Inhalt

Scannen auf Anforderung

Scan16 von VirusScan ermöglicht das Scannen auf Anforderung. Das ist die benutzergesteuerte Erkennung von bekannten Boot-Sektor- und Dateiviren sowie von mutierenden, mehrteiligen, getarnten, verschlüsselten und polymorphen Viren in Dateien, Laufwerken und auf Disketten.

Klicken Sie hier, um Scan16 zu starten.

Hinweis

Um Scan16 vom Desktop aus zu konfigurieren, öffnen Sie die VirusScan-Programmgruppe, und doppelklicken Sie auf das VirusScan-Symbol.

Konfigurieren von VShield

So konfigurieren Sie VShield:

1. Öffnen Sie den VShield-Konfigurationsmanager. Der VShield-Konfigurationsmanager wird geöffnet, und die Seite **Erkennung** wird angezeigt.
2. Bestimmen Sie, welche Dateien VShield wann auf Viren überprüfen soll.
3. Bestimmen Sie, wie VShield auf ein Virus reagieren soll.
4. Wählen Sie die gewünschten VShield-Benachrichtigungsoptionen.
5. Bestimmen Sie, welche Informationen VShield in seinem Virusaktivitätsprotokoll festhalten soll.
6. Wählen Sie die Dateien aus, die nicht gescannt werden sollen.
7. Schützen Sie VShield durch ein Kennwort.

Die Seite "Erkennung"

Mit der Seite **Erkennung** konfigurieren Sie Speicherort und Typ der zu scannenden Dateien. So konfigurieren Sie die Seite **Erkennung**:

1. Öffnen Sie den VShield-Konfigurationsmanager. Der VShield-Konfigurationsmanager wird geöffnet, und die Seite **Erkennung** wird angezeigt.
2. Bestimmen Sie, wann VShield Dateien nach Viren durchsuchen soll. VShield kann nach Viren suchen, wenn Dateien kopiert, erstellt oder umbenannt werden.
3. Bestimmen Sie, wann VShield Disketten nach Viren durchsuchen soll. VShield kann beim Zugriff auf die Diskette oder beim Herunterfahren nach Viren suchen.
4. Aktivieren Sie das Kontrollkästchen **Alle Dateien**, um alle Dateitypen auf Viren zu überprüfen. Um nur die Dateien zu scannen, die am anfälligsten für Infizierungen sind, klicken Sie auf die Optionsschaltfläche Nur Programmdateien. Klicken Sie auf **Erweiterungen**, um die Dateitypen in der Liste der Programmdateien zu ändern.
5. Aktivieren Sie das Kontrollkästchen **Komprimierte Dateien**, um komprimierte Dateien zu scannen.
6. Aktivieren Sie das Kontrollkästchen **VShield beim Start laden**, um VShield für das Laden beim Systemstart zu konfigurieren.
7. Aktivieren Sie das Kontrollkästchen **VShield kann deaktiviert werden**, um das Deaktivieren von VShield zu ermöglichen.
8. Klicken Sie auf **Anwenden**, und wählen Sie eine weitere Eigenschaftenseite aus, um die Änderungen zu speichern und mit der Konfiguration von VShield fortzufahren. Klicken Sie auf **OK**, um die Änderungen zu speichern und den Vorgang zu beenden. Um den Vorgang zu beenden, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

Siehe auch

Bestimmen, wie VShield auf ein Virus reagiert
Auswählen der VShield-Benachrichtigungsoptionen
Bestimmen, welche Informationen im Virusaktivitätsprotokoll von VShield festgehalten werden
Auswählen von Dateien und Ordnern, die nicht gescannt werden sollen
Kennwortschutz für VShield

Die Seite "Aktion"

Auf der Seite **Aktion** wird festgelegt, wie VShield auf infizierte Dateien reagieren soll. So konfigurieren Sie die Seite **Aktion**:

1. Öffnen Sie den VShield-Konfigurationsmanager. Der VShield-Konfigurationsmanager wird geöffnet, und die Seite **Erkennung** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Aktion**.
3. Bestimmen Sie, wie VShield auf infizierte Dateien reagieren soll:
   Eingabe anfordern
   Infizierte Dateien in ein Verzeichnis verschieben
   Infizierte Dateien säubern
   Infizierte Dateien löschen
   Scanvorgang fortsetzen
4. Klicken Sie auf **Anwenden**, und wählen Sie eine weitere Eigenschaftenseite aus, um die Änderungen zu speichern und mit der Konfiguration von VShield fortzufahren. Klicken Sie auf **OK**, um die Änderungen zu speichern und den Vorgang zu beenden. Um den Vorgang zu beenden, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

Siehe auch

Bestimmen, wann VShield welche Dateien nach Viren durchsucht
Auswählen der VShield-Benachrichtigungsoptionen
Bestimmen, welche Informationen im Virusaktivitätsprotokoll von VShield festgehalten werden
Auswählen von Dateien und Ordnern, die nicht gescannt werden sollen
Kennwortschutz für VShield

Die Seite "Warnung"

So wählen Sie die Warnoptionen aus:

1. Öffnen Sie den VShield-Konfigurationsmanager. Der VShield-Konfigurationsmanager wird geöffnet, und die Seite **Erkennung** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Warnung**.
3. Um VShield so zu konfigurieren, daß Benachrichtigungen an Server mit installiertem NetShield gesendet werden, aktivieren Sie das Kontrollkästchen **Netzwerkwarnung senden**. Geben Sie den Pfad für den Ordner der zentralen Warung ein, oder klicken Sie auf **Durchsuchen**, um den Ordner zu suchen.
4. Wenn bei einem Virus ein Warnton ausgegeben werden soll, aktivieren Sie das Kontrollkästchen **Warnton ausgeben**.
5. Wenn bei einem Virus eine benutzerdefinierte Meldung angezeigt werden soll, aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Meldung anzeigen**, und geben Sie eine Meldung ein (bis zu 256 Zeichen).
6. Klicken Sie auf **Anwenden**, und wählen Sie eine weitere Eigenschaftenseite aus, um die Änderungen zu speichern und mit der Konfiguration von VShield fortzufahren. Klicken Sie auf **OK**, um die Änderungen zu speichern und den Vorgang zu beenden. Um den Vorgang zu beenden, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

Siehe auch

Bestimmen, wann VShield welche Dateien nach Viren durchsucht
Bestimmen, wie VShield auf ein Virus reagiert
Bestimmen, welche Informationen im Virusaktivitätsprotokoll von VShield festgehalten werden
Auswählen von Dateien und Ordnern, die nicht gescannt werden sollen
Kennwortschutz für VShield

Die Seite "Bericht"

Auf der Seite **Bericht** wird festgelegt, wie VShield Informationen über Virusaktivitäten festhalten soll. So konfigurieren Sie die Seite **Bericht**:

1. Öffnen Sie den VShield-Konfigurationsmanager. Der VShield-Konfigurationsmanager wird geöffnet, und die Seite **Erkennung** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Bericht**.
3. Aktivieren Sie das Kontrollkästchen **Protokollieren in Datei**, damit VShield eine Protokolldatei führt. Geben Sie einen Namen und einen Pfad für die Protokolldatei ein (Standard: C:\MCAFEE\VIRUSCAN\VSHLOG.TXT).
4. Um die Größe der Protokolldatei zu beschränken, aktivieren Sie das Kontrollkästchen **Größe der Protokolldatei beschränken auf**, und geben Sie die maximale Größe ein.
5. Wählen Sie unter **Zu protokollierende Vorgänge** aus, welche Informationen protokolliert werden sollen.

   Viruserkennung
   Virusbeseitigung
   Löschen von infizierten Dateien
   Verschieben von infizierten Dateien
   Sitzungseinstellungen
   Sitzungsübersicht
   Datum und Uhrzeit
   Benutzername
6. Klicken Sie auf **Anwenden**, und wählen Sie eine weitere Eigenschaftenseite aus, um die Änderungen zu speichern und mit der Konfiguration von VShield fortzufahren. Klicken Sie auf **OK**, um die Änderungen zu speichern und den Vorgang zu beenden. Um den Vorgang zu beenden, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

Siehe auch

Bestimmen, wann VShield welche Dateien nach Viren durchsucht
Bestimmen, wie VShield auf ein Virus reagiert
Auswählen der VShield-Benachrichtigungsoptionen
Auswählen von Dateien und Ordnern, die nicht gescannt werden sollen
Kennwortschutz für VShield

Die Seite "Ausschließen"

So schließen Sie Dateien, Verzeichnisse oder Laufwerke vom Scanvorgang aus:

1. Öffnen Sie den VShield-Konfigurationsmanager. Der VShield-Konfigurationsmanager wird geöffnet, und die Seite **Erkennung** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Ausschließen**.
3. Klicken Sie auf **Hinzufügen**, um ein Element aufzunehmen, das nicht gescannt werden soll. Das Dialogfeld **Element ausschließen** wird angezeigt.

   Geben Sie den vollständigen Pfad für die Datei, das Laufwerk oder das Verzeichnis ein, oder klicken Sie auf **Durchsuchen**.

   Aktivieren Sie das Kontrollkästchen **Unterverzeichnisse einschließen**, um Unterverzeichnisse von dem Scanvorgang auszuschließen.

   Aktivieren Sie das Kontrollkästchen **Scannen von Dateien**, um das Element vom Scannen von Dateien auszuschließen. Um das Element vom Scannen von Boot-Sektoren auszuschließen, aktivieren Sie das Kontrollkästchen **Scannen von Boot-Sektoren**.

   Klicken Sie auf **OK**.
4. Wiederholen Sie Schritt 3 für jedes auszuschließende Element.
5. Um ein Scanelement zu bearbeiten, wählen Sie das Element aus, und klicken Sie auf **Bearbeiten**.
6. Um ein Scanelement zu entfernen, wählen Sie das Element aus, und klicken Sie auf **Entfernen**.
7. Klicken Sie auf **Als Standard speichern**, um diese Änderungen als Standard-Scanprofil zu speichern.
8. Klicken Sie auf **Anwenden**, und wählen Sie eine weitere Eigenschaftenseite aus, um die Änderungen zu speichern und mit der Konfiguration von VShield fortzufahren. Klicken Sie auf **OK**, um die Änderungen zu speichern und den Vorgang zu beenden. Um den Vorgang zu beenden, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

Siehe auch

Bestimmen, wann VShield welche Dateien nach Viren durchsucht
Bestimmen, wie VShield auf ein Virus reagiert
Auswählen der VShield-Benachrichtigungsoptionen
Bestimmen, welche Informationen im Virusaktivitätsprotokoll von VShield festgehalten werden
Kennwortschutz für VShield

Die Seite "Sicherheit"

Zur Optimierung von Virusschutz und Sicherheit kann jede Seite von VShield durch ein Kennwort geschützt werden. Sie können also selbst entscheiden, welche VShield-Eigenschaftenseite geschützt werden soll. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie den VShield-Konfigurationsmanager. Der VShield-Konfigurationsmanager wird geöffnet, und die Seite **Erkennung** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Sicherheit**.
3. Bestimmen Sie, welche Eigenschaftenseiten geschützt werden sollen. Vor geschützten Seiten steht  . Vor nicht geschützten Seiten steht

 .

4. Klicken Sie auf **Kennwort**. Das Dialogfeld **Kennwort festlegen** wird angezeigt.
5. Geben Sie das Kennwort ein. Wiederholen Sie die Eingabe, und klicken Sie auf **OK**. Sie kommen dann wieder zum Dialogfeld **Kennwortschutz** zurück.
6. Klicken Sie auf **Anwenden**, und wählen Sie eine weitere Eigenschaftenseite aus, um die Änderungen zu speichern und mit der Konfiguration von VShield fortzufahren. Klicken Sie auf **OK**, um die Änderungen zu speichern und den Vorgang zu beenden. Um den Vorgang zu beenden, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

Hinweise

Groß- und Kleinschreibung wird beim Kennwortschutz nicht beachtet. Wenn Sie beispielsweise das Kennwort "VirusScan" festlegen, wird "VIRUSSCAN", "virusscan" und selbst "ViRuSsCaN" akzeptiert.

Beim Zugriff auf eine geschützte Seite wird der Benutzer aufgefordert, das Kennwort einzugeben.

Sie werden nur einmal pro Sitzung zur Eingabe des Kennworts aufgefordert.

Siehe auch

Bestimmen, wann VShield welche Dateien nach Viren durchsucht
Bestimmen, wie VShield auf ein Virus reagiert
Auswählen der VShield-Benachrichtigungsoptionen
Bestimmen, welche Informationen im Virusaktivitätsprotokoll von VShield festgehalten werden
Auswählen von Dateien und Ordnern, die nicht gescannt werden sollen

Reagieren auf ein Virus

Viren greifen Computersysteme an, indem Sie Dateien infizieren. Meist sind dies ausführbare Programmdateien oder Microsoft Word-Dokumente und -Vorlagen. VShield kann die meisten Viren sicher aus infizierten Dateien entfernen und den Schaden beheben. Einige Viren richten an Ihren Dateien jedoch Schäden an, die sich nicht mehr beheben lassen. Solche sogenannten "beschädigten" Dateien können von VShield in ein Quarantäneverzeichnis verschoben oder gelöscht werden, um eine weitere Infizierung Ihres Systems zu verhindern.
Wenn VShield ein Virus findet, führen Sie eine der folgenden Aktionen durch:

Virus entfernen, das in einer Datei gefunden wurde
Virus entfernen, das im Arbeitsspeicher gefunden wurde

Hinweis

Bei Verdacht auf falschen Alarm lesen Sie die Informationen unter Falscher Alarm.

