Konfigurieren von Sophos Anti-Virus

In diesem Abschnitt werden die Optionen erläutert, die Sie konfigurieren können. Diese Optionen finden Sie in den Menüs ‘Optionen’ und ‘Ansicht’ in der Symbolleiste der **Benutzeroberfläche** von Sophos Anti-Virus.

Konfigurationsoptionen

Betriebsart
Maßnahmen
Bericht
Dateiliste
Zeitplan
Überprüfung (nur Windows NT)
Ausnahmen (nur Windows NT)

Benachrichtigungsoptionen

InterCheck-Protokoll (nur Windows NT)
Benachrichtigung auf dem Desktop
Ereignisprotokoll (nur Windows NT)
Netzwerkmeldungen (nur Windows NT)
E-mail per SMTP
E-mail per MAPI (nur Windows 95/98)

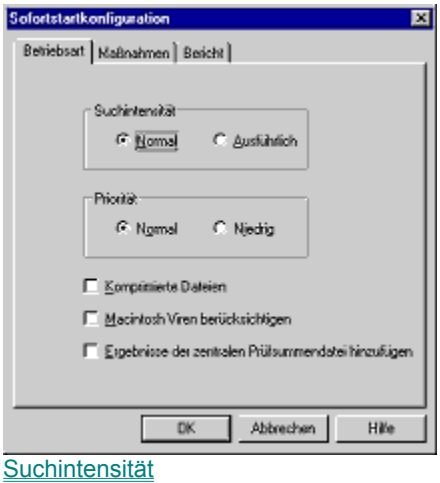
Weitere Optionen

Ausführbare Dateien
Ausnahmeliste
Standard herstellen
Protokoll löschen
Prüfsummen löschen (nur Windows NT)
Sicherheit (nur Windows NT)
Statusanzeige

Dialog Betriebsart

Betriebsart

Auf dieser Konfigurationsseite kann man die Virenüberprüfungen von Sophos Anti-Virus konfigurieren. Sie ist für alle Registerkarten des Hauptfensters möglich.



Suchintensität
Priorität
Komprimierte Dateien
Macintosh-Viren berücksichtigen (nur Windows NT)
Ergebnisse der zentralen Prüfsummendatei hinzufügen (nur Windows NT)

Zurück zu **Konfigurationsmenü**

Überschriften **Betriebsart**

Suchintensität

Es gibt zwei Möglichkeiten der Überprüfung.

Die normale Überprüfung untersucht die Bereiche der Datei, die wahrscheinlich Viren enthalten. Diese Einstellung ist normalerweise ausreichend.

Die ausführliche Überprüfung untersucht den gesamten Inhalt jeder Datei. Dies erhöht die Sicherheit, da so auch Viren aufgespürt werden, die sich in anderen Bereichen der Datei verstecken oder Mutationen und Defekte aufweisen.

Hinweis: Eine ausführliche Überprüfung ist wesentlich langsamer als eine normale.

Wählen Sie zwischen normaler und ausführlicher Suchintensität.

Zurück zu **Betriebsart**

Zurück zu **Konfigurationsmenü**

Priorität

Soll Sophos Anti-Virus die Systemleistung möglichst wenig beeinträchtigen, kann man niedrige Priorität wählen. Diese Einstellung verlängert allerdings die Überprüfungszeit von Sophos Anti-Virus.

Wählen Sie zwischen normaler und niedriger Priorität.

Zurück zu **Betriebsart**

Zurück zu **Konfigurationsmenü**

Komprimierte Dateien

Sophos Anti-Virus kann Dateien auf Viren überprüfen, die komprimiert sind.

Hinweis: InterCheck bietet automatischen Schutz vor Viren in komprimierten Dateien, da der Zugriff auf unbekannte Dateien (z.B. auf eine gerade erst entpackte Datei) erst dann gewährt wird, wenn diese auf Viren überprüft wurde.

Kreuzen Sie das Kästchen an, wenn Sophos Anti-Virus den Inhalt von komprimierten Dateien überprüfen soll.

Zurück zu **Betriebsart**

Zurück zu **Konfigurationsmenü**

Macintosh-Viren berücksichtigen (nur Windows NT)

Sophos Anti-Virus für Windows NT kann Macintosh-Dateien auf Viren untersuchen. Ist diese Option aktiviert, überprüft Sophos Anti-Virus *alle* Macintosh-Programme, unabhängig von ihrer Dateierweiterung.

Kreuzen Sie das Kästchen an, wenn Sophos Anti-Virus nach Macintosh-Dateien suchen soll.

Zurück zu **Betriebsart**

Zurück zu **Konfigurationsmenü**

Ergebnisse der zentralen Prüfsummendatei hinzufügen (nur Windows NT)

Jede Datei, die für virenfrei befunden wurde, kann der zentralen **Prüfsummendatei** hinzugefügt werden. Arbeitsplatzrechner die mit InterCheck von einem Fileserver aus arbeiten, können diese zentrale Prüfsummendatei zusätzlich zu ihrer eigenen, lokalen Prüfsummendatei verwenden. Auf diese Weise kann mehrfaches Überprüfen und Freigabe identischer Dateien vermieden werden.

Kreuzen Sie das Kästchen an, wenn Sophos Anti-Virus virenfreie Dateien zur zentralen Prüfsummendatei hinzufügen soll.

Hinweis: Diese Option ist nur verfügbar, wenn InterCheck installiert ist.

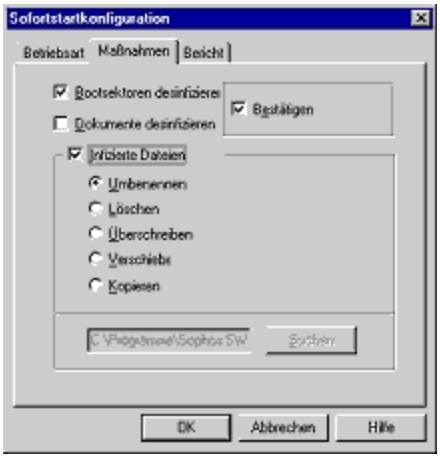
Zurück zu **Betriebsart**

Zurück zu **Konfigurationsmenü**

Dialog Maßnahmen

Maßnahmen

Der Dialog Maßnahmen ist für alle Registerkarten (außer für die Registerkarte SAVI) der **Benutzeroberfläche** von Sophos Anti-Virus möglich. Bei einigen Konfigurationsdialogen sind bestimmte Maßnahmenoptionen nicht verfügbar (in hellgrau gekennzeichnet).



Bootsektoren desinfizieren
Dokumente desinfizieren
Infizierte Dateien

Bestätigen

Zurück zu **Konfigurationsmenü**

Überschriften Maßnahmen

Bootsektoren desinfizieren

Es gibt zwei Arten von Bootsektoren:

Diskettenbootsektoren

Sophos Anti-Virus kann die meisten der auf Disketten zu findenden Bootsektorviren entfernen.

Festplattenbootsektoren

Sophos Anti-Virus entfernt Bootsektorviren *nicht* automatisch von Festplatten. Sie müssen Viren aus Festplattenbootsektoren manuell entfernen. (siehe Viren manuell entfernen).

Kreuzen Sie das Kästchen ‘Bootsektoren infizieren’ an, wenn infizierte Bootsektoren behandelt werden sollen.

Zurück zu **Maßnahmen**

Zurück zu **Konfigurationsmenü**

Dokumente desinfizieren

Sophos Anti-Virus kann Viren aus bestimmten Dokumenten entfernen (Dateien, die **Makros** enthalten).

Kann der Virus aus einem Dokument nicht entfernt werden, wird das infizierte Dokument wie jede andere infizierte Datei behandelt, die auf dem System gefunden wird. (siehe Infizierte Dateien)

Kreuzen Sie das Kästchen ‘Dokumente desinfizieren’ an, wenn Sophos Anti-Virus infizierte Dokumente behandeln soll. (siehe Viren manuell entfernen)

Zurück zu **Maßnahmen**

Zurück zu **Konfigurationsmenü**

Infizierte Dateien

Eine infizierte Datei kann mit verschiedenen Maßnahmen entschärft werden:

- Umbenennen oder Verschieben vermindert die Wahrscheinlichkeit, daß eine infizierte ausführbare Datei ausgeführt wird. Mit diesen Optionen wird die Datei *nicht* gelöscht.
- Löschen oder **Überschreiben** stellt sicher, daß die Datei versehentlich geöffnet oder ausgeführt wird. Das Überschreiben ist die sicherste Methode. Mit diesen Optionen wird die Datei vernichtet.

Kreuzen Sie das Kästchen ‘Infizierte Dateien’ an und wählen Sie die Maßnahme, mit der Sophos Anti-Virus infizierte Dateien behandeln soll. (siehe Viren manuell entfernen)

Zurück zu **Maßnahmen**

Zurück zu **Konfigurationsmenü**

Bestätigen

Sophos Anti-Virus kann eine Bestätigung anfordern, bevor eine Maßnahme, mit der eine infizierte Datei behandelt werden soll, ausgeführt wird.

Diese Option ist nur für Sofortstart-Aufträge verfügbar und standardmäßig aktiviert.

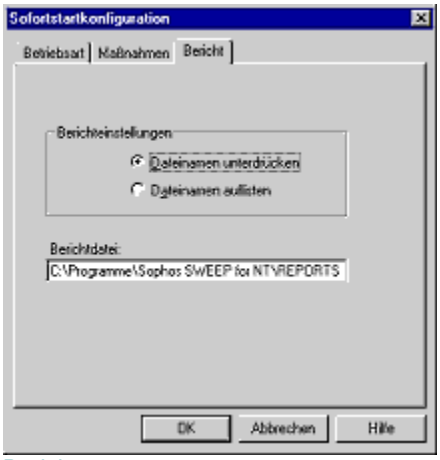
Zurück zu **Maßnahmen**

Zurück zu **Konfigurationsmenü**

Dialog **Bericht**

Bericht

Benutzer können durch Konfigurieren dieser Seite Protokolle über Sofortstart- und zeitgesteuerten Aufträge erhalten.



Berichte
Berichtdatei

Zurück zu **Konfigurationsmenü**

Überschriften Berichte

Berichte

Wählen Sie ‘Dateinamen unterdrücken’, damit überprüfte Dateien nicht in der Berichtdatei aufgeführt werden.
Wählen Sie ‘Dateinamen auflisten’, damit überprüfte Dateien in der Berichtdatei aufgeführt werden.

Zurück zu **Bericht**
Zurück zu **Konfigurationsmenü**

Berichtdatei

Standardmäßig befindet sich die Berichtdatei im Sophos-Anti-Virus-Verzeichnis unter Berichte. Falls gewünscht, kann dieses Verzeichnis vom Benutzer geändert werden.

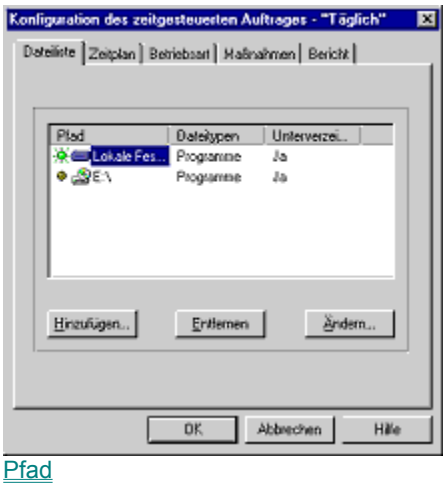
Zurück zu **Bericht**

Zurück zu **Konfigurationsmenü**

Dateiliste

Dateiliste

In der Dateiliste werden die Pfade, Verzeichnisse und Dateien aufgeführt, die bei Bedarf überprüft werden können (Sofortstart- und zeitgesteuerte Aufträge). Der Inhalt der Liste kann vom Benutzer bestimmt werden.



