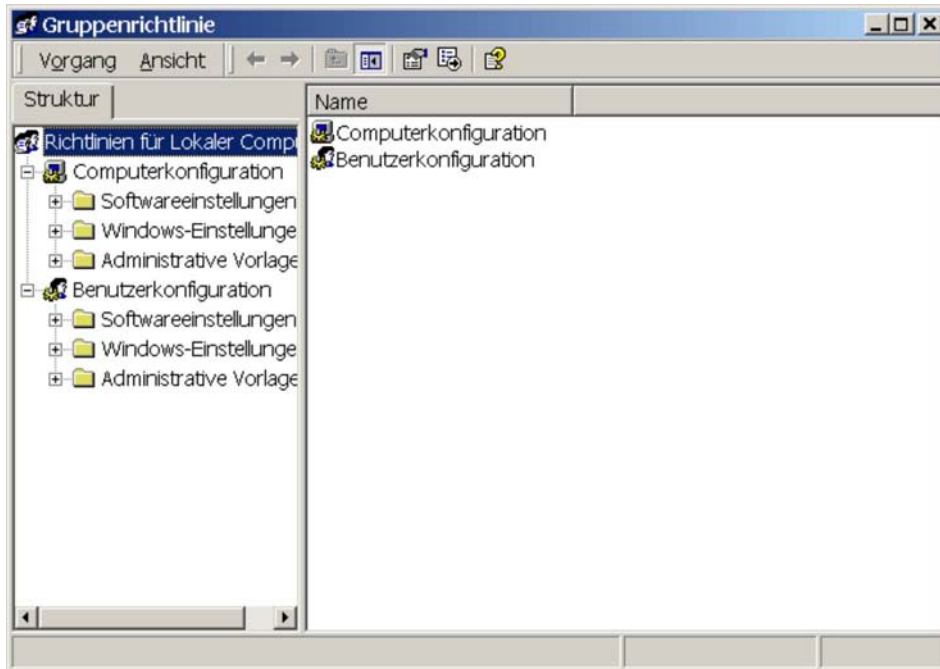


Abb. 69.: Hauptfenster des Gruppenrichtlinien-Editors.

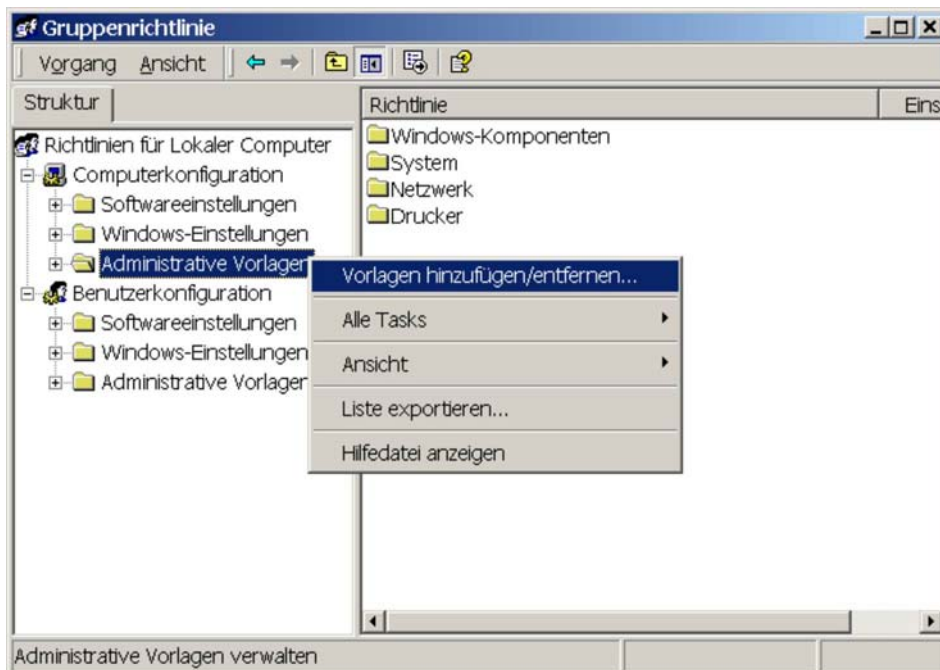


Abb. 70: Bei „Computerkonfiguration“, „Administrative Vorlagen“ öffnet man mit Rechtsklick das Menü und wählt „Vorlagen hinzufügen/entfernen“ aus.