Reagieren auf ein Virus in einer Datei

Wenn VShield ein Virus in einer Datei erkennt, führt es die Aktion durch, die Sie bei der Konfiguration angegeben haben. Siehe dazu Seite Aktion.

Eingabe anfordern
Infizierte Dateien in ein Verzeichnis verschieben
Infizierte Dateien säubern
Infizierte Dateien löschen
Scanvorgang fortsetzen

Siehe auch

Reagieren auf ein Virus im Arbeitsspeicher
Falscher Alarm

Entfernen eines Virus: Eingabe anfordern

Wenn Sie auf der Eigenschaftenseite Aktion **Eingabe anfordern** ausgewählt haben und VShield findet ein Virus, dann wird das Dialogfeld **Virus gefunden** angezeigt.

Wählen Sie eine der folgenden Optionen aus:

Fortfahren
Stoppen
Säubern
Löschen
Ausschließen

Entfernen eines Virus: Verschieben infizierter Dateien in ein Verzeichnis

Wenn Sie auf der Eigenschaftenseite Aktion **Infizierte Dateien in ein Verzeichnis verschieben** ausgewählt haben und ein Virus wird gefunden, dann werden alle infizierten Dateien in das angegebene Verzeichnis kopiert.

Nachdem die Datei in das Quarantäneverzeichnis verschoben wurde, können Sie sie säubern oder mit Hilfe von Sicherungskopien wiederherstellen und wieder an ihrem ursprünglichen Speicherort ablegen. Damit Sie die Infizierungsquelle leichter ermitteln können, wird der Pfad zu der infizierten Datei im Quarantäneverzeichnis dupliziert. Befand sich also zum Beispiel eine infizierte Datei im Verzeichnis C:\WINDOWS\SYSTEM und Sie haben C:\INFECTED als Quarantäneverzeichnis festgelegt, wird die Datei nach C:\ INFECTED \WINDOWS\SYSTEM kopiert.

Entfernen eines Virus: Säubern infizierter Dateien

Wenn Sie auf der Eigenschaftenseite Aktion **Infizierte Datei säubern** ausgewählt haben und ein Virus wird gefunden, dann versucht VShield automatisch, die Datei zu säubern.

Hinweis

Falls das Virus nicht erfolgreich beseitigt werden konnte, fordert Sie VShield auf, eine andere Aktion zu wählen. Wählen Sie Löschen, und stellen Sie die Datei mit Hilfe Ihrer Sicherungskopie wieder her.

Entfernen eines Virus: Löschen infizierter Dateien

Wenn Sie auf der Eigenschaftenseite Aktion **Infizierte Datei löschen** ausgewählt haben und VShield findet ein Virus, dann wird die infizierte Datei automatisch gelöscht.

Hinweis

Bei dieser Option sollten Sie sich vergewissern, daß die Berichtprotokollierung aktiviert ist. Dadurch wird aufgezeichnet, welche Dateien gelöscht wurden, damit Sie die Dateien über Sicherungskopien wiederherstellen können. Siehe dazu Bericht.

Entfernen eines Virus: Fortsetzen des Scanvorgangs

Wenn Sie auf der Eigenschaftenseite Aktion **Scanvorgang fortsetzen** ausgewählt haben und VShield findet ein Virus, dann wird der Scanvorgang fortgesetzt, ohne daß eine Aktion vorgenommen wird.

Hinweis

Diese Option wird nicht empfohlen.

Eingabe anfordern: Fortfahren

VShield setzt den Scanvorgang fort, ohne eine Aktion durchzuführen.

Hinweis

Diese Option wird nicht empfohlen.

Eingabe anfordern: Stoppen

Der Scanvorgang wird angehalten, und Sie kehren zum Hauptfenster zurück.

Eingabe anfordern: Säubern

VShield versucht, die Datei zu säubern.

Hinweis

Falls die Datei nicht erfolgreich gesäubert werden konnte, fordert Sie VShield auf, eine andere Aktion durchzuführen. Wählen Sie Löschen, und stellen Sie die Datei mit Hilfe Ihrer Sicherungskopie wieder her.

Eingabe anfordern: Löschen

VShield löscht die infizierte Datei.

Bei dieser Option sollten Sie sich vergewissern, daß die Berichtprotokollierung aktiviert ist. Dadurch wird aufgezeichnet, welche Dateien gelöscht wurden, damit Sie die Dateien über Sicherungskopien wiederherstellen können. Siehe dazu Bericht.

Eingabe anfordern: Ausschließen

Schließt die Datei von künftigen Scanvorgängen aus.

Hinweis

Diese Option wird nicht empfohlen.

Öffnen des VShield-Konfigurationsmanagers

Öffnen Sie die VirusScan-Programmgruppe, und klicken Sie auf das Symbol für VShield-Konfigurationsmanager.

Anzeigen des Virusaktivitätsprotokolls

Zum Anzeigen des VShield-Aktivitätsprotokolls öffnen Sie einfach die auf der Seite **Bericht** angegebene Datei mit einem beliebigen Texteditor (z.B. Editor, Word usw.), oder klicken Sie hier.

Anzeigen der Virenliste

Klicken Sie hier, um die Virenliste anzuzeigen. Die Virenliste wird geladen.

Hinweis

Die Virenliste ist über 250 Seiten lang. Das Öffnen kann deshalb einige Zeit in Anspruch nehmen.

Context-sensitive, below

Die Seite "Erkennung"

Mit der Seite **Erkennung** konfigurieren Sie Speicherort und Typ der zu scannenden Dateien. So konfigurieren Sie die Seite **Erkennung**:

1. Bestimmen Sie, wann VShield Dateien nach Viren durchsuchen soll. VShield kann nach Viren suchen, wenn Dateien kopiert, erstellt oder umbenannt werden.
2. Bestimmen Sie, wann VShield Disketten nach Viren durchsuchen soll. VShield kann beim Zugriff auf die Diskette oder beim Herunterfahren nach Viren suchen.
3. Aktivieren Sie das Kontrollkästchen **Alle Dateien**, um alle Dateitypen auf Viren zu überprüfen. Um nur die Dateien zu scannen, die am anfälligsten für Infizierungen sind, klicken Sie auf die Optionsschaltfläche Nur Programmdateien. Klicken Sie auf **Erweiterungen**, um die Dateitypen in der Liste der Programmdateien zu ändern.
4. Aktivieren Sie das Kontrollkästchen **Komprimierte Dateien**, um komprimierte Dateien zu scannen.
5. Aktivieren Sie das Kontrollkästchen **VShield beim Start laden**, um VShield für das Laden beim Systemstart zu konfigurieren.
6. Aktivieren Sie das Kontrollkästchen **VShield kann deaktiviert werden**, um das Deaktivieren von VShield zu ermöglichen.
7. Klicken Sie auf **Anwenden**, und wählen Sie eine weitere Eigenschaftenseite aus, um die Änderungen zu speichern und mit der Konfiguration von VShield fortzufahren. Klicken Sie auf **OK**, um die Änderungen zu speichern und den Vorgang zu beenden. Um den Vorgang zu beenden, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

Die Seite "Aktion"

Mit der Seite **Aktion** konfigurieren Sie, wie VShield auf infizierte Dateien reagiert. So konfigurieren Sie die Seite **Aktion**:

1. Bestimmen Sie, wie VShield auf infizierte Dateien reagieren soll.
   Eingabe anfordern
   Infizierte Dateien in ein Verzeichnis verschieben
   Infizierte Dateien säubern
   Infizierte Dateien löschen
   Scanvorgang fortsetzen

2. Klicken Sie auf **Anwenden**, und wählen Sie eine weitere Eigenschaftenseite aus, um die Änderungen zu speichern und mit der Konfiguration von VShield fortzufahren. Klicken Sie auf **OK**, um die Änderungen zu speichern und den Vorgang zu beenden. Um den Vorgang zu beenden, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

Die Seite "Warnung"

So wählen Sie die Warnoptionen aus:

1. Um VShield so zu konfigurieren, daß Benachrichtigungen an Server mit installiertem NetShield gesendet werden, aktivieren Sie das Kontrollkästchen **Netzwerkwarnung senden**. Geben Sie den Pfad für den Ordner der zentralen Warung ein, oder klicken Sie auf **Durchsuchen**, um den Ordner zu suchen.

2. Wenn bei einem Virus ein Warnton ausgegeben werden soll, aktivieren Sie das Kontrollkästchen **Warnton ausgeben**.

3. Wenn bei einem Virus eine benutzerdefinierte Meldung angezeigt werden soll, aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Meldung anzeigen**, und geben Sie eine Meldung ein (bis zu 256 Zeichen).

4. Klicken Sie auf **Anwenden**, und wählen Sie eine weitere Eigenschaftenseite aus, um die Änderungen zu speichern und mit der Konfiguration von VShield fortzufahren. Klicken Sie auf **OK**, um die Änderungen zu speichern und den Vorgang zu beenden. Um den Vorgang zu beenden, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

Die Seite "Bericht"

Auf der Seite **Bericht** wird festgelegt, wie VShield Informationen über Virusaktivitäten festhalten soll. So konfigurieren Sie die Seite **Bericht**:

1. Aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Meldung anzeigen**, und geben Sie eine Meldung ein, wenn bei jedem Virus eine Meldung angezeigt werden soll.
2. Aktivieren Sie das Kontrollkästchen **Warnton ausgeben**, wenn bei einem Virus ein Warnton ausgegeben werden soll.
3. Aktivieren Sie das Kontrollkästchen **Protokollieren in Datei**, damit VShield eine Protokolldatei führt. Geben Sie einen Namen und einen Pfad für die Protokolldatei ein (Standard: C:\Programme\McAfee\VirusScan\VSLOG.TXT).
4. Um die Größe der Protokolldatei zu beschränken, aktivieren Sie das Kontrollkästchen **Größe der Protokolldatei beschränken auf,** und geben Sie die maximale Größe ein.
5. Wählen Sie unter **Zu protokollierende Vorgänge** aus, welche Informationen protokolliert werden sollen.
6. Klicken Sie auf **Anwenden**, und wählen Sie eine weitere Eigenschaftenseite aus, um die Änderungen zu speichern und mit der Konfiguration von VShield fortzufahren. Klicken Sie auf **OK**, um die Änderungen zu speichern und den Vorgang zu beenden. Um den Vorgang zu beenden, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

Die Seite "Ausschließen"

So schließen Sie Dateien, Verzeichnisse oder Laufwerke vom Scanvorgang aus:

1. Klicken Sie auf **Hinzufügen**, um ein Element aufzunehmen, das nicht gescannt werden soll. Das Dialogfeld **Element ausschließen** wird angezeigt.

   Geben Sie den vollständigen Pfad für die Datei, das Laufwerk oder das Verzeichnis ein, oder klicken Sie auf **Durchsuchen**.

   Aktivieren Sie das Kontrollkästchen **Unterverzeichnisse einschließen**, um Unterverzeichnisse von dem Scanvorgang auszuschließen.

   Aktivieren Sie das Kontrollkästchen **Scannen von Dateien**, um das Element vom Scannen von Dateien auszuschließen. Um das Element vom Scannen von Boot-Sektoren auszuschließen, aktivieren Sie das Kontrollkästchen **Scannen von Boot-Sektoren**.

   Klicken Sie auf **OK**.

2. Wiederholen Sie Schritt 1 für jedes auszuschließende Element.

3. Klicken Sie auf **Anwenden**, und wählen Sie eine weitere Eigenschaftenseite aus, um die Änderungen zu speichern und mit der Konfiguration von VShield fortzufahren. Klicken Sie auf **OK**, um die Änderungen zu speichern und den Vorgang zu beenden. Um den Vorgang zu beenden, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

Tips

Wenn Sie ein Scanelement bearbeiten möchten, wählen Sie es aus, und klicken Sie auf **Bearbeiten**.

Wenn Sie ein Scanelement entfernen möchten, wählen Sie es aus, und klicken Sie auf **Entfernen**.

Die Seite "Sicherheit"

Zur Optimierung von Virusschutz und Sicherheit kann jede Seite von VShield durch ein Kennwort geschützt werden. Sie können also selbst entscheiden, welche VShield-Eigenschaftenseite geschützt werden soll. Gehen Sie dazu folgendermaßen vor:

1. Bestimmen Sie, welche Eigenschaftenseiten geschützt werden sollen. Vor geschützten Seiten steht  . Vor ungeschützten Seiten steht

 .

2. Klicken Sie auf **Kennwort**. Das Dialogfeld **Kennwort festlegen** wird angezeigt.
3. Geben Sie das Kennwort ein. Wiederholen Sie die Eingabe, und klicken Sie auf **OK**. Sie kommen dann wieder zum Dialogfeld **Kennwortschutz** zurück.
4. Klicken Sie auf **Anwenden**, und wählen Sie eine weitere Eigenschaftenseite aus, um die Änderungen zu speichern und mit der Konfiguration von VShield fortzufahren. Klicken Sie auf **OK**, um die Änderungen zu speichern und den Vorgang zu beenden. Um den Vorgang zu beenden, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

Hinweise

Groß- und Kleinschreibung wird beim Kennwortschutz nicht beachtet. Wenn Sie beispielsweise das Kennwort "VirusScan" festlegen, wird "VIRUSSCAN", "virusscan" und selbst "ViRuSsCaN" akzeptiert.