Pfad
Dateitypen
Unterverzeichnisse

Zurück zu **Konfigurationsmenü**

Überschriften Dateiliste

Pfad

Unter Pfad wird angezeigt, wo sich die Dateien oder Verzeichnisse befinden, die man überprüfen lassen möchte.

Zurück zu **Dateiliste**

Zurück zu **Konfigurationsmenü**

Dateitypen

Dateitypen können entweder Ausführbare Dateien/Programme oder Alle Dateien sein.

Zurück zu **Dateiliste**
Zurück zu **Konfigurationsmenü**

Unterverzeichnisse

Sollen auch die Unterverzeichnisse der Dateien des Pfads überprüft werden sollen, kreuzen Sie das Kästchen ‘Unterverzeichnisse’ an.

Zurück zu **Dateiliste**

Zurück zu **Konfigurationsmenü**

Dialog Zeitplan

Zeitplan

Sophos Anti-Virus kann so konfiguriert werden, daß Aufträge zu bestimmten Uhrzeiten an gewählten Wochentagen zeitgesteuert ausgeführt werden.

Uhrzeit hinzufügen

Um einen zeitgesteuerten Auftrag neu aufzunehmen, markieren Sie den Auftrag und wählen Sie Ändern. Im Menü Zeitplan geben Sie die Wochentage und Uhrzeiten, an denen Sie die Überprüfungen durchführen lassen möchten, klicken Sie auf hinzufügen und bestätigen Sie mit OK.

Standardmäßig überprüft Sophos Anti-Virus den Rechner beim Starten auf Viren und täglich um 21.00 Uhr unter Windows NT bzw. um 13.00 Uhr unter Windows 95/98.

Beim Starten überprüfen

Zurück zu **Konfigurationsmenü**

Überschriften Zeitplan

Beim Starten überprüfen(nur Windows NT).

Kreuzen Sie das Kästchen ‘Beim Starten überprüfen’ an, damit der markierte Auftrag den Computer bei jedem Neustart auf Viren überprüft.

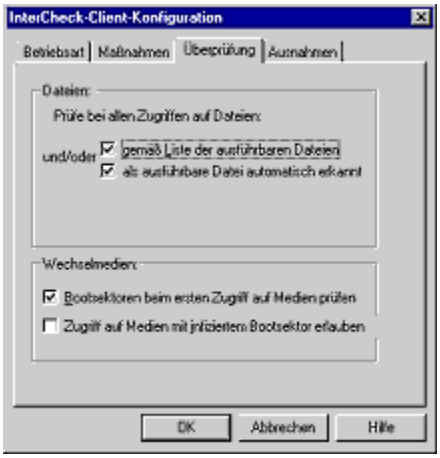
Zurück zu **Zeitplan**

Zurück zu **Konfigurationsmenü**

Dialog Überprüfung

Überprüfung (nur Windows NT)

Auf dieser Seite können die Dateitypen angegeben werden, die InterCheck überprüfen soll.



Dateien
Wechselmedien

Zurück zu **Konfigurationsmenü**

Dateien

Kreuzen Sie das Kästchen ‘Gemäß Liste der ausführbaren Dateien’ an, um Dateien überprüfen zu lassen, die als Programme definiert sind. (siehe Ausführbare Dateien/Programme)

Kreuzen Sie das Kästchen ‘Als ausführbare Datei automatisch erkannt’ an, um Dateien, die auf Grund ihrer Struktur ausführbare Dateien sein könnten, unabhängig von ihrer Erweiterung überprüfen zu lassen.

Zurück zu **Überprüfung**

Zurück zu **Konfigurationsmenü**

Wechselmedien

Kreuzen Sie das Kästchen ‘Bootsektoren beim ersten Zugriff auf Datenträger’ an, wenn InterCheck die Bootsektoren aller austauschbaren Datenträger beim ersten Gebrauch auf Viren überprüfen soll.

Kreuzen Sie das Kästchen ‘Zugriff auf Datenträger mit infizierten Bootsektoren gewähren’ an, wenn InterCheck den Zugriff auf Laufwerke mit infizierten Bootsektoren ermöglichen soll. Mit dieser Option können Dateien von einer Diskette, die mit einem Bootsektorvirus infiziert sind, herunterkopiert werden.

ACHTUNG! Starten Sie den Computer nicht mit einer infizierten Diskette. Dadurch kann ihr Computer infiziert werden.

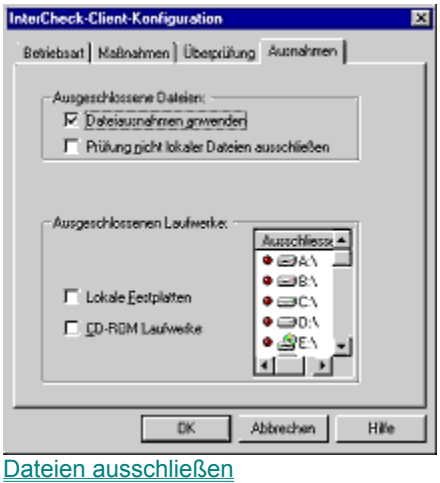
Zurück zu **Überprüfung**

Zurück zu **Konfigurationsmenü**

Dialog Ausnahmen

Ausnahmen (nur Windows NT)

Dieser Konfigurationsdialog ist verfügbar, wenn die Registerkarte IC-Client gewählt wurde. Hier können die Dateien ausgesucht werden, die InterCheck nicht überprüfen soll.



Dateien ausschließen
Laufwerke ausschließen

Zurück zu **Konfigurationsmenü**

Dateien ausschließen

Kreuzen Sie das Kästchen ‘Dateiausnahmen anwenden’ an, damit InterCheck keine Dateien überprüft, die von Sofortstart- und zeitgesteuerten Aufträgen ausgeschlossen sind.

Kreuzen Sie das Kästchen ‘Prüfung nicht lokaler Dateien ausschließen’ an, um Dateien auf Netzlaufwerken auszuschließen.

Zurück zu **Ausnahmen**

Zurück zu **Konfigurationsmenü**

Laufwerke ausschließen

Es wird eine Liste aller möglichen **Laufwerkszuordnungen** angezeigt, unabhängig davon, ob die Zuordnung im Einzelfall verfügbar ist. InterCheck überprüft KEINES der gewählten Laufwerke.

Kreuzen Sie das Kästchen ‘Lokale Festplatten ausschließen’ an, damit lokale Festplatten nicht überprüft werden, unabhängig davon, ob sie unter ‘Laufwerke ausschließen’ bestimmt wurden.

Kreuzen Sie das Kästchen ‘CD-ROM-Laufwerke ausschließen’ an, damit CD-ROM-Laufwerke nicht überprüft werden, unabhängig davon, ob sie unter ‘Laufwerke ausschließen’ bestimmt wurden.

Zurück zu **Ausnahmen**

Zurück zu **Konfigurationsmenü**

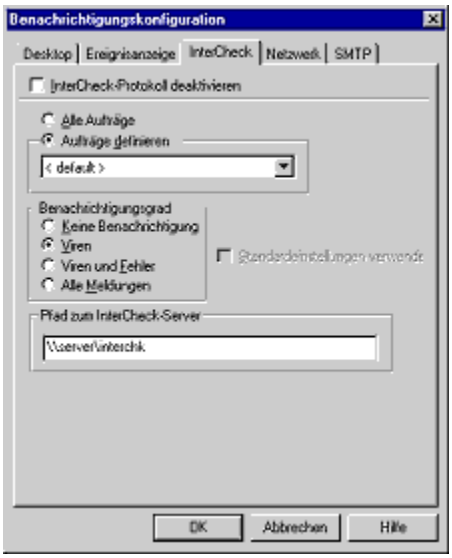
Benachrichtigungen: InterCheck-Protokoll

InterCheck-Protokoll (nur Windows NT)

Arbeitsplatzrechner können Protokollmeldungen an das COMMS-Verzeichnis eines InterCheck-Servers senden.

Die Meldungen können auf dem InterCeck-Server protokolliert werden und können weitere Benachrichtigungen veranlassen.

Diese Option kann auf jeden Auftrag zugeschnitten werden (z.B. kann die Art von Benachrichtigung für einzelne Aufträge angegeben werden).



Benachrichtigungsgrad
Pfad zum InterCheck-Server

Zurück zu **Konfigurationsmenü**

Pfad zum InterCheck-Server

Es muß ein **UNC**-Pfad angeben werde, z.B.:
`\\ServerName\INTERCHK\COMMMS`

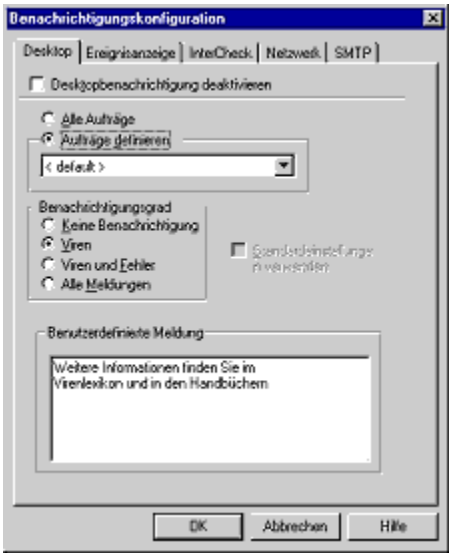
Zurück zu **InterCheck-Protokoll**
Zurück zu **Konfigurationsmenü**

Benachrichtigungen: Desktop

Benachrichtigung auf dem Desktop

Unter Windows NT kontrollieren Desktop-Benachrichtigungen Meldungen, die bei einem Virenfund angezeigt werden, während die **Benutzeroberfläche** von Sophos nicht aktiv ist.

Unter Windows 95/98 sind Desktop-Benachrichtigungen nicht möglich, währen die Benutzeroberfläche von Sophos nicht aktiv ist.



Benachrichtigungsgrad
Benutzerdefinierte Meldungen

Zurück zu **Konfigurationsmenü**

Benachrichtigungen: Benachrichtigungsgrad

Benachrichtigungsgrad

Wählen Sie den entsprechenden Benachrichtigungsgrad:

Keine Benachrichtigung

Viren

Viren und Fehler

Alle Meldungen

Zurück zu **Konfigurationsmenü**

Benutzerdefinierte Meldungen

Jede Meldung, die vom Benutzer hinzugefügt wird, wird am Ende der Standardmeldung bei einem Virenfund angehängt.

Zurück zu **Benachrichtigung auf dem Desktop**

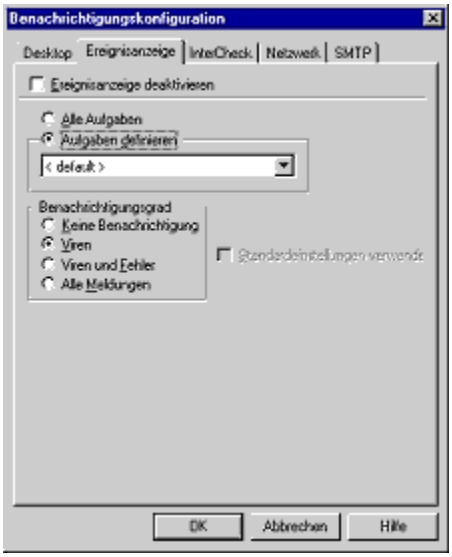
Zurück zu **Konfigurationsmenü**

Benachrichtigungen: Ereignisprotokoll

Ereignisprotokoll (nur Windows NT)

Das Ereignisprotokoll ermöglicht dem Administrator die Art der Benachrichtigung zu bestimmen, die an das Windows-NT-Ereignisprotokoll angehängt werden soll.

