Einführung

Die Ausweitung der Kommunikationsnetze in den letzten Jahren und dabei insbesondere das schwindelerregende Wachstum des Internets hat zu einem sprunghaften Anstieg der E-Mail-Nutzung geführt.

Einer der größten Vorteile der E-Mails ist die Möglichkeit, Dateien zu senden und zu empfangen. Gleichzeitig hat sich damit aber auch eine neue Eintrittstür für Viren geöffnet.

Dokumente werden heute sehr oft per E-Mail ausgetauscht. Das hat im wesentlichen zur enormen Ausbreitung von Word- und Excel-Viren geführt. Dabei sollte jedoch nicht vergessen werden, daß über die E-Mail jede Art von Viren gesendet und empfangen werden kann und nicht nur die Word- und Excel-Viren.

Die herkömmlichen Antiviren-Programme sind aus den folgenden Gründen nicht fähig, auf effiziente Weise Viren aufzuspüren und zu vernichten, die sich in den E-Mail-Nachrichten befinden:

1. Normalerweise werden die E-Mail-Nachrichten in besonderen E-Mail-Datenbanken abgespeichert. Diese verfügen über ein eigenes Format und besondere Komprimierungs- und/oder Verschlüsselungstechniken, die das Scannen mit herkömmlichen Antiviren-Programmen unmöglich machen.

2. Sehr häufig werden E-Mail-Nachrichten und deren Attachments in einem Server gespeichert, zu dem ein herkömmliches Antiviren-Programm keinen Zugang hat.

Aus den o.g. Gründen muß ein Antivirus für die E-Mail speziell entwickelt werden, um dort befindliche Viren entdecken und vernichten zu können. Ein Antivirus für E-Mails muß daher folgende Grundfähigkeiten besitzen:

- Automatisches Scannen aller Nachrichten im Augenblick ihres Empfangs.
- Automatisches Scannen aller Nachrichten, wenn sie geöffnet werden.
- Automatisches Scannen aller Nachrichten beim Versuch sie zu senden. Auf diese Weise wird die Möglichkeit ausgeschlossen, mit Viren verseuchte Nachrichten zu versenden.
- Automatisches Scannen aller zu speichernden Nachrichten.
- Scannen aller E-Mail-Nachrichten in dem vom Benutzer gewünschten Moment.
- Integration in das E-Mail-Programm.
- Möglichkeit, komprimierte Dateien zu scannen.
- Möglichkeit, verschachtelte Nachrichten (Nachrichten, die sich in anderen Nachrichten befinden) zu scannen.

Panda Antivirus für Exchange/Outlook ist ein Antivirus für die E-Mail, das alle diese Fähigkeiten besitzt. Darüber hinaus verfügt es auch noch über einige andere Eigenschaften, die seine Funktionalität vervollständigen und es zu einem potenten Werkzeug mit vielen Einstellmöglichkeiten machen, das alle Risiken bei der Arbeit mit E-Mail-Nachrichten ausschließt.

HINWEIS
In diesem Handbuch werden die folgenden Produkte beschrieben:

- Panda Antivirus Exchange/Outlook

- Panda Antivirus Exchange/Outlook Network Client

Das erste Produkt wird in Einzelplatzcomputern installiert und das zweite ermöglicht die Verteilung des genannten Antivirus auf alle Arbeitsplätze eines Netzes, um so die Arbeit des Netzwerkadministrators zu erleichtern.

Nähere Informationen über das von Ihnen gekaufte Produkt finden Sie im entsprechenden Teil des Handbuchs.

Installation

Systemanforderungen

Panda Antivirus Exchange/Outlook benötigt:

- IBM kompatibler Computer, mit dem Windows 95, 98 oder Windows NT Workstation 3.51 oder 4.0 ausgeführt werden kann.
- MS-Exchange und/oder MS-Outlook
- 3 MB Speicherkapazität auf der Festplatte.

Installation

Zum Installieren von Panda Antivirus Exchange/Outlook legen Sie einfach die Diskette 1 in das Diskettenlaufwerk und führen das Programm SETUP.EXE aus.

Während des Installationsprozesses öffnet sich eine Reihe von Fenstern, in denen Sie aufgefordert werden, die für die Installation notwendigen Daten einzugeben.

Nach Abschluß der Installation sollte der Computer neu gestartet werden. Starten Sie Exchange/Outlook neu, damit das Antivirus für Exchange/Outlook funktionsbereit ist.

Deinstallation

Um Panda Antivirus Exchange/Outlook zu deinstallieren, müssen Sie zunächst das E-Mail-Programm Exchange/Outlook schließen. Gehen Sie dann in die *Systemsteuerung*, wählen Sie dort die Option *Software* und markieren Sie in der Liste Panda Antivirus Exchange/Outlook. Klicken Sie danach auf *Hinzufügen/Entfernen*. Nach einigen Augenblicken ist die Deinstallation abgeschlossen. Versuchen Sie nicht, diese Version durch Löschen des Ordners zu deinstallieren, in dem sie installiert wurde. Führen Sie die Deinstallation immer nach den vorgegebenen Anweisungen durch.

Wie mit Panda Antivirus Exchange/Outlook gescannt wird

Scan auf Abruf

Zum Scannen eines bestimmten Ordners müssen Sie diesen zunächst markieren. Wenn Sie einen Ordner auswählen, der seinerseits Ordner enthält (z.B. eine Mail-Box), dann werden auch diese untergeordneten Ordner gescannt. Nachdem Sie den Ordner ausgewählt haben, klicken Sie auf die Schaltfläche Scannen in der Standard-Symbolleiste von MS-Exchange/Outlook oder wählen Sie innerhalb der Option Extras im Hauptmenü von MS-Exchange/Outlook die Option Nach Viren scannen.

Nachdem der Scan beendet ist, wird der Ergebnisbericht angezeigt, in dem alle während des Scans entdeckten Vorfälle aufgeführt werden.

Panda Antivirus Exchange/Outlook bietet auch die Möglichkeit, eine oder mehrere Nachrichten zu scannen. Wählen Sie dazu die Nachricht(en) aus, die gescannt werden soll(en). Klicken Sie dann zum Starten des Vorgangs auf Scannen.

Um verschiedene Nachrichten auszuwählen, klicken Sie bei gedrückter Strg-Taste auf die gewünschten Nachrichten. Wenn Sie eine Nachrichtengruppe auswählen möchten, klicken Sie bei gedrückter Shift-Taste auf die erste und letzte Nachricht dieser Gruppe.

Schutz in Echtzeit

Der permanente Schutz ermöglicht es Ihnen, Ihr E-Mail-Programm ohne Angst vor Viren zu nutzen, da Panda Antivirus Exchange/Outlook alle Operationen überwacht, bei denen Sie ein Virenrisiko vermuten.

Der permanente Schutz kümmert sich um das Aufspüren von Viren in:

- allen neu eingehenden Nachrichten.
- allen Nachrichten, die gesendet werden sollen.
- allen Nachrichten, die geöffnet werden, unabhängig davon, ob sie vor oder nach der Installation des Antivirus empfangen wurden.
- allen Nachrichten, die gespeichert werden sollen.

Der permanente Schutz kann ganz einfach durch entsprechendes Klicken auf die entsprechende Schaltfläche in der Standard-Symbolleiste von MS-Exchange/Outlook aktiviert oder deaktiviert werden.

Ihr Panda Antivirus Exchange/Outlook kann sogar komprimierte Dateien und verschachtelte Nachrichten (Nachrichten in anderen Nachrichten) scannen und bietet Ihnen dadurch den bestmöglichen Schutz.

Funktionsweise von Panda Antivirus Exchange/Outlook

Ihr Panda Antivirus Exchange/Outlook ist vollständig in MS-Exchange/Outlook integriert und kann deshalb direkt im E-Mail-Programm gesteuert werden.

Panda Antivirus Exchange/Outlook fügt der Standard-Symbolleiste von MS-Exchange/Outlook die vier folgenden Schaltflächen hinzu:

Scannen: Mit dieser Schaltfläche kann das Scannen des Ordners oder der Nachrichten, die vor Beginn des Scans ausgewählt wurden, gestartet werden. Es werden alle Ordner gescannt, die dem angegebenen Ordner untergeordnet sind. In einem Fenster kann der Scan-Vorgang verfolgt werden. Dort werden die Gruppe der zu scannenden Ordner, der im jeweiligen Moment gescannte Ordner und eine Statusleiste angezeigt.

Ergebnisbericht: Über diese Schaltfläche kann ein Bericht mit den vom Antivirus entdeckten Vorfällen angezeigt werden. Dieser Bericht wird solange gespeichert, bis Benutzer entscheidet, ihn zu löschen.

Antivirus aktivieren oder deaktivieren: Durch Klicken auf diese Schaltfläche kann der permanente Schutz des Panda Antivirus aktiviert bzw. deaktiviert werden. Ist dieser permanente Schutz deaktiviert, durchsucht Ihr Panda Antivirus Exchange/Outlook keine der neu empfangenen oder gesendeten Nachrichten nach Viren. Ebensowenig wird in jenen Nachrichten nach Viren gesucht, die zur Einsicht geöffnet werden. Es ist allerdings möglich, durch Klicken auf die Schaltfläche Scannen jederzeit einen bestimmten Ordner zu durchsuchen. Der Scan beim Starten von Exchange/Outlook wird auch bei deaktiviertem permanentem Schutz durchgeführt.

