Viren und Windows 95

Nahezu alle Viren wurden für DOS geschrieben, die meisten arbeiten jedoch auch unter Windows 95. Windows 95 ermöglicht es Ihnen DOS Programme zu starten. Dadurch kann ein Virus, der an einem DOS Programm hängt auch gestartet werden. Auch wenn die Fähigkeit vieler DOS-basierender parasitärer Viren andere Programme zu infizieren eingeschränkt ist, besonders bei Windows 95 Programmen, funktionieren die Nebeneffekte meist weiterhin. Auch sind die meisten Bootsektorviren eher PC-Viren, als DOS Viren, sie sind daher in der Lage, unabhängig vom Betriebssystem einen PC zu infizieren. Weiterhin können Makroviren Dokumente auf allen Betriebssystemen infizieren, das von der entsprechenden Applikation unterstützt wird.

Wie kann SWEEP helfen

Computerviren enthalten oftmals Nebeneffekte, die relativ harmlose aber auch verheerende Auswirkungen zeigen können. Viren können sich weit verbreiten, bevor diese Nebeneffekte bemerkt werden, daher ist es äußerst wichtig, sie so früh wie möglich zu entdecken und vernichten. Das ist die Hauptaufgabe von SWEEP.

SWEEP für Windows 95:

- Prüft die lokalen Festplatten, Disketten und Netzwerke auf das Vorhandensein von allen Viren, die Sophos bei der SWEEP Programmerstellung bekannt sind.
- Es sieht sowohl nach Virenfragmenten (kleine feste Bestandteile der Viren, die zur Erkennung benutzt werden können) und Virenidentitäten (eine Menge bekannter Eigenschaften eines Virus) wodurch eine zuverlässige Erkennung polymorpher Viren möglich wird.
- Die einfache Erkennung polymorpher Viren durch die Verwendung von Sophos' fortschrittlicher Virenbeschreibungssprache (VDL) und einem eingebauten Codeemulator.
- Erkennt und desinfiziert Microsoft Word und Excel Makroviren.
- Wird zwölfmal im Jahr aktualisiert. Dringende Zwischenupdates können per Fax, Email oder über den Download von der Sophos Webseite erfolgen.
- Unterstützt automatisches Updaten von vernetzten PCs.
- Bietet zwei Sicherheitsstufen an, einen "Normalen Sweep", der in den Datenbereichen nach Virenidentitäten sucht, in denen sie sich normalerweise befinden, und einem "Ausführlichen Sweep", der in allen Teilen aller Dateien nach Virenfragmenten sucht.
- Bietet einen "Sofortstart" Modus, der es erlaubt bei Bedarf zu suchen, ebenso wie einen "Zeitgesteuerten Modus", der diverse zeitgesteuerte Virensuchläufe für den automatischen Ablauf anbietet.
- Kann Netzwerkmanager automatisch über Microsoft Exchange benachrichtigen, wenn ein Virus gefunden wurde.
- Enthält eine ausführliche integrierte Vireninformationsdatenbank.
- Ist eine echte 32-Bit Applikation und voll Windows 95 Kompatibel.

SWEEP ist auch für DOS/Windows, Windows NT (i386 & Alpha AXP), Novell NetWare, OpenVMS (VAX & Alpha AXP), OS/2 und Banyan VINES erhältlich.

Updaten von SWEEP

Updaten von SWEEP

Registrierte Benutzer von SWEEP bekommen die aktuelle SWEEP-Version in jeder ersten Woche eines jeden Monats. SWEEP für Windows 95's "Autoupgrade" Möglichkeit macht das Installieren diese Upgrades einfach.

Dringende SWEEP Zwischenupdates

Viren werden mit Hilfe von der Sophos' eigenen Virenbeschreibungssprache (VDL) gefunden. VDL Identitäten können für die Erkennung und die Desinfektion von Viren zu IDE (Identität) Dateien kodiert werden, die einen Satz druckbarer ASCII Zeichen enthalten. Neue Identitäten können daher per Fax, Email oder über den Download von der Sophos' Webseite (http://www.sophos.com) bezogen werden. Sichern Sie dieses VDL Update in eine ASCII Datei mit der Extension "IDE" (z.B. NEUVIRUS.IDE), und kopieren Sie diese Datei in das SWEEP-Verzeichnis. SWEEP muß angehalten und neu gestartet werden, damit die Neuerungen dann aktiv werden können.