Diese Option kann auf jeden Auftrag zugeschnitten werden (z.B. kann die Art der Benachrichtigung für einzelne Aufträge angegeben werden).



Benachrichtigungsgrad

Zurück zu **Konfigurationsmenü**

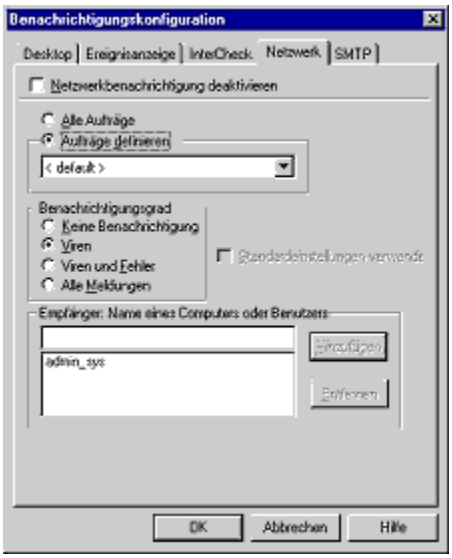
Benachrichtigungen: Benachrichtigung über das Netzwerk

Benachrichtigung über das Netzwerk (nur Windows NT)

Sophos Anti-Virus kann so konfiguriert werden, daß Meldungen über das Netzwerk an genannte Rechner oder Benutzer verschickt werden.

Diese Option kann auf jeden Auftrag zugeschnitten werden (z.B. kann die Art der Benachrichtigung für einzelne Aufträge angegeben werden).

Hinweis: Auf Rechnern unter Windows 95/98, die mit einem Windows-NT-Server vernetzt sind, muß WinPopup laufen, damit Meldungen empfangen werden können.



Benachrichtigungsgrad

Empfängercomputer oder Benutzername

Zurück zu **Konfigurationsmenü**

Empfängercomputer oder Benutzername

Auf Grund von Einschränkungen des Benachrichtigungssystems des LAN-Managers, kann nur eine Meldung pro Computername oder Benutzername verschickt werden. Selbst wenn also ein Benutzername auf mehreren Computern angemeldet ist, empfängt nur der erste Computer die Meldung.

Es ist daher empfehlenswert, statt Benutzer- Rechnernamen als Empfänger anzugeben.

Zurück zu **Benachrichtigung über das Netzwerk**

Zurück zu **Konfigurationsmenü**

Benachrichtigungen: SMTP

E-mail per SMTP

Es können E-mail-Adressen von Empfängern der Meldungen hinzugefügt oder entfernt werden. Klicken Sie auf **SMTP konfigurieren**, um den Namen des Hosts oder eine **IP-Adresse** des SMTP-Servers anzugeben.

Diese Option kann auf jeden Auftrag zugeschnitten werden (z.B. kann man angeben, welche Art der Benachrichtigung für einzelne Aufträge verwendet werden soll).

Benachrichtigungsgrad

Empfängeradressen von E-mails

SMTP konfigurieren

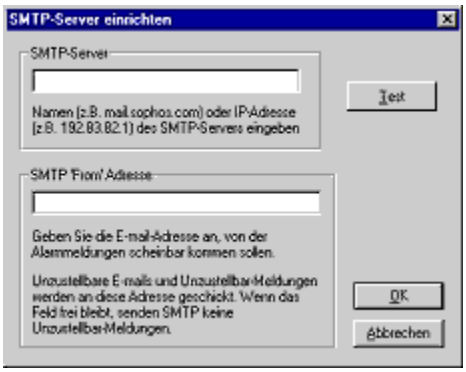
Zurück zu **Konfigurationsmenü**

Empfängeradressen von E-mails

Es können E-mail-Adressen von Empfängern der Meldungen hinzugefügt oder entfernt werden.

Zurück zu **Konfigurationsmenü**

SMTP konfigurieren



SMTP-Server

Sie können die **IP**-Adresse Ihres **SMTP**-Servers hier eingeben.

„From“-Adresse von SMTP

Geben Sie eine Adresse an, die im Absender der Benachrichtigung stehen soll. Bedenken Sie, daß Empfänger möglicherweise eine Antwort senden möchten. Die Adresse sollte also eine Mailbox sein, deren Eingangspost regelmäßig abgerufen wird.

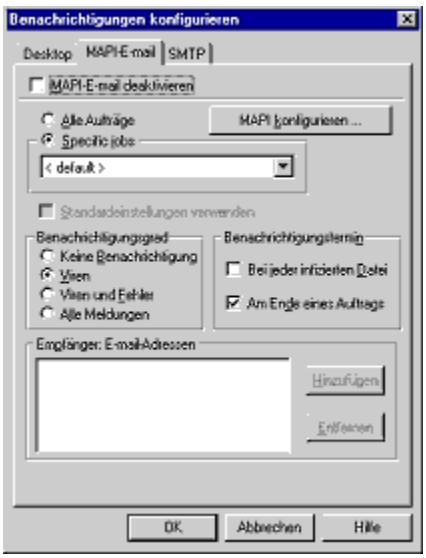
Zurück zu **E-mail per SMTP**

Zurück zu **Konfigurationsmenü**

E-mail per MAPI (nur Windows 95/98)

MAPI-E-mails erstellen, verändern, übertragen und speichern E-mail-Nachrichten.

Entdeckt Sophos Anti-Virus einen oder mehrere Viren, so können mit der Option MAPI-E-mail Benachrichtigungen verschickt werden.



Benachrichtigungsgrad

Empfängeradressen von E-mails

Zeitpunkt der Benachrichtigung

Zurück zu **Konfigurationsmenü**

Zeitpunkt der Benachrichtigung

Die Benachrichtigung kann als vollständiger Bericht am Ende jedes Auftrags verschickt werden oder als Kurznachricht, wenn eine infizierte Datei gefunden wird.

Zurück zu **E-mail per MAPI**

Zurück zu **Konfigurationsmenü**

Weitere Dialoge

Ausführbare Dateien/Programme

Diese Liste zeigt, welche ausführbaren Dateien und Programme von Sophos Anti-Virus überprüft werden, wenn laut Konfiguration nur Programme überprüft werden sollen. Die aktuelle Liste kann geändert werden.

Zurück zu **Konfigurationsmenü**

Ausnahmeliste

Hier können alle Dateien angegeben werden, die nicht von Sofortstart- oder zeitgesteuerten Aufträgen überprüft werden sollen. InterCheck wird diese Dateien ebenfalls standardmäßig ausschließen.

Um die Ausnahmelist nicht für die Einstellungen von InterCheck zu übernehmen, deaktivieren Sie das Kästchen ‘Dateiausnahmen anwenden’ im Dialog Ausnahmeliste.

Hinweis: Diese Option ist nur für den Dialog IC-Client verfügbar.

Zurück zu **Konfigurationsmenü**

Standard herstellen

Hiermit werden alle Optionen von Sophos Anti-Virus auf ihren ursprünglichen Wert nach der Installation zurückgestellt, nachdem der Benutzer dies bestätigt.

Hinweis: Dies betrifft auch alle Optionen zeitgesteuerter Aufträge.

Benutzer können mit dieser Option nur die Einstellungen von Sofortstart-Aufträgen zurückstellen. Unter Windows NT muß man über die Rechte eines Administrators verfügen, um die Standardvorgaben wiederherzustellen.

Zurück zu **Konfigurationsmenü**

Protokoll löschen

Das **Bildschirmprotokoll** erfaßt die Vorkommnisse der laufenden Überprüfung sowie die aller zeitgesteuerten Aufträge und der InterCheck-Aktivitäten (unter Windows NT) ab dem Start des Dienstes. Die Protokollmeldungen werden sowohl auf dem Bildschirm angezeigt als auch in die **Protokolldatei** geschrieben. Die Option ‘Protokoll löschen’ löscht das Bildschirmprotokoll, ohne die Protokolldatei zu beeinflussen.

Zurück zu **Konfigurationsmenü**

Prüfsummen löschen (nur Windows NT)

Es gibt zwei Arten von **Prüfsummendateien**: die zentrale Prüfsummendatei (mit Dateien, die von InterCheck-Server für die Verwendung auf Arbeitsplatzrechnern freigegeben wurden) und die lokale Prüfsummendatei (mit Dateien, die von der lokalen Installation von InterCheck freigegeben wurden).

Beide Prüfsummendateien werden mit dieser Option gelöscht.

Zurück zu **Konfigurationsmenü**

Sicherheit (nur Windows NT)

Kreuzen Sie das Kästchen ‘Sofortstart-Konfiguration obligatorisch’ an, um zu verhindern, daß Benutzer (die keine Administratoren sind) die Konfiguration ihrer Sofortstart-Aufträge ändern können.

Klicken Sie auf Konfigurieren, um die Einstellungen der benutzerdefinierten Konfiguration für Administratoren zu ändern.

Zurück zu **Konfigurationsmenü**

Statusanzeige

Die Statusanzeige veranschaulicht, wieweit die Ausführung eines Auftrags abgeschlossen ist.

Sophos Anti-Virus muß zunächst die zu prüfenden Dateien zählen, bevor die Statusanzeige korrekt angezeigt werden kann. Dies bedeutet, daß die Überprüfungszeit länger dauern kann.

Bei großen Laufwerken kann durch Deaktivierung dieser Option Zeit gespart werden. Aufträge von Sophos Anti-Virus, die bereits laufen sind hiervon nicht betroffen.

Hinweis: Die Statusanzeige für Sofortstart- und zeitgesteuerte Aufträge müssen getrennt voneinander eingestellt werden.

Zurück zu **Konfigurationsmenü**

Benachrichtigungen

Auf fünf Seiten kann gewählt werden, wie man über das Auftreten eines Virus benachrichtigt werden möchte: *Ereignisprotokoll*, Benachrichtigen über das *Netzwerk*, E-mail per *SMTP*, Benachrichtigung auf dem *Desktop* und mit dem *InterCheck*-Protokoll.

Benachrichtigung deaktivieren

Die jeweilige Benachrichtigung kann – entsprechend der gewählten Seite – abgestellt werden.

Auftrag definieren

Mit der Option ‘Alle Aufträge’ gelten alle Konfigurationen der jeweiligen Benachrichtigungsweise sowohl für Sofortstart- als auch für zeitgesteuerte Aufträge und (soweit möglich) für den InterCheck-Modus.

Mit der Option ‘Aufträge definieren’ können für Sofortstarts, jeden einzelnen, zeitgesteuerten Auftrag und die InterCheck-Modi unterschiedliche Konfigurationen der jeweiligen Benachrichtigungsweise gewählt werden. Wenn ein bestimmter Auftrag nicht explizit konfiguriert wird, wird er gemäß den Einstellungen unter <default> (Standard) ausgeführt.

Benachrichtigungsgrad

Man kann unter vier Benachrichtigungsgraden wählen:

keine Benachrichtigung; Viren; Viren und Fehler; alle Meldungen, wobei auch Informationen wie etwa die Anfangszeit eines Auftrags angezeigt werden.

Die Einstellung des Benachrichtigungsgrades beeinflußt nicht den Informationsgehalt der Berichtdatei, des Bildschirmprotokolls oder der Protokolldatei.

InterCheck-Protokoll

Benachrichtigung auf dem Desktop

Ereignisprotokoll

Benachrichtigung über das Netzwerk

E-mail per SMTP

Zurück zu **Konfigurationsmenü**

Wie verwendet man SAV?