Beim Zugriff auf eine geschützte Seite wird der Benutzer aufgefordert, das Kennwort einzugeben.

Sie werden nur einmal pro Sitzung zur Eingabe des Kennworts aufgefordert.

Funktionen von VirusScan

- Der Scanner mit NCSA-Zertifikat gewährleistet die Erkennung von mehr als 90 % der von der National Computer Security Association identifizierten Viren und 100 % der anderweitig gefundenen Viren. Informationen zum Status der Zertifizierung finden Sie auf der NCSA-Website unter www.NCSA.com.
- VShield, der Scanner auf Zugriff von VirusScan, ermöglicht Echtzeit-Identifikation bekannter und unbekannter Viren beim Zugriff auf Dateien, beim Erstellen, Kopieren, Umbenennen und Ausführen von Dateien sowie beim Einlegen einer Diskette und beim Starten und Herunterfahren des Systems.
- Scannen auf Anforderung ermöglicht die benutzergesteuerte Erkennung von bekannten Boot- und Dateiviren sowie von mutierenden, mehrteiligen, getarnten, verschlüsselten und polymorphen Viren in Dateien, Laufwerken und auf Disketten.
- Beim Code Trace™-, Code Poly™- und Code Matrix™-Scanning werden Viren durch McAfee-eigene Technologien mit höchster Präzision identifiziert.
- Bei VirusScan kann festgelegt werden, welche automatische Reaktion auf die Viruserkennung erfolgt: Meldung, Protokollierung, Löschung, Isolierung oder Säuberung.
- Das VirusScan Scan-Fenster, das Aktivitätsprotokoll und die Virenliste zeigen Einzelheiten des Scanergebnisses sowie Informationen über erkannte Viren an.
- Monatliche Aktualisierungen von Virensignaturen, die eine zuverlässige Erkennung und Beseitigung der Viren gewährleisten, sind im Kaufpreis einer McAfee-Abonnementlizenz enthalten. Siehe dazu Aktualisieren von VirusScan.

Siehe auch

Info über Viren
Arten von Viren
Warum nach Viren suchen?
Info über McAfee

Info über Viren

Computerviren können sich, wie die meisten Benutzer wissen, vernichtend auf die Produktivität auswirken. Was viele dieser Benutzer nicht haben, sind Informationen darüber, wo diese Viren herkommen, wie sie arbeiten usw. Informationen, mit deren Hilfe sie sich vor Infizierungen schützen können.

Die Anfänge

Das Grundkonzept für Viren gab es bereits viel früher als die tatsächliche Bedrohung durch Viren. Auch wenn sich die Viren-"Historiker" nicht über Zeitpunkt und Ort der Entstehung von Computerviren einig sind, weiß man, daß Pläne für Viren bereits zu der Zeit entstanden, als Computer noch riesige, teure Maschinen waren, die sich nur Großunternehmen und Regierungen, jedoch nicht der Normalverbraucher leisten konnten. Auch wenn viele der heute kursierenden Viren schädlich sind, war die Zerstörung von Daten nicht im ursprünglichen Konzept der Viren vorgesehen.

Am Anfang stand die Idee, daß, angesichts der Möglichkeit, ein Computerprogramm zu erstellen, das sich selbst kopieren oder vermehren kann, es auch möglich sein muß, daß sich ein Computerprogramm selbst weiterentwickelt. Wenn im Vermehrungsprozeß ein Fehler entsteht, stellt der dabei entstehende Code (die Informationen, aus denen das Programm besteht) eine Mutation dar. Ebenso, wie eine Mutation des genetischen Codes die Fähigkeit eines biologischen Virus zu überleben und sich fortzupflanzen, erhöht oder vermindert, könne auch die Mutation eines digitalen Codes die Überlebensfähigkeit eines elektronischen Virus in einer Computerumgebung erhöhen oder vermindern. Wenn man einem Computervirus genügend Zeit gäbe, so die logische Fortführung der Theorie, könnte sich aus ihm so etwas wie künstliche Intelligenz entwickeln. Science Fiction sieht vor diesem Hintergrund eher wie Wissenschaft und weniger wie Fiktion aus.

Was Viren wirklich sind

Im Grunde genommen ist ein Virus einfach nur ein Programm mit einem Ziel: sich selbst zu vermehren. Zur Verwirklichung dieses Ziels kommt es unter anderem darauf an, unentdeckt zu bleiben. Wird ein Virus von einem Benutzer entdeckt, wird es mit großer Wahrscheinlichkeit zerstört, und das ist seinen Vermehrungsplänen nicht gerade förderlich. Wie jedes Programm muß auch ein Virus ausgeführt werden, um seine Arbeit zu verrichten. Und da kein Benutzer ein Virus absichtlich ausführt, muß sich das Virus an eine Datei anhängen, die der Benutzer ausführen wird. Dies betrifft ausführbare Dateien und Dokumentdateien mit eingebetteten Makros, wie wir an späterer Stelle sehen werden. Eine andere Art von Datei - zum Beispiel eine reine Textdatei - zu infizieren, wäre für das Virus unproduktiv: das vorrangige Ziel ist schließlich die Vermehrung.

Computer mit Schnupfen?

Noch einmal zu den Ähnlichkeiten zwischen Computerviren und biologischen Viren: Ein Computervirus infiziert ein Wirtsprogramm ebenso, wie ein biologisches Virus eine Wirtszelle befällt. Es schreibt seinen eigenen Code zwischen die Codeabschnitte, aus denen das Wirtsprogramm besteht. So wie ein biologisches Virus Ressourcen seines Wirts verwendet, um sich zu vermehren, wird ein Computervirus jedesmal ausgeführt, wenn das infizierte Wirtsprogramm ausgeführt wird, und das Virus kopiert sich dabei selbst. Diese Kopien infizieren dann andere Programme, und der Kreislauf beginnt von neuem.

Ebenso wie biologische Viren sind auch Computerviren schädlich. Die ersten Computerviren waren lediglich Experimente von Wissenschaftlern zur Untermauerung ihrer Theorie: man wollte einfach sehen, ob es funktioniert. Ihre Theorie bestätigte sich, doch sie erkannten auch, daß Viren einige ungünstige Nebeneffekte hatten. Viren drangen in normale Prozesse des Computers ein und verursachten Fehler. Viele Viren sind heute speziell darauf programmiert, einige Funktionen zu erfüllen, die über die Selbstvermehrung hinausgehen. Diese Funktion, die als Ladung (englisch: "payload") bezeichnet wird, kann so harmlos sein, daß lediglich eine Meldung auf dem Bildschirm erscheint, oder so schädlich, daß Daten auf den Festplatten des Systems zerstört werden. Die Funktion wird erfüllt, wenn das auslösende Ereignis, zum Beispiel die Betätigung einer bestimmten Tastenkombination, ein bestimmtes Datum oder eine bestimmmte Anzahl von Aktionen, eintritt.

Wer schreibt Viren?

Der Grund für das veränderte Verhalten von Viren von harmloser Vermehrung im Experiment hin zu bösartigen, hinterhältigen Angriffen liegt darin, daß heutzutage andere Menschen Viren schreiben. Viruscodes werden heute meist von Menschen entwickelt, denen es weniger darum geht, die Möglichkeit künstlicher Intelligenz zu studieren, sondern vielmehr darum, anderen Benutzern Schaden zuzufügen. Einige tun es aus reiner Gehässigkeit, andere sind geleitet vom Ideal des im Untergrund agierenden Hackers, der in weiten Bereichen der Popkultur als

Freiheitskämpfer des digitalen Zeitalters romantisiert wird. Die Gründe für das Schreiben von Viruscodes sind wohl ebenso vielfältig und eigenartig wie die Gründe für die Verübung anderer zerstörerischer Taten.

Manche Virenschreiber geben sich sogar zu erkennen, wie zum Beispiel die pakistanischen Brüder, die das Brain-Virus schrieben. Die Brüder schlossen Namen, Adresse und Telefonnummer Ihrer Softwarefirma in den Virencode ein. Wenn die Ladung freigesetzt wurde, erschien diese Information auf dem Bildschirm. Offensichtlich schrieben die Brüder das Virus, um zu zeigen, wie weitverbreitet "Softwarepiraterie" ist. Sie infizierten mit dem Code die Software, die ihr Büro verließ, mit der Überlegung, daß überall dort, wo das Virus auftauchen würde, auch ihre Software verbreitet worden sei. Was sie dabei natürlich übersahen, war die Tatsache, daß sich das Virus auch verbreitete, indem es andere Programme außer den von ihnen herausgegebenen befiel.

Andere Virenschreiber sind verärgerte Angestellte, die auf Rache sinnen. Wieder andere sind Schüler, die einfach beweisen wollen, daß sie Viren schreiben können. Das berühmte Stoned-Virus ist angeblich von einem solchen Jugendlichen geschrieben worden. Nach dem er es geschrieben hatte, fürchtete er die Folgen einer Freisetzung des Virus und vernichtete deshalb alle Kopien davon - bis auf eine, die er zu Hause aufbewahrte. Seinem jüngeren Bruder und einigen Freunden gelang es jedoch, sich die Kopie zu verschaffen, und sie infizierten einige Disketten zum Spaß. Doch die Infizierung breitete sich schnell aus und war nach kurzer Zeit nicht mehr zu stoppen.
Was auch immer die Motivation sein mag, die Zahl der Anwender, die in der Lage sind, Viren zu schreiben, wächst im gleichen Maße wie die Computerindustrie. Für diejenigen, die der Gefahr einer Vireninfizierung ausgesetzt sind, das heißt, für alle, die einen Computer benutzen, muß dies ein Alarmsignal sein.

Es kommt noch schlimmer

In gewisser Weise macht erst die Tatsache, daß so viele Benutzer heute alarmiert sein müssen, eine massenhafte Ausbreitung der Viren möglich. Als die Computerwelt noch ausschließlich aus riesigen, teuren Maschinen bestand, mußte ein Virus nicht weit gehen, nachdem es gestartet wurde. Mit dem Aufkommen von Personalcomputern gab es für Viren plötzlich viele potentielle Ziele. Mit dem Anwachsen des Internet, der Möglichkeit, Dateien an E-Mail-Nachrichten anzuhängen, und der zunehmenden Abhängigkeit der Welt von ihren Computern werden immer bessere Bedingungen für die Ausbreitung von Computerviren geschaffen.

Neue Entwicklungen

Es gibt heute aber auch noch andere Gründe, besorgt zu sein. Im gleichen Maße, wie die Computertechnologie insgesamt immer weiter entwickelt und komplexer wird, werden es auch die Viren. Erst in den letzten Jahren sind hochentwickelte, gefährliche neue Viren wie etwa polymorphe Viren und Makroviren aufgetaucht. Polymorphe Viren sind besonders tückisch, da sie sich jedesmal verändern, wenn sie eine neue Datei infizieren. Konnten Anti-Viren-Programme einst noch anhand seiner "Signatur" (einem Codeabschnitt, der sich bei jedem Virus unterscheidet) nach einem Virus suchen, muß die Software heute in der Lage sein, Viren zu finden, deren Signatur sich bei jeder Infizierung einer Datei ändert.

Makroviren infizieren Dokumente und Dokumentvorlagen - ein ganz neues Terrain für Viren. Bisher waren Dokumente vor einem Virenbefall sicher, da eine Dokumentdatei bis vor wenigen Jahren keinen ausführbaren Code enthielt. Nachdem jedoch in Anwendungen wie Microsoft Word und Microsoft Excel die Möglichkeit besteht, Makros einzubetten, können Viren Dokumente infizieren, die in diesen Anwendungen mit Hilfe der Makrosprache erstellt werden.

All dies geschah erst in den letzten Jahren. Und Viren als ernsthafte Bedrohung gibt es erst seit etwa zehn Jahren. Sich vorzustellen, was die Zukunft bringt, wenn Computer noch komplexer werden und in noch stärkerem Maße zum alltäglichen Leben gehören, ist beängstigend. Glücklicherweise haben Sie den besten Schutz vor Virusinfizierungen erworben, den es heute gibt. Und dank der hervorragenden Unterstützung und den weltweiten Anti-Virus-Forschungsteams von McAfee können Sie sicher sein, daß Ihre Schutzvorkehrungen mit den ständigen Veränderungen der Computerwelt mithalten können.

Siehe auch

Funktionen von VirusScan
Arten von Viren
Warum nach Viren suchen?
Info über McAfee

Arten von Computerviren

Ein Virus ist ein Softwareprogramm, das sich selbst an ein anderes Programm auf einem Datenträger anhängt oder im Arbeitsspeicher des Computers auf die Gelegenheit lauert, von einem Programm auf das nächste überzugreifen.

Neben der Fähigkeit, sich zu vermehren, haben Viren auch die Fähigkeit, Daten zu beschädigen, Computer zum Absturz zu bringen und anstößige oder lästige Meldungen anzuzeigen.

Boot-Virus
Dateivirus
Getarntes Virus
Mehrteiliges Virus
Mutierendes Virus
Verschlüsseltes Virus
Polymorphes Virus

Siehe auch

Info über Viren
Funktionen von VirusScan
Warum nach Viren suchen?
Info über McAfee

Boot-Virus

Ein Boot-Virus kopiert sich selbst vom Boot-Sektor eines Laufwerks in den eines anderen (z.B. von einem Diskettenlaufwerk auf die Festplatte).