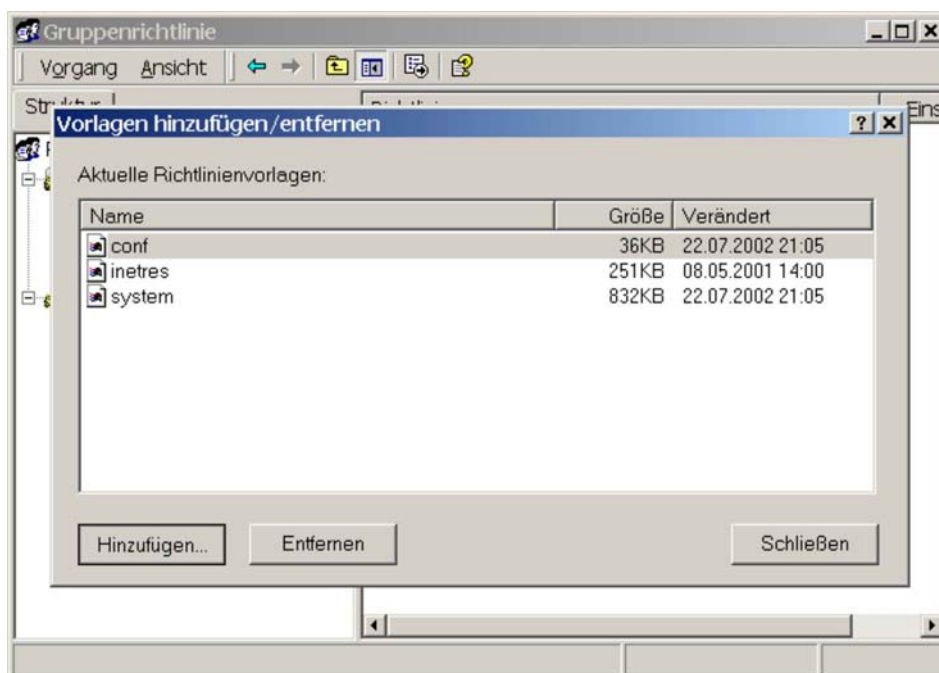


Abb. 71: Hier sieht man die im Moment aktiven Vorlagen. Falls bereits „wuau“ in der Liste steht, muss man es zuerst entfernen. Ansonsten klickt man auf „Hinzufügen“.

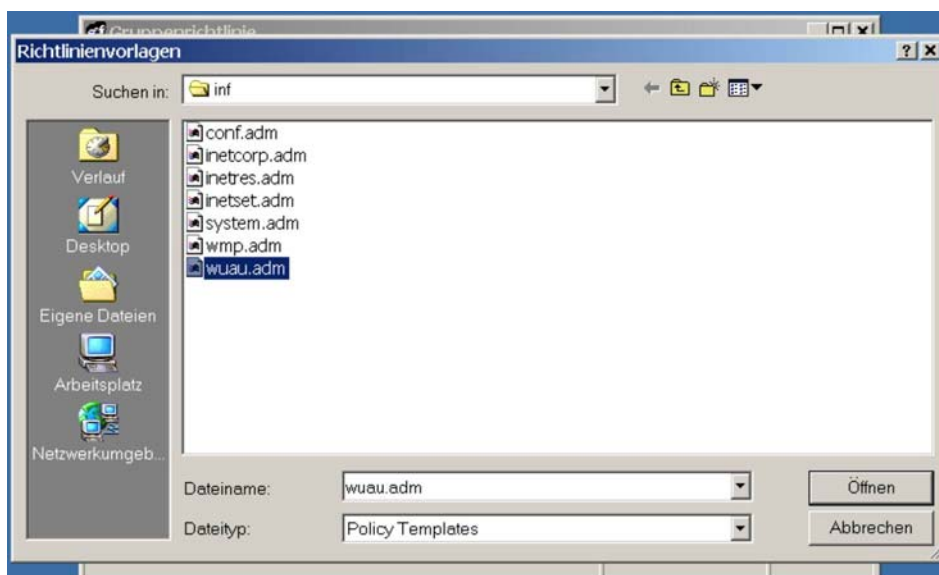


Abb. 72: Nun lädt man die neue wuau.adm.