Die Benutzeroberfläche von Sophos Anti-Virus

Die **Benutzeroberfläche** von Sophos Anti-Virus besteht aus Symbolschaltflächen, **Registerkarten** und einem Bildschirmprotokoll.

Durch Klicken auf eine der folgenden Schaltflächen werden die Erläuterungen angezeigt.



Es können bis zu fünf Registerkarten auf der Benutzeroberfläche angezeigt werden. Es handelt sich um die verschiedenen Überprüfungsmodi. Um mehr über die Registerkarten zu erfahren, klicken Sie einfach auf einen der folgenden Links:

Registerkarte Sofortstart

Registerkarte Zeitgesteuert

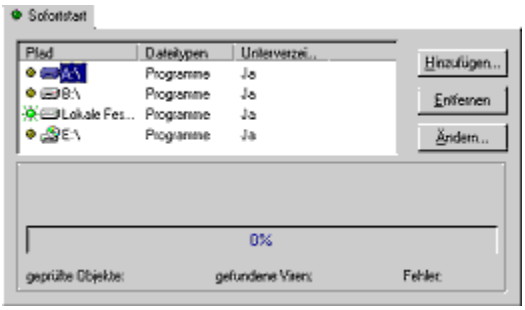
Registerkarte IC-Server (nur NT)

Registerkarte IC-Client (nur NT)

Registerkarte SAVI

Das Bildschirmprotokoll zeigt Informationen über laufende Überprüfungen sowie (wenn Sie als Administrator angemeldet sind) alle zeitgesteuerten Aufträge und die InterCheck-Protokollmeldungen ab Beginn des Dienstes.

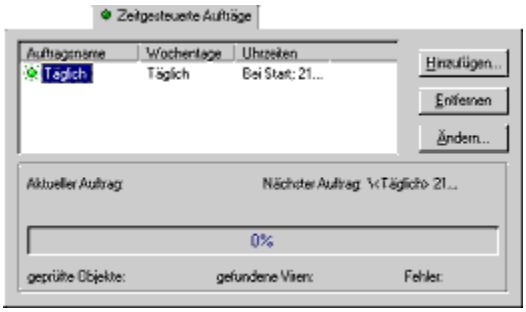
Registerkarte Sofortstart



Der Sofortstartmodus wird beim Starten angezeigt. Durch Klicken auf Hinzufügen kann man Dateien hinzufügen. Einträge der **Dateiliste** können entfernt oder geändert werden, indem man ein Objekt markiert und entsprechend auf Entfernen oder Ändern klickt. Die **Anzeigelämpchen** zeigen an, welche Dateien zur Überprüfung ausgewählt sind.

Zurück zur **Benutzeroberfläche von Sophos Anti-Virus**

Registerkarte Zeitgesteutert



Standardmäßig überprüft Sophos Anti-Virus bei jedem Systemstart auf Viren und täglich um 21.00 Uhr unter Windows NT bzw. 13.00 Uhr unter Windows 95/98.
Durch Klicken auf Hinzufügen kann ein zeitgesteuerter Auftrag hinzugefügt werden. Zeitgesteuerte Aufträge können entfernt oder geändert werden, indem man in der **Dateiliste** Einträge markiert und entsprechend auf Entfernen oder Ändern klickt. Die Anzeigelämpchen zeigen an, welche Aufträge z.Zt. für eine Prüfung ausgewählt sind.

In der Registerkarte Dateiliste kann angegeben werden, welche Dateien oder Verzeichnisse auf Viren überprüft werden sollen, in der Registerkarte Zeitplan der Termin.

Hinweis: Die Registerkarte Zeitgesteuert ist unter Windows 95/98 für Benutzer jederzeit zugänglich, ebenso für Benutzer, die als Administratoren unter Windows NT angmeldet sind.

Zurück zur **Benutzeroberfläche von Sophos Anti-Virus**

Registerkarte IC-Server (nur Windows NT)

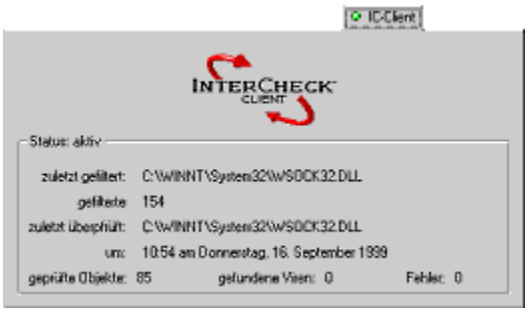
Der InterCheck-Server, eine Komponente von Sophos Anti-Virus, die normalerweise auf einem Fileserver läuft, sammelt und protokolliert Virenmeldungen von vernetzten Arbeitsplatzrechnern, auf denen Sophos Anti-Virus läuft. Der InterCheck-Server ermöglicht auch Virenüberprüfungen bei Dateizugriff für Arbeitsplatzrechner mit vernetzten InterCheck-Installationen.
Diese Registerkarte zeigt an, ob der InterCheck-Server aktiv ist und gibt Informationen über den Prüfvorgang.

Administratoren können den InterCheck-Server starten, beenden und konfigurieren.

Hinweis: Stellen Sie sicher, daß der InterCheck-Server installiert wurde.

Zurück zur **Benutzeroberfläche von Sophos Anti-Virus**

Registerkarte IC-Client (nur Windows NT)

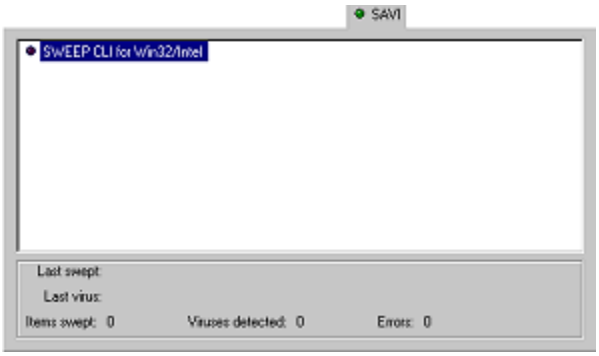


InterCheck, eine Komponente von Sophos Anti-Virus, stellt sicher, daß auf unbekannte Dateien (z.B. Programme, Dokumente, E-mail-Anlagen oder Internet-Downloads) und Laufwerke nicht zugegriffen werden kann, bis sie auf Viren überprüft wurden.
Diese Registerkarte zeigt an, ob InterCheck-Client aktiv ist und gibt Informationen über den Prüfvorgang. Administratoren können den InterCheck-Client starten, beenden und konfigurieren.

Hinweis: Stellen Sie sicher, daß der InterCheck-Client installiert wurde.

Zurück zur **Benutzeroberfläche von Sophos Anti-Virus**

Registerkarte SAVI (nur Windows NT)



Benutzt ein Administrator zu irgendeinem Zeitpunkt eine Anwendung eines Fremdanbieters, die SAVI (Sophos Anti-Virus Interface) benutzt, so wird eine weitere Registerkarte angezeigt. Diese Registerkarte listet Anwendungen auf, die SAVI verwenden und zeigt Informationen über die Laufzeit an.

Zurück zur **Benutzeroberfläche von Sophos Anti-Virus**

Sophos

Sophos Plc wurde 1980 als Elektronikgesellschaft gegründet. 1985 verlagerten sich die Aktivitäten auf den Bereich Datensicherheit und Sophos Plc ist heute ein weltweit führender Entwickler von Antiviren-Software und Software für Datensicherheit. Schlüssel zu diesem Erfolg ist das hohe Renommee für innovative und ausgereifte Produkte, die von einem kompetenten Support unterstützt werden.

Alle Produkte von Sophos werden von der Firma entwickelt, hergestellt und unterstützt und über ein weltweites Netz von Tochtergesellschaften und internationalen Vertragshändlern exportiert. Zu diesen Produkten gehören:

- Sophos Anti-Virus, bestehend aus „SWEEP“ für die Virensuche bei Bedarf und „InterCheck“ für die Virensuche bei Dateizugriff
- D-FENCE für die Freigabe und Verschlüsseln von Datenträgern
- VACCINE für die Virenerkennung durch Prüfsummen
- E-DES für die Datenverschlüsselung unter DOS und Windows

Sophos Anti-Virus

Wie erreicht man Sophos?

Sophos Anti-Virus

Sophos Anti-Virus kann:

bei Bedarf überprüfen

zeitgesteuert überprüfen

bei Dateizugriff überprüfen

automatische Berichte geben

Viren entfernen

Wie funktioniert es?

Die Virenüberprüfung von Sophos Anti-Virus besteht aus zwei Komponenten:

- SWEEP ermöglicht sofortige und zeitgesteuerte Überprüfungen aller Laufwerke, Dateien und Dokumente
- InterCheck überprüft jede Datei, sobald auf sie zugegriffen wird und ermöglicht den Zugriff nur, wenn sie virenfrei ist

---

Zurück zu **Sophos**

Wie erreicht man den technischen Support?

Auf der Webseite unter http://www.sophos.com/

finden Sie immer wieder gestellte Fragen (Frequently Asked Questions) und deren Antworten, Virenanalysen, die neuesten **IDE**-Dateien, die Möglichkeit, Programme herunterzuladen und technische Berichte.

Per E-mail unter support@sophos.com

Das Supportzentrum in England erreichen Sie unter support@sophos.com, deutschsprachigen Support erhalten Sie unter support@de.sophos.com.

Bitte geben Sie uns möglichst detaillierte Informationen, vor allem welche SWEEP und InterCheck-Version Sie verwenden (jede Version hat eine eigene Nummer), die genaue Bezeichnung des Betriebssystems, möglichst mit Patch-Stand sowie eine exakte Wiedergabe der Fehlermeldungen

Per Telefon

Das Sophos-Supportzentrum in England ist rund um die Uhr an 365 Tagen telephonisch unter +44-1235/55 99 33 für Sie erreichbar.

Deutschsprachigen Support erhalten Sie unter Tel. +49-(0)6136/91193.

Wie erreicht man Sophos?

Internet

www.sophos.com.

E-mail

Allgemeine Anfragen
enquiries@sophos.com

Vertrieb
sales@sophos.com

Technischer Support:
support@sophos.com

Telefon und Fax

Großbritannien und international:
Telefon +44 1235 559933
Fax +44 1235 559935

Australien:
Telefon +02 9212 1600
Fax +02 9212 1788

Deutschland:
Telefon 06136 91193
Fax 06136 911940

Frankreich:
Telefon 01 46 92 24 42
Fax 01 46 92 24 00

USA:
Telefon 781 213 3456
Fax 781 213 5466

Adressen

Großbritannien:	Sophos Plc The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP
Australien:	Sophos Pty Ltd Level 4 - 725 George Street, Sydney, NSW 2000
Deutschland:	Sophos GmbH Am Hahnenbusch 21, D-55268 Nieder-Olm,
Frankreich:	Sophos Plc 2, Place de la Défense BP 240, 92053 Paris la Défense,
USA:	50-S Audubon Road, Wakefiled, MA 01880

Zurück zu **Sophos**

Fehlersuche

Fehlersuche

In diesem Abschnitt finden Sie Antworten auf einige Probleme, die bei der Verwendung von Sophos Anti-Virus auftreten können.

Das Auto-Update wird nicht durchgeführt

Die aktualisierten Dateien sind nicht im zentralen Verzeichnis

Stellen Sie sicher, daß die **zentralen Updates** in das zentrale Installationsverzeichnis auf dem Fileserver kopiert werden, wo die lokalen SWEEP-Installationen nach den Updates suchen werden.