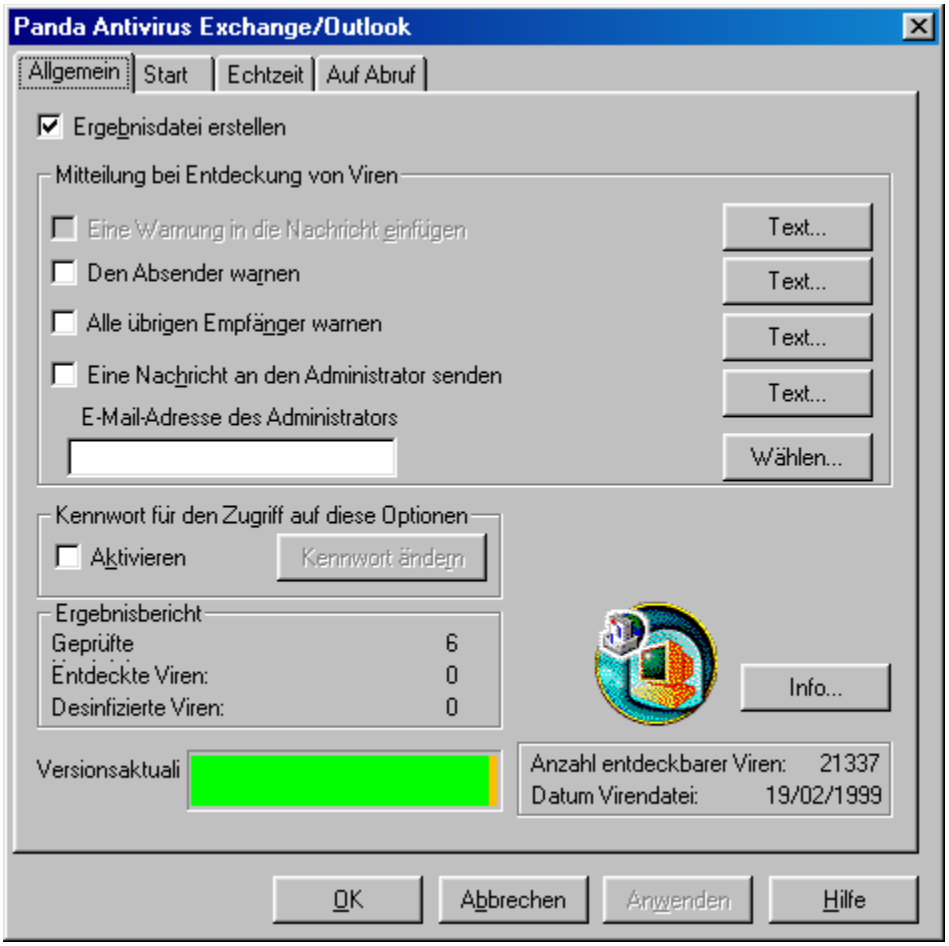
Konfigurieren: Mit dieser Schaltfläche kann das Konfigurationsfenster von Panda Antivirus Exchange/Outlook geöffnet werden. Über dieses Fenster kann das allgemeine Verhalten des Antivirus konfiguriert werden, ebenso wie sein Verhalten beim Start des E-Mail-Programms und das Verhalten des permanenten Schutzes und des Schutzes auf Abruf. Das Konfigurationsfenster von Panda Antivirus Exchange/Outlook kann auch über Optionen im Menü Extras der Menüleiste von MS-Exchange/Outlook erreicht werden. In dem Optionen-Fenster, das sich öffnet, erscheint eine Registerkarte mit dem Namen Panda Antivirus Exchange/Outlook. In dieser Registerkarte kann das Antivirus konfiguriert werden.

Konfiguration des Panda Antivirus Exchange/Outlook

Panda Antivirus Exchange/Outlook bietet vielfältige Einstellungsmöglichkeiten für jede seiner Funktionen. Das Konfigurationsfenster enthält verschiedene Registerkarten, in denen jeweils ein bestimmter Teil des Antivirus konfiguriert werden kann.

Allgemein

Die Optionen in dieser Registerkarte ermöglichen allgemeine Einstellungen, die das grundlegende Verhalten des Antivirus bestimmen. Folgende Optionen sind verfügbar:



Ergebnisdatei erstellen. Wenn Sie diese Option aktivieren, werden alle Vorfälle während der Scan-Operationen des Antivirus in einer Ergebnisdatei aufgezeichnet.

Eine Warnung in die Nachricht einfügen. Wenn Sie diese Option aktivieren, und es wird ein Virus in einer Nachricht entdeckt, wird dieser Nachricht ein Text mit einer Warnung hinzugefügt. Diese Warnung wird unabhängig von der Aktion hinzugefügt, die bei Entdecken des Virus durchgeführt werden soll. Die Warnung kann persönlich, nach Wunsch des jeweiligen Benutzers formuliert werden.

Den Absender warnen. Wenn Sie diese Option aktivieren, wird jedesmal bei Entdecken eines Virus in einer Nachricht eine Nachricht an den Absender der infizierten Datei gesendet, um diesen über den Vorfall zu informieren. Der Text der Nachricht, die der Absender erhält, kann vorher persönlich verfaßt werden.

Alle übrigen Empfänger warnen. Wenn Sie diese Option aktivieren, und es wird in einer Nachricht ein Virus gefunden, dann werden alle übrigen Empfänger der infizierten Nachricht, falls es sie gibt, davon benachrichtigt. Auf diese Weise können Benutzer gewarnt werden, die eventuell nicht über einen Schutz vor Viren verfügen. Der Text der Nachricht an die übrigen Empfänger kann persönlich

verfaßt werden.

Eine Nachricht an den Administrator senden. Wenn Sie diese Option aktivieren, und es wird die E-Mail-Adresse des Administrators angegeben, wird bei jedem Entdecken eines Virus eine Warnung an den Systemadministrator gesendet. Der Text kann persönlich formuliert werden.

Kennwort aktivieren. Wenn Sie diese Option aktivieren, bleibt die Konfiguration des Panda Antivirus Exchange/Outlook kennwortgeschützt. Auf diese Weise kann die Konfiguration des Antivirus nicht von unbefugten Benutzern geändert werden.

Kennwort ändern. Diese Schaltfläche ermöglicht es, das Kennwort zum Schutz der Konfiguration des Panda Antivirus Exchange/Outlook zu ändern.

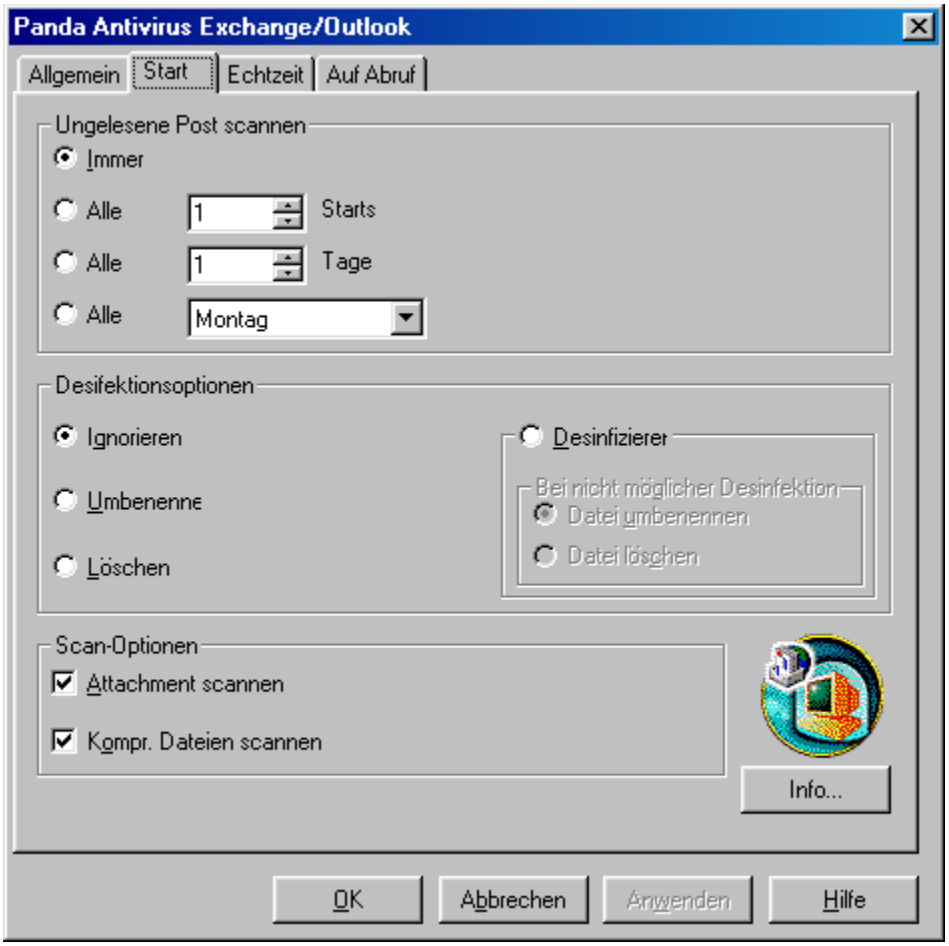
Ergebnisbericht. In diesem Bereich werden Informationen über die Anzahl der gescannten Nachrichten, der entdeckten sowie der vernichteten Viren angezeigt.

Versionsaktualisierung. Hier wird graphisch der Aktualisierungsstand des Antivirus angezeigt.