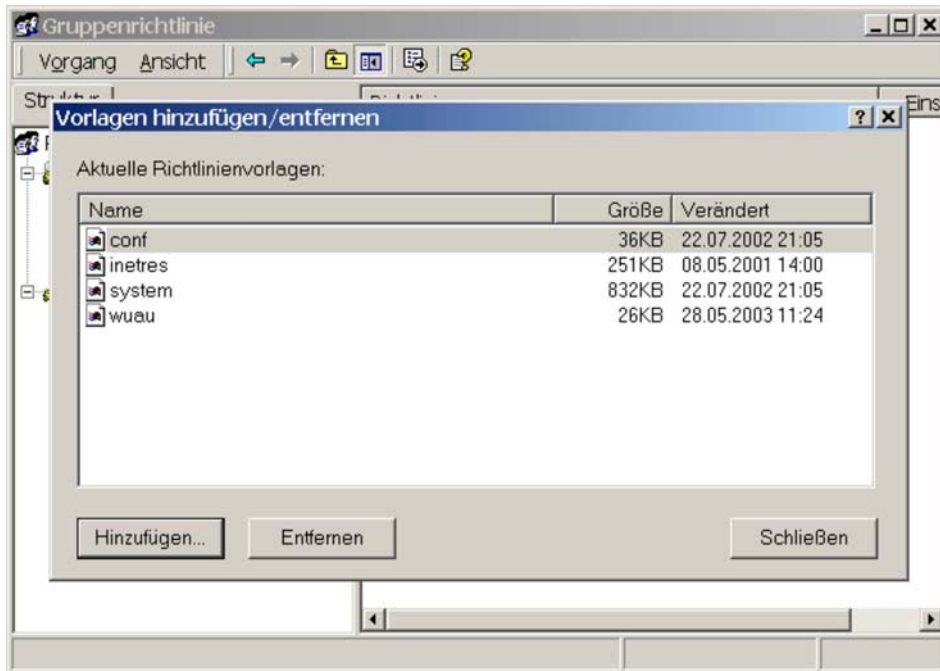


Abb. 73: Nun sollte es so aussehen und man kann das Fenster schließen.

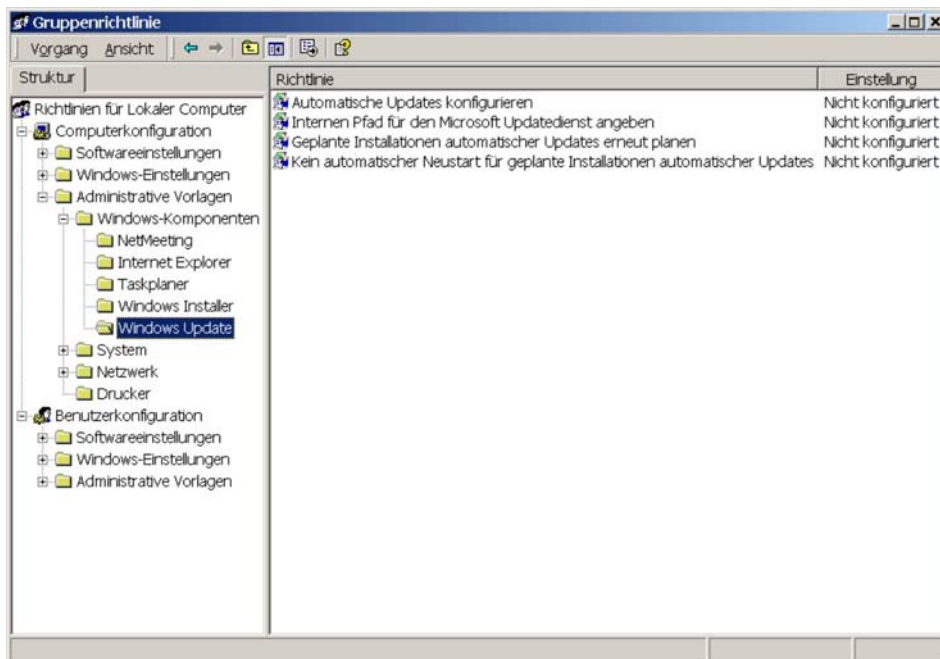


Abb. 74: Unter „Computerkonfiguration“, „Administrative Vorlagen“, „Windowskomponenten“, „Windows Update“ kann man nun die Windows Update-Funktion des Clientrechners konfigurieren.