Unzureichende Rechte für das Installationsverzeichnis

Das automatische Aktualisieren nutzt den Netzwerkdienst von SWEEP für Windows NT. Dies muß als Benutzerkonto mit ausreichenden Rechten für einen Zugriff auf das zentrale Installationsverzeichnis von SWEEP registriert werden. Genauere Angaben finden Sie in Kapitel ‘Verwalten der SWEEP-Dienste’ im Handbuch Sophos Anti-Virus für Windows NT, das auf der CD unter Dokumentation enthalten ist. Im zentralen Installationsverzeichnis müssen sich auch die SETUP.EXE und WSWEEPNT.CFG befinden

Hinweis: Dieser Abschnitt betrifft nur Benutzer von Windows NT.

Zurück zu **Fehlersuche**

Falschmeldungen

SWEEP meldet gelegentlich einen Virus in einer Datei, die nicht infiziert ist. Polymorphe Viren enthalten sogar absichtlich Code, der auch dem in normalen Programmen ähnelt.

Sollten Sie einmal nicht sicher sein, wenden Sie sich bitte an den Technischen Support von Sophos.

Um die Wahrscheinlichkeit eines Fehlalarms zu verringern:

- lassen Sie nur Programmdateien überprüfen (siehe Ausführbare Dateien/Programme)
- setzen Sie die Suchintensität auf ‘normal’ statt ‘ausführlich' (siehe Suchintensität)

Zurück zur Fehlersuche

Der InterCheck-Server läuft langsam (nur Windows NT)

Eine große Anzahl von Anfragen von Arbeitsplatzrechnern verlangsamt den InterCheck-Server. Dateien, die noch überprüft werden sollen, werden im COMMS-Verzeichnis des InterCheck-Servers gespeichert.

Hinweis: Beachten Sie bitte, daß es in einem Netzwerk mehrere InterCheck-Server geben kann, und daß einige oder alle Arbeitsplatzrechner lokal mir InterCheck arbeiten können und nicht nur von einem Fileserver.

Zurück zu Fehlersuche

Neue Viren

Jede Antiviren-Software erkennt nur die Viren, die dem Hersteller zur Zeit der Programmerstellung bekannt. Sophos Anti-Virus wird jeden Monat aktualisiert, trotzdem kann in selten Fällen ein neuer Virus auftreten, der nicht gemeldet wird.

Wird ein Virus vermutet, der Sophos Anti-Virus unbekannt ist, senden Sie bitte so schnelle wie möglich eine Kopie mit einer kurzen Beschreibung an Sophos. Sollte es sich um einen Virus handeln, muß Sophos Anti-Virus unverzüglich aktualisiert werden. Wurde der Virus analysiert (was zwischen zehn Minuten und einigen Tagen dauern kann), senden wir Ihnen per Fax oder E-mail die **IDE-Datei** zu, mit der SWEEP aktualisiert werden kann. Die aktuellsten IDE-Dateien können auch von der Sophos Webseite heruntergeladen werden.

Zurück zu Fehlersuche

SWEEP läuft langsam

Ausführliche Suche

Der Geschwindigkeitsunterschied zwischen "normal" und "ausführlich" hängt von der Konfiguration des Systems ab, "normal" ist jedoch üblicherweise 5 bis 10 mal schneller als "ausführlich". Sophos Anti-Virus überprüft standardmäßig mit normaler Suchintensität.

Prüfen aller Dateien

Standardmäßig überprüft Sophos Anti-Virus nur Dateien, die als Programm definiert sind. Überprüft Sophos Anti-Virus alle Dateien untersucht, dauert dies wesentlich länger.

Ausgewählte Netzlaufwerke

Einige Netzlaufwerke sind wesentlich größer als lokale Festplatten, daher dauert das Überprüfen unter Umständen länger. Die meisten Netzwerkkarten bieten auch nur erheblich langsamere Zugriffe als es bei lokalen Laufwerken der Fall ist, wodurch die Geschwindigkeit ebenfalls stark beeinträchtigt werden kann.

Aktive Statusanzeige

Ist die Statusanzeige aktiviert, muß Sophos Anti-Virus alle zu untersuchenden Dateien durchzählen. Dieser Vorgang kann auf großen Netzlaufwerken einige Minuten dauern.

Zurück zu Fehlersuche

Virenfragmente

Die Meldung eines Virenfragments bedeutet, daß ein Bereich einer Datei mit einem Teil eines Virus übereinstimmt. Dies kann zwei Ursachen haben:

Variante eines bekannten Virus

Viele neue Viren basieren auf existierenden. Daher können Fragmente von Virencode, die typisch für einen bestimmten Virus sind, in Dateien mit einem neuen Virus enthalten sein. Wird ein Virenfragment gemeldet, ist es möglich, daß SWEEP einen neuen Virus gefunden hat, der aktiv werden könnte.

Beschädigte Viren

Viele Viren enthalten Fehler in ihren Verbreitungsmechanismen, wodurch Zieldateien manchmal nicht richtig infiziert werden. Ein Teil des Virencodes (möglicherweise ein großer Teil) kann sich in der Datei befinden, aber wegen eines Fehlers niemals aktiviert werden. In diesem Fall wird Sophos Anti-Virus eher ein ‘Virenfragment’ als einen ‘Virus’ melden. Ein beschädigter Virus kann sich nicht verbreiten.

Wird ein Virenfragment gemeldet, wenden Sie sich bitte an den Technischen Support von Sophos.

Zurück zu Fehlersuche

Ein Virus wurde nicht entfernt

Eine Meldung von Sophos Anti-Virus kann lauten, daß ein Virus nicht entfernt wurde. In diesem Falle

- überprüfen Sie, ob ‘Dokumente desinifzieren’ aktiviert ist;
- vergewissern Sie sich, sollte es sich um eine Diskette oder anderen Datenträger handeln, daß dieser nicht schreibgeschützt ist;
- stellen Sie sicher, sollte es sich um eine Datei auf einem **NTFS-Laufwerk** handeln, daß SWEEP über ausreichend Zugriffsrechte verfügt.

Hinweis: Sophos Anti-Virus entfernt keine Virenfragmente, da es keine genaue Übereinstimmung gibt.

Zurück zu Fehlersuche

Protokollmeldungen

Meldungen bei Virenfund

Ein Doppelklick auf eine Zeile mit dem Namen eines Virus zeigt weitere Informationen über diesen Virus an.

- 'Name des Virus in **Fundort** gefunden
  Es wurde keine Maßnahme durchgeführt
- 'Name des Virus in Fundort gefunden
  Datei gelöscht
- 'Name des Virus in Fundort gefunden
  Datei umbenannt in Dateiname
- 'Name des Virus in Fundort gefunden
  Datei überschrieben
- 'Name des Virus in Fundort gefunden
  Datei verschoben nach Verzeichnis
- 'Name des Virus in Fundort gefunden
  Datei kopiert nach Verzeichnis
- 'Name des Virus in Fundort gefunden
  Fehler bei Maßnahme
- 'Name des Virus in Fundort gefunden
  Virus wurde entfernt
- 'Name des Virus in Fundort gefunden
  Fehler: Entfernung des Virus fehlgeschlagen
- 'Name des Virus in **Fundort** gefunden
  InterCheck-Anfrage um Uhrzeit
  Benutzer Benutzer
  Knoten Netzwerkadresse
  Keine Maßnahme durchgeführt
- 'Name des Virus in Fundort gefunden
  InterCheck-Anfrage um Uhrzeit
  Benutzer Benutzer
  Knoten Netzwerkadresse
  Datei kopiert nach Verzeichnis
- **Quelle des Berichts** :
  Meldung
  um Uhrzeit
  Benutzer Benutzer
  Knoten Netzwerkadresse
  'Name des Virus in Fundort gefunden
  InterCheck-Anfrage um Uhrzeit
  Benutzer Benutzer
  Knoten Netzwerkadresse
  Fehler beim Kopieren nach Verzeichnis

Fehlermeldungen

- **InterCheck-Bericht:**:
  Meldung
  um Uhrzeit
  Benutzer Benutzer
  Knoten Netzwerkadresse
- **Ungültige InterCheck-Anfrage in Datei Dateiname erhalten:**
  Datei
  um Uhrzeit
  Benutzer Benutzer
- **Fehlerhafte InterCheck-Anfrage in Datei Dateiname erhalten:**
  Datei
  um Uhrzeit
  Benutzer Benutzer
- **InterCheck-Version ist neuer als diese SWEEP-Version:**
  Bitte aktualisieren Sie diese SWEEP-Version.
- **InterCheck konnte nicht gestartet werden**:
  InterCheck-Markerdatei Dateiname konnte nicht geöffnet werden
  um Uhrzeit
- **Datei Dateiname konnte nicht geöffnet werden:**
- **Datei Dateiname konnte nicht gelesen werden:**
- **Sektorgröße von Laufwerk ist zu groß:**
- **Berichtdatei Dateiname/Verzeichnis konnte nicht geöffnet werden:**
- **Protokolldatei Dateiname konnte geöffnet werden:**
  Protokolldaten werden nicht gespeichert.

Reaktion auf einen Virenalarm

Viren entfernen

Meldet Sophos Anti-Virus einen Virenfund, so gibt es folgende Möglichkeiten:

Viren automatisch entfernen

Viren manuell entfernen

Viren automatisch entfernen

In den meisten Fällen kann Sophos Anti-Virus die infizierten Dateien automatisch behandeln, vorausgesetzt, es wurde richtig konfiguriert. Weitere Informationen finden Sie unter Registerkarte Maßnahmen.

Sophos Anti-Virus kann

- bestimmte Arten von **Makroviren** aus Dokumenten entfernen
- Bootsektorviren von infizierten Disketten entfernen
- infizierte Programme und ausführbare Dateien behandeln

Zurück zu **Viren entfernen**

Viren manuell entfernen

In manchen Fällen, wenn etwa das automatische Entfernen von Viren deaktiviert oder ein Bootsektor infiziert ist, müssen Viren möglicherweise manuell entfernt werden.

Wie ein Virus manuell beseitigt werden kann hängt auch jeweils vom speziellen Virus ab, sehen Sie also bitte im Sophos-Virenlexikon nach, bevor Sie versuchen, einen Virus zu entfernen.

Bootsektor

Masterbootsektorviren auf Festplatten

Partitionsbootsektorviren auf Festplatten

Bootsektorviren auf Disketten

Programme

Viren in Programmen

Dokumente

Viren in Dokumenten

Zurück zu **Viren entfernen**

Masterbootsektorviren auf Festplatten

Ist die Festplatte mit einem Bootsektorvirus infiziert, kann Sophos Anti-Virus den Virus *nicht* automatisch entfernen. Stellen Sie sicher, daß Sie von allen wichtigen Daten der Festplatte stets Backups haben.

Starten Sie den Computer mit einer sauberen Bootdiskette. Verwenden Sie Sophos Anti-Virus für DOS/Windows 3.x, um den Virus zu entfernen, z.B. mit dem Befehl

```
SWEEP -DI
```

Oder Sie starten den Computer mit einer sauberen Bootdiskette und überprüfen, daß der Inhalt des infizierten Laufwerks sichtbar ist (z.B. mit `DIR`). Ersetzen Sie dann den Masterbootsektor mit dem Befehl

```
FDISK /MBR
```

Sollte der Inhalt der Festplatte nach einem sauberen Bootvorgang nicht sichtbar sein, wenden Sie sich bitte an den Technischen Support von Sophos. Für manche Bootsektorviren sind zusätzliche Maßnahmen erforderlich, um eine vollständige Wiederherstellung zu erreichen. Der Virus *OneHalf* beispielsweise verschlüsselt den Bootsektor so, daß er nur dann lesbar ist, wenn sich der Virus im Hauptspeicher befindet.