Informationen über die Version. Die Anzahl der entdeckbaren Viren und das Datum der Virendatei geben Auskunft über die Version des installierten Antivirus.

Start

In dieser Registerkarte kann das Verhalten des Antivirus beim Starten des E-Mail-Programms MS-Exchange/Outlook festgelegt werden. Folgende Optionen sind verfügbar:



Ungelesene Post immer scannen. Wenn Sie diese Option wählen, werden bei jedem Start von MS-Exchange/Outlook alle ungelesenen Nachrichten des Posteingangs gescannt.

Ungelesene Post regelmäßig nach einer bestimmten Anzahl von Starts scannen. Wenn Sie diese Option wählen, werden die nicht gelesenen Nachrichten im Posteingang jedesmal dann gescannt, wenn die angegebene Anzahl der Starts des E-Mail-Programms durchgeführt wurde.

Ungelesene Post regelmäßig nach einer bestimmten Anzahl von Tagen scannen. Wenn Sie diese Option wählen, werden die nicht gelesenen Nachrichten im Posteingang nach Ablauf der angegebenen Tage gescannt.

E-Mails an bestimmten Tagen scannen. Wenn Sie diese Option wählen, werden die nicht gelesenen Nachrichten nur an dem ausgewählten Wochentag gescannt.

Desinfektion - Ignorieren: Wenn Sie diese Option wählen, und es wird ein Virus gefunden, dann zeigt das Antivirus lediglich ein Fenster an, um über das Entdecken eines Virus zu informieren, ohne

irgendeine weitere Aktion durchzuführen.

Desinfektion - Umbenennen: Wenn Sie diese Option wählen, und es wird ein Virus entdeckt, dann wird die infizierte Datei umbenannt.

Desinfektion - Löschen: Wenn Sie diese Option wählen, und es wird ein Virus entdeckt, dann löscht das Antivirus die infizierte Datei.

Desinfektion - Desinfizieren: Wenn Sie diese Option wählen, und es wird ein Virus entdeckt, dann versucht das Antivirus, die infizierte Datei zu desinfizieren.

Desinfektion - Bei nicht möglicher Desinfektion, umbenennen: Wenn das Antivirus eine verseuchte Datei nicht desinfizieren kann, dann wird diese umbenannt.

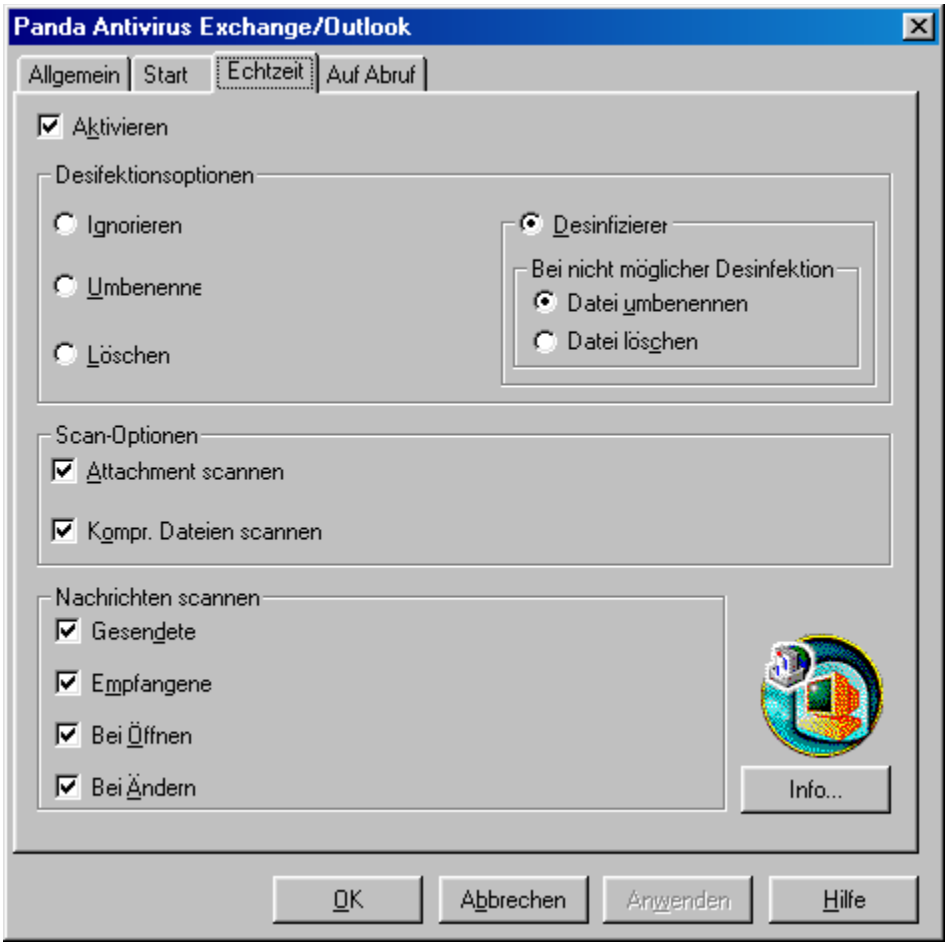
Desinfektion - Bei nicht möglicher Desinfektion, löschen: Wenn das Antivirus eine verseuchte Datei nicht desinfizieren kann, dann wird diese gelöscht.

Verschachtelte Nachrichten scannen: Wenn Sie diese Option aktivieren, werden verschachtelte Nachrichten gescannt. Das heißt, wenn sich eine Nachricht in einer anderen befindet, dann werden beide gescannt. Die Anzahl der Verschachtelungsebenen, die gescannt werden können, hängt von den Systemressourcen ab.

Kompr. Dateien scannen: Wenn Sie diese Option aktivieren, und es wird eine komprimierte Datei gefunden, wird diese gescannt, so als würde es sich um eine normale Datei handeln.

Echtzeit

In dieser Registerkarte kann der permanente Schutz des Antivirus konfiguriert werden. Folgende Optionen sind verfügbar:



Aktivieren: Wenn Sie diese Option aktivieren, wird der permanente Schutz aktiviert. Das bedeutet, daß automatisch alle Nachrichten gescannt werden, die empfangen, gesendet, geöffnet oder gespeichert werden.

Desinfektion - Ignorieren: Wenn Sie diese Option wählen, und es wird ein Virus entdeckt, dann zeigt das Antivirus lediglich ein Fenster an, um über das Entdecken eines Virus zu informieren, ohne irgendeine weitere Aktion durchzuführen.

Desinfektion - Umbenennen: Wenn Sie diese Option wählen, und es wird ein Virus entdeckt, dann wird die infizierte Datei umbenannt.

Desinfektion - Löschen: Wenn Sie diese Option wählen, und es wird ein Virus entdeckt, dann löscht das Antivirus die infizierte Datei.

Desinfektion - Desinfizieren: Wenn Sie diese Option wählen, und es wird ein Virus gefunden, dann versucht das Antivirus, die infizierte Datei zu desinfizieren.

Desinfektion - Bei nicht möglicher Desinfektion, umbenennen: Wenn das Antivirus eine verseuchte Datei nicht desinfizieren kann, dann wird diese umbenannt.

Desinfektion - Bei nicht möglicher Desinfektion, löschen: Wenn das Antivirus eine verseuchte Datei nicht desinfizieren kann, dann wird diese gelöscht.

Verschachtelte Nachrichten scannen: Wenn Sie diese Option aktivieren, werden verschachtelte Nachrichten gescannt. Das heißt, wenn sich eine Nachricht in einer anderen befindet, dann werden beide gescannt. Die Anzahl der Verschachtelungsebenen, die gescannt werden können, hängt von den Systemressourcen ab.

Kompr. Dateien scannen: Wenn Sie diese Option aktivieren, und es wird eine komprimierte Datei gefunden, wird diese gescannt, so als würde es sich um eine normale Datei handeln.

Gesendete Dateien scannen: Wenn Sie diese Option aktivieren, werden die Nachrichten vor dem Versenden gescannt. Auf diese Weise wird das Versenden infizierter Dateien verhindert.