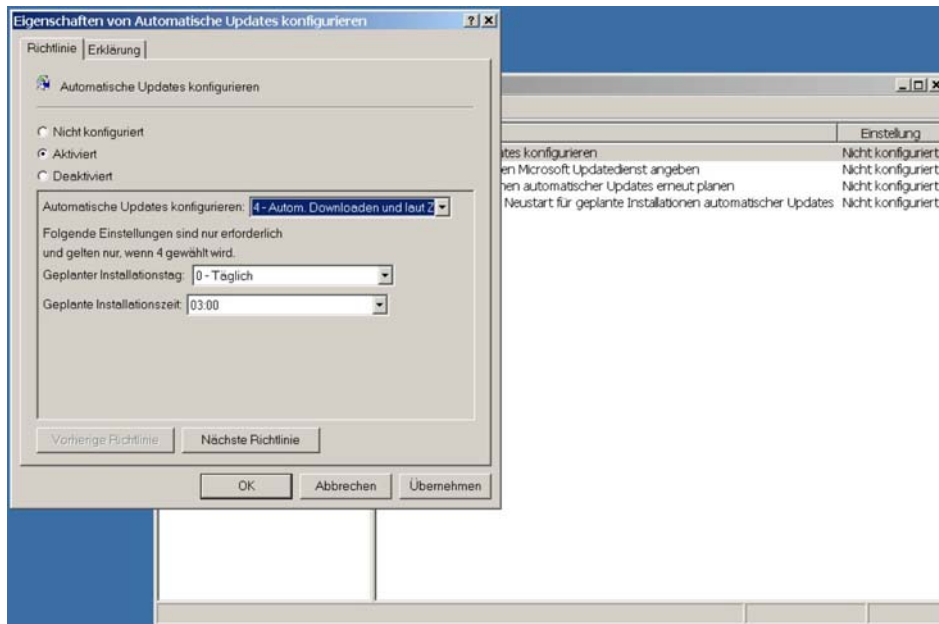


Abb. 75: „Automatische Updates konfigurieren“ aktiviert man und wählt die entsprechenden Installationsoptionen aus. „4 – Autom. Downloaden und laut Zeitplan installieren“ entspricht der 3. Option im Windows Update Menü in der Systemsteuerung (vgl. Abb. 67).

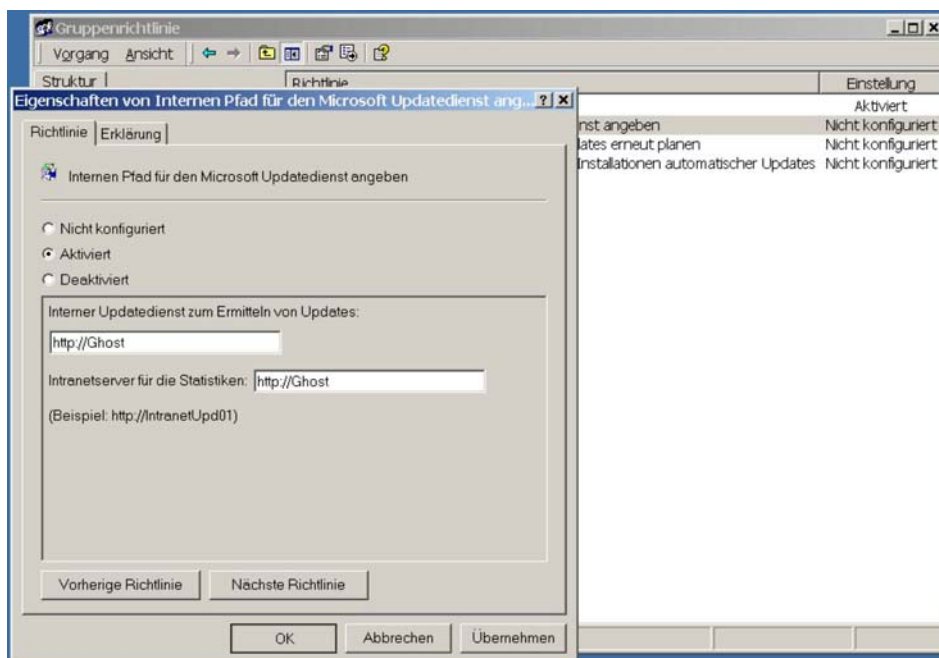


Abb. 76: Bei „Interner Pfad für den Microsoft Updatedienst angeben“ ist zweimal der Name des SUS Servers einzutragen (in unserem Fall „http://Ghost“).