Zurück zu **Viren manuell entfernen**

Zurück zu **Viren entfernen**

Partitionsbootsektorviren auf Festplatten

Für infizierte Partitionsbootsektoren sind manchmal besondere Maßnahmen notwendig. Die meisten Viren sind in DOS geschrieben und gehen davon aus, daß der Rechner einen DOS-Bootsektor anstelle eines Partitionsbootsektor hat. Wenden Sie sich bitte an den Technischen Support von Sophos.

Zurück zu **Viren manuell entfernen**

Zurück zu **Viren entfernen**

Bootsektorviren auf Disketten

Starten Sie den Computer mit einer sauberen Bootdiskette und kopieren Sie alle wichtigen Daten von der infizierten Diskette in ein sauberes Zielverzeichnis (es ist sicher, Dateien zu kopieren, wenn der Computer mit einer sauberen Bootdiskette gestartet wurde). Formatieren Sie dann die Diskette neu.

Zurück zu **Viren manuell entfernen**

Zurück zu **Viren entfernen**

Viren in Programmen

Viren von infizierten Programmen und ausführbaren Dateien zu entfernen ist generell nicht empfehlenswert, da nicht sicher festgestellt werden kann, ob die Dateien nach dem Entfernen des Virus wieder vollständig repariert sind. Das Programm könnte instabil sein und ein Risiko für wertvolle Daten sein.

Starten Sie den Computer mit einer sauberen Bootdiskette neu und suchen Sie alle infizierten ausführbaren Dateien, löschen Sie sie und ersetzen Sie sie durch virenfreie Versionen von den originalen Installationsdatenträgern, von einem virenfreien Computer oder von sicheren Backups.

Zurück zu **Viren manuell entfernen**

Zurück zu **Viren entfernen**

Viren in Dokumenten

Wenn Sie Viren aus Dokumenten entfernen, müssen Sie den Computer nicht mit einer sauberen Bootdiskette neu starten.

Achtung! Stellen Sie sicher, daß die Anwendung, mit der das infizierte Dokument erstellt wurde, nicht geöffnet ist, während Sie versuchen, den Virus zu entfernen.

In manchen Fällen kann man die Makros von infizierten Dokumenten mit Hilfe der entsprechenden Anwendung manuell ändern. Einige **Makroviren** arbeiten mit Tarnungen, um zu verhindern, daß Benutzer Makros ändern können. Der Virus *Winword/ShareFun* beispielweise macht es unmöglich, Extras/Makro und Datei/Dokumentvorlage im Menü zu wählen.

Wenden Sie sich bitte an den Technischen Support von Sophos, bevor Sie versuchen, Makroviren manuell zu entfernen.

Zurück zu **Viren manuell entfernen**

Zurück zu **Viren entfernen**

Behandlung von Nebenwirkungen

Mögliche Nebenwirkungen sind vom jeweiligen Virus abhängig. Bei harmlosen Viren (*Cascade*) sind keine Wiederherstellungsmaßnahmen notwendig, während bei anderen (*Michelangelo*) die ganze Festplatte wiederhergestellt werden muß.

Manche Viren (*Winword/Wazzu*) verändern Daten nach und nach. Diese allmählichen Veränderungen sind oft sehr schwer zu entdecken und sehr unangenehm.

Sichere Backups sind das Wichtigste bei der Behandlung von Virennebenwirkungen. Originale sollten auf schreibgeschützten Datenträgern aufbewahrt werden, so daß jedes infizierte Programm leicht durch eine virenfreie Originalversion ersetzt werden.

Gelegentlich ist es möglich, Daten von durch einen Virus beschädigten Datenträger wiederherzustellen. Geeignete Hilfsprogramme erhalten Sie von Sophos. Bitte wenden Sie sich an den Technischen Support von Sophos.

Zurück zu **Viren manuell entfernen**

Zurück zu **Viren entfernen**

Prüfsummen

Ein Wert, der anhand von Daten einer Datei errechnet wird, mit denen ein Empfänger überprüfen kann, ob die Datei geändert wurden. Normalerweise sind sie 32 oder 64 Bits lang.

Benutzeroberfläche (GUI)

Graphical User Interface (GUI); das Sophos-Anti-Virus-Fenster, von wo aus man Überprüfungen bei Bedarf ausführen lassen kann.

Überschreiben

Eine sehr sicher Methode, Dateien zu löschen, indem der Inhalt der Datei überschrieben wird.

Keine Benachrichtigung

Wird dies gewählt, werden keine Mitteilungen verschickt.

Viren

Wird dies gewählt, werden nur Meldungen über Viren verschickt.

Viren und Fehler

Wird dies gewählt, werden Meldungen über Viren und Fehler verschickt.

Alle Meldungen

Wird dies gewählt, werden alle Meldungen verschickt.

UNC

Universal Naming Convention; ein Standardsystem für die Benennung von Netzlaufwerken.

STMP

Simple Mail Transport Protocol; das Zustellsystem für Internet-E-mail.

IP

Internet Protocol; ein Internetstandard, über das der Benutzer mit Internet-Anwendungen kommuniziert.

Bildschirmprotokoll

Es enthält Informationen über den momentanen Prüfvorgang. Dem Administrator stehen auch alle Meldungen seit Start des Dienstes über zeitgesteuerte Aufträge und das InterCheck-Protokoll zur Verfügung.

Protokolldatei

Sie enthält ein fortlaufendes Protokoll über alle Aktivitäten von Sophos Anti-Virus und administrative Meldungen.

Laufwerkszuordnung

Ein Netzlaufwerk ist lokal unter seiner zugeordneten Bezeichnung bekannt, z.B. kann der UNC-Verzeichnispfad \\MAIN\USERS\ auf einem bestimmten Rechner im Netzwerk dem Laufwerksbuchstaben F:\ zugeordnet sein.

Registerkarten

Auf der Benutzeroberfläche von Sophos Anti-Virus GUI werden auf Registerkarten die verschiedenen Überprüfungsfunktionen, die von SWEEP und InterCheck verwendet werden, angezeigt.

Virenüberprüfungen bei Bedarf

Der Benutzer kann auf bekannte Viren überprüfen lassen.

Zeitgesteuerte Virenüberprüfungen

Dateien werden zu bestimmten Terminen auf bekannte Viren überprüft.

Virenüberprüfungen bei Dateizugriff

Dies geschieht automatisch, um sicherzustellen, daß jede Datei auf bekannte Viren überprüft wurde, bevor auf sie zugegriffen wird.

Automatische Berichte

Es wird automatisch Alarm gegeben, wenn ein bekannter Virus oder ein Virenfragment gefunden wird.

Entfernen von Viren

Das Entfernen von Viren von bestimmten Dateien geschieht automatisch, wenn dies vom Benutzer angegeben wurde.

IDE

Diese Erweiterung wird an Dateien vergeben, die eine Virenkennung enthalten, die mit der Sophos-eigenen Virus Description Language (VDL) verschlüsselt wurden. Sie erscheint als eine ASCII-Zeichenkette.

Zentrale Updates

Die zentralen Installationsdateien werden auf einen Fileserver abgelegt, von wo aus lokale Arbeitsinstallationen automatisch aktualisiert werden können.

NTFS
NT File System; ein Dateiensystem unter Windows NT.

Symbol des Sophos-Virenlexikons

Mit einem Klicken auf dieses Symbol wird das Sophos-Virenlexikon geöffnet, das Informationen über Viren und deren Entfernung enthält.

Makros

Dies sind Anleitungen in einer Datei, mit welcher Programmbefehle automatisch ausgeführt werden. Sie haben meist Zugriff auf eine Reihe von Funktionen wie das Öffnen, Ändern und Schließen von Dateien.

GO-Symbol

Mit einem Klick auf diese Symbol werden alle ausgewählten Dateien der Dateiliste auf Viren überprüft.

STOP-Symbol

Mit einem Klick auf dieses Symbol wird eine Virenüberprüfung angehalten.

Konfigurations-Symbol

Mit einem Klick auf dieses Symbol gelangt man in den Dialog Konfigurationsoptionen.

Virenalarm-Symbol

Mit einen Klick auf dieses Symbol gelangt man in den Dialog Benachrichtigungsoptionen.

Symbol des Sophos-Virenlexikons

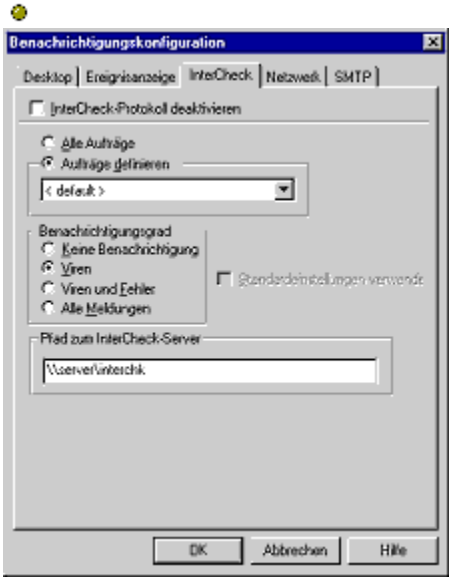
Mit einem Klick auf dieses Symbol startet man das Sophos-Virenlexikon. Wird das Symbol auf der Benutzeroberfläche nur in hellgrau angezeigt, kann das Sophos-Virenlexikon nicht gefunden werden.

Dateiliste

Sie zeigt die Laufwerk, Pfade und Dateien, die bei Bedarf auf Viren überprüft werden können. Der Inhalt der Liste kann vom Benutzer bestimmt werden.

Anzeigelämpchen

bedeutet, daß ein Objekt für eine Virenüberprüfung ausgewählt wurde.



bedeutet, daß ein Objekt nicht für eine Virenüberprüfung vorgesehen ist.

Pop-up-Meldungen des Bildschirmprotokolls über Virenfunde

Durch einen Doppelklick auf eine Zeile werden weitere Informationen über einen Virus angezeigt. Die ‘Virus gefunden’-Meldung von Sophos Anti-Virus gibt den Namen an und Informationen über getroffene Maßnahmen.

Der Fundort kann sein:
Dateiname
Laufwerk `Laufwerk`: Sektor `Sektorennummer`
Laufwerk `Laufwerk` Zylinder `Zylinder` Kopf `Kopf` Sektor `Sektor`
Arbeitsspeicherblock bei Adresse 8-stellige-Hexadezimal-Adresse

Es wird keine Maßnahme durchgeführt, wenn Sophos Anti-Virus nicht dazu konfiguriert wurde, Viren aus Bootsektoren zu entfernen oder infizierte Dateien umzubenennen, zu löschen, zu überschreiben, zu verschieben oder zu kopieren.

Die Datei, in der der Virus gefunden wurde, wurde gelöscht.

Der `Dateiname` besteht aus dem alten Namen, dessen Erweiterung durch eine Nummer ersetzt wurde. Wenn ein Virus beispielsweise VIRUS.EXE heißt, wird er in VIRUS.000 oder in VIRUS.001, wenn es eine Datei namens VIRUS.000 bereits gibt.

Die infizierte Datei wurde gelöscht und kann nicht wiederhergestellt werden.

Das `Verzeichnis` ist das, welches in der Registerkarte Maßnahmen des Konfigurationsdialogs angegeben ist.

Das `Verzeichnis` ist das, welches in der Registerkarte Maßnahmen des Konfigurationsdialogs angegeben ist.