Zentrale Verwaltung der IDE Dateien

Mit einer zentralen Installation von SWEEP mit aktivierter "Autoupgrade" Funktion, kann die IDE-Datei in das SWEEP Zielverzeichnis auf dem Datenserver kopiert werden. Die lokale Installation empfängt die neue IDE-Datei bei dem nächsten automatischen Upgrade.

IDE-Dateien und der InterCheck-Client

Eine neue IDE-Datei, die einer lokalen SWEEP für Windows 95 Installation zugefügt wird, wird vom InterCheck-Client nicht bemerkt, bis InterCheck neu gestartet wurde. Wenn InterCheck neu gestartet wird, wird die Virenprüfung beim Neustart sich so verhalten, als ob SWEEP upgedatet wurde. Die lokale Prüfsummendatei wird daher im Normalfall gelöscht. Weitere Informationen Hierzu finden Sie im Abschnitt "Was wird von InterCheck geprüft?" des Kapitels "Konfigurieren des InterCheck-Clients".

Benutzen des SWEEP Moduls

Überblick über die Bildschirmausgabe von SWEEP

Die Menü und Werkzeugleiste

Die Icons in der Werkzeugleiste bieten schnellen Zugriff auf häufig benutzte Menüoptionen.

Die Karteikarten für den Sofortstart und den zeitgesteuerten Start.

Beim Programmstart wird die Seite für den Sofortstart angezeigt. Sie enthält die Dateiliste und den Fortschrittsbalken für den Sofortstart.

Die Dateiliste zeigt die Laufwerke, Pfade und Dateien an, die auf Bedarf untersucht werden können. Eine “Aktivitätslampe“ zeigt derzeitig aktivierte Einträge an. Der Selektionsstatus eines Eintrags kann geändert werden, indem man auf den Indikator links neben dem Laufwerksicon klickt.

Der Fortschrittsbalken zeigt den Status eines aktiven Suchlaufs an. Beim zeitgesteuerten Programmlauf wird hier zusätzlich Name und Zeit des nächsten zeitgesteuerten Auftrags angezeigt.

Bildschirm Log

Wenn eine Virensuche das erstemal gestartet wird, erweitert sich die Anzeige von SWEEP um eine Mitteilungsseite auf dem Bildschirm. Diese beinhaltet Informationen über den aktuellen Virensuchlauf, ebenso, wie alle Log Nachrichten, die seit dem Programmstart aufgetreten sind.

Sofortstart Modus

Starten eines sofortigen Suchdurchlaufs

Um alle ausgewählten Laufwerke, Pfade und Dateien zu durchsuchen, müssen Sie entweder *Sweep* aus dem *Dateimenü* aktivieren, oder auf das zugehörige “START“ Schild klicken.

Jede einzelne Zeile in dem Anzeigefenster des Sofortstartmodus kann durch einen Doppelklick auf den Eintrag in der Liste einzeln aktiviert werden.

Standarddateiliste

Alle lokalen Laufwerke werden im Auswahlfenster angezeigt und sind angewählt.

Zufügen neuer Dateien oder Bereiche für den sofortigen Sweepvorgang

Um neue Dateien und Bereiche zuzufügen, müssen Sie die *Hinzufügen* Taste im Auswahlfenster des Sofortstartmodus betätigen. Jetzt wird Ihnen ein Dialogfenster angezeigt, in dem Sie neue Einträge vornehmen können.

- Pfadname
- Dateiarten
- Unterverzeichnisse

Entfernen von Dateien oder Bereichen aus dem Menüfenster

Markieren Sie den Pfadnamen, der entfernt werden soll und klicken Sie auf *Entferne*. Markiert wird ein Eintrag in der Auswahlliste, indem auf den Pfadnamen geklickt wird.

Das Editieren eines Eintrags

Um einen Eintrag in der Dateiliste zu editieren, müssen Sie den Pfadnamen in der Liste erst markieren und dann *Editieren* anklicken. Es wird ein Menü angezeigt, indem die Angaben editiert werden können. Das Menü entspricht dem oben erwähnten im Abschnitt “Zufügen neuer Dateien oder Bereiche...“.