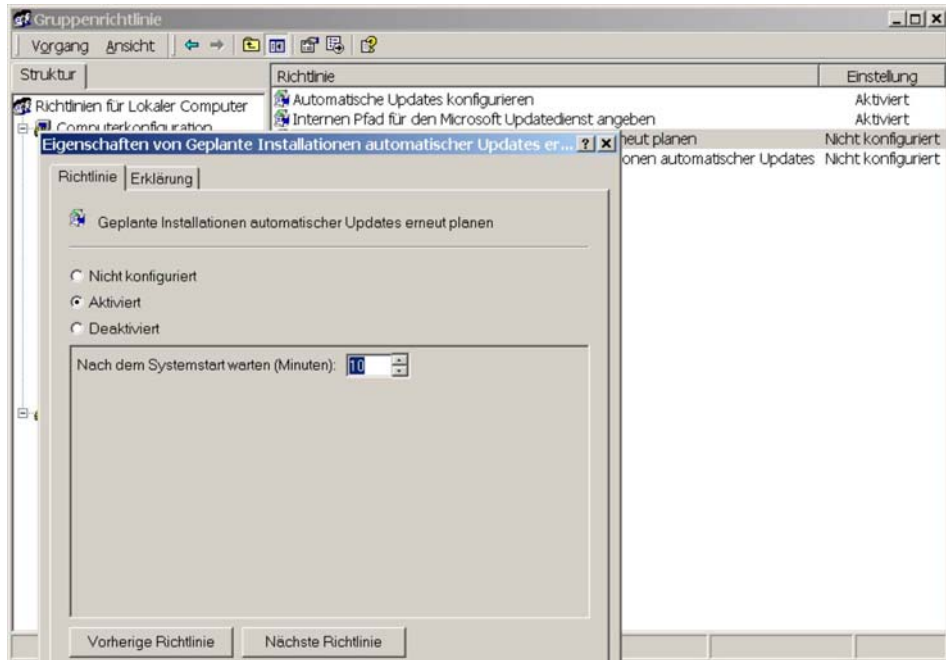


Abb. 77: Bei „Geplante Installation automatischer Updates erneut planen“ haben wir wie in [SUS01] empfohlen 10 Minuten gewählt.

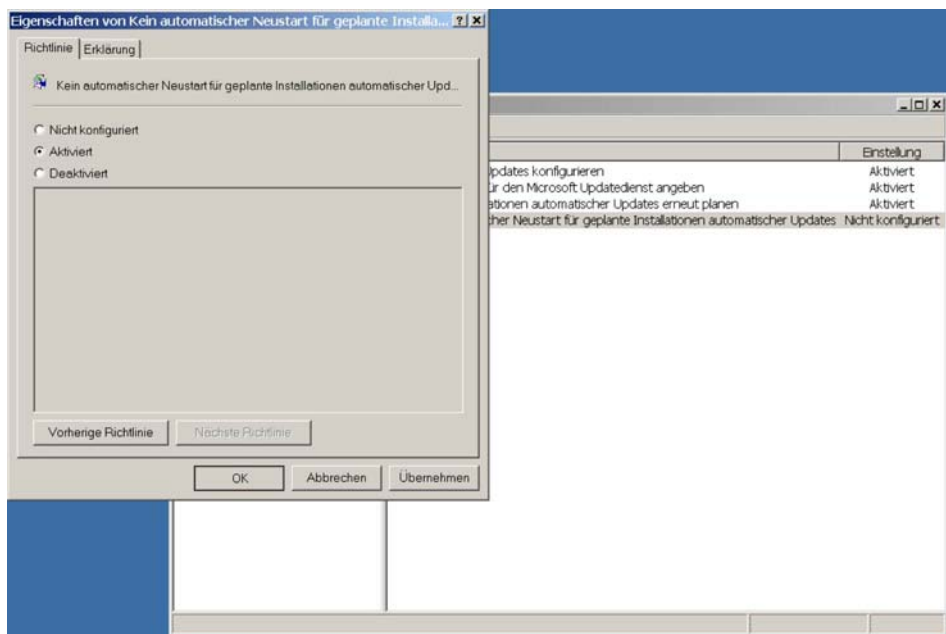


Abb. 78: „Kein automatischer Neustart für geplante Installationen automatischer Updates“ sollte aktiviert werden. Diese Option verhindert, dass der Rechner automatisch neu gestartet wird, während ein Benutzer eingeloggt ist.