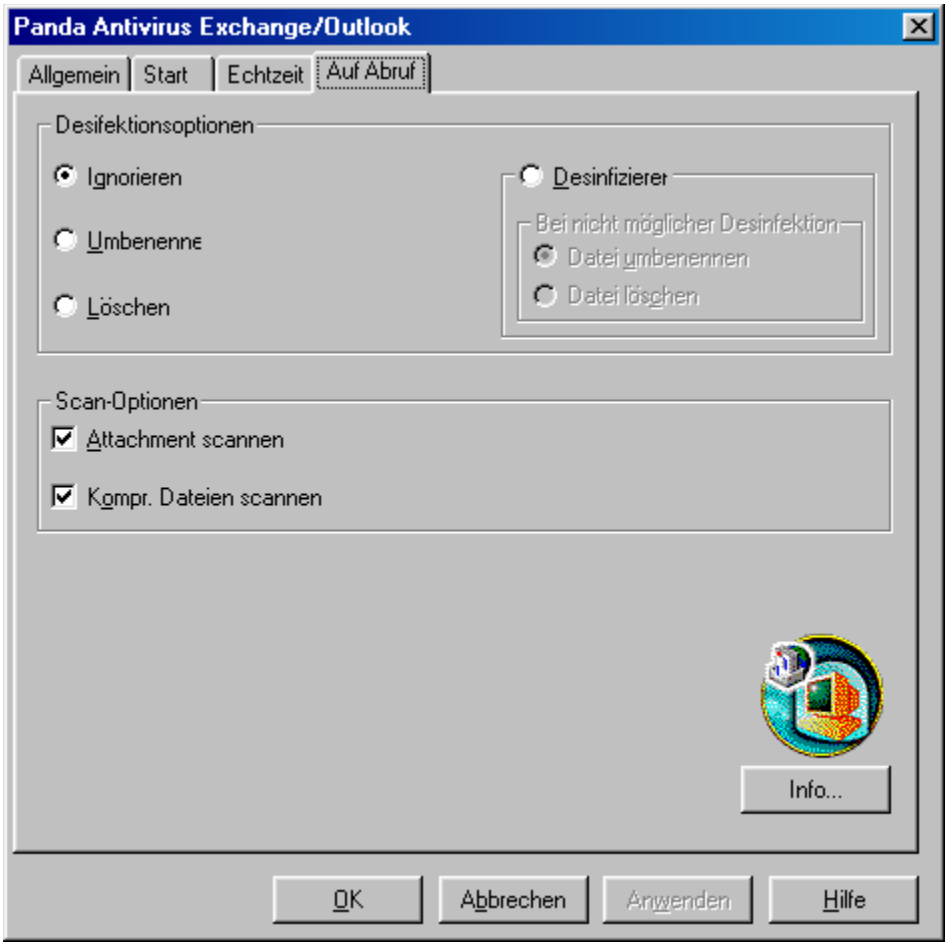
Empfangene Dateien scannen: Wenn Sie diese Option aktivieren, werden alle Nachrichten beim Empfang und noch bevor sie geöffnet werden, gescannt.

Nachrichten bei Öffnen scannen: Wenn Sie diese Option aktivieren, werden alle Nachrichten gescannt, die geöffnet werden, unabhängig davon, wann sie empfangen wurden.

Nachrichten bei Ändern scannen: Wenn Sie diese Option aktivieren, werden alle Nachrichten gescannt, die gespeichert werden.

Auf Abruf

In dieser Registerkarte kann der Scan auf Abruf des Antivirus konfiguriert werden. Folgende Optionen sind verfügbar:



Desinfektion - Ignorieren: Wenn Sie diese Option wählen, und es wird ein Virus gefunden, dann zeigt das Antivirus lediglich ein Fenster an, um über das Entdecken eines Virus zu informieren, ohne irgendeine weitere Aktion durchzuführen.

Desinfektion - Umbenennen: Wenn Sie diese Option wählen, und es wird ein Virus gefunden, dann wird die infizierte Datei umbenannt.

Desinfektion - Löschen: Wenn Sie diese Option wählen, und es wird ein Virus gefunden, dann wird die infizierte Datei gelöscht.

Desinfektion - Desinfizieren: Wenn Sie diese Option wählen, und es wird ein Virus gefunden, versucht das Antivirus, die infizierte Datei zu desinfizieren.

Desinfektion - Bei nicht möglicher Desinfektion, umbenennen: Wenn das Antivirus eine verseuchte Datei nicht desinfizieren kann, dann wird diese umbenannt.

Desinfektion - Bei nicht möglicher Desinfektion, löschen: Wenn das Antivirus eine verseuchte Datei nicht desinfizieren kann, dann wird diese gelöscht.

Verschachtelte Nachrichten scannen: Wenn Sie diese Option aktivieren, werden verschachtelte Nachrichten gescannt. Das heißt, wenn sich eine Nachricht in einer anderen befindet, dann werden beide gescannt. Die Anzahl der Verschachtelungsebenen, die gescannt werden können, hängt von den Systemressourcen ab.

Kompr. Dateien scannen: Wenn Sie diese Option aktivieren, und es wird eine komprimierte Datei gefunden, wird diese gescannt, so als würde es sich um eine normale Datei handeln.

Einführung in die Verteilung über ein Netz

Der Grundgedanke und Zweck der Verteilung des Antivirus über ein Netz ist die Arbeitserleichterung für den Netzwerkadministrator, der eine ganze Gruppe von Arbeitsplätzen auf schnelle und bequeme Art schützen möchte.

Die Vorgehensweise sieht dabei folgendermaßen aus:

1. Der Netzwerkadministrator kopiert das Antivirus in ein Verzeichnis im Server oder in ein gemeinsam genutztes Verzeichnis, auf das alle Benutzer Zugriff haben. Dieser Kopiervorgang wird von einen speziell dafür entwickelten Installationsprogramm ausgeführt. Dabei wird das Antivirus NICHT im Server installiert, sondern es werden lediglich die Dateien kopiert, die für die Installation des Antivirus in den einzelnen Arbeitsplätzen notwendig sind.

2. Jedesmal, wenn sich ein Arbeitsplatz in das Netz einloggt, wird überprüft, ob das Antivirus in ihm installiert und aktualisiert ist. Sollte dies so sein, geschieht nichts. Ist das Antivirus jedoch nicht installiert oder nicht aktualisiert, dann wird automatisch eine Installation bzw. Aktualisierung durchgeführt.

Wie bereits erwähnt, dient der Server (bzw. die gemeinsam genutzte Ressource) nur als Zwischenstation bei Verteilung des Antivirus auf die Arbeitsplätzen.

Dieses Verfahren funktioniert praktisch bei jeder Art von Netzen, wobei es bei der konkreten Durchführung von Netz zu Netz leichte Unterschiede geben kann. Im folgenden soll dieses Verfahren für die herkömmlichsten Netze erklärt werden.

Wie das Antivirus über ein Netz verteilt wird

Systemanforderungen

Für die Verteilung des Panda Antivirus Exchange/Outlook über das Netz sind erforderlich:

- IBM kompatibler Computer mit dem Windows 95, 98 oder Windows NT Workstation 3.51 oder 4.0 ausgeführt werden kann.
- 3 MB Festplattenspeicherplatz im Server, der als Verteiler dient.
- 3 MB Festplattenspeicherplatz in jedem Computer, in dem das Antivirus installiert werden soll.

Problemlose Verteilung des Antivirus auf alle Netzwerkarbeitsplätze

Das Verfahren zur Verteilung des Antivirus auf alle Netzwerkarbeitsplätze besteht aus zwei Teilschritten:

1. Kopieren des Antivirus in ein Verzeichnis, auf das alle Benutzer Zugriff haben.

2. Verteilung des Antivirus mit dem Programm RINSTALL auf alle Arbeitsplätze, sobald diese sich in das Netz einloggen.

Im Folgenden wird die Ausführung der beiden Schritte detailliert erklärt. Bei einigen Punkten des Installationsprozesses sind Kenntnisse über den Typ des Netzes erforderlich, über das die Verteilung des Antivirus erfolgen soll. Sollten Sie Zweifel hinsichtlich des Netztyps haben, können Sie in den entsprechenden Abschnitten detaillierte Informationen darüber nachlesen.

Kopieren des Antivirus in ein Verzeichnis, auf das alle Benutzer Zugriff haben

Der erste Schritt bei der Verteilung des Antivirus über das Netz ist das Kopieren der Dateien in ein Verzeichnis eines der Serverfestplatten. Dabei ist es sehr wichtig, daß das Kopieren von Dateien zum Server in einer virenfreien Umgebung durchzuführen ist. Sollte dies nicht der Fall sein, könnten die Dateien des Antivirus infiziert werden. Bei deren Verteilung an die Arbeitsplätze, die sich ins Netz einloggen, würde sich das Virus ebenfalls verbreiten. Um sowohl ein sicheres Kopieren der Dateien zu gewährleisten als auch eine zukünftige Infizierung dieser Dateien durch irgendeinen Arbeitsplatz zu vermeiden, ist der Kopiervorgang entsprechend folgender Anweisungen durchzuführen:

1. Der Administrator muß zunächst sicherstellen, daß sein Computer frei von Viren ist. Dazu ist es ratsam, er installiert das geeignete Antivirus von Panda Software in seinem Computer und aktiviert den permanenten Schutz. Die Installation sollte nicht fortgesetzt werden, solange nicht sichergestellt ist, daß der Computer, von dem aus das Antivirus installiert wird, frei von Viren ist.

2. Im entsprechenden Server ist ein Verzeichnis auszuwählen, in das die Dateien kopiert werden sollen. Wir empfehlen, ein neues Verzeichnis mit dem Namen PAVEXCLI zu erstellen, zu dem alle Benutzer durch eine Leseberechtigung Zugriff haben. Es ist wichtig, daß kein Benutzer bei diesem Verzeichnis über eine *Schreib- oder Löschberechtigung* verfügt, denn sonst könnte jeder Benutzer die Dateien des Antivirus versehentlich oder absichtlich infizieren oder löschen, was schwerwiegende Folgen haben kann.

3. Sobald das Zielverzeichnis erstellt wurde, ist die Diskette 1 oder die CD-ROM in das entsprechende Laufwerk einzulegen, dieses zu markieren und das Programm SETUP.EXE auszuführen.

Während des Installationsprozesses werden einige Fenster geöffnet, in denen Sie aufgefordert werden, über bestimmte, für die Durchführung der Installation notwendige Daten Auskunft zu geben. Eine der Fragen ist die nach dem Zielverzeichnis. Wählen Sie das zu diesem Zweck von Ihnen erstellte Verzeichnis, damit die Dateien des Antivirus dorthin kopiert werden können.

Verteilung des Antivirus

In diesem Schritt wird der Vorteil unseres Antivirus für Netzcomputer deutlich. Sie müssen zum Installieren des Antivirus nicht von einem Arbeitsplatz zum anderen gehen, weil es sich ganz automatisch in den Arbeitsplätzen installiert, sobald diese sich ins Netz einloggen.