Zeitgesteuerter Modus

Um Optionen für einen Zeitgesteuerten Programmablauf anzusehen oder zu editieren, müssen Sie die Karteikarte für den Zeitgesteuerten-Sweep anklicken.

Standardliste für den zeitgesteuerten Suchlauf

Standardmäßig ist ein zeitgesteuerter Auftrag mit dem Namen “Standard“ vorhanden. Hierbei wird der PC täglich um 13.00 Uhr nach Viren abgesucht, solange bis der Auftrag demarkiert, oder aus der Liste der Aufträge entfernt wurde.

Hinzufügen eines neuen zeitgesteuerten Auftrags

Um einen neuen zeitgesteuerten Auftrag hinzuzufügen, müssen Sie den Hinzufügen-Knopf auf der Seite für den zeitgesteuerten Modus betätigen. Sie werden dann nach einem Auftragsnamen gefragt, dann wird die Konfigurationsseite für den zeitgesteuerten Job angezeigt. Weitere Angaben zu dieser Konfigurationsseite entnehmen Sie dem Kapitel Konfigurieren von SWEEP.

Das Entfernen eines zeitgesteuerten Auftrags

Markieren Sie den entsprechenden Eintrag in der Liste und betätigen dann den Schalter *Entfernen*.

Editieren eines zeitgesteuerten Auftrags

Markieren Sie den Namen des zeitgesteuerten Auftrag und betätigen den Schalter *Editieren*. Es wird die Konfigurationsseite für den zeitgesteuerten Job angezeigt. Weitere Angaben zu dieser Konfigurationsseite entnehmen Sie dem Kapitel Konfigurieren von SWEEP.

Einzelplatz und Netzwerk Windows 95 InterCheck Clients

Es gibt zwei Arten des InterCheck Clients für Windows 95: Einzelplatz und Netzwerkmodus. Für einen Überblick über InterCheck, und die Arten von InterCheck, schauen Sie ins Kapitel Was ist InterCheck?.

Installieren von Windows 95 InterCheck Clients

Einzelplatzclients werden mit dem SWEEP Installationsprogramm installiert, Netzwerkclients werden vom Server installiert.

Benutzen der Windows 95 InterCheck Clients

Starten der InterCheck Clients

Einzelplatz Windows 95 InterCheck Clients werden jedesmal beim Start von Windows 95 mitgestartet, bevor Netzwerkverbindungen aktiviert werden.

Vernetzte Windows 95 InterCheck Clients werden vom Benutzerloginskript gestartet.

InterCheck Clients bei der Arbeit

Weder der Einzelplatz, noch der Netzwerkmodus der InterCheck Clients erwarten beim Normalen Betrieb Eingaben vom Benutzer.

InterCheck unterbricht jeden Zugriff auf Programmdateien. Dies beinhaltet auch Zugriffe eines Programms zum auspacken seines Icons, wie es der Explorer macht, wenn ein Programicon das erste Mal angezeigt wird. Hierdurch kann eine kurze Zeitverzögerung hervorgerufen werden, wenn man das Netzwerk durchsucht, und InterCheck aktiv ist.

Das umbenennen von Programmdateien wird nicht abgefangen, Dateien können in einem logischen Laufwerk umbenannt oder bewegt werden ohne geprüft zu werden.

Die Windows 95 InterCheck Clients unterbinden den Zugriff auf Disketten, die mit einem Bootsektorvirus infiziert sind.

Einzelplatz Windows 95 InterCheck Clients zeigen die Mitteilung “requesting authorisation“ nicht an, was den Prüfprozess beschleunigt.

Vernetzte Windows 95 InterCheck Clients zeigen die Mitteilung “requesting authorisation“ an, wenn sie mit einem InterCheck Server kommunizieren. Es kann vorkommen, das bis zum Anzeigen der Mitteilung eine gewisse Zeit vergeht, da Windows 95 die grafische Anzeige nicht aktualisiert, solange wichtige Systemfunktionen ausgeführt werden.