Die Datei konnte nicht gelöscht, umbenannt, überschrieben, verschoben oder kopiert werden. Wenn die infizierte Datei auf einer Diskette gefunden wurde, überprüfen Sie, ob die Diskette schreibgeschützt ist.
`Maßnahmen` sind:

- Löschen der Datei
- Umbenennen in *Dateiname*
- Überschreiben der Datei
- Verschieben nach *Verzeichnis*
- Kopieren nach *Verzeichnis*

Achtung! Eine kopiert infizierte Datei bleibt unverändert und ist weiterhin in der Lage, andere Dateien oder Datenträger zu infizieren.

Sophos Anti-Virus kann bestimmte Bootsektorviren auf Disketten automatisch entfernen, wenn die Option ‘Bootsektoren desinfizieren’ aktiviert ist. Um Bootsektorviren von Festplatten zu entfernen, wird Sophos Anti-Virus für DOS/Windows 3.x benötigt. SWEEP kann auch bei bestimmten Makroviren die Virenmakros aus infizierten Dokumenten automatisch entfernen.

Sophos Anti-Virus konnte den Virus nicht aus dem Bootsektor entfernen. Weitere Informationen finden Sie im Handbuch.

Achtung! Der infizierte Datenträger bleibt unverändert und kann andere Dateien oder Datenträger infizieren.

Die Meldung ‘Virenfragment gefunden’ gibt den Namen und Fundort des Virenfragments an. Der *Fundort* ist:
Dateiname Dateiname
Laufwerk Laufwerk: Sektor Sektorennummer
Laufwerk Laufwerk Zylinder Zylinder Kopf Kopf Sektor Sektor

Sophos Anti-Virus entfernt keine Virenfragmente.

Die Quelle des Berichts ist entweder SWEEP oder InterCheck, je nachdem, ob der Bericht von der InterCheck-Software oder von Sophos Anti-Virus für DOS/Windows 3.x auf dem lokalen InterCheck-Arbeitsplatzrechner stammt.

Die Meldung enthält den Bericht.

Pop-up-Fehlermeldungen des Bildschirmprotokolls

Dieser Fehler wird von der InterCheck-Software gemeldet.

Der Fehler wird in der `Meldung` beschrieben.

Empfängt der InterCheck-Server eine InterCheck-Anfrage, die er nicht als solche erkennt, zeigt er eine Fehlermeldung an. Tritt dieser Fehler regelmäßig auf, ist die InterCheck-Installation eventuell grundsätzlich fehlerhaft.

Jede InterCheck-Anfrage, die vom Client an den Server übergeben wird, wird von einer Prüfsumme geschützt. Erhält der InterCheck-Server eine Anfrage mit einer falschen Prüfsumme, zeigt er diese Fehlermeldung an. Tritt der Fehler regelmäßig auf, ist die InterCheck-Installation eventuell grundsätzlich fehlerhaft.

Diese Fehlermeldung wird angezeigt, wenn der InterCheck-Server eine Anfrage von InterCheck erhält, die von einer neueren und damit nicht kompatiblen Version einer lokalen InterCheck-Installation stammt. Das Problem kann durch das Aktualisieren von SWEEP gelöst werden.

InterCheck benötigt Lese- und Schreibrechte auf das COMMS-Verzeichnis (normalerweise ein Unterverzeichnis des SWEEP-Verzeichnisses, das COMMS heißt), um mit InterCheck kommunizieren zu können.

Die Datei `Dateiname` war in der Liste der zu überprüfenden Dateien, konnte jedoch für eine nicht Überprüfung geöffnet werden. Prüfen Sie, ob die Datei bereits geöffnet oder verwendet wird.

Die Datei `Dateiname` war in der Liste der zu überprüfenden Dateien, konnte jedoch nicht gelesen werden. Dies kann ein Hinweis darauf sein, daß die Datei oder der Datenträger fehlerhaft ist.

SWEEP kann zur Zeit nur Sektoren mit einer Größe von bis zu 2 Kb überprüfen. Es ist sehr unwahrscheinlich, daß jemals größere Sektoren zu überprüfen sind.

SWEEP braucht für den Bericht freien Hauptspeicher, wenn er an die Benutzer auf der Mitteilungsliste verschickt werden soll. Ist der Bericht zu lang, kann SWEEP ihn nicht in den Speicher laden, um ihn zu versenden. Die Berichtdatei kann sehr lang werden, wenn sie so konfiguriert ist, daß alle überprüften Dateien aufgelistet sollen.

Der Name und das Verzeichnis der Berichtdatei werden in der Registerkarte ‘Bericht’ des Konfigurationsdialogs angegeben. SWEEP kann die Berichtdatei nicht öffnen, wenn der Dateiname nicht gültig ist oder keine ausreichenden Zugriffsrechte auf das Verzeichnis bestehen. Beachten Sie bitte, daß die Berichtdatei bei sofortigen Überprüfungen unter der Benutzer-ID des momentanen GUI-Benutzers und bei zeitgesteuerten Überprüfungen unter der Benutzer-ID des Dienstes geschrieben wird.

Das Verzeichnis der Protokolldatei wird über das Menü Datei – Protokollordner wählen bestimmt. SWEEP kann die Protokolldatei nicht öffnen, wenn keine ausreichenden Zugriffsrechte auf das Verzeichnis bestehen. Beachten Sie bitte, daß unter Windows NT die Protokolldatei unter der Benutzer-ID des Dienstes und nicht der des GUI-Benutzers geschrieben wird.

Was ist InterCheck?

InterCheck

InterCheck, eine Komponente von Sophos Anti-Virus, stellt sicher, daß auf unbekannte Dateien (z.B. Programme, Dokumente, E-mail-Anlagen oder Internet-Downloads) und Datenträger vor einer Virenüberprüfung nicht zugegriffen werden kann.

Die Freigabe von Dateien durch InterCheck erfolgt in zwei Vorgängen:

Überwachung aller Zugriffe auf Dateien und Datenträger

Sobald auf eine Datei zugegriffen wird, gleicht InterCheck sie mit einer Liste freigegebener Dateien ab. Wird die eine passende Datei gefunden, wird der Zugriff gewährt, wenn nicht, wird die Datei auf Viren überprüft.

Überprüfung unbekannter Dateien

Kann InterCheck eine Datei nicht erkennen, wird sie zur Überprüfung übergeben. Ist die Datei virenfrei, wird sie in die Liste der freigegebenen Dateien aufgenommen (Prüfsummendatei) und der Zugriff wird gewährt. Danach wird der Zugriff auf diese Datei sofort gewährt, es sei denn sie wurde geändert. Wird jedoch ein Virus gefunden, verhindert InterCheck den Zugriff, so daß der Arbeitsplatzrechner nicht infiziert werden kann.

Lokale und vernetzte InterCheck-Installationen

Lokale und vernetzte InterCheck-Installationen

Es gibt zwei Arten von InterCheck-Installationen:

Lokaler InterCheck

Ein lokaler InterCheck läßt alle Dateien auf einem lokalen Rechner überprüfen. Er ermöglicht eine schnelle Freigabe und kann auf Rechner verwendet werden, die nicht ständig an das Netzwerk angeschlossen sind.

Lokale InterChecks ist für Arbeitsplatzrechner unter Windows NT, Windows 95/98, Windows für Workgroups und DOS/Windows 3.x erhältlich.

Vernetzter InterCheck

Ein vernetzter InterCheck übergibt alle unbekannten Dateien zur Virenüberprüfung an den InterCheck-Server auf einem Netzwerkrechner. Er ist leicht zu verwalten und benötigt nur geringe Kapazität auf dem Arbeitsplatzrechner.

Vernetzte InterChecks sind für Arbeitsplatzrechner unter Windows 95/98, DOS/Windows 3.x und Macintosh erhältlich.

Unter dem entsprechenden Link finden Sie mehr über die von Ihnen benötigte InterCheck-Installation:

InterCheck für Arbeitsplatzrechner unter Windows NT

InterCheck für Arbeitsplatzrechner unter Windows 95/98

InterCheck für Nicht-NT-Arbeitsplatzrechner in einem NT-Netzwerk

---

Zurück zu **InterCheck**

InterCheck für Arbeitsplatzrechner unter Windows NT

InterCheck für Windows NT (der Windows-NT-IC-Client) ist Teil der Software Sophos Anti-Virus für Windows NT und überprüft lokal bei Dateizugriff auf Viren.

Start von InterCheck

InterCheck für Windows NT startet automatisch bei jedem Start von Windows NT, noch bevor die Netzwerkverbindungen erstellt werden.

Der Benutzer muß während eines normalen Arbeitsprozesses von InterCheck keine Eingaben machen. Es werden keine Meldungen ‘Requesting authorisation’ angezeigt

---

Zurück zu **Lokale und vernetzte InterCheck-Installationen**

Zurück zu **InterCheck**

InterCheck für Nicht-Windows-NT-Arbeitsplatzrechner in einem Windows-NT-Netzwerk

Sophos Anti-Virus für Windows NT ermöglicht zentrale Überprüfungen auf Viren bei Dateizugriff für Nicht-NT-Arbeitsplatzrechner, die mit einem Windows-NT-Server verbunden sind.

Vergewissern Sie sich, daß der InterCheck-Server installiert ist und die Arbeitsplatzrechner für Lokale und vernetzte InterCheck-Installationen von einem Fileserver konfiguriert sind.

Hinweis: Viele Plattformen arbeiten mit lokalen InterCheck-Installationen. Für nähere Informationen wenden Sie sich bitte an Sophos.

Zurück zu **Lokale und vernetzte InterCheck-Installationen**

Zurück zu **InterCheck**

InterCheck für Arbeitsplatzrechner unter Windows 95/98

InterCheck für Windows 95/98 ist Teil der Software von Sophos Anti-Virus für Windows 95/98 und überprüft lokal auf Viren.

Hinweis: Arbeitsplatzrechner unter Windows 95/98 in einem Netzwerk können, soweit gewünscht, mit einem vernetzten InterCheck arbeiten. Weitere Informationen finden Sie im *InterCheck Advanced User Guide* (englisch) auf der Sophos-Anti-Virus-CD.

Start von InterCheck

InterCheck startet automatisch bei jedem Start von Windows 95/98, noch bevor die Netzwerkverbindungen erstellt werden. Der Benutzer muß während eines normalen Arbeitsprozesses von InterCheck keine Eingaben machen.

Back to **Local and networked installations of InterCheck**

Zurück zu **InterCheck**

InterCheck-Server

InterCheck-Server

Der InterCheck-Server, eine Komponente von Sophos Anti-Virus, die normalerweise auf einem Fileserver läuft, sammelt und protokolliert Virenmeldungen von vernetzten Arbeitsplatzrechnern, auf denen Sophos Anti-Virus läuft.

Der InterCheck-Server ermöglicht auch Virenüberprüfungen bei Dateizugriff für jene Arbeitsplatzrechner mit vernetzten InterCheck-Installationen.

Der Administrator kann wählen, in welchem Umfang Informationen für das Protokoll von den Arbeitsplatzrechnern an das COMMS-Verzeichnis geschickt werden.

BENUTZEN: Was?

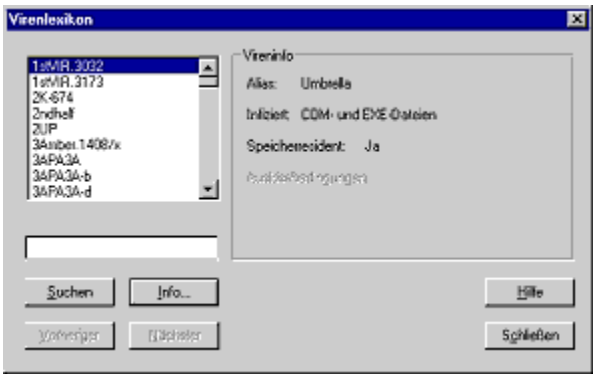
Was ist das Sophos-Virenlexikon?