Ebenso wie beim Starten eines Computers, werden auch beim Einloggen eines Computers in ein Netz eine Reihe von Befehlen oder Programmen ausgeführt, um diesen für die Arbeit im Netz vorzubereiten. Diese Reihe von Befehlen und/oder Programmen sind als *Login Skript* bekannt.

Unser Antivirus ist mit dem Programm **RINSTALL** ausgerüstet, das sich um die automatische Verteilung des Antivirus kümmert. Daher ist es genauso einfach die automatische Verteilung des Antivirus durchzuführen, wie die Anweisung **RINSTALL** in das *Login Skript* einzusetzen.

RINSTALL wird jedesmal ausgeführt, wenn sich ein Arbeitsplatz ins Netz einloggt. Zunächst überprüft **RINSTALL**, ob in dem Arbeitsplatzcomputer, der eingeloggt werden soll, das Antivirus installiert ist. Wenn das Antivirus in dem Computer installiert und aktualisiert ist, fährt das Programm fort, die restlichen Befehle des *Login Skript* normal auszuführen. Ist das Antivirus jedoch nicht installiert oder es ist nicht aktualisiert, wird es von **RINSTALL** installiert. Nachdem dies geschehen ist, werden die restlichen Befehle des *Login Skript* normal ausgeführt.

Da **RINSTALL** vollkommen automatisch funktioniert, muß der Netzwerkadministrator nur die Dateien kopieren und das *Login Skript* ändern, damit das Antivirus in den Arbeitsplatzcomputern installiert werden kann, wenn diese sich in das Netz einloggen.

Verteilung des Antivirus im Netz von Novell NetWare

Damit das Antivirus automatisch in allen Computern installiert werden kann, sobald sie sich in ein Netz von Novell NetWare einloggen, ist die folgende Zeile in das *System Login Script* einzufügen:

```
#F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

Im Abschnitt Novell NetWare finden Sie hierzu detailliertere Informationen.

Wie in dem Beispiel zu sehen ist, muß der Ort im Server angegeben werden, an dem sich die Dateien des Antivirus befinden. Aus diesem Grunde muß die o.g. Zeile *nach* dem Mapping der Laufwerke erscheinen, wobei dieser Teil des *System Login Scripts* wie folgt aussieht:

```
MAP ROOT F:=ALFA\SYS:
#F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

(vorausgesetzt, der Server hat den Namen Alfa und die Dateien befinden sich in SYS).

Verteilung des Antivirus in einem Windows NT Netz

Damit sich das Antivirus automatisch in den Arbeitsplatzcomputern installiert, sobald diese sich einloggen, muß die folgende Zeile der *Datei der Sitzungseröffnungsbefehle* unter Verwendung des Programms Profile Manager hinzugefügt werden:

Im Abschnitt Windows NT finden Sie hierzu detailliertere Informationen.

```
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

Wie in dem Beispiel zu sehen ist, muß der Ort angegeben werden, an den die Dateien des Antivirus kopiert wurden. Aus diesem Grunde muß die o.g. Zeile *nach* dem Mapping der gemeinsamen Ressourcen erscheinen, wobei dieser Teil der *Datei der Sitzungseröffnungsbefehle* wie folgt aussieht:

```
NET USE F: \\ALFA\SYS
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

(vorausgesetzt, der Server hat den Namen Alfa, und die Dateien befinden sich in Sys).

Verteilung des Antivirus in einem OS/2 Netz

Damit sich das Antivirus automatisch in den Arbeitsplatzcomputern installiert, sobald diese sich einloggen, muß die folgende Zeile der Datei PROFILE.BAT (oder PROFILE.CMD) hinzugefügt werden:

Im Abschnitt OS/2 finden Sie hierzu detaillierte Informationen.

```
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

Wie in dem Beispiel zu sehen ist, muß der Ort angegeben werden, an den die Dateien des Antivirus kopiert wurden. Aus diesem Grunde muß die o.g. Zeile nach dem Mapping der gemeinsamen Ressourcen erscheinen, wobei dieser Teil der Datei PROFILE.BAT wie folgt aussieht:

```
NET USE F: \\ALFA\SYS
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

(vorausgesetzt, der Server hat den Namen Alfa, und die Dateien befinden sich in Sys).

Verteilung des Antivirus in einem Pathworks Netz

Damit sich das Antivirus automatisch in den Arbeitsplatzcomputern installiert, sobald diese sich einloggen, muß die folgende Zeile der Verbindungssequenz der Gruppe hinzugefügt werden, in der sich alle Benutzer befinden, bei denen das Antivirus installiert werden soll:

```
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

Wie in dem Beispiel zu sehen ist, muß der Ort angegeben werden, an den die Dateien des Antivirus kopiert wurden. Aus diesem Grunde sollte die Bezeichnung der Laufwerke vor Ausführen von RINSTALL definiert werden.

Verteilung des Antivirus in einem Netz von Banyan-Vines

Damit sich das Antivirus automatisch in den Arbeitsplatzcomputern installiert, sobald diese sich einloggen, muß die folgende Zeile dem Profil jedes Benutzers hinzugefügt werden, dessen Computer geschützt werden soll. Das Benutzerprofil ist die Befehlsfolge, die immer dann ausgeführt wird, wenn sich der jeweilige Benutzer in das Netz einloggt.

Es reicht aus, das Profil mit dem Befehl MUSER zu bearbeiten und folgende Zeile hinzuzufügen:

```
POSTLOGIN F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

wenn F das Serverlaufwerk ist und die Dateien in das Verzeichnis **PAVEXCLI** kopiert wurden.

Es wird empfohlen, das Mapping der Laufwerke vor Ausführung von **RINSTALL** zu definieren, um sicherzustellen, daß die Festplatte des Servers in allen Arbeitsplätzen gleich bezeichnet wird.

Die Benutzerprofile einzeln, eines nach dem anderen zu ändern, kann sehr viel Arbeitsaufwand bedeuten, wenn viele Benutzer vorhanden sind. Normalerweise gibt es ein gemeinsames Profil, das von allen Benutzern verwendet wird. Dieses Profil wird von den verschiedenen Benutzerprofilen aufgerufen. Mit folgendem Befehl kann ein Profil von einem anderen aus aufgerufen werden:

```
USE Sample_Profile@Gruppe@Unternehmen
```

Sample_Profile ist hierbei ein fiktiver Benutzer, und Gruppe und Unternehmen sind die entsprechenden Elemente in der jeweiligen Unternehmensstrukturen.

Auf diese Weise ist es ausreichend, die notwendigen Änderungen im Profil *Sample_Profile* vorzunehmen, damit sie auf das Profil jener Benutzer übertragen werden, die es von ihrem eigenen aus aufrufen.

Installation des Antivirus in einem Arbeitsplatz, der nicht mit dem Netz verbunden ist

Um Panda Antivirus Exchange/Outlook in einem Arbeitsplatz zu installieren, der nicht mit dem Netz verbunden ist, sind folgende Schritte auszuführen:

1. Legen Sie die Diskette 1 oder die CD-ROM des Panda Antivirus Exchange/Outlook in das Laufwerk ein, markieren Sie das entsprechende Laufwerk und führen Sie das Programm SETUP.EXE aus. Während des Installationsvorganges werden einige Fenster geöffnet, in denen Sie aufgefordert werden, über bestimmte, für die Durchführung der Installation notwendige Daten Auskunft zu geben. Eine der Fragen ist die nach dem Zielverzeichnis. Wählen Sie entsprechend den vorherigen Beschreibungen das Verzeichnis in dem Computer aus, in dem das Programm installiert werden soll und nicht ein Verzeichnis des Servers.

2. Nachdem der Installationsvorgang abgeschlossen ist, führen Sie den folgenden Befehl aus:

   ```
   C:\PAVEXCLI\RINSTALL PAVEX.SCR
   ```

   (wenn das Antivirus in einem anderen Laufwerk oder Verzeichnis installiert wurde, geben Sie dieses an).

3. Nach Abschluß des Verteilungsprozesses ist das Antiviren-Programm für MS-Exchange/Outlook in Ihrem Computer installiert.

4. Löschen Sie das Verzeichnis, in das das Antivirus im 1. Schritt installiert wurde. Es wird nicht mehr benötigt.

Problemlösungen bei der Verteilung

Sollte sich das Antivirus in einem oder mehreren Computern nicht korrekt installieren, überprüfen Sie

dort folgendes:

1. Ist es möglich, von diesem Computer aus eine Verbindung zu dem Server herzustellen, in den das Antivirus kopiert wurde?

2. Versuchen Sie **RINSTALL** auszuführen. Begeben Sie sich in den Server, in den das Antivirus kopiert wurde und führen Sie **RINSTALL** PAVEX.SCR aus.

Wenn beide Überprüfungen keine Fehler ergeben haben, prüfen Sie den Login Skript und versichern Sie sich, daß der richtige Skript geändert wurde, und daß die Zeile der in diesem Handbuch abgebildeten Zeile entspricht.

Erweiterte Eigenschaften

Wie Sie verhindern, daß die Benutzer die Konfiguration des Panda Antivirus Exchange/Outlook ändern können

Wenn Sie vermeiden möchten, daß die Benutzer, bei denen Panda Antivirus Exchange/Outlook automatisch installiert wird, dessen Konfiguration ändern können, folgen Sie den nachstehenden Anweisungen:

1. Installieren Sie Panda Antivirus Exchange/Outlook im Computer des Netzwerkadministrators.

2. Öffnen Sie das E-Mail-Programm MS-Exchange/Outlook und nehmen Sie die gewünschten Einstellungen am Antivirus vor.