Dateivirus

Ein Dateivirus hängt sich an ein Programm an. Immer wenn das Programm ausgeführt wird, hängt sich das Virus an andere Programme an.

Getarntes Virus

Ein getarntes Virus versteckt sich, um nicht erkannt zu werden. Ein getarntes Virus kann ein Boot-Virus oder ein Dateivirus sein.

Mehrteiliges Virus

Ein mehrteiliges Virus verhält sich wie ein Boot-Virus und ein Dateivirus: Es breitet sich über Boot-Sektoren und Dateien aus.

Mutierendes Virus

Mutierende Viren ändern ihre Gestalt, um nicht erkannt zu werden. Viele mutierenden Viren sind auch verschlüsselte Viren.

Verschlüsseltes Virus

Verschlüsselte Viren verschlüsseln einen Teil ihres Codes, um nicht erkannt zu werden. Viele verschlüsselte Viren sind auch mutierende Viren.

Polymorphes Virus

Polymorphe Viren ähneln mutierenden Viren. Jedesmal, wenn sie sich selbst kopieren, ändern polymorphe Viren ihren Code ein wenig, um nicht erkannt zu werden.

Warum nach Viren suchen?

Heutzutage sind Sicherheitsmaßnahmen am Computer kein Luxus mehr, sondern eine Notwendigkeit. Computerviren befallen nicht allein Ihre Computerumgebung. Sie befallen alle Computerumgebungen, mit der Sie in Kontakt kommen - über Disketten, Netzwerke, Modems und Dateien, die Sie mit Mitarbeitern austauschen.
Denken Sie einmal darüber nach, wieviel die Daten, die auf Ihrem Computer gespeichert sind, wert sind. Wahrscheinlich sind sie unersetzbar, oder es würde viel Zeit und Geld erfordern, sie zu ersetzen. Denken Sie nun an den Wert der Daten auf allen Computern, zu denen Sie in Kontakt treten, und auf allen Computern, zu denen diese Computer in Kontakt treten usw.
Die Virensuchlösungen von McAfee sollten in der Liste Ihrer Sicherheitsmaßnahmen am Computer an erster Stelle stehen. Regelmäßiges Scannen Ihres Computers nach einem bestimmten Zeitplan bietet zusätzliche Sicherheit bei Ihren Vorkehrungen zur Vermeidung von Virusinfizierungen.

Siehe auch

Info über Viren
Funktionen von VirusScan
Arten von Viren
Info über McAfee

Info über McAfee

McAfee Inc., gegründet 1989, ist der führende Hersteller von produktiven Computer-Tools für DOS-, OS/2-, UNIX- und Windows-Umgebungen. Unsere Anti-Viren-Produkte sind weltweit in mehr als 16000 Unternehmen im Einsatz. Unsere Hilfsprogramme sorgen für Datensicherheit, automatische Versionsaktualisierungen sowie Inspektion und Bearbeitung des Systems. Darüber hinaus ist McAfee Pionier und Marktführer unter den Herstellern elektronisch verbreiteter Software. Alle McAfee-Produkte können entweder über den Handel bezogen oder über Mailboxen (Bulletin Board Systems) und Online-Dienste in der ganzen Welt heruntergeladen werden.
McAfee arbeitet unaufhörlich an der Entwicklung der besten Anti-Virus- und Hilfsprogramme der Welt. Dieses Produktangebot wird begleitet vom branchenweit besten Service und von hervorragender technischer Unterstützung. Die Produktunterstützung wird gewährleistet durch ein Vollzeit-Mitarbeiterteam aus Virenforschern, Programmierern und Support-Profis. Diese Dienstleistung wird direkt von McAfee oder über unser Netzwerk von autorisierten Vertragspartnern in mehr als 50 Ländern erbracht.

Siehe auch

Info über Viren
Funktionen von VirusScan
Arten von Viren
Warum nach Viren suchen

Entfernen eines Virus, das im Arbeitsspeicher gefunden wurde

Wenn VirusScan ein Virus im Arbeitsspeicher entdeckt, gehen Sie wie folgt vor:

1. Schalten Sie Ihren Computer aus.
2. Führen Sie keinen Neustart mit Hilfe der Reset-Taste oder mit Strg+Alt+Entf durch; bei dieser Methode können Viren erhalten bleiben oder ihre zerstörerische Wirkung freisetzen.
3. Legen Sie die McAfee-Erste-Hilfe-Diskette in das Diskettenlaufwerk ein. Siehe dazu Erstellen einer Erste-Hilfe-Diskette.
4. Schalten Sie den Computer ein.
5. Befolgen Sie die Anweisungen auf dem Bildschirm, und entfernen Sie alle gefundenen Viren.

Wenn die Viren entfernt wurden

Wenn VirusScan alle Viren erfolgreich entfernt hat, fahren Sie Ihren Computer herunter, und entnehmen Sie die Diskette. Beginnen Sie mit der Installation, wie im VirusScan Benutzerhandbuch beschrieben.
Scannen Sie Ihre Disketten unmittelbar nach der Installation, um die Quelle der Infizierung zu finden und auszuschalten.

Wenn die Viren nicht entfernt wurden

Falls VirusScan ein Virus nicht entfernen kann, erscheint folgende Meldung:

Virus konnte nicht entfernt werden.

Wenn das Virus in einer Datei gefunden wurde und sich mit VirusScan nicht entfernen läßt, sollten Sie die Datei löschen und die obengenannten Schritte wiederholen. Wurde das Virus im Master-Boot-Datensatz gefunden, lesen Sie die entsprechenden Dokumente über manuelles Entfernen von Viren auf der McAfee-Website. Weitere Informationen finden Sie unter Kontaktaufnahme mit McAfee.

Falscher Alarm

Von einem falschen Alarm spricht man, wenn ein Virus in einer Datei oder dem Arbeitsspeicher gemeldet wird, ohne daß es wirklich existiert. Die Wahrscheinlichkeit, daß falscher Alarm ausgelöst wird, ist größer, wenn Sie Virenschutzprogramme verschiedener Marken verwenden, da einige Anti-Virus-Programme ihre Virussignatur-Zeichenfolgen ungeschützt im Arbeitsspeicher aufbewahren.

Gehen Sie stets davon aus, das jedes Virus, das von VirusScan gefunden wird, tatsächlich vorhanden und gefährlich ist, und ergreifen Sie die notwendigen Maßnahmen, um es aus Ihrem System zu entfernen. Wenn es jedoch Anzeichen dafür gibt, daß VirusScan einen falschen Alarm auslöst (z.B. wenn es ein Virus in nur einer Datei entdeckt, die Sie seit Jahren ohne Probleme verwenden), sollten Sie sich die nachstehende Liste der möglichen Ursachen durchlesen:

- Wenn mehrere Anti-Virus-Programme gleichzeitig ausgeführt werden, kann VirusScan einen falschen Alarm auslösen. Richten Sie Ihren Computer so ein, daß immer nur ein Anti-Virus-Programm ausgeführt wird. Deaktivieren Sie in der Datei AUTOEXEC.BAT die Zeilen, die auf andere Anti-Virus-Programme verweisen. Schalten Sie Ihren Computer aus, warten Sie einige Sekunden, und schalten Sie ihn wieder ein, um sicherzustellen, daß alle Codes von anderen Anti-Virus-Programmen aus dem Arbeitsspeicher gelöscht werden.
- Einige BIOS-Chips sind mit einer Anti-Virus-Funktion ausgestattet, die die Ursache für einen falschen Alarm sein kann. Weitere Informationen hierzu finden Sie im Benutzerhandbuch Ihres Computers.
- Wenn Sie Validierungs- oder Wiederherstellungscodes verwenden, kann es vorkommen, daß bei nachfolgenden Scanvorgängen Änderungen in validierten Dateien entdeckt werden. Dadurch kann ein falscher Alarm ausgelöst werden, sofern es sich um selbstmodifizierende oder selbstprüfende ausführbare Dateien handelt. Wenn Sie Validierungscodes verwenden, erstellen Sie eine Ausnahmeliste, um solche Dateien von der Überprüfung auszuschließen.
- Bei einigen älteren Hewlett-Packard- und Zenith-PCs wird der Boot-Sektor jedesmal geändert, wenn das System gestartet (gebootet) wird. VirusScan erkennt solche Änderungen unter Umständen als mögliche Infizierung, auch wenn kein Virus vorhanden ist. Informationen darüber, ob Ihr PC mit einem selbstmodifizierenden Boot-Code arbeitet, finden Sie im Benutzerhandbuch Ihres Computers. Zur Lösung des Problems speichern Sie Validierungs-/Wiederherstellungsinformationen in den ausführbaren Dateien selbst; bei dieser Methode werden keine Informationen über den Boot-Sektor oder den Master-Boot-Datensatz gespeichert.
- Es kann vorkommen, daß VirusScan Viren im Boot-Sektor oder Master-Boot-Datensatz bestimmter kopiergeschützter Disketten meldet.

Aktualisieren von VirusScan

Um den bestmöglichen Schutz vor Viren zu gewährleisten, aktualisiert McAfee ständig die Dateien, die VirusScan zum Aufspüren von Viren verwendet. Nach einem bestimmten Zeitraum wird Sie VirusScan darauf hinweisen, daß Sie die Virusdefinitions-Datenbank aktualisieren sollten. Für einen optimalen Schutz ist es wichtig, diese Dateien in regelmäßigen Abständen zu aktualisieren.

Was ist eine Datendatei?
Die Dateien CLEAN.DAT, NAMES.DAT und SCAN.DAT stellen der VirusScan-Software Informationen über Viren zur Verfügung; sie sind die Datendateien, von denen in diesem Abschnitt die Rede ist.

Warum brauche ich eine neue Datendatei?
Jeden Monat werden durchschnittlich mehr als 100 neue Viren entdeckt. Häufig werden diese neuen Viren mit älteren Datendateien nicht erkannt. Mit den Datendateien, die mit Ihrer VirusScan-Software geliefert wurden, werden Viren, die erst nach Ihrem Kauf der Software entdeckt wurden, unter Umständen nicht erkannt.
Die Virenforscher von McAfee arbeiten laufend daran, weitere und neuere Virusdefinitionen in diese Datendateien aufzunehmen. Die aktualisierten Datendateien werden etwa alle vier bis sechs Wochen herausgegeben.

So aktualisieren Sie Ihre McAfee-Datendateien:

1. Laden Sie die Datendatei (z.B. DAT-9705.ZIP) von einem Online-Service von McAfee herunter. Bei den meisten Services ist diese Datei im Anti-Virus-Bereich zu finden.
2. Kopieren Sie die Datei in ein neues Verzeichnis.
3. Die Datei liegt in komprimierter Form vor. Dekomprimieren Sie sie mit einer beliebigen PKUNZIP-kompatiblen Dekomprimierungssoftware. Falls Sie keine solche Dekomprimierungssoftware besitzen, können Sie PKUNZIP (Shareware) von McAfee-Servern herunterladen.
4. Suchen Sie die Verzeichnisse auf der Festplatte, in denen VirusScan installiert ist. Normalerweise sind die Dateien im Verzeichnis C:\MCAFEE\VIRUSCAN gespeichert.
5. Kopieren Sie die neuen Dateien in das jeweilige Verzeichnis, indem Sie die alten Datendateien überschreiben. *Einige Datendateien können in anderen Verzeichnissen gespeichert sein. Kopieren Sie in diesem Fall jede aktualisierte Datei in das entsprechende Verzeichnis.*
6. Starten Sie Ihren Computer neu, um die Änderungen sofort wirksam werden zu lassen.

Hinweise

McAfee kann keine rückwirkende Kompatibilität von Virussignaturdateien zu früheren Versionen der Software garantieren. Wenn Sie das Aktualisierungsabonnement in Anspruch nehmen und Ihre VirusScan-Software regelmäßig auf den neuesten Stand bringen, sorgen Sie für umfassenden Virusschutz für mindestens ein Jahr nach dem Kauf von VirusScan.

Beachten Sie bitte, daß Ihre Möglichkeit, auf die Aktualisierungen zuzugreifen, durch die Nutzungsbedingungen, die in der der Software beigefügten Datei README.1ST zusammengefaßt und in der Software-Lizenzvereinbarung detailliert aufgeführt sind, gesetzlich beschränkt ist.

Kontaktaufnahme mit McAfee

Wählen Sie eines der folgenden Themen:

Kundendienst
Technische Unterstützung
Training

Kundendienst

Wenn Sie Produkte bestellen oder Produktinformationen anfordern möchten, wenden Sie sich an unsere Kundendienstabteilung unter der Nummer +1-408-988-3832 oder unter folgender Adresse:

McAfee, Inc.
2710 Walsh Avenue
Santa Clara, CA 95051-0963
U.S.A.

Siehe auch

Technische Unterstützung

Training

Technische Unterstützung

McAfee ist berühmt für sein engagiertes Bemühen um die Zufriedenheit seiner Kunden. In Fortsetzung dieser Tradition hat McAfee viel Zeit und Arbeit investiert, um seine Website zu einer wertvollen Ressource für die Aktualisierung der McAfee-Software und zu einer stets aktuellen Nachrichten- und Informationsquelle zu machen. Wenn Sie weitere Informationen über die technische Unterstützung von McAfee wünschen, sollten Sie unsere Website besuchen:

World Wide Web	http://www.mcafee.com

Klicken Sie hier, um zur McAfee-Website zu gelangen.