Konfigurieren des Windows 95 InterCheck Clients

Beide Clientarten werden mit der Konfigurationsdatei von InterCheck konfiguriert.

Konfigurieren von SWEEP

Über das Konfigurieren von SWEEP

Wählen Sie *Konfiguration* aus dem *Optionen* Menü oder klicken Sie auf das entsprechende Icon, um die Konfigurationsseite für den Modus aufzurufen, dessen Karteikarte sich im Vordergrund befindet.

Sofortstart und zeitgesteuerte Modi werden unabhängig voneinander konfiguriert.

Sweep Modus

- Suchintensität
- Priorität
- Komprimierte Dateien

Aktionen bei Virenfund

- Desinfiziere Bootsektoren
- Desinfiziere Dokumente
- Infizierte Dateien
- Bestätigung erforderlich

Benachrichtigung bei Virenfund

Wenn SWEEP einen oder mehrere Viren entdeckt, kann es mit Microsoft Exchange eine Benachrichtigung versenden. Wenn Microsoft Exchange nicht installiert ist, ist diese Option nicht verfügbar.

- Benachrichtigungszeitpunkt
- Mitteilungsliste

Erstellen eines Ereignisreports

Die Reportdatei enthält Informationen über individuelle Sofortstart, oder zeitgesteuerte Aufträge. Sie wird zusätzlich zu der fortgesetzten Log-Datei erzeugt.

- Reporteinstellungen
- Name der Reportdatei

Dateiliste (nur bei zeitgesteuerten Aufträgen)

Die Dateiliste für den zeitgesteuerten Auftrag entspricht der Dateiliste für den Sofortstartmodus, gibt aber die Dateien und Bereiche an, die im zeitgesteuerten Auftrag geprüft werden sollen. Die Standardliste für den zeitgesteuerten Modus ist identisch mit der Liste für den Sofortstartmodus. Ausnahme ist, daß lokale Diskettenlaufwerke nicht gelistet sind.

Zeiten (nur bei zeitgesteuerten Aufträgen)

SWEEP kann so konfigurierte werden, daß es zu bestimmten Zeiten an bestimmten Tagen, z.B. einmal am Tag an Wochentagen und zweimal täglich am Wochenende, automatisch startet.

Das Virenlexikon

Starten des Virenlexikons

Wählen Sie *Virenlexikon* aus dem Menü *Betrachten*, oder klicken Sie auf das entsprechende Icon, um das eingebaute Virenlexikon zu starten.

Informationen über einen bestimmten Virus

Informationen über einen hervorgehobenen Virus kann angezeigt werden, indem Sie auf *Info* gehen, oder einfach ein Doppelklick auf dem Namen durchführen. Die Informationen beinhalten Hilfen für das Desinfizieren.

Suche nach einem bestimmten Virus

Das Virenlexikon kann nach Viren mit bestimmten Charakteristischen Merkmalen durchsucht werden. Um das Suchkriterium anzugeben gehen Sie auf den Schalter *Finde...* .

- Infizierte Objekte
- Speicherresident
- Desinfizierbar mit SWEEP
- Auslösebedingungen
- Text in Beschreibung

Nach der Suche können Sie mit den Schaltern *Vorheriger* und *Nächster* zwischen den einzelnen Einträgen, die mit der Suchbestimmung übereinstimmen wechseln.

SWEEP Optionen

SWEEP Kommandozeilenoptionen

-AUTO Autostart und Stop

Starten Sie SWEEP für Windows 95 an der Kommandozeile auf die folgende Weise

```
SWEEP95 -AUTO
```

Hierdurch wird SWEEP dazu gebracht, einen Sofortsuchvorgang zu starten, bei dem alle Benutzereingaben, Halte und Entladeoptionen abgeschaltet sind. Wenn keine Viren oder Fehler entdeckt werden, wird SWEEP am Ende des Suchvorgangs wieder entladen. Wenn Viren oder Fehler aufgetreten sind, wird SWEEP seine üblichen Mitteilungen anzeigen und alle Kontrollen reaktivieren.

-I Autostart

Die Kommandozeilenoption -I bringt SWEEP dazu einen Sofortsuchvorgang durchzuführen, sobald es geladen ist. Benutzereingaben sind nicht deaktiviert, und SWEEP wird sich am Ende des Suchvorgangs nicht automatisch entladen.