Im Virenlexikon findet man die Bezeichnung und die wichtigsten Informationen über Viren, u.a. eine Beschreibung, ob es weitere Bezeichnungen für einen Virus, einen sogenannten Alias gibt, Auslösebedingungen, welche Dateien bedroht sind und ob SWEEP den Virus aus den infizierten Dateien entfernen kann.

Suche nach einem bekannten Virus
Suche nach einem unbekannten Virus
Warum kann man einen bestimmten Virus nicht finden?
Wie kann man die Suche eingrenzen oder erweitern?

BENUTZEN: Wie?

Wie sucht man nach einem bekannten Virus?



Suche nach einen bekannten Virus

Um Informationen über einen bekannten Virus zu finden, geben Sie den Namen den Virus (oder die ersten Buchstaben des Namen) im Textfeld ein. In der Liste wird der erste Namen markiert (alphabetisch geordnet), der Ihrer Eingabe entspricht. Ist der markierte Virus nicht der von Ihnen gesuchte, können Sie *Vorheriger* und *Nächster* nach dem Virus suchen — eventuell beginnen mehrere Viren mit den eingegebenen Buchstaben.

Achtung! Manchmal wird Virenbezeichnungen ein Präfix vorangestellt. Vergewissern Sie sich, daß Sie auf *Nächster* klicken, bis das Virenlexikon den Namen eines bestimmten Virus (z.B. befindet sich der Virus Melissa unter WM97/Melissa, da er Word-97-Dokumente infiziert).

Wurde der gesuchte Virus gefunden, vergewissern Sie sich, daß er markiert ist. Im Feld *Vireninfo* findet man die wichtigsten Informationen über den Virus. Detailliertere Auskunft über den Virus erhält man, indem man auf *Info…* klickt oder auf den Namen des Virus doppelklickt.

Zurück zum **Hauptmenü**

Wie sucht man nach einem unbekannten Virus?

Suche nach einem unbekannten Virus

Ist ein Virus unbekannt, klicken Sie auf *Suchen*, womit Sie in den Dialog *Suchkriterien* gelangen.

Hier können Sie Buchstaben, von denen Sie wissen, daß sie im Namen vorkommen eingeben, angeben, welche Arten von Objekten der Virus infiziert, ob er speicherresident ist, ob SWEEP ihn entfernen kann, Ihnen bekannte Auslösebedingungen nennen oder den Virus beschreiben. Es muß nicht alles ausgefüllt werden.

Nachdem alle wichtigen Informationen eingegeben wurden, klicken Sie auf *Suche starten*. In der Liste wird der erste Namen markiert (alphabetisch geordnet), der Ihrer Eingabe entspricht. Ist der markierte Virus nicht der von Ihnen gesuchte, können Sie *Vorheriger* und *Nächster* nach dem Virus suchen — eventuell beginnen mehrere Viren mit den eingegebenen Buchstaben.

Achtung! Manchmal wird Virenbezeichnungen ein Präfix vorangestellt. Vergewissern Sie sich, daß Sie auf *Nächster* klicken, bis das Virenlexikon den Namen eines bestimmten Virus (z.B. befindet sich der Virus Melissa unter WM97/Melissa, da er Word-97-Dokumente infiziert).

War die Suche nicht erfolgreich, gehen Sie zum Dialog *Suchkriterien* zurück und variieren Sie Ihre Kriterien.

Wurde der gesuchte Virus gefunden, vergewissern Sie sich, daß er markiert ist. Im Feld *Vireninfo* findet man die wichtigsten Informationen über den Virus. Detailliertere Auskunft über den Virus erhält man, indem man auf *Info…* klickt oder auf den Namen des Virus doppelklickt.

Zurück zum **Hauptmenü**

Wie kann man die Suche eingrenzen oder erweitern?

Eine Suche eingrenzen

Entsprechen zu viele Virenbezeichnungen den eingegebenen Anfangsbuchstaben, klicken Sie auf *Suchen*, um den Dialog *Suchkriterien* zu öffnen. Gibt man weitere Informationen ein, kann die Suche ähnliche Namen ausschließen, die nicht den korrekten Kriterien entsprechen.

Suche nach unbekanntem Virus

Eine Suche erweitern

Konnte mit der Suche ein bestimmter Virus nicht gefunden werden, ändern Sie die Spezifikationen der Suche, indem Sie bestimmte Kriterien weglassen. Wenn Sie den Namen des Virus nur teilweise kennen, lassen Sie alle anderen Kriterien weg und versuchen Sie eine Suche nur mit dem Ihnen bekannten Bruchteil der Bezeichnung. Danach können Sie nach und nach weitere Kriterien hinzufügen.

Sollten Sie sicher sein, daß ein Ihnen bekannter Virus nicht in der Liste zu finden ist, wenden Sie sich bitte an den technischen Support von Sophos.

Telefon +44 1235 559933
Fax +44 1235 559935

E-mail support@sophos.com

Zurück zum **Hauptmenü**

BENUTZEN: Warum?

Warum kann man einen bestimmten Virus nicht finden?

Möglicherweise ist die Suche nach dem Namen des Virus zu eng oder zu weit angelegt. Weiter Informationen finden Sie unter Wie kann man die Suche eingrenzen oder erweitern?.

Sollten Sie sicher sein, daß ein Ihnen bekannter Virus nicht in der Liste zu finden ist, wenden Sie sich bitte an den technischen Support von Sophos.

Telefon +44 1235 559933
Fax +44 1235 559935

E-mail support@sophos.com

Zurück zum **Hauptmenü**

Glossar

In diesem Abschnitt finden Sie Links zum Glossar von Sophos Anti-Virus.

Glossar A - H

Bootsektor:	Teil des Betriebssystems, das zuerst von der Festplatte in den Hauptspeicher eingelesen wird, wenn der PC gestartet wird. Das Programm, das im Bootsektor gespeichert ist, wird dann ausgeführt, woraufhin der Rest des Betriebssystems von den Systemdateien der Festplatte in den Hauptspeicher geladen wird.
Bootsektorviren:	Computerviren, die die Initialisierung des Bootvorgangs unterwandern. Bootsektorviren greifen entweder den Masterbootsektor oder den DOS-Bootsektor an.
Booten:	siehe Starten.
Datenkompression:	Verkleinern einer Datei, indem man ihre Bitstruktur in eine kürzere Form umwandelt.
DOS:	Disk Operating System; siehe MS-DOS.
DOS-Bootsektor:	Der Bootsektor, der DOS in den Arbeitsspeicher des PC lädt und die Ausführung veranlaßt; häufiges Angriffsziel von Bootsektorviren.

Zurück zu **Glossar**

Glossar I - P

IDE:	Erweiterung einer Datei, die eine Virenkennung in der Sophos-eigenen Sprache Virus Description Language (VDL) enthält, die als ASCII-Zeichenkette erscheint.
InterCheck:	Sophos-eigene Technologie, mit der sichergestellt wird, daß auf unbekannte Dateien und Laufwerke erst zugegriffen werden kann, nachdem sie auf Viren überprüft wurden.
InterCheck-Server:	Komponente von InterCheck, die zentrale Protokolle, Berichte und Updates sowie auf bestimmten vernetzten Arbeitsplatzrechnern Virenüberprüfungen bei Dateizugriff ermöglicht.
IP-Adresse:	Numerische Internet-Adresse; eine 32-Bit Binärzahl, z.B. '194.82.145.1'.
Komprimierte Dateien:	siehe Datenkompression.
Makroviren:	Viren, die Makros in Dateien benutzt, um im Speicher aktiv zu werden und die sich an andere Dateien anhängen. Im Gegensatz zu herkömmlichen Viren können Makroviren relativ leicht, mit wenig Spezialwissen, geschrieben werden. Sie sind häufig bis zu einem gewissen Grad plattformunabhängig.
Masterbootsektor:	Der erste Bereich einer Festplatte (Sektor 1, Kopf 0, Spur 0), der beim Starten des PCs geladen und ausgeführt wird. Er enthält die Partitionstabelle sowie den Code, um den Bootsektor der 'aktiven' Partition zu laden und auszuführen. Er ist ein häufiges Angriffsziel von Bootsektorviren.
MS-DOS:	Betriebssystem von Microsoft; es ist das weltweit gebräuchlichste Betriebssystems für Mikrocomputer und lauft auf dem IBM PC.
Mehrteilige Viren:	Viren, die Bootsektoren und ausführbare Dateien infizieren und somit Charakteristika von Bootsektorviren und parasitären Viren aufweisen.
NTFS:	NT File System; ein Dateiensystem von Windows NT.
Polymorphe Viren:	Sich ständig verändernde, verschlüsselte Viren.
Prüfsumme:	Wert, der anhand von Daten errechnet wird und mit dem der Empfänger der Daten nachprüfen kann, ob sie verändert wurden; normalerweise ist der Wert 32 oder 64 Bit lang.

Zurück zu **Glossar**

Glossar Q - Z

SMTP: Simple Mail Transport Protocol; Zustellsystem für Internet-E-mail.

Speicherresidente Viren: Viren, die im Hauptspeicher verbleiben, nachdem sie ausgeführt wurden und unter bestimmten Voraussetzungen andere Objekte infizieren. Nicht speicherresidente Viren sind nur aktiv, während die infizierte Anwendung läuft.

Starten: Vorgang, der ausgeführt wird, wenn ein Computer angeschaltet oder neu gestartet wird, wobei das Betriebssystem von der Festplatte geladen wird.

SWEEP: Komponente von Sophos Anti-Virus, die sofortige und zeitgesteuerte Virenüberprüfungen ausführt und Viren entfernt.

Tarnviren: Viren, die ihr Vorhandensein vor dem PC-Benutzer und vor Antiviren-Programmen ‘verheimlichen’, meist indem sie Dienste abfangen.

Trojaner: Computerprogramm, dessen Ausführung zu unerwünschten Nebenwirkungen führt, die im allgemeinen überraschend für den Benutzer sind. Trojaner-Programme geben ansonsten vor, normal zu funktionieren.

TSR: Terminate and Stay Resident; Begriff, der ein MS-DOS-Programm bezeichnet, das im Hauptspeicher bleibt, nachdem es ausgeführt wurde. Ein TSR kann entweder durch eine bestimmte Tastenkombination, eine bestimmte Zeitspanne oder ein Signal von einem I/O-Port reaktiviert werden.

UNC: Universal Naming Convention; Standardsystem für die Benennung von Netzlaufwerken, das UNC-Verzeichnis \\MAIN\BENUTZER\ beipielsweise würde das BENUTZER-Verzeichnis auf dem Server MAIN beziehen.

VDL: Virus Description Language; eine Sophos-eigene Sprache, mit der Virencharakteristika algorithmisch beschrieben werde. Sie ist sehr gut für den Umgang mit polymorphen Viren geeignet.

Virenkennung: Algorithmus, der die verschiedenen Charakteristika eines Virus beschreibt und für die Erkennung von Viren verwendet wird. Sophos beschreibt Viren mit der Sophos-eigenen Virus Description Language (VDL).

Zugeordneter Pfad: Netzlaufwerk, das mit seinem lokalen Namen bezeichnet wird; das UNC-Verzeichnis \\MAIN\BENUTZER\ beipielsweise kann dem Laufwerksbuchstaben F:\ auf einem bestimmten Computer im Netzwerk zugeordnet sein.

Zurück zu **Glossar**