3. Schützen Sie die Konfiguration durch ein Kennwort. Dies können Sie im Konfigurationsfenster des Antivirus machen.

4. Kopieren Sie die Datei PAVEXCLI.CFG aus dem Verzeichnis WINDOWS\SYSTEM im Computer des Administrator in das Netzverzeichnis, von dem aus das Antivirus verteilt wird.

5. Führen Sie die Änderungen des *Login Skript* durch, damit die Verteilung des Antivirus auf alle Netzarbeitsplätze erfolgen kann.

WICHTIG: Das o.g. Verfahren ist vor der Verteilung des Antivirus auf die Netzarbeitsplätze durchzuführen.

Notwendige Kenntnisse über Novell NetWare

Die Verteilung des Antivirus über ein Netz von Novell NetWare erfordert einige Grundkenntnisse über dieses System. Im Folgenden wird anhand von Beispielen beschrieben, wie das System richtig vorzubereiten ist.

Befehle, die beim Start einer Netzwerksitzung ausgeführt werden

Normalerweise werden beim Hochfahren des Computers eine Reihe von in einer Datei definierten Befehlen ausgeführt. Bei MS-DOS oder Windows ist diese Datei die AUTOEXEC.BAT.

Ebenso werden für gewöhnlich eine Reihe von Befehlen ausgeführt, wenn ein Computer in ein Netz eingeloggt wird. Diese Befehle und/oder Programme sind als *Login Skript* bekannt.

Das *Login Skript* kann allgemein für alle Benutzer gelten oder es gibt für jeden Benutzer ein eigenes. Es ist auch eine Mischform möglich, bei der es ein allgemeines Login Skript für alle Benutzer und ein spezielles Login Skript für jeden einzelnen Benutzer gibt.

Da das *Login Skript* immer dann ausgeführt wird, wenn sich ein Benutzer in das Netz einloggt, ist es der geeignete Ort, um das Antivirus auf die Arbeitsplätze im Netz zu verteilen. Dabei reicht es vollkommen aus, im *Login Skript* das Verteilungsprogramm des Antivirus von Panda Software auszuführen, damit sich das Antivirus auf den Arbeitsplätzen im Netz installiert wird, sobald diese sich einloggen.

System Login Script

Bei Novell NetWare wird das für alle Benutzer geltende Login Skript als *System Login Script* bezeichnet. Diese Datei muß geöffnet werden, um ihr die Ausführung des Antivirusverteilungsprogramms von Panda Software hinzuzufügen. Um das *System Login Script* zu bearbeiten sind folgende Schritte auszuführen:

1. Wenn Sie über die Version Novell NetWare 3.x verfügen, verwenden Sie das Programm SYSCON. Wenn Sie mit der Version Novell NetWare 4.x arbeiten, nehmen Sie das Programm NETADMIN. Alle Novell NetWare Server besitzen einen Datenträger mit der Bezeichnung SYS und innerhalb dieses Datenträgers befindet sich immer ein Verzeichnis PUBLIC. Die beiden erwähnten Programme (SYSCON und NETADMIN) befinden sich in diesem Verzeichnis.

2. Um das *System Login Script* mit dem Programm SYSCON zu bearbeiten, muß dieses Programm ausgeführt, die Option *Supervisor Options* und dann die Option *System Login Script* gewählt werden.

3. Um das *System Login Script* mit dem Programm NETADMIN zu bearbeiten, muß dieses Programm zunächst ausgeführt werden. Dann sind die beiden Punkte (..) im linken Feld auszuwählen bis die genannte Option nicht mehr erscheint. In diesem Moment ist eine einzige Option zu sehen (auf der rechten Seite wird sie als eine *Organisation* bezeichnet). Jetzt muß diese Option ausgewählt und auf die Taste F10 gedrückt werden. Im daraufhin erscheinenden Menü ist die Option *Objekteigenschaften anzeigen oder bearbeiten* auszuwählen. Wählen Sie im danach erscheinenden Menü die Option *Login Skript* aus. Danach kann das *System Login Script* geändert werden.

Im *System Login Script* sind zwei Zeilen einzugeben: eine Zeile, die sich auf das *Mapping* (dieser Begriff wird im nächsten Abschnitt erklärt) bezieht und eine Zeile, die sich auf die automatische

Verteilung des Antivirus bezieht.

Zuordnung eines Laufwerksbuchstaben

In diesem Abschnitt wird der Begriff *Mapping* erklärt. In einem Computer wird die Festplatte normalerweise mit dem Buchstaben C, das Diskettenlaufwerk mit den Buchstaben A oder B und das CD-ROM-Laufwerk mit D, E usw. bezeichnet, je nachdem wie viele Festplatten vorhanden sind.

Die Datenträger (“Festplatten”) des Servers Novell NetWare müssen auch einen Laufwerksbuchstaben haben, damit von den Arbeitsplätzen problemlos auf die Verzeichnisse und Dateien in diesen Datenträgern zugegriffen werden kann. Die Operation zur Zuordnung eines Laufwerksbuchstaben zu einem Datenträger wird *Mapping*. genannt.

Es ist sehr interessant, daß alle Arbeitsplätze dieselben *Mappings* haben, damit sichergestellt wird, daß für sie alle die gleichen Zuordnungen zu den verschiedenen Datenträgern des Servers vorhanden sind. Dies wird erreicht, indem der Mappingbefehl in das *System Login Script* eingefügt wird. Im Allgemeinen werden für die Datenträger Laufwerksbuchstaben ab F gewählt. Es kann aber auch jeder andere nicht besetzte Laufwerksbuchstabe benutzt werden. Der Mappingbefehl wäre gemäß dieser Beschreibung folgender:

```
MAP ROOT F:=NAME_SERVER\NAME_DATENTRÄGER
```

Wäre der Servername ALFA und die Datenträgerbezeichnung SYS, dann würde der Befehl folgendermaßen sein:

```
MAP ROOT F:=ALFA\SYS:
```

Notwendige Kenntnisse über Windows NT

Die Verteilung des Antivirus über ein Netz von Windows NT erfordert einige Grundkenntnisse über dieses System. Im Folgenden wird anhand von Beispielen beschrieben, wie das System richtig vorzubereiten ist.

Befehle, die beim Start einer Netzwerksitzung ausgeführt werden

Normalerweise werden beim Hochfahren eines Computers eine Reihe von in einer Datei definierten Befehlen ausgeführt. Bei MS-DOS oder Windows ist diese Datei die AUTOEXEC.BAT.

Ebenso werden für gewöhnlich eine Reihe von Befehlen ausgeführt, wenn ein Computer in ein Netz eingeloggt wird. Diese Befehle und/oder Programme sind als *Login Skript* bekannt. Bei Windows NT wird der Name *Datei der Sitzungseröffnungsbefehle* verwendet.

Bei Windows NT verfügt jeder Benutzer über seine eigenen Datei der Sitzungseröffnungsbefehle . Im Prinzip müssen deshalb die Dateien für die Befehle der Sitzungseröffnung aller Benutzer geändert werden, in denen das Antivirus installiert werden soll. Um sich diese mühevolle Aufgabe zu ersparen, hat Panda Software das Dienstprogramm Profile Manager entwickelt. Seine Funktionsweise wird im Folgenden beschrieben.

Da die Datei der Sitzungseröffnungsbefehle jedesmal ausgeführt wird, wenn sich ein Benutzer ins Netz einloggt, ist dies der geeignete Ort von dem aus die Verteilung des Antivirus auf die Arbeitsplätze durchgeführt werden kann. In der Datei der Sitzungseröffnungsbefehle muß nur das Programm zur Verteilung des Antivirus von Panda Software ausgeführt werden, damit die Installation des Antivirus immer dann vorgenommen werden kann, wenn sich ein Benutzer in das Netz einloggt.

Befehlsdateien für den Start einer Profile Manager Sitzung

Zur Installation des Profile Managers, der die gleichzeitige Änderung aller Dateien für die Befehle der Sitzungseröffnung ermöglicht, muß die mit *Startbefehlseditor für Windows NT* beschriftete Diskette eingelegt werden oder das Programm **SETUP.EXE**. im entsprechenden Verzeichnis der CD-ROM ausgeführt werden. Zum Beispiel:

```
A:\SETUP
```

Führen Sie nach der Installation folgende Schritte aus:

1. Führen Sie das Programm aus.
2. Wählen Sie den vereinfachten Modus.
3. Wählen Sie im Menü *Datei* die Option *Domänenstartbefehle bearbeiten*.
4. Im unteren Bereich des Fensters befindet sich Texteditor. In diesem Editor können die notwendigen Änderungen vorgenommen werden, die sich auf alle Dateien für die Befehle der Sitzungseröffnung auswirken.
5. Speichern Sie die Änderungen, und verlassen Sie das Programm.

In der *Datei der Sitzungseröffnungsbefehle* sind zwei Zeilen einzugeben: die Zeile, die sich auf das *Mapping* (dieser Begriff wird im folgenden Abschnitt erklärt) bezieht und die Zeile, die sich auf die automatische Verteilung des Antivirus bezieht.