Damit ist Software Update Service auf dem Client konfiguriert.

Bei dieser Gelegenheit kann gegebenenfalls auch gleich noch eine für den Betrieb mit einem Samba-Server empfohlene Option aktiviert werden:

### Windows XP Service Pack 1

There is a security check new to Windows XP (or maybe only Windows XP service pack 1). It can be disabled via a group policy in the Active Directory.

The policy is called:

Computer Configuration\Administrative Templates\System\User Profiles\  
Do not check for user ownership of Roaming Profile Folders

This should be set to Enabled.

Quelle: [Samb], S. 356

Auch bei Windows 2000 SP4 findet sich diese Option:

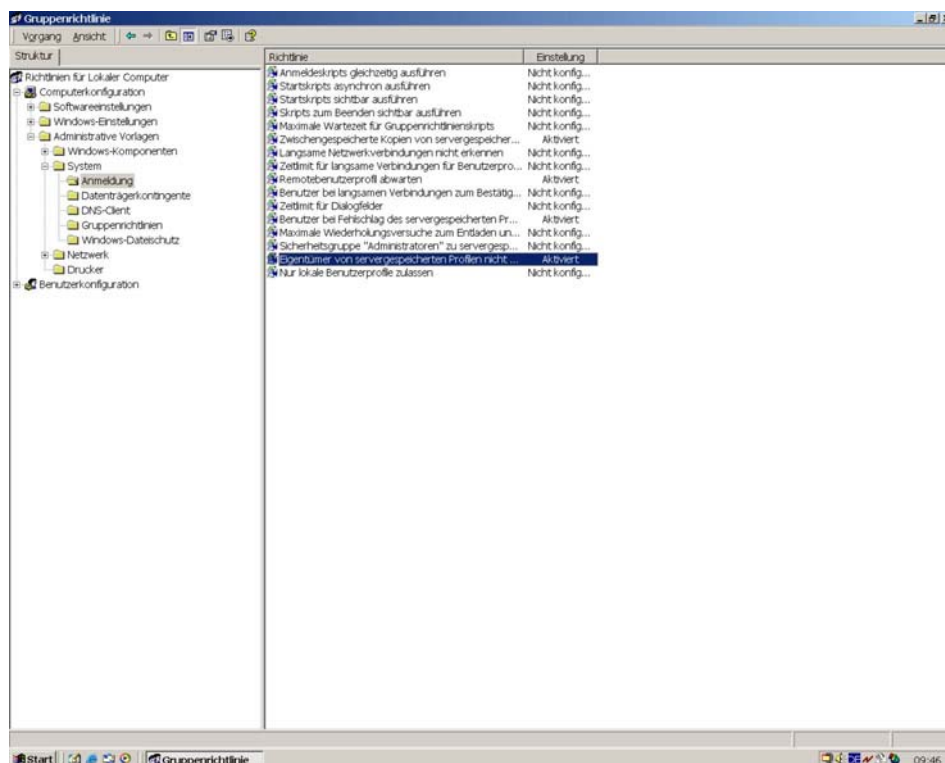


Abb. 79: Die Option „Eigentümer von servergespeicherten Profilen nicht prüfen“ sollte im Zusammenspiel mit einem Samba-Server aktiviert werden.

Software Update Service auf dem Client prüft in einem Intervall von etwa 24h den angegebenen SUS Server und lädt neue freigegebene Updates automatisch von diesem herunter. Das Prüfungsintervall ist nicht konfigurierbar.

Die heruntergeladenen Updates werden dann zum definierten Zeitpunkt automatisch installiert und der Rechner wird gegebenenfalls neu gestartet.

Dazu muss zum Installationszeitpunkt Windows 2000 auf dem Rechner laufen (siehe auch „Allgemeines“, S. 2). Auch sollte der Rechner bei einem Neustart wieder zu Windows 2000 booten.

## 5. Schluss

Die gestellte Aufgabe konnte im Rahmen des Praktikums mit den beiden Software Produkten „Symantec Ghost“ und „Microsoft System Update Service“ nahezu vollständig gelöst werden.