SWEEP kann dazu gebracht werden, zusammen mit Windows 95 zu starten, wenn es in die Autostartgruppe von Windows 95 eingetragen wird.

-NI ohne Unterbrechung

Unterbindet alle Optionen, die SWEEP beenden könnten. Der STOP Schalter und alle internen Entlademechanismen sind deaktiviert. In Kombination mit der Option -I , sind alle diese Optionen bis zu Beenden des Sofortsuchvorgangs deaktiviert, danach werden die Optionen reaktiviert.

-NM keine Speicherdurchsuchung

Die Kommandozeilenoption -NM unterbindet die Durchsuchung des Speichers, beim Start von SWEEP.

-NW keine Warnmitteilungen

Die Kommandozeilenoption -NW unterdrückt beim Starten von SWEEP alle Warnnachrichten. Diese Option wird verwendet, wenn SWEEP für den automatischen Start konfiguriert wurde.

Speicherprüfung

SWEEP prüft den Speicher automatisch auf das Vorhandensein speicherresidenter Viren, wenn es zum ersten Mal gestartet ist. Der Speicher kann auch zu anderen Zeiten geprüft werden, indem im Dateimenü die Speicherprüfung aktiviert wird.

Setzen des Logverzeichnisses

SWEEP erstellt eine Log-Datei über alle seine Aktivitäten. Diese Datei enthält administrative Mitteilungen, zusammen mit den Nachrichten, die unter Virenmitteilungen und Fehlermeldungen beschrieben sind. Mit der Option *Protokollordner wählen* aus dem *Datei* Menü kann das Zielverzeichnis der Log-Datei angegeben werden.

Standardmäßig wird die Datei im Wurzelverzeichnis der ersten Festplatte angelegt, dies kann aber im Menü *Protokollordner wählen* aus dem *Dateimenü* geändert werden.

Dateierweiterungen

Die Liste der Dateiendungen, die von SWEEP als ausführbar angesehen werden kann mit dieser Option editiert werden. Diese Liste wird nur verwendet, wenn SWEEP konfiguriert wurde “Ausführbare Dateien“ und nicht “alle Dateien“ zu durchsuchen.

Ausnahmeliste

Die Ausnahmeliste enthält spezielle Dateien, die von allen SWEEP-Vorgängen ausgeschlossen werden sollen.

Benachrichtigungsprofil

Diese Option ist nur verfügbar, wenn Microsoft Exchange installiert ist.

Um Benachrichtigungen zu verschicken, muß SWEEP in der Lage sein sich in Microsoft Exchange einloggen zu können, ohne ein Paßwort angeben zu müssen. Wenn Ihr Standardprofil ein Paßwort erfordert, dann erstellen Sie ein neues Profil mit einem vordefinierten Paßwort und benutzen dann diese Option um es auszuwählen.

Grundeinstellung herstellen

Diese Option setzt, nachdem sie noch einmal nachgefragt hat, alle SWEEP Optionen auf die Standardwerte zurück. Dies wird alle zeitgesteuerten Aufträge löschen, und alle anderen Optionen werden zurückgesetzt.

Protokoll löschen

Der Bildschirm-Log bietet eine Aufzeichnung aller Aktivitäten, der augenblicklichen Sitzung und stellt die Informationen dar, die an die kontinuierliche Log-Datei angehängt werden. Diese Option löscht die Bildschirmanzeige, hat aber keinen Einfluß auf die Log-Datei auf der Festplatte.

Fortschrittsbalken

Um den Fortschrittsbalken anzeigen zu können, muß SWEEP alle zu prüfenden Daten vor der Virensuche durchzählen. Auf großen Netzwerklaufwerken kann das einen gewissen Zeitraum dauern, um dies zu vermeiden, kann man diese Option abschalten. Diese Optionseinstellung hat keinen Einfluß auf Suchvorgänge, die schon gestartet sind.