Zuordnung eines Laufwerksbuchtaben

In diesem Abschnitt wird der Begriff *Mapping* erklärt. In einem Computer wird die Festplatte normalerweise mit dem Buchstaben C, das Diskettenlaufwerk mit den Buchstaben A oder B und das CD-ROM-Laufwerk mit D, E usw. bezeichnet, je nachdem wie viele Festplatten vorhanden sind.

Bei einem Netz von Windows NT steht der Begriff *Mapping* mit dem Begriff *gemeinsame Ressourcen* in Beziehung. Die Gesamtheit oder irgendein Teil der Festplatte(n) des Servers kann gemeinsam genutzt werden und wird so zur *gemeinsamen Ressource*. Diese gemeinsamen Ressourcen müssen zugeordnet werden, damit später von den Arbeitsplätzen auf sie zugegriffen werden kann.

Es ist sehr interessant, daß alle Arbeitsplätze dieselben *Mappings* haben, damit sichergestellt wird, daß für sie alle die gleichen Zuordnungen zu den verschiedenen Datenträgern des Servers vorhanden sind. Dies wird erreicht, indem der Mappingbefehl in die *Datei der Sitzungseröffnungsbefehle* eingefügt wird. Im Allgemeinen werden für die Datenträger Laufwerksbuchstaben ab F gewählt. Es kann aber auch jeder andere nicht besetzte Laufwerksbuchstabe benutzt werden. Der Mappingbefehl wäre gemäß dieser Beschreibung folgender:

```
NET USE  F: \\NAME_SERV\NAME_RESSOURCE
```

Wäre der Servername ALFA und der Name der gemeinsamen Ressource SYS, dann würde der Befehl folgendermaßen sein:

```
NET USE F: \\ALFA\SYS
```

Notwendige Kenntnisse über OS/2

Die Verteilung des Antivirus über ein OS/2 Netz erfordert einige Grundkenntnisse über dieses System. Im Folgenden wird anhand von Beispielen beschrieben, wie das System richtig vorzubereiten ist.

Befehle, die beim Starten einer Netzwerksitzung ausgeführt werden

Normalerweise werden beim Hochfahren eines Computers eine Reihe von in einer Datei definierten Befehlen ausgeführt. Bei MS-DOS oder Windows ist diese Datei die AUTOEXEC.BAT.

Ebenso werden für gewöhnlich eine Reihe von Befehlen ausgeführt, wenn ein Computer in ein Netz eingeloggt wird. Diese Befehle und/oder Programme sind als *Login Skript* bekannt. Bei OS/2 besitzt jeder Benutzer die Datei PROFILE.BAT (oder PROFILE.CMD), die jedesmal ausgeführt wird, wenn sich der Benutzer in das Netz einloggt.

Da jeder Benutzer über eine eigene Datei der Sitzungseröffnungsbefehle verfügt, muß die Datei PROFILE.BAT bei jedem Benutzer geändert werden, bei dem das Antivirus installiert werden soll. Das Unangenehme daran ist, das bei zukünftigen Änderungen immer alle PROFILE.BAT Dateien bearbeitet werden müßten. Das kann durch die Erstellung der Datei BAT vermieden werden, die die für die Verteilung des Antivirus notwendigen Zeilen enthält, durch das Aufrufen dieser Datei von den entsprechenden PROFILE.BAT Dateien. Später in der BAT Datei vorgenommene Änderungen werden auf die gleiche Weise bei den Benutzern wirksam.

Da das Login Skript jedesmal ausgeführt wird, wenn sich ein Benutzer ins Netz einloggt, ist dies der geeignete Ort von dem aus die Verteilung des Antivirus auf die Arbeitsplätze durchgeführt werden kann. Im Login Skript muß nur das Programm zur Verteilung des Antivirus von Panda Software ausgeführt werden, damit die Installation des Antivirus immer dann vorgenommen werden kann, wenn sich ein Benutzer in das Netz einloggt.

Zuordnung eines Laufwerksbuchstaben

In diesem Abschnitt wird der Begriff *Mapping* erklärt. In einem Computer wird die Festplatte normalerweise mit dem Buchstaben C, das Diskettenlaufwerk mit den Buchstaben A oder B und das CD-ROM-Laufwerk mit D, E usw. bezeichnet, je nachdem wie viele Festplatten vorhanden sind.

Bei einem Netz von OS/2 steht der Begriff *Mapping* mit dem Begriff *gemeinsame Ressourcen* in Beziehung. Die Gesamtheit oder irgendein Teil der Festplatte(n) des Servers kann gemeinsam genutzt werden und wird so zur *gemeinsamen Ressource*. Diese gemeinsamen Ressourcen müssen zugeordnet werden, damit später von den Arbeitsplätzen auf sie zugegriffen werden kann.

Es ist sehr interessant, daß alle Arbeitsplätze dieselben *Mappings* haben, damit sichergestellt wird, daß für sie alle die gleichen Zuordnungen zu den verschiedenen Datenträgern des Servers vorhanden sind. Dies wird erreicht, indem der Mappingbefehl in die Datei PROFILE aller Benutzer eingefügt wird. Im Allgemeinen werden für die Datenträger Laufwerksbuchstaben ab F gewählt. Es kann aber auch jeder andere nicht besetzte Laufwerksbuchstabe benutzt werden. Der Mappingbefehl wäre gemäß dieser Beschreibung folgender:

```
NET USE  F: \\NAME_SERV\NAME_RESSOURCE
```

Wäre der Servername ALFA und der Name der gemeinsamen Ressource SYS, dann würde der Befehl folgendermaßen sein:

```
NET USE F: \\ALFA\SYS
```

Syntax der Skriptbefehle (.SRC)

In dieser Dokumentation konnte festgestellt werden, daß dem Programm **RINSTALL** immer ein Parameter hinzugefügt wird. Bei diesem Parameter handelt es sich um den Namen einer Datei mit der Erweiterung SCR (Skriptdatei). Eine Skriptdatei ist eine Textdatei, die in Bereiche aufgeteilt ist, in denen pro Zeile ein Befehl angegeben wird. Die Skriptdatei bestimmt das Verhalten des Programms **RINSTALL**.

Die für **RINSTALL** geeigneten SCR Dateien können 6 verschiedene Bereiche haben:

Gemeinsamer Bereich **[COMMON]**: diese Befehle werden immer ausgeführt.

Bereich DOS **[DOS]**: die Befehle dieses Bereichs werden unter DOS, Windows 3.1x und Windows 95 ausgeführt.

Bereich Windows 3.1x **[WIN]**: die Befehle dieses Bereichs werden unter DOS, Windows 3.1x und Windows 95 ausgeführt; aber nur, wenn das Verzeichnis von Windows 3.1x auf der Festplatte des Arbeitsplatzes gefunden wird.

Bereich Windows 95 **[WIN95]**: die Befehle dieses Bereichs werden unter DOS, Windows 3.1x und Windows 95 ausgeführt; aber nur, wenn das Verzeichnis von Windows 95 auf der Festplatte des Arbeitsplatzes gefunden wird.

Bereich Windows NT **[WINNT]**: die Befehle dieses Bereichs werden nur unter Windows NT ausgeführt.

Bereich OS/2 **[OS/2]**: die Befehle dieses Bereichs werden nur unter OS/2 ausgeführt.

Es gibt drei Befehlsarten:

1. **Zu kopierende Dateien:** Alle Zeilen, die NICHT mit dem Zeichen # beginnen, weisen auf eine Datei hin, die im Quellverzeichnis vorhanden sein und in das Zielverzeichnis kopiert werden muß. Standardmäßig werden die Dateien nur kopiert, wenn sie nicht im Zielverzeichnis existieren oder wenn die im Zielverzeichnis vorhandene Datei älter ist als diejenige im Quellverzeichnis.

2. **Zuordnungen:** Diese Befehle beginnen mit dem Zeichen # und besitzen folgende Struktur: #Variable = Wert. Sie dienen dazu, einer Variable einen bestimmten Wert zuzuordnen. Nachstehend werden die verschiedenen Variablen aufgeführt, die in den Skriptdateien (SCR) zur Verfügung stehen.

Name der Variable	**Beschreibung**
Win3xDir	Verzeichnis von Windows 3.1x
Win95Dir	Verzeichnis von Windows 95
WinNTDir	Verzeichnis von Windows NT

BaseSourcePath	Basisquellverzeichnis
BaseTargetPath	Basiszielverzeichnis
RelSourcePath	relatives Quellverzeichnis
RelTargetPath	relatives Zielverzeichnis

SourcePath	BaseSourcePath + RelSourcePath
TargetPath	BaseTargetPath + RelTargetPath

CopyMode	Gibt die Kopierbedingungen der Dateien an. Drei Werte sind möglich. COPY gibt an, daß die Dateien nur kopiert werden, wenn sie nicht im Zielverzeichnis existieren. UPDATE gibt an, daß die Dateien nur kopiert werden, wenn die zu kopierende Version neuer ist als die im Zielverzeichnis. OVERWRITE gibt an, daß die Dateien in jedem Fall kopiert werden.
ErrorMode	Gibt an, ob Fehlermeldungen angezeigt werden sollen oder nicht. Es kann der Wert 0 (die Meldungen werden nicht angezeigt) oder der Wert 1 (die Meldungen werden angezeigt) zugewiesen werden.