Hierbei kam uns zu Hilfe, dass Microsoft im Verlauf des Praktikums eine neue SUS Version (SUS 1.0 SP1) freigegeben hat, die nun auch die Distribution von Service Packs zulässt.

Zukünftige Versionen des Software Update Services sollen laut Ankündigung von Microsoft weitere Features bieten und u. a. auch die Distribution von Treiberupdates gestatten [SUS05]. Ein Umstieg auf die neuere Version dürfte dann ggf. lohnend sein.

Was SUS (noch) nicht leisten konnte, war allerdings in fast allen Fällen mit Ghost machbar. Lediglich in einem Einzelfall (Internet Explorer 6) kamen wir mit keinem der beiden Softwareprodukte zum Erfolg. Verantwortlich dafür ist die enge Verzahnung dieses Browsers mit dem Betriebssystem sowie der störrische Systemdateischutz (SFP) in neueren MS Betriebssystemen. In solchen Ausnahmefällen muss dann wieder auf die manuelle Installation oder auf Images zurückgegriffen werden.

Im Laufe unseres Praktikums machten uns Hardware- und Softwarefehler des Clients nicht selten das Leben schwer. Sobald wir ein hartnäckiges Problem gelöst hatten, kam nahezu jedes Mal ein Neues dazu. Im Ganzen hatten wir aber trotz der vielen grauen Haare viel Spaß an der Arbeit.

## 6. Quellenverzeichnis

- [Samb] <http://us1.samba.org/samba/devel/docs/Samba-HOWTO-Collection.pdf>
- [SGIh] Symantec Ghost Implementationshandbuch, Version 7.5, PN 07-30-00482-GE
- [SUS01] [http://www.microsoft.com/windows2000/docs/SUS\\_Deployguide\\_sp1.doc](http://www.microsoft.com/windows2000/docs/SUS_Deployguide_sp1.doc)
- [SUS02] <http://www.microsoft.com/windowsserversystem/sus/default.mspx>
- [SUS03] <http://www.microsoft.com/windows2000/downloads/recommended/susclient/default.asp>
- [SUS04] <http://www.microsoft.com/windowsserversystem/sus/susfaq.mspx>
- [SUS05] Karsten Violka. „Erste Einblicke in SUS 2.0“ c't 24/2003, S. 54
- [WU] <http://v4.windowsupdate.microsoft.com/de/default.asp>
- [Wuau] <http://download.microsoft.com/download/2/d/c/2dc07364-2fcb-4b82-adc7-2553915997b3/wuau.adm>



## 7. Anhang

### Performance-Messungen

#### a) Symantec Ghost AutoInstall

Softwarepaket	Installationsdauer	Deinstallationsdauer	Paketgröße	Installationsgeschwindigkeit
Microsoft Office 2000 Premium	1min57sec	-	130.699.039 Bytes	1.091 KB/sec
Opera 7.20	53sec	18sec	35.282.625 Bytes	650 KB/sec
Netscape Navigator 7.01	48sec	33sec	26.254.135 Bytes	534 KB/sec
Jasc Paintshop Pro 7.04	1min	-	68.366.450 Bytes	1113 KB/sec
Adobe Photoshop 6.0	1min17sec	22sec	89.954.078 Bytes	1141 KB/sec
Winzip 8.1 SR-1	34sec	16sec	2.639.337 Bytes	76 KB/sec

Je nach Paketgröße wird für die Installation etwa 1-2 Minuten benötigt. Die Performance hängt weiterhin auch von der Geschwindigkeit der Clientrechner und des Netzwerks ab. Im Test wurden unter Optimalbedingungen teilweise über 1000 KB/sec erreicht.

#### b) Microsoft Software Update Service

**Servicepack 4** für Windows 2000 (129 MByte)

Zeit für Download vom Server: 27sec

Zeit für Installation: 6min21sec (inklusive Neustart des Rechners)

Im Gegensatz zu Symantec Ghost AI wird bei Microsoft SUS zuerst das Softwarepaket vom Server heruntergeladen und anschließend installiert. Die Geschwindigkeit des Downloadvorganges hängt von Netz- und Serverlast ab, der Installationsvorgang erfolgt lokal auf dem Client. Die Geschwindigkeit ist unterschiedlich, die meisten SUS-Pakete sind jedoch nur wenige Megabyte groß und werden daher innerhalb von etwa 30-60 Sekunden installiert. Der anschließend notwendige Neustart benötigt in der Regel nochmals zwei Minuten.