Behandeln von Vireninfektionen

Das Erzeugen einer sauberen Umgebung für die Desinfektion

Ein Virus kann aus dem Speicher eines infizierten PC's entfernt werden, indem er ausgeschaltet und von einer nicht infizierten (und vorzugsweise schreibgeschützten) Systemdiskette gebootet wird. Diesen Vorgang bezeichnet man als sicheres oder sauberes Booten. Er ist unbedingt notwendig, um eine saubere Umgebung zu schaffen, von der aus der Desinfektionsprozeß gestartet werden kann.

Vorausgesetzt, der Speicher ist virenfrei, ist es am sichersten, infizierte Dateien, wie unten beschrieben zu bewegen, oder zu kopieren.

Infizierte Disketten

Wenn ein Virus auf einer Diskette gefunden wurde, die gerade erst eingetroffen ist, dann können Sie recht einfach damit umgehen.

Infizierte Dateien und Dokumente können automatisch umbenannt, gelöscht, überschrieben, bewegt oder kopiert werden, wenn die jeweilige Option in der Konfigurationseinstellung aktiviert ist.

Disketten, die mit einem Bootsektorvirus infiziert sind, können normalerweise automatisch von SWEEP desinfiziert werden. Wenn SWEEP den Virus trotzdem nicht entfernt, können Sie die Daten problemlos auf die Festplatte sichern und die Diskette dann neu formatieren. Das Formatieren der Diskette zerstört alle Daten auf dem Medium inklusive aller Viren.

Die Quelle der infizierten Diskette sollte dann ausfindig gemacht werden, und alle anderen infizierten Disketten ebenso.

Wichtig! Wenn auch nur eine infizierte Diskette nicht entdeckt wird, können andere Disketten und PC's sich schnell wieder infiziere

Bemerkung: Es ist empfehlenswert eine deutlich markierte infizierte Diskette zur Analyse und Beweissicherung zu behalten

Infizierte Festplatten

Wenn SWEEP einen Virus auf der Festplatte entdeckt, so ist es wahrscheinlich, daß die Infektion schon weit verbreitet ist, und möglicherweise ein größerer Aufwand betrieben werden muß, um die Virenattacke abzuwehren. Der erste Schritt ist es, alle infizierten PC's und Laufwerke ausfindig zu machen.

Als nächstes geht es darum, den Virus daran zu hindern, sich zu verbreiten. Infizierte PC's sollten vom Netzwerk getrennt werden und jeglicher Diskettentausch zwischen den Rechnern sollte unterbunden werden.

Nachdem der Virenausbruch eingedämmt ist, kann der Wiederherstellungsprozeß beginnen. Der Virus muß wie oben beschrieben von allen infizierten Disketten entfernt werden, ebenso wie von allen infizierten Festplatten.

Wenn nur Dateien auf der Festplatte infiziert sind, kann wie oben beschrieben vorgegangen werden.

Wenn aber der Bootsektor der Festplatte infiziert ist, dann wird SWEEP für Windows 95 ihn nicht desinfizieren. Sie sollten nach einem sauberen Bootvorgang hierfür die DOS Version von SWEEP benutzen. Schauen Sie für weitere Informationen ins DOS SWEEP Benutzerhandbuch, oder wenden Sie sich an unseren technischen Support.

Nach der Desinfektion

Da sind eine Menge anderer Dinge, die es wert sind, während einer Virenbeseitigung im Kopf zu haben:

- Finden und schließen Sie Schlupflöcher, durch die ein Virus bei Ihnen eindringen kann.
- Informieren Sie jeden möglichen Empfänger infizierter Disketten außerhalb Ihrer Firma darüber, daß Sie möglicherweise von einem Virus betroffen sind.
- In England, informieren Sie die *Computer Crime Unit* von *New Scotland Yard* in London über die Attacke (Tel 0171 230 1177, Fax 0171 230 1275).

Fehlersuche

SWEEP läuft langsam

Ausführlicher Sweep

Standardmäßig untersucht SWEEP nur die Bereiche in Dateien, die üblicherweise Viren enthalten (Normaler Sweep). Der “ausführliche“ Sweep ist um einiges langsamer. Der Geschwindigkeitsunterschied zwischen dem “ausführlichen“ und dem “normalen“ Sweep hängt von der Konfiguration Ihres Rechners ab. Üblicherweise ist der “normale“ Modus 5 bis 10 mal schneller als der “ausführliche“ Modus.