Falls Sie dort nicht finden, was Sie suchen, oder falls über keinen WWW-Zugang verfügen, probieren Sie einen der automatischen Services von McAfee aus:

Automatisches Telefon- und Fax-Antwortsystem	+1-408-988-3034
Internet	support@mcafee.com
McAfee BBS	+1-408-988-4004 1200 bps bis 28.800 bps 8 Bit, keine Parität, 1 Stopbit Rund um die Uhr, das ganze Jahr
CompuServe	GO MCAFEE
America Online	Schlüsselwort MCAFEE
Microsoft Network (MSN)	MCAFEE

Falls Sie Ihr Problem nicht mit Hilfe der automatischen Services lösen konnten, wenden Sie sich direkt an McAfee, und zwar montags bis freitags von 9.00 bis 17.00 Uhr.

Telefon	+1-408-988-3832
Fax	+1-408-970-9727

notieren Sie sich bitte folgendes, bevor Sie uns anrufen, damit wir Ihnen möglichst schnell weiterhelfen können:

- Name und Version des Produkts
- Marke und Modell des Computers und gegebenenfalls zusätzlicher Hardware
- Typ und Version des Betriebssystems
- Netzwerktyp und Version
- Inhalt der Dateien AUTOEXEC.BAT und CONFIG.SYS und des System-LOGIN-Skripts
- Gegebenenfalls Schritte, die Sie unternommen haben, um das Problem zu wiederholen

Siehe auch

Kundendienst

Training

McAfee-Training

Informationen zur Planung von Vor-Ort-Trainings für jedes beliebige McAfee-Produkt erhalten sie unter der Telefonnummer +1-800-338-8754.

Siehe auch

Kundendienst

Technische Unterstützung

Vermeiden von Virusinfizierungen

VirusScan ist ein effizientes Werkzeug zur Vermeidung, Erkennung und Beseitigung einer Virusinfizierung. Am effizientesten ist es jedoch, wenn es im Rahmen eines umfassenden Computersicherheitsplans eingesetzt wird, zu dem verschiedene Sicherheitsmaßnahmen wie regelmäßiges Erstellen von Sicherungskopien, ein sinnvoller Kennwortschutz, Benutzertraining und ständige Wachsamkeit gehören.
Zur Schaffung einer sicheren Systemumgebung und zur Verminderung der Infizierungsgefahr sollten Sie die Informationen zu den folgenden Themen lesen:

Erkennen von neuen Viren
Erstellen einer Erste-Hilfe-Diskette
Disketten mit Schreibschutz versehen

Erstellen einer Erste-Hilfe-Diskette

Die Erste-Hilfe-Diskette ist ein sehr wichtiger Bestandteil einer wirksamen Vorbeugung vor Virusinfizierungen. Sollte Ihr System infiziert werden, können Sie mit einer Erste-Hilfe-Diskette Ihren Computer von einer sauberen Umgebung aus starten.

Zur Erstellung einer Boot-Diskette muß Ihr System virenfrei sein. Ein in Ihrem System vorhandenes Virus könnte auf Ihre Boot-Diskette übertragen werden und das System erneut infizieren. Wenn Ihr Computer infiziert ist, gehen Sie zu einem anderen Computer, und scannen Sie ihn; ist er virenfrei, führen Sie eine der nachstehend genannten Aktionen durch.

Wählen Sie eine der folgenden Aktionen aus, um eine Erste-Hilfe-Diskette zu erstellen:

Automatisches Erstellen einer Erste-Hilfe-Diskette
Manuelles Erstellen einer Erste-Hilfe-Diskette

Automatisches Erstellen einer Erste-Hilfe-Diskette

So können Sie mit dem VirusScan-Hilfsprogramm automatisch eine Erste-Hilfe-Diskette erstellen:

1. Öffnen Sie die VirusScan-Programmgruppe, und doppelklicken Sie auf das Symbol für Erstellung der Erste-Hilfe-Diskette, oder klicken Sie hier.
2. Legen Sie eine leere 3,5-Zoll-Diskette in Laufwerk A: ein.
3. Klicken Sie auf **OK**. Das Hilfsprogramm beginnt, die Erste-Hilfe-Diskette zu erstellen.
4. Wenn die Erstellung abgeschlossen ist, entnehmen Sie die Diskette, aktivieren Sie den Schreibschutz, versehen Sie sie mit der Aufschrift "VirusScan Erste-Hilfe-Diskette", und bewahren Sie sie an einem sicheren Ort auf.

Manuelles Erstellen einer Erste-Hilfe-Diskette

Beginnen Sie diesen Prozeß an einer Eingabeaufforderung (C:\>). Wenn Sie sich in Windows befinden, müssen Sie eine DOS-Shell öffnen, um zu dieser Eingabeaufforderung zu gelangen.

1. Legen Sie eine leere Diskette in Laufwerk A: ein.
2. Formatieren Sie die Diskette, indem Sie an der Eingabeaufforderung C:\> folgenden Befehl eingeben:

   format a: /s /u

   Dadurch werden alle Daten überschrieben, die auf der Diskette vorhanden sind. Wenn Sie DOS 5.0 oder eine frühere Version verwenden, geben Sie **/u** nicht ein. Falls Sie nicht genau wissen, welche Version Sie verwenden, geben Sie **ver** bei der Eingabeaufforderung C:\> ein.
3. Wenn Sie das System zur Eingabe einer Datenträgerbezeichnung auffordert, geben Sie einen geeigneten Namen aus maximal 11 Zeichen ein.
4. Wechseln Sie in das VirusScan-Verzeichnis.
5. Kopieren Sie die Befehlszeilenversion von VirusScan auf die Diskette, indem Sie die folgenden Befehle an der Eingabeaufforderung eingeben:

   copy scan.exe a:

   copy scan.dat a:

   copy clean.dat a:

   copy names.dat a:
6. Wechseln Sie wieder in das Stammverzeichnis, indem Sie cd\ eingeben.
7. Kopieren Sie nützliche Befehlszeilenprogramme auf die Diskette, indem Sie einen der folgenden Befehle an der Eingabeaufforderung C:\> eingeben:

   copy c:\dos\chkdsk.* a:
8. Wiederholen Sie den letzten Schritt für die anderen nützlichen Programme:

   debug.*
   diskcopy.*
   fdisk.*
   format.*
   label.*
   mem.*
   sys.*
   xcopy32.*
9. Beschriften Sie die Diskette, und versehen Sie sie mit Schreibschutz; bewahren Sie sie dann einem sicheren Ort auf. Siehe dazu Diskette mit Schreibschutz versehen.

Hinweis

Wenn Sie ein Hilfsprogramm zur Datenträgerkomprimierung verwenden, kopieren Sie unbedingt auch die Treiber, die zum Zugriff auf die komprimierten Verzeichnisse erforderlich sind, auf die saubere Boot-Diskette. Nähere Informationen zu diesen Treibern finden Sie in der Dokumentation des jeweiligen Komprimierungsprogramms.

Diskette mit Schreibschutz versehen

Disketten sind praktische, tragbare Medien zum Speichern und Abrufen von Computerdaten. Disketten dienen zum Speichern (Schreiben) und zum Wiederherstellen (Lesen) von Dateien. Sie sind aber auch das Medium, mit dem Viren am häufigsten in ein Computerssystem eingeschleppt werden.

Eine Möglichkeit, eine Infizierung über eine Diskette zu vermeiden, besteht darin, Disketten, deren Daten nur zum Lesen vorgesehen sind, mit Schreibschutz zu versehen. Wenn Ihr System mit einem Virus infiziert wird, verhindert der Schreibschutz eine Infizierung der Disketten und somit eine Neuinfizierung des Systems, nach dem es gesäubert wurde.

Alle Disketten, die nicht schreibgeschützt sind, sollten gescannt und gegebenenfalls gesäubert werden, bevor Sie sie mit Schreibschutz versehen.

Wählen Sie eines der folgenden Themen:

5,25-Zoll-Disketten mit Schreibschutz versehen
3,5-Zoll-Disketten mit Schreibschutz versehen

5,25-Zoll-Disketten mit Schreibschutz versehen

1. Halten Sie die Diskette mit der beschrifteten Seite nach oben, so daß die Beschriftung von Ihnen abgewandt ist.
2. Die Kerbe hinten rechts ist die Schreibschutzkerbe. Wenn diese Kerbe zu sehen ist, können Sie Daten von der Diskette lesen und auf sie schreiben. Wenn die Kerbe mit einem Klebestreifen abgedeckt wird, kann die Diskette nicht mehr beschrieben werden. Dies verhindert, daß die Daten versehentlich geändert werden und daß Viren die Diskette infizieren.
3. Überdecken Sie die Kerbe mit einem Klebestreifen oder Klebeband, um die Diskette mit Schreibschutz zu versehen.

3,5-Zoll-Disketten mit Schreibschutz versehen

1. Halten Sie die Diskette mit der beschrifteten Seite nach unten, so daß die Metallabdeckung Ihnen zugewandt ist.
2. Sehen Sie sich die kleine, rechteckige Aussparung in der hinteren linken Ecke an. Sie sollte ein quadratisches Kunststoffteil enthalten, das in der Aussparung vor- und zurückgeschoben werden kann.
3. Um die Diskette mit Schreibschutz zu versehen, schieben Sie das Kunststoffteil zur Diskettenkante hin, so daß die Aussparung geöffnet ist.
4. Falls das Kunststoffteil fehlt und die Aussparung geöffnet ist, ist die Diskette schreibgeschützt.

Komprimierte Dateien

Wenn diese Option aktiviert ist, entpackt VirusScan mit LZexe und PKLite komprimierte Dateien und scannt sie in dekomprimierter Form. Dateien mit den Erweiterungen .ZIP und .LZH werden nicht nach Viren durchsucht.

Infizierte Dateien verschieben

Wenn diese Option ausgewählt ist, verschiebt VirusScan infizierte Dateien automatisch in das angegebene Verzeichnis. Zur Auswahl eines Verzeichnisses geben Sie den Verzeichnispfad ein, oder klicken Sie auf **Durchsuchen**, um ein Verzeichnis direkt auszuwählen.

Wenn die Datei in das Quarantäneverzeichnis verschoben wurde, können Sie sie säubern oder anhand einer Sicherungskopie wiederherstellen und sie anschließend in das ursprüngliche Verzeichnis zurückkopieren. Das ursprüngliche Verzeichnis ersehen Sie aus der VSHIELD-Protokolldatei (VSHLOG.TXT) oder aus der VirusScan-Protokolldatei für Scannen auf Anforderung (VSCLOG.TXT).

Infizierte Dateien säubern

Wenn diese Option gewählt ist, versucht VirusScan automatisch, das Virus aus der infizierten Datei zu beseitigen.

Infizierte Dateien löschen

Wenn diese Option gewählt ist, löscht VirusScan infizierte Dateien automatisch. Gelöschte Dateien können anschließend mit Hilfe der Sicherungskopie wiederhergestellt werden.

Bei dieser Option sollten Sie sich vergewissern, daß die Berichtprotokollierung aktiviert ist. Dadurch wird aufgezeichnet, welche Dateien gelöscht wurden, damit Sie die Dateien über Sicherungskopien wiederherstellen können.

Scanvorgang fortsetzen

Wenn diese Option gewählt ist, setzt VirusScan den Scanvorgang fort, ohne irgendwelche Maßnahmen zu ergreifen. Sie können im Hauptfenster von VirusScan manuell auf jede infizierte Datei reagieren, sobald der Scanvorgang abgeschlossen ist.

Diese Option ist nicht für unbeaufsichtigt laufende Computer zu empfehlen.

Eingabe anfordern

Wenn diese Option gewählt ist, fordert Sie VirusScan bei jeder infizierten Datei zu einer entsprechenden Eingabe auf.

Sicherheitsmaßnahmen am Computer

Sicherheitsmaßnahmen am Computer umfassen folgendes:

Schutz vor Viren
Regelmäßiges Erstellen von Sicherungskopien
Verwendung sinnvoller Kennwörter
Training und Wachsamkeit

Zentrale Warnung

Die zentrale Warnung ist das Virenmeldungssystem von McAfee für Unternehmens-Netzwerke. Einmal eingerichtet, senden Workstations, auf denen VirusScan ausgeführt wird, Virenmeldungen an Server, auf denen NetShield läuft. So können Administratoren die Quelle von Virusinfizierungen ermitteln und eine Ausbreitung verhindern.

So konfigurieren Sie die zentrale Warnung:

1. Fragen Sie einen Systemadministrator nach dem Namen eines Servers, auf dem NetShield läuft, und nach dem Verzeichnis für die zentrale Warnung.
2. Vergewissern Sie sich, daß Sie eine Zugriffsberechtigung für dieses Verzeichnis haben.
3. Konfigurieren Sie VShield- und VirusScan-Tasks für das Senden von Netzwerkmeldungen an dieses Verzeichnis.

Programmdateien

Wenn Sie Dateitypen der Programmdateienliste hinzufügen oder aus ihr löschen möchten, klicken Sie auf **Erweiterungen**. Das Dialogfeld **Programmdatei-Erweiterungen** erscheint.