3. **Funktionen:** Diese Befehle beginnen ebenfalls mit dem Zeichen # und dienen dazu, bestimmte Operationen durchzuführen. Ihre Syntax sieht folgendermaßen aus: #Funktion Parameter1, Parameter2, ... Folgende Funktionen stehen zur Verfügung:

AddProfileEntry

Diese Funktion fügt in einem Bereich einer INI Datei einen Eintrag hinzu. Sie erhält 4 Parameter:

Parameter 1:	gibt den Bereich an, in dem der Eintrag erstellt werden soll.
Parameter 2:	gibt das Feld an (1. Teil des Eintrags).
Parameter 3:	gibt den Wert an (2. Teil des Eintrags).
Parameter 4:	gibt den Pfad der INI Datei an.

Beispiel:

```
#AddProfileEntry Windows, Load,
f:\pavfn\winkir.exe, c:\windows\win.ini
```

AppendLine

Diese Funktion fügt einer Textdatei eine Zeile hinzu. Sie erhält 3 Parameter:

Parameter 1:	gibt den Pfad zur Textdatei an.
Parameter 2:	gibt die hinzuzufügende Textzeile an.
Parameter 3:	LITERAL (optional). Bei Angabe dieses Parameters wird sichergestellt, daß die Textzeile genauso erscheint wie sie geschrieben wurde. Es wird dadurch vermieden, daß eventuell eingegebenen Änderungen erscheinen.

Beispiel:

```
#AppendLine c:\autoexec.bat,
c:\pavfn\sentinel.com
```

AppendLineBefore
Diese Funktion fügt einer Textdatei eine Zeile hinzu, aber immer vor einer anderen angegebenen Zeile. Sie erhält 4 Parameter:

Parameter 1:	gibt den Pfad zur Textdatei an.
Parameter 2:	gibt die hinzuzufügende Textzeile an.
Parameter 3:	gibt die Textzeile an, die der hinzuzufügenden Textzeile folgt.
Parameter 4:	LITERAL (optional). Bei Angabe dieses Parameters wird sichergestellt, daß die Textzeile genauso erscheint wie sie geschrieben wurde. Es wird dadurch vermieden, daß eventuell eingegebenen Änderungen erscheinen.

Beispiel:

```
#AppendLineBefore c:\autoexec.bat,
c:\pavfn\sentinel.com, win, LITERAL
```

DeleteLine
Diese Funktion löscht eine Zeile einer Textdatei. Sie erhält 2 Parameter:

Parameter 1:	gibt den Pfad zur Textdatei an.
Parameter 2:	gibt die zu löschende Textzeile an.

Beispiel:

```
#DeleteLine c:\autoexec.bat,
c:\pavfn\sentinel.com
```

InsertLine
Diese Funktion fügt am Anfang einer Textdatei eine Zeile hinzu. Sie erhält 3 Parameter:

Parameter 1:	gibt den Pfad zur Textdatei an.
Parameter 2:	gibt die einzufügende Textzeile an.
Parameter 3:	LITERAL (optional). Bei Angabe dieses Parameters wird sichergestellt, daß die Textzeile genauso erscheint wie sie geschrieben wurde. Es wird dadurch vermieden, daß eventuell eingegebenen Änderungen erscheinen.

Beispiel:

```
#InsertLine c:\autoexec.bat,
c:\pavfn\sentinel.com
```

MakeDir
Diese Funktion erstellt ein Verzeichnis. Sie erhält einen Parameter:

Parameter 1:	gibt den Pfad zum Verzeichnis an, das erstellt werden soll.

Beispiel:

```
#MakeDir c:\pavfn
```

NoWinLoad
In der Datei WIN.INI gibt es einen Bereich [Windows], der einen Eintrag mit dem Namen Load hat. Dieser Befehl sorgt dafür, daß bei Windows-Start eine Reihe von Programmen geladen wird. Es kann mehr als ein Programm in einem Load Befehl vorhanden sein. Der Befehl NoWinLoad löscht das Programm, das mit dem Befehl Load geladen werden soll. Es gibt einen Parameter:

Parameter 1: gibt das Programm an, das nicht geladen werden soll.

Beispiel:

```
#NoWinLoad c:\pavfn\winkir.exe
```

ReplaceLine
Diese Funktion ersetzt eine Zeile in einer Textdatei. Sie erhält 3 Parameter:

Parameter 1: gibt den Pfad zur Textdatei an.
Parameter 2: gibt die zu ersetzende Textzeile an.
Parameter 3: gibt die neue Textzeile an.

Beispiel:

```
#ReplaceLine c:\autoexec.bat,
«TargetPath»SENTINEL.COM,
«TargetPath»SENTINEL.COM /OE
```

SetProfileEntry
Diese Funktion weist einem Eintrag in einem bestimmten Bereich einer INI Datei einen Wert zu. Die Funktion versucht, diesen Bereich zu finden. Wenn sie ihn findet, weist sie ihm den Wert zu. Wenn nicht, erstellt sie den Eintrag und weist ihm den Wert zu. Sollte der Bereich nicht existieren, würde sie auch diesen erstellen. Sie erhält 4 Parameter:

Parameter 1: gibt den Bereich der INI Datei an
Parameter 2: gibt das Feld an (1. Teil des Eintrags)
Parameter 3: gibt den Wert an (2. Teil des Eintrags)
Parameter 4: gibt den Pfad zur INI Datei an.

Beispiel:

```
#SetProfileEntry Windows, Load,
c:\pavfn\winkir.exe, c:\windows\win.ini
```

WinLoad
In der Datei WIN.INI gibt es einen Bereich [Windows], der einen Eintrag mit dem Namen Load hat.

Dieser Befehl sorgt dafür, daß bei Windows-Start eine Reihe von Programmen geladen wird. Es kann mehr als ein Programm in einem Load Befehl vorhanden sein. Der Befehl WinLoad fügt dem Befehl Load ein Programm hinzu. Es gibt einen Parameter:

Parameter 1: gibt das Programm an, das geladen werden soll.

Beispiel:

```
#WinLoad c:\pavfn\winkir.exe
```

AdminRequired

Durch diese Funktion wird angezeigt, dass die Befehle zwischen #AdminRequired und #EndAdminRequired nur von einem Administrator ausgeführt werden können. Die Funktion ist nur wirksam, wenn der Befehl RInstall mit dem Parameter /Local ausgeführt wird. Für die Funktion selbst gibt es keine Parameter.

Beispiel:

```
#AdminRequired
```

EndAdminRequired

Wenn diese Funktion erscheint, können alle nachfolgenden Befehle auch ohne Administratorrechte ausgeführt werden. Sie ist nur wirksam, wenn der Befehl RInstall mit dem Parameter /Local ausgeführt wird. Für die Funktion selbst gibt es keine Parameter.

Beispiel:

```
#EndAdminRequired
```

ResetMode

Zeigt an, ob in diesem Augenblick ein Neustart durchgeführt werden muß oder nicht. Der Wert 0 zeigt an, dass kein Neustart durchgeführt wird und der Wert 1 zeigt an, das in diesem Moment ein Neustart durchgeführt wird. In beiden Fällen erscheint eine Meldung.

CheckSpace

Mit diesem Befehl wird der verfügbare Speicherplatz (in Mb) im Ziellaufwerk überprüft. Sollte nicht genügend Speicherplatz vorhanden sein, erscheint eine entsprechende Meldung, und die Dateien werden nicht kopiert.

Parameter 1: zeigt den notwendigen Speicherplatz in Mb an.

Beispiel:

```
#CheckSpace 8
```

CopyFileAs

Kopiert eine Datei von einem Speicherort zu einem anderen und zeigt dabei den Kopiermodus an. Dabei ist es möglich, den Dateinamen zu ändern. Drei Parameter sind verfügbar:

Parameter 1: zeigt den Originalpfad der Datei an.

Parameter 1: zeigt den Zielpfad der Datei an.

Parameter 1: zeigt den Kopiermodus an. Dabei gibt es verschiedene Möglichkeiten: COPY (die Datei wird nur kopiert, wenn sie noch nicht am Zielspeicherort existiert), UPDATE (die Datei wird nur kopiert, wenn die zu kopierende Version neuer ist, als die am Zielspeicherort bereits vorhandene), OVERWRITE (die Datei wird in jedem Fall kopiert, selbst wenn sie am Ursprungs- und Zielspeicherort identisch sind) und ONCHANGE (die Datei wird immer dann kopiert, wenn die Dateien am Ursprungs- und Zielspeicherort nicht identisch sind). ONCHANGE zeigt an, dass der Kopiervorgang nur ausgeführt wird, wenn die Ursprungsdatei sich von der Zieldatei unterscheidet. Das Alter der Dateien ist dabei unerheblich.

DeteleDirDelayed

Nachdem der Befehl RInstall ausgeführt wurde (nach den Befehlen #Run), löscht dieser Befehl ein komplettes Verzeichnis mit den dazugehörigen Unterverzeichnissen.

Parameter 1: zeigt das zu löschende Verzeichnis an.

Beispiel:

```
#DeleteDirDelayed c:\pavfn
```

ExchangeRequired

Mit diesem Befehl wird angezeigt, ob es notwendig ist, dass ein Exchange/Outlook-Client installiert ist, um mit der Bearbeitung des aktuellen Bereichs fortfahren zu können. Die Eingabe von Parametern ist nicht möglich.

Beispiel:

```
#ExchangeRequired
```

EndExchangeRequired

Mit diesem Befehl wird angezeigt, dass es nicht mehr notwendig ist, dass ein Exchange/Outlook-Client installiert ist, um mit der Bearbeitung des aktuellen Bereichs fortfahren zu können. Die Eingabe von Parametern ist nicht möglich.

Beispiel:

```
#EndExchangeRequired
```