Untersuchen aller Dateien oder Sektoren

Standardmäßig untersucht SWEEP nur Dateien, die als ausführbar definiert sind. Wenn SWEEP *alle Dateien prüft braucht er daher länger, als wenn er nur ausführbare Dateien absucht*.

Netzwerklaufwerke

Einige Netzwerklaufwerke können wesentlich größer als lokale Festplatten sein, daher kann es wesentlich länger dauern sie zu prüfen. Die meisten Netzwerkkarten bieten nur wesentlich langsamere Zugriffszeiten als die lokale Festplatte, hierdurch kann die Geschwindigkeit zusätzlich beeinträchtigt werden.

Aktivierter Fortschrittsbalken

Wenn der Fortschrittsbalken angewählt ist, muß SWEEP vor der Virensuche alle Dateien durchzählen, die geprüft werden sollen. Dies kann auf großen Netzwerklaufwerken einige Minuten dauern.

Virenfragmente

Wird ein Virenfragment gefunden heißt das, daß ein Teil einer Datei mit einem Teil eines Virus übereinstimmt. Hierfür gibt es drei mögliche Ursachen:

Variante eines bekannten Virus

Obwohl neue Viren jederzeit auftreten können, so basieren doch viele von ihnen auf existierenden Viren, daher können typische Fragmente eines bekannten Virus in Dateien gefunden werden, die mit einem neuen Virus infiziert sind. SWEEP bietet hier durch seine Suche nach Virenfragmenten einen guten Schutz. Näheres entnehmen Sie dem Abschnitt Neue Viren.

Defekte Viren

Viele Viren enthalten in ihren Vermehrungsroutinen Fehler, so daß sie manchmal Zieldateien nicht korrekt infizieren. Ein Teil des Virenkörpers (möglicherweise ein entscheidender Teil) könnte sich in der Empfangsdatei befinden, aber möglicherweise in einem Bereich, in dem er nie aktiviert wird. In diesem Fall wird SWEEP ein “Virenfragment“ statt eines “Virus“ anzeigen. Ein defekter Virus kann sich nicht verbreiten.

Wenn eine Datei einen defekten Virus enthält, entfernen Sie die infizierte Datei und ersetzen sie durch eine saubere Kopie.

Falsche Virenmeldungen

Unter seltenen Umständen kann es passieren, daß in einer uninfizierten Datei ein Virus angezeigt wird. Dies kann durch verschiedene Umstände verursacht werden. Auslagerungsdateien können z.B. auf Computern die vor kurzem virenbehaftete Dateien enthielten Fragmente echter Viren enthalten.

Wenn Sie sich nicht sicher sind, kontaktiere Sie einfach den technischen Support für weitere Hilfe, oder senden Sie uns Beispiele. Es könnte ja auch ein neuer Virus sein.

Um die Wahrscheinlichkeit falscher Virenmeldungen einzugrenzen:

- Untersuchen Sie nur ausführbare Dateien.
- Nehmen Sie besser den “Normalen Sweep“ statt dem “Ausführlichen Sweep“.

Nicht gemeldete Viren

Nicht gemeldete Viren sind das Gegenteil von falschen Virenmeldungen, das heißt, wenn SWEEP einen Virus in einer infizierten Datei nicht erkennt.

Wenn Sie einen nicht gemeldeten Virus vermuten:

- Stellen Sie sicher, daß Sie die aktuellste Version von SWEEP benutzen.
- Wenn Sie einen Word Makrovirus entdeckt haben, stellen Sie sicher, daß alle Dateiarten untersucht werden.

Virus wird nicht desinfiziert

Wenn ein Virus nicht desinfiziert wurde:

- Stellen Sie sicher, daß “desinfiziere Dokumente“ aktiviert ist.
- Stellen Sie sicher, daß die Diskette nicht schreibgeschützt ist.

Neue Viren

Jede spezielle Antivirensoftware entdeckt nur Viren, die dem Hersteller zur Zeit der Programmerstellung bekannt sind. Wenn ein Virus vermutet wird, der SWEEP unbekannt ist, senden Sie Sophos bitte möglichst früh ein Beispiel und eine Beschreibung der Symptome. Es besteht die Möglichkeit, daß der Virus sich verbreitet, und je eher wir den Virus in SWEEP einarbeiten können, desto besser.