1. Wenn Sie eine Dateinamenerweiterung hinzufügen möchten, klicken Sie auf **Hinzufügen**. Geben Sie die Erweiterung eines neuen Dateityps ein, der gescannt werden soll, und klicken Sie auf **OK**. Wiederholen Sie den Vorgang so oft, bis alle gewünschten Erweiterungen eingegeben sind.
2. Wenn Sie eine Dateinamenerweiterung löschen möchten, wählen Sie sie aus, und klicken Sie auf **Löschen**.
3. Wenn Sie wieder die Standarderweiterungen verwenden möchten, klicken Sie auf **Standard**.

Wenn Sie mit der Bearbeitung der Erweiterungsliste fertig sind, klicken Sie auf **OK**.

Name des Virus

Nennt den Namen des Virus.

Infiziert folgendes

Nennt die Dateitypen, die von diesem Virus infiziert werden. Dies können folgende Dateitypen sein:

Ausführbare Dateien (.EXE)
COM-Dateien (.COM)
Word-Dateien (.DO?)
Excel-Dateien (.XLS)

Virusgröße

Gibt die Größe in Kilobyte an.

Speicherresident

Gibt an, ob das Virus im Arbeitsspeicher vorhanden ist.

Verschlüsselt

Gibt an, ob es sich um ein verschlüsseltes Virus handelt.

Polymorph

Gibt an, ob es sich um ein polymorphes Virus handelt.

Reparabel

Gibt an, ob Dateien, die mit diesem Virus infiziert sind, repariert werden können.

Makrovirus

Gibt an, ob es sich um ein Word- oder Excel-Makrovirus handelt.

Typ

Gibt den infizierten Dateityp an (z.B. ausführbare Datei, Word-Datei, Excel-Datei)

Speicherort

Gibt das Verzeichnis an, in dem die infizierte Datei gespeichert ist.

Größe

Gibt die Größe der infizierten Datei an.

MS-DOS-Name

Gibt den Namen der infizierten Datei an.

Erstellt

Gibt das Datum an, zu dem die infizierte Datei erstellt wurde.

Geändert

Gibt das Datum an, zu dem die infizierte Datei zuletzt geändert wurde.

Zugriff

Gibt an, zu welchem Datum zuletzt auf die infizierte Datei zugegriffen wurde.

Schreibgeschützt

Gibt an, ob es sich um eine schreibgeschützte Datei handelt.

Verborgen

Gibt an, ob es sich um eine verborgene Datei handelt.

Archivdatei

Gibt an, ob es sich um eine Archivdatei handelt.

Systemdatei

Gibt an, ob es sich um eine Systemdatei handelt.

VirusScan-DOS-Fehlerebenen

Wenn Sie VirusScan in der DOS-Umgebung ausführen, gelten verschiedene DOS-Fehlerebenen. Sie können ERRORLEVEL in Stapeldateien verwenden, so daß je nach Ergebnis des Scanvorgangs unterschiedliche Aktionen durchgeführt werden. Weitere Informationen hierzu finden Sie in der Dokumentation zu Ihrem DOS-Betriebssystem.

VirusScan kann folgende Fehlerebenen melden:

ERRORLEVEL	Beschreibung
0	Keine Fehler aufgetreten; keine Viren gefunden.
1	Fehler beim Zugriff auf eine Datei (beim Lesen oder Schreiben).
2	Eine VirusScan-Datendatei ist beschädigt.
3	Fehler beim Zugriff auf eine Diskette (beim Lesen oder Schreiben).
4	Fehler beim Zugriff auf die mit der Option /AF erstellte Datei; die Datei wurde beschädigt.
5	Zu wenig Speicher zum Laden des Programms oder zum Beenden der Operation.
6	Interner Programmfehler (Fehler durch Speichermangel).
7	Fehler beim Zugriff auf eine internationale Meldungsdatei (MCAFEE.MSG).
8	Eine zum Ausführen von VirusScan notwendige Datei (z.B. SCAN.DAT) fehlt.
9	Inkompatible oder nicht erkannte Optionen oder Optionsargumente in der Befehlszeile angegeben.
10	Virus im Arbeitsspeicher gefunden.
11	Interner Programmfehler.
12	Fehler beim Versuch, ein Virus zu entfernen, z.B. Datei CLEAN.DAT nicht gefunden, oder VirusScan konnte Virus nicht entfernen.
13	Ein oder mehrere Viren im Master-Boot-Datensatz, im Boot-Sektor oder in Dateien gefunden.
14	Datei SCAN.DAT ist nicht mehr aktuell; VirusScan-Datendateien müssen aktualisiert werden.
15	VirusScan-Selbstprüfung gescheitert; möglicherweise infiziert oder beschädigt.
16	Fehler beim Zugriff auf ein angegebenes Laufwerk oder eine angegebene Datei.
17	Kein Laufwerk, kein Verzeichnis oder keine Datei zum Scannen angegeben.
18	Eine validierte Datei wurde geändert (/CF oder /CV Optionen).
19-99	Reserviert.
100+	Betriebssystemfehler; VirusScan fügt der ursprünglichen Nummer 100 hinzu.
102	Scanvorgang wurde mit STRG+C oder STRG+PAUSE unterbrochen. (STRG+C und STRG+PAUSE können mit der Befehlszeilenoption /NOBREAK deaktiviert werden.)

Dateiformat VSC

Die VSC-Datei ist eine Konfigurationstextdatei, die ähnlich wie die Windows-INI-Datei formatiert ist; in ihr sind die VirusScan-Einstellungen festgehalten. Jede Variable in der Datei hat einen Namen, auf den ein Gleichheitszeichen (=) und ein entsprechender Wert folgen. Die Werte bestimmen, welche Einstellungen für die VirusScan-Konfiguration gewählt wurden. Die Variablen sind in drei Gruppen unterteilt: ScanOptions, AlertOptions und ActivityLogOptions. Zum Bearbeiten kann eine VSC-Datei mit jedem Texteditor geöffnet werden.

Hinweis

Bei Booleschen Variablen sind nur die Werte 0 und 1 möglich. Mit dem Wert 0 wird die jeweilige Einstellung deaktiviert; 1 bedeutet, daß die Einstellung aktiviert ist.

ScanOptions

Variable	Beschreibung
bAutoStart	Typ: Boolescher Wert (1/0) Weist VirusScan an, sofort mit dem Scannen zu beginnen, wenn es gestartet wird. Standardwert: 0
bAutoExit	Typ: Boolescher Wert (1/0) Beendet VirusScan, wenn der Scanvorgang abgeschlossen ist und keine Viren gefunden wurden. Standardwert: 0
bAlwaysExit	Typ: Boolescher Wert (1/0) Beendet VirusScan, wenn der Scanvorgang abgeschlossen ist. Standardwert: 0
bSkipMemoryScan	Typ: Boolescher Wert (1/0) Weist VirusScan an, den Arbeitsspeicher nicht zu scannen. Standardwert: 0
bSkipBootScan	Typ: Boolescher Wert (1/0) Weist VirusScan an, den Boot-Sektor nicht zu scannen. Standardwert: 0
bSkipSplash	Typ: Boolescher Wert (1/0) Weist VirusScan an, beim Programmstart nicht das Einführungsbild anzuzeigen. Standardwert: 0

DetectionOptions

Variable	Beschreibung
bScanAllFiles	Typ: Boolescher Wert (1/0) Weist VirusScan an, alle Dateien zu scannen Standardwert: 0
bScanCompressed	Typ: Boolescher Wert (1/0) Weist VirusScan an, komprimierte Dateien zu scannen Standardwert: 1
szProgramExtensions	Typ: Zeichenfolge Bestimmt die Erweiterungen der Dateitypen, die gescannt werden. Standardwert: EXE COM DO? XL?
szDefaultProgram Extensions	Typ: Zeichenfolge Bestimmt, welche Dateinamenerweiterungen bei der Scankonfiguration als Standardprogrammerweiterungen verwendet werden. Standardwert: EXE COM DO? XL?

AlertOptions

Variable	Beschreibung
bNetworkAlert	Typ: Boolescher Wert (1/0) Weist VirusScan an, eine Meldung für eine zentrale Warnung an einen Server zu senden, der auf NetShield ausgeführt wird. Standardwert: 0
szNetworkAlertPath	Typ: Zeichenfolge Bestimmt den Pfad zu dem Server, auf dem NetShield ausgeführt wird. Standardwert: keiner
bSoundAlert	Typ: Boolescher Wert (1/0) Weist VirusScan an, einen Warnton auszugeben, wenn ein Virus erkannt wird. Standardwert: 1

ActionOptions

Variable	Beschreibung
bDisplayMessage	Typ: Boolescher Wert (1/0) Bestimmt, ob beim Erkennen eines Virus eine benutzerdefinierte Meldung angezeigt wird. Standardwert: 0
uScanAction	Typ: Ganzzahl (1-5) Weist VirusScan an, die angegebene Aktion durchzuführen, wenn ein Virus erkannt wird. Mögliche Werte: 1 - Eingabe anfordern 2 - Infizierte Dateien in einen Ordner verschieben 3 - Infizierte Dateien automatisch säubern 4 - Infizierte Dateien automatisch löschen 5 - Scanvorgang fortsetzen Standardwert: 2
bButtonClean	Typ: Boolescher Wert (1/0) Der Benutzer erhält die Möglichkeit, die Datei zu säubern, wenn **Eingabe anfordern** gewählt ist und ein Virus erkannt wird. Standardwert: 1
bButtonDelete	Typ: Boolescher Wert (1/0) Der Benutzer erhält die Möglichkeit, die Datei zu löschen, wenn **Eingabe anfordern** gewählt ist und ein Virus erkannt wird. Standardwert: 1
bButtonExclude	Typ: Boolescher Wert (1/0) Der Benutzer erhält die Möglichkeit, die Datei auszuschließen, wenn **Eingabe anfordern** gewählt ist und ein Virus erkannt wird. Standardwert: 1
bButtonMove	Typ: Boolescher Wert (1/0) Der Benutzer erhält die Möglichkeit, die Datei zu verschieben, wenn **Eingabe anfordern** gewählt ist und ein Virus erkannt wird. Standardwert: 1
bButtonContinue	Typ: Boolescher Wert (1/0) Der Benutzer erhält die Möglichkeit, den Scanvorgang fortzusetzen, wenn **Eingabe anfordern** gewählt ist und ein Virus erkannt wird.

	Standardwert: 1
bButtonStop	Typ: Boolescher Wert (1/0) Der Benutzer erhält die Möglichkeit, den Scanvorgang zu stoppen, wenn **Eingabe anfordern** gewählt ist und ein Virus erkannt wird. Standardwert: 1
szMoveToFolder	Typ: Zeichenfolge Bestimmt den Ordner, in den infizierte Dateien verschoben werden sollen. Standardwert: \Infected
szCustomMessage	Typ: Zeichenfolge Bestimmt die benutzerdefinierte Meldung, die beim Erkennen eines Virus angezeigt werden soll. Standardwert: Ihre benutzerdefinierte Meldung

ReportOptions

Variable	Beschreibung
bLogToFile	Typ: Boolescher Wert (1/0) Bestimmt, ob die Scanergebnisse in einer Protokolldatei festgehalten werden. Standardwert: 0
bLimitSize	Typ: Boolescher Wert (1/0) Bestimmt, ob die Größe des Protokolls beschränkt wird. Standardwert: 1
uMaxKilobytes	Typ: Ganzzahl Bestimmt die maximale Größe der Protokolldatei in Kilobyte. Standardwert: 100
bLogDetection	Typ: Boolescher Wert (1/0) Bestimmt, ob die Scanergebnisse protokolliert werden. Standardwert: 1
bLogClean	Typ: Boolescher Wert (1/0) Bestimmt, ob die Ergebnisse einer Säuberung protokolliert werden. Standardwert: 1
bLogDelete	Typ: Boolescher Wert (1/0) Bestimmt, ob das Löschen von Dateien protokolliert wird. Standardwert: 1
bLogMove	Typ: Boolescher Wert (1/0) Bestimmt, ob das Verschieben von infizierten Dateien protokolliert wird. Standardwert: 1
bLogSetting	Typ: Boolescher Wert (1/0) Bestimmt, ob die Sitzungseinstellungen beim Herunterfahren protokolliert werden. Standardwert: 1
bLogSummary	Typ: Boolescher Wert (1/0) Bestimmt, ob die Sitzungsübersicht beim Herunterfahren protokolliert wird. Standardwert: 1
bLogDateTime	Typ: Boolescher Wert (1/0) Bestimmt, ob Datum und Uhrzeit eines Ereignisses protokolliert werden. Standardwert: 1
bLogUserName	Typ: Boolescher Wert (1/0) Bestimmt, ob der Benutzername protokolliert wird. Standardwert: 1
szLogFileName	Typ: Zeichenfolge Bestimmt den Namen der Protokolldatei.

Standardwert: VSCLOG.TXT

ScanItems

Variable	Beschreibung
szScanItem_0	Typ: Zeichenfolge Bestimmt das zu scannende Element. Standardwert: C:\

SecurityOptions

Variable	Beschreibung
szPasswordProtect	Typ: Boolescher Wert (1/0) Bestimmt, ob Kennwortschutz aktiviert ist. Standardwert: 0
szPasswordCRC	
bInheritSecurity	

ExcludedItems

Variable	Beschreibung
NumExcludeItems	Typ: Ganzzahl (0-n) Bestimmt die Zahl der Elemente, die vom Scannen auf Zugriff ausgeschlossen sind. Standardwert: 1
ExcludedItem_x, wobei x ein nullbasierter Index ist	Typ: Zeichenfolge Weist Vshield an, das Element vom Scannen auf Zugriff auszuschließen. Standardwert: \Recycled|*.*|1|1 * * Die Zeichenfolge wird mit Hilfe des senkrechten Strichs (|) in Felder unterteilt: Feld 1 - Ordnerangabe des auszuschließenden Elements. Lassen Sie dieses Feld leer, wenn eine einzelne Datei an einem unbestimmten Ort im System angegeben werden soll. Feld 2 - Dateiangabe des auszuschließenden Elements. Lassen Sie dieses Feld leer, wenn ein ganzer Ordner ohne bestimmte Datei ausgeschlossen werden soll. Feld 3 - Ganzzahl (1-3) Mögliche Werte: 1 - Vom Scannen bei Dateizugriff ausschließen 2 - Vom Scannen des Boot-Datensatzes ausschließen 3 - Vom Scannen des Boot-Datensatzes und bei Dateizugriff ausschließen Feld 4 - Boolescher Wert (1/0) Mögliche Werte: 0 - Weist VShield an, auch untergeordnete Ordner des ausgeschlossenen Elements auszuschließen. 1 - Weist VShield an, untergeordnete Ordner nicht auszuschließen.

Dateiformat VSH

Die VSH-Datei ist eine Konfigurationstextdatei, die ähnlich wie die Windows-INI-Datei formatiert ist; in ihr sind die VShield-Einstellungen festgehalten. Jede Variable in der Datei hat einen Namen, auf den ein Gleichheitszeichen (=) und ein entsprechender Wert folgen. Die Werte bestimmen, welche Einstellungen für die VShield-Konfiguration gewählt wurden. Die Variablen sind in fünf Gruppen unterteilt: DetectionOptions, ActionOptions, ReportOptions, General und ExcludedItems. Zum Bearbeiten kann eine VSH-Datei mit jedem Texteditor geöffnet werden

Hinweis

Bei Booleschen Variablen sind nur die Werte 0 und 1 möglich. Mit dem Wert 0 wird die jeweilige Einstellung deaktiviert; 1 bedeutet, daß die Einstellung aktiviert ist.

General

Variable	Beschreibung
bCanBeDisabled	Typ: Boolescher Wert (1/0) Bestimmt, ob VShield deaktiviert werden kann. Standardwert: 1
bShowTaskbarIcon	Typ: Boolescher Wert (1/0) Bestimmt, ob das VShield-Taskleistensymbol angezeigt wird. Standardwert: 1
bLoadAtStartup	Typ: Boolescher Wert (1/0) Bestimmt, ob VShield beim Systemstart geladen werden soll. Standardwert: 1
bNoSplash	Typ: Boolescher Wert (1/0) Weist VShield an, beim Programmstart kein Einführungsbild anzuzeigen. Standardwert: 0

DetectionOptions

Variable	Beschreibung
bScanOnExecute	Typ: Boolescher Wert (1/0) Weist VShield an, Dateien zu scannen, wenn sie ausgeführt werden. Standardwert: 1
bScanOnOpen	Typ: Boolescher Wert (1/0) Weist VShield an, Dateien zu scannen, wenn sie geöffnet werden. Standardwert: 1
bScanOnCreate	Typ: Boolescher Wert (1/0) Weist VShield an, Dateien zu scannen, wenn sie erstellt werden. Standardwert: 1
bScanOnRename	Typ: Boolescher Wert (1/0) Weist VShield an, Dateien zu scannen, wenn sie umbenannt werden. Standardwert: 1
bScanOnShutdown	Typ: Boolescher Wert (1/0) Weist VShield an, den Boot-Datensatz von Laufwerk A: zu scannen, wenn das System heruntergefahren wird. Standardwert: 1
bScanOnBootAccess	Typ: Boolescher Wert (1/0) Weist VShield an, den Boot-Datensatz eines

	Datenträgerlaufwerks zu scannen, wenn zum ersten Mal darauf zugegriffen wird. Standardwert: 1
bScanAllFiles	Typ: Boolescher Wert (1/0) Weist das Programm an, alle Dateien zu scannen. Standardwert: 0
bScanCompressed	Typ: Boolescher Wert (1/0) Weist das Programm an, komprimierte Dateien zu scannen. Standardwert: 0
szProgramExtensions	Typ: Zeichenfolge Bestimmt die Erweiterungen der Dateitypen, die gescannt werden sollen. Standardwert: EXE COM DO? XL?
szDefaultProgramExtensions	Typ: Zeichenfolge Bestimmt, welche Dateinamenerweiterungen bei der Scankonfiguration als Standardprogrammerweiterungen verwendet werden sollen. Standardwert: EXE COM DO? XL?

AlertOptions

Variable	Beschreibung
bNetworkAlert	Typ: Boolescher Wert (1/0) Weist VirusScan an, eine Meldung für eine zentrale Warnung an einen Server zu senden, auf dem NetShield ausgeführt wird. Standardwert: 0
szNetworkAlertPath	Typ: Zeichenfolge Bestimmt den Pfad zu dem Server, auf dem NetShield ausgeführt wird. Standardwert: keiner

ActionOptions

Variable	Beschreibung
bDisplayMessage	Typ: Boolescher Wert (1/0) Bestimmt, ob beim Erkennen eines Virus eine benutzerdefinierte Meldung im Dialogfeld **Eingabe anfordern** angezeigt wird. Standardwert: 0
uVshieldAction	Typ: Ganzzahl (1-5) Weist VShield an, die angegebene Aktion durchzuführen, wenn ein Virus erkannt wird. Mögliche Werte: 1 - Eingabe anfordern 2 - Infizierte Dateien in einen Ordner verschieben 3 - Infizierte Dateien automatisch säubern (Zugriff verweigern, wenn Dateien nicht gesäubert werden können) 4 - Infizierte Dateien automatisch löschen 5 - Zugriff auf infizierte Dateien verweigern Standardwert: 1
bButtonClean	Typ: Boolescher Wert (1/0) Der Benutzer erhält die Möglichkeit, die Datei zu

	säubern, wenn **Eingabe anfordern** gewählt ist und ein Virus erkannt wird. Standardwert: 1
bButtonDelete	Typ: Boolescher Wert (1/0) Der Benutzer erhält die Möglichkeit, die Datei zu löschen, wenn **Eingabe anfordern** gewählt ist und ein Virus erkannt wird. Standardwert: 1
bButtonExclude	Typ: Boolescher Wert (1/0) Der Benutzer erhält die Möglichkeit, die Datei auszuschließen, wenn **Eingabe anfordern** gewählt ist und ein Virus erkannt wird. Standardwert: 1
bButtonContinue	Typ: Boolescher Wert (1/0) Der Benutzer erhält die Möglichkeit, den Scanvorgang fortzusetzen, wenn **Eingabe anfordern** gewählt ist und ein Virus erkannt wird. Standardwert: 1
bButtonStop	Typ: Boolescher Wert (1/0) Der Benutzer erhält die Möglichkeit, den Scanvorgang zu stoppen, wenn **Eingabe anfordern** gewählt ist und ein Virus erkannt wird. Standardwert: 1
szMoveToFolder	Typ: Zeichenfolge Bestimmt den Ordner, in den infizierte Dateien verschoben werden sollen. Standardwert: \Infected
szCustomMessage	Typ: Zeichenfolge Bestimmt die benutzerdefinierte Meldung, die angezeigt werden soll, wenn **Eingabe anfordern** gewählt ist und ein Virus erkannt wird. Standardwert: Ihre benutzerdefinierte Meldung

ReportOptions

Variable	**Beschreibung**
bLogToFile	Typ: Boolescher Wert (1/0) Bestimmt, ob die Scanergebnisse in einer Protokolldatei festgehalten werden. Standardwert: 0
bLimitSize	Typ: Boolescher Wert (1/0) Bestimmt, ob die Größe des Protokolls beschränkt wird. Standardwert: 1
uMaxKilobytes	Typ: Ganzzahl (10-999) Bestimmt die maximale Größe der Protokolldatei in Kilobyte. Standardwert: 100
bLogDetection	Typ: Boolescher Wert (1/0) Bestimmt, ob die Ergebnisse des Scanvorgangs protokolliert werden. Standardwert: 1
bLogClean	Typ: Boolescher Wert (1/0) Bestimmt, ob die Ergebnisse einer Säuberung protokolliert werden. Standardwert: 1
bLogDelete	Typ: Boolescher Wert (1/0) Bestimmt, ob das Löschen von infizierten Dateien protokolliert wird. Standardwert: 1

bLogMove	Typ: Boolescher Wert (1/0) Bestimmt, ob das Verschieben von infizierten Dateien protokolliert wird. Standardwert: 1
bLogSettings	Typ: Boolescher Wert (1/0) Bestimmt, ob die Sitzungseinstellungen beim Herunterfahren protokolliert werden. Standardwert: 1
bLogSummary	Typ: Boolescher Wert (1/0) Bestimmt, ob die Sitzungsübersicht beim Herunterfahren protokolliert wird. Standardwert: 1
bLogDateTime	Typ: Boolescher Wert (1/0) Bestimmt, ob Datum und Uhrzeit eines Ereignisses protokolliert werden. Standardwert: 1
bLogUserName	Typ: Boolescher Wert (1/0) Bestimmt, ob der Benutzername protokolliert wird. Standardwert: 1
szLogFileName	Typ: Zeichenfolge Bestimmt den Namen der Protokolldatei. Standardwert: C:\Programme\McAfee\VShield Activity Log.txt

SecurityOptions

Variable	Beschreibung
szPasswordProtect	Typ: Boolescher Wert (1/0) Bestimmt, ob Kennwortschutz aktiviert ist. Standardwert: 0
szPasswordCRC	

ExcludedItems

Variable	Beschreibung
NumExcludedItems	Typ: Ganzzahl (0-n) Bestimmt die Zahl der Elemente, die vom Scannen auf Zugriff ausgenommen sind. Standardwert: 1
ExcludedItem_x, wobei x ein nullbasierter Index ist	Typ: Zeichenfolge Weist Vshield an, das Element vom Scannen auf Zugriff auszuschließen. Standardwert: \Recycled|*.*|1|1 * * Die Zeichenfolge wird mit Hilfe des senkrechten Strichs (|) in Felder unterteilt: Feld 1 - Ordnerangabe des auszuschließenden Elements. Lassen Sie dieses Feld leer, wenn eine einzelne Datei an einem unbestimmten Ort im System angegeben werden soll. Feld 2 - Dateiangabe des auszuschließenden Elements. Lassen Sie dieses Feld leer, wenn ein ganzer Ordner ohne bestimmte Datei ausgeschlossen werden soll. Feld 3 - Ganzzahl (1-3) Mögliche Werte: 1 - Vom Scannen bei Dateizugriff ausschließen

2 - Vom Scannen des Boot-Datensatzes ausschließen
3 - Vom Scannen des Boot-Datensatzes und bei Dateizugriff ausschließen
Feld 4 - Boolescher Wert (1/0)
Mögliche Werte:
0 - Weist VShield an, auch untergeordnete Ordner des ausgeschlossenen Elements auszuschließen
1 - Weist VShield an, untergeordnete Ordner nicht auszuschließen

Dateiformat ALR für zentrale Warnung

Die ALR-Datei ist der Text für die zentrale Warnung, der Variablen für Virusereignisse enthält. Jede Variable in der Datei hat einen Namen, auf den ein Gleichheitszeichen (=) und ein entsprechender Wert folgen. Im folgenden finden Sie eine Beschreibung der einzelnen Zeilen der ALR-Datei für zentrale Warnungen:

[CentralAlert]	Kennung der zentralen Warnung
uFileVersion	Typ: Ganzzahl Versionsnummer der zentralen Warnung
uStatus	
szVirusName	Typ: Zeichenfolge Name des Virus
szItemName	Typ: Zeichenfolge Name und Pfad der infizierten Datei
szUserName	Typ: Zeichenfolge Name des Benutzers
szSoftware	Typ: Zeichenfolge Name der McAfee-Anti-Virus-Anwendung, die auf dem Computer, von dem die Meldung stammt, installiert ist
szSoftwareVersion	Typ: Zeichenfolge Version der Anti-Virus-Anwendung
szComputerName	Typ: Zeichenfolge Name des Computers, von dem die Meldung stammt
uYear	Typ: Ganzzahl (0000-9999) Jahr des Ereignisses
uMonth	Typ: Ganzzahl (1-12) Monat des Ereignisses
uDay	Typ: Ganzzahl (1-31) Tag des Ereignisses
uHour	Typ: Ganzzahl (0-23) Stunde des Ereignisses
uMinute	Typ: Ganzzahl (0-59) Minute des Ereignisses
uSecond	Typ: Ganzzahl (0-59) Sekunde des Ereignisses

Testen der Installation

Die Datei "Eicar Standard AntiVirus Test File" wurde von Antivirus-Programm-Vertreibern auf der ganzen Welt gemeinsam als einheitliche Norm entwickelt, anhand der ihre Kunden die Installation ihrer Antivirenprogramme überprüfen können. Kopieren Sie, um Ihre Installation zu testen, folgende Zeile in eine eigene Datei, und nennen Sie sie EICAR.COM.

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Diese Datei hat dann eine Größe von 69 oder 70 Byte.

Eine Prüfung der Datei mit VirusScan ergibt, daß der Virus EICAR-STANDARD-AV-TEST-FILE gefunden wurde. DIESE DATEI IST KEIN VIRUS! Löschen Sie die Datei, nachdem der Installationstest abgeschlossen ist, damit andere Benutzer nicht unnötig beunruhigt werden.

Hinweis

Da die Datei "Eicar Standard AntiVirus Test File" keine echte Virusinfizierung darstellt, ist es nicht möglich, die infizierte Datei zu säubern oder zu reparieren.

Macros, below

McAfee-Virus-Informationsbibliothek

Die McAfee-Virusinformationsbibliothek enthält detaillierte Informationen über Viren. Dazu gehören der Name des Virus, seine Merkmale, seine Infizierungsmethode, Kennzeichen einer Infizierung sowie Möglichkeiten der Säuberung.

Auf die McAfee-Virus-Informationsbibliothek kann auf verschiedene Weise zugegriffen werden:

Klicken Sie hier, um automatisch zur aktuellsten Version der Virus-Informationsbibliothek zu gelangen.

Rufen Sie http://www.mcafee.com/support/techdocs/vinfo/index.html auf, um manuell zur aktuellsten Version der Virus-Informationsbibliothek zu gelangen.

Wenn Sie die Hilfedatei-Version der Virus-Informationsbibliothek in Ihr VirusScan-Programmdateiverzeichnis kopiert haben, klicken Sie hier.

Wenn Sie die Hilfedatei-Version der Virus-Informationsbibliothek nicht in Ihr VirusScan-Programmdateiverzeichnis kopiert haben, starten Sie den Datei-Manager, gehen Sie zur VirusScan-CD-ROM, und doppelklicken Sie auf MCAFEE.HLP.

McAfee-Virus-Informationsbibliothek (Hilfedatei)

Bitte warten Sie, bis die McAfee-Virus-Informationsbibliothek geladen ist.

Hinweis

Wenn der Ladevorgang länger als 10-15 Sekunden dauert, ist die Virus-Informationsbibliothek möglicherweise nicht auf Ihrem System installiert. Um sie zu installieren, kopieren Sie einfach die Datei MCAFEE.HLP in Ihr VirusScan-Verzeichnis (standardmäßig C:\MCAFEE\VIRUSCAN).

Wenn Sie die Virus-Informationsbibliothek manuell starten möchten, öffnen Sie den Datei-Manager, und doppelklicken Sie auf die Hilfedatei MCAFEE.HLP.

McAfee-Virus-Informationsbibliothek (McAfee-Website)

Bitte warten Sie, bis der Zugriff auf die McAfee-Virus-Informationsbibliothek erfolgt ist.

Hinweise

Damit auf diese Version der Virus-Informationsbibliothek zugegriffen werden kann, muß eine aktive Verbindung zum Internet sowie Netscape Navigator oder Microsoft Internet Explorer vorhanden sein. Wenn Sie über keinen dieser Browser verfügen, aber Zugriff auf das World Wide Web haben, können Sie auf die Bibliothek unter http://www.mcafee.com/support/techdocs/vinfo/index.html zugreifen.

Hilfsprogramm zur Erstellung einer Erste-Hilfe-Diskette

Bitte warten Sie, bis das Hilfsprogramm zur Erstellung einer Erste-Hilfe-Diskette geladen ist.

Hinweis

Wenn der Ladevorgang länger als einige Sekunden dauert, starten Sie das Hilfsprogramm zur Erstellung einer Erste-Hilfe-Diskette manuell. Öffnen Sie dazu die VirusScan-Programmgruppe, und doppelklicken Sie auf das Symbol für Erstellung einer Erste-Hilfe-Diskette.

McAfee-Website

Bitte warten Sie, bis der Zugriff auf die McAfee-Website erfolgt ist.

Hinweise

Damit auf die McAfee-Website zugegriffen werden kann, muß eine aktive Verbindung zum Internet sowie Netscape Navigator oder Microsoft Internet Explorer vorhanden sein. Wenn Sie über keinen dieser Browser verfügen, aber Zugriff auf das World Wide Web haben, können Sie auf die Website unter http://www.mcafee.com zugreifen.

VShield-Eigenschaften

Bitte warten Sie, bis VShield geladen ist.

Hinweis

Wenn der Ladevorgang länger als einige Sekunden dauert, starten Sie VShield manuell. Öffnen Sie dazu die VirusScan-Programmgruppe, und doppelklicken Sie auf das VShield-Symbol.

VirusScan-Konsole

Bitte warten Sie, bis die VirusScan-Konsole geladen ist.

Hinweis

Wenn der Ladevorgang länger als einige Sekunden dauert, starten Sie die VirusScan-Konsole manuell. Öffnen Sie dazu die VirusScan-Programmgruppe, und doppelklicken Sie auf das Symbol für VirusScan-Konsole.

Scannen auf Anforderung von VirusScan

Bitte warten Sie, bis VirusScan geladen ist.

Hinweis

Wenn der Ladevorgang länger als einige Sekunden dauert, starten Sie VirusScan manuell. Öffnen Sie dazu die VirusScan-Programmgruppe, und doppelklicken Sie auf das VirusScan-Symbol.

NCSA-Website

Bitte warten Sie, bis der Zugriff auf die NCSA-Website erfolgt ist.

Hinweis

Damit auf die NCSA-Website zugegriffen werden kann, muß eine aktive Verbindung zum Internet sowie Netscape Navigator oder Microsoft Internet Explorer vorhanden sein. Wenn Sie über keinen dieser Browser verfügen, aber Zugriff auf das World Wide Web haben, können Sie auf die Website unter http://www.ncsa.com zugreifen.

Adobe-Website

Bitte warten Sie, bis der Zugriff auf die Adobe-Website erfolgt ist.

Hinweis

Damit auf die Adobe-Website zugegriffen werden kann, muß eine aktive Verbindung zum Internet sowie Netscape Navigator oder Microsoft Internet Explorer vorhanden sein. Wenn Sie über keinen dieser Browser verfügen, aber Zugriff auf das World Wide Web haben, können Sie auf die Website unter http://www.adobe.com zugreifen.

Virusaktivitätsprotokoll von VShield

Bitte warten Sie, bis das Aktivitätsprotokoll geladen ist.

Hinweis

Wenn das Aktivitätsprotokoll nicht geöffnet wird, ist entweder die Option **Protokollieren in Datei** deaktiviert, oder Sie verwenden nicht den standardmäßigen Protokolldateinamen. Um das VShield-Aktivitätsprotokoll manuell zu öffnen, öffnen Sie einfach die auf der Seite **Report** definierte Datei mit einem beliebigen Texteditor (z.B. Editor, Word usw.).

Virusaktivitätsprotokoll für Scannen auf Anforderung

Bitte warten Sie, bis das Aktivitätsprotokoll geladen ist.

Hinweis

Wenn das Aktivitätsprotokoll nicht geöffnet wird, ist entweder die Option **Protokollieren in Datei** deaktiviert, oder Sie verwenden nicht den standardmäßigen Protokolldateinamen. Um das Aktivitätsprotokoll zu öffnen, wählen Sie **Aktivitätsprotokoll anzeigen** aus dem Menü **Datei**.

Virenliste

Bitte warten Sie, bis die Virenliste geladen ist.

Hinweis

Wenn der Ladevorgang länger als einige Sekunden dauert, starten Sie die Virenliste manuell. Starten Sie dazu den Datei-Manager, gehen Sie zum VirusScan-Verzeichnis, und doppelklicken Sie auf VIRLST16.EXE.

end macros

VirusScan-Benutzerhandbuch

Das VirusScan-Benutzerhandbuch liegt im Adobe Acrobat-Format (PDF) vor und ist auf der VirusScan-CD-ROM zu finden. Starten Sie Adobe Acrobat, und öffnen Sie WSCDOC31.PDF, um das VirusScan-Benutzerhandbuch zu öffnen.

Hinweis

Zum Lesen des Handbuchs müssen Sie den Adobe Acrobat Reader installiert haben. Der Acrobat Reader ist auf der CD-ROM-Version des Produkts zu finden. Außerdem kann er von www.adobe.com heruntergeladen werden. Klicken Sie hier, um zur Adobe-Website zu gelangen.

Context-sensitive, below

Programmdateien

1. Zum Hinzufügen einer Dateinamenerweiterung klicken Sie auf **Hinzufügen**.
2. Geben Sie die Erweiterung eines weiteren Dateityps ein, der gescannt werden soll, und klicken Sie auf **OK**.
3. Wiederholen Sie die Schritte 1 und 2 so oft, bis alle gewünschten Erweiterungen eingegeben sind.
4. Wenn Sie mit dem Bearbeiten der Erweiterungsliste fertig sind, klicken Sie auf **OK**.

Tips

Wenn Sie eine Erweiterung löschen möchten, wählen Sie sie aus, und klicken Sie auf **Löschen**.
Wenn Sie wieder die Standarderweiterungen verwenden möchten, klicken Sie auf **Standard**.

Scanelement hinzufügen

Wählen sie eine oder mehrere der folgenden Möglichkeiten:

- Wenn Sie alle Laufwerke scannen möchten, die an Ihren Computer angeschlossen sind, klicken Sie auf die Optionsschaltfläche **Zu scannendes Element auswählen**, und wählen Sie **Mein Computer**.
- Wenn Sie alle entfernbaren Medien, einschließlich Disketten, scannen möchten, klicken Sie auf die Optionsschaltfläche **Zu scannendes Element auswählen**, und wählen Sie **Alle entfernbaren Medien**.
- Wenn Sie alle Festplattenlaufwerke scannen möchten, die an Ihren Computer angeschlossen sind, klicken Sie auf die Optionsschaltfläche **Zu scannendes Element auswählen**, und wählen Sie **Alle Festplatten**.
- Wenn Sie alle eingehängten Netzlaufwerke scannen möchten, klicken Sie auf die Optionsschaltfläche **Zu scannendes Element auswählen**, und wählen Sie **Alle Netzlaufwerke**.
- Wenn Sie ein einzelnes Laufwerk oder Verzeichnis scannen möchten, klicken Sie auf die Optionsschaltfläche **Zu scannendes Laufwerk oder Verzeichnis auswählen**, und geben Sie den Pfad zu dem zu scannenden Element ein, oder klicken Sie auf **Durchsuchen**, um danach zu suchen.

Nachdem Sie ein Scanelement ausgewählt haben, klicken Sie auf **OK**. Wenn Sie das Dialogfeld schließen möchten, ohne ein Scanelement hinzuzufügen, klicken Sie auf **Abbrechen**.

Ausschlußelement hinzufügen

1. Geben Sie den vollständigen Pfad zu einer Datei, einem Laufwerk oder einem Verzeichnis ein, oder klicken Sie auf **Durchsuchen**, um nach dem gewünschten Element zu suchen.
2. Aktivieren Sie das Kontrollkästchen **Unterverzeichnisse einschließen**, um Unterverzeichnisse vom Scannen auszuschließen.
3. Aktivieren Sie das Kontrollkästchen **Scannen von Dateien**, um das Element vom Scannen der Dateien auszuschließen.
4. Aktivieren Sie das Kontrollkästchen **Scannen von Boot-Sektoren**, um das Element vom Scannen der Boot-Sektoren auszuschließen.
5. Klicken Sie auf **OK**, um das Ausschlußelement hinzuzufügen. Wenn Sie das Dialogfeld schließen möchten, ohne das Ausschlußelement hinzuzufügen, klicken Sie auf **Abbrechen**.

Hinweise

Wenn Sie ein Scanelement bearbeiten möchten, wählen Sie es aus, und klicken Sie auf **Bearbeiten**.

Wenn Sie ein Scanelement entfernen möchten, wählen Sie es aus, und klicken Sie auf **Entfernen**.

Kennwort ändern

1. Geben Sie ein neues Kennwort ein.
2. Geben Sie das Kennwort erneut ein.

Virenliste

Mit Hilfe der Virenliste finden Sie wichtige Grundinformationen über Ihr Virus. Wenn Sie Einzelheiten über Ihr Virus erfahren möchten, gehen Sie folgendermaßen vor:

1. Suchen Sie Ihr Virus, indem Sie die Virenliste durchgehen oder indem Sie auf **Virus suchen** klicken und den Virusnamen eingeben.

2. Heben Sie den Virusnamen hervor, und klicken Sie auf **Virus-Info**. Es erscheint die Seite **Virusinformationen**.

3. Darauf finden Sie folgende Angaben:

   Virusinformationen:
   Name des Virus
   Infiziert folgendes
   Virusgröße

   Virusmerkmale:
   Speicherresident
   Verschlüsselt
   Polymorph
   Reparabel
   Makrovirus

Virusinformationen

Das Dialogfeld enthält folgende Angaben:

Virusinformationen

Name des Virus
Infiziert folgendes
Virusgröße

Virusmerkmale

Speicherresident
Verschlüsselt
Polymorph
Reparabel
Makrovirus

Informationen über infizierte Elemente

Dieses Dialogfeld enthält folgende Angaben:

Name des Virus

Dateiinformationen

Typ
Speicherort
Größe

MS-DOS-Name und Datumsangaben

MS-DOS-Name
Erstellt
Geändert
Zugriff

Dateiattribute

Schreibgeschützt
Verborgen
Archiv
System