Das infizierte Beispiel kann per E-Mail an support@de.sophos.com gesendet werden. Sie können es auch auf unsere ftp Seite (ftp.sophos.com) laden oder auf unsere Sicherheitsmailbox (+44 1235 559936) nachdem Sie Sophos kontaktiert haben. Wenn der Virus analysiert wurde (was zwischen 10 Minuten und einigen Tagen dauern kann), werden wir Ihnen per Fax oder E-Mail eine IDE-Datei zusenden, die SWEEP um den neuen Virus erweiert. Die aktuellsten IDE-Dateien können auch von unsere Webseite runtergeladen werden (http://www.sophos.com).

Log-Mitteilungen auf dem Bildschirm

Virus gefunden Nachrichten

Virus: '*Virenname*' gefunden in *Ort*
Infizierte Objekte wurden nicht desinfiziert

Virus: '*Virenname*' gefunden in *Ort*
Datei gelöscht

Virus: '*Virenname*' gefunden in *Ort*
Datei umbenannt in *filename*

Virus: '*Virenname*' gefunden in *Ort*
´Datei überschrieben

Virus: '*Virenname*' gefunden in *Ort*
Datei bewegt nach *neuer Ort*

Virus: '*Virenname*' gefunden in *Ort*
Datei kopiert nach *neuer Ort*

Virus: '*Virenname*' gefunden in *Ort*
Fehler aufgetreten

Virus: '*Virenname*' gefunden in *Ort*
Desinfektion erfolgreich

Virus: '*Virenname*' gefunden in *Ort*
Fehler: Desinfektion erfolglos

Virus Fragment: '*Virenname*' gefunden in *Ort*
Infizierte Objekte wurden nicht desinfiziert

Fehlermeldungen

Fehler: Kann *Dateiname* nicht öffnen

Error: Kann *Dateiname* nicht öffnen

Error: Sektorgröße von Laufwerk *Laufwerk* ist zu groß

Error: Kann Reportdatei *Dateiname/Verzeichnis* nicht öffnen

Error: Log Datei *Dateiname* konnte nicht geöffnet werden.
Log Daten werden nicht gespeichert.

Error: Kann *Benutzer* nicht benachrichtigen

Error: Kann Mailsystem nicht initialisieren

Error: Kann nicht in Mailsystem einloggen

Error: Kann Speicher für *Dateiname/Verzeichnis* nicht freigeben

Bildschirmmeldungsfenster bei Virenaufspürung

Doppelklicken auf eine Zeile mit einem Virennamen zeigt Ihnen weitere Informationen zu diesem Virus an. SWEEP's Mitteilung "Virus gefunden" enthält den Namen und den Aufenthaltsort des Virus, gefolgt von der Information, welche Aktion SWEEP durchgeführt hat. Diese Aktion hängt von den Einstellungen der Konfigurationsseite ab.

Der *Aufenthaltsort* kann sein:

Dateiname
Laufwerk *Laufwerksname*: Sektor *Sektornummer*
Laufwerk *Laufwerksname* Zylinder *Zylinder* Kopf *Kopf* Sektor *Sektor*
Speicherblock bei Adresse *8 digit Hexadezimal Adresse*

Wenn SWEEP konfiguriert wurde, Bootsektoren oder Dokumente nicht zu desinfizieren, und infizierte Dateien weder umzubenennen, zu löschen, überschreiben, bewegen oder kopieren, dann wird SWEEP keine Aktion durchführen.

Die Datei in der Virus gefunden wurde ist gelöscht worden.

Der *Dateiname* wird umgewandelt in den alten Dateinamen, wobei die Dateiendung sich in eine Nummer ändert. Wenn zum Beispiel ein Virus den Namen VIRUS.EXE hat, wird er umbenannt in VIRUS.000, oder VIRUS.001 wenn schon eine Datei mit dem Namen VIRUS.000 existiert.

Die infizierte Datei wurde gelöscht und kann nicht wieder hergestellt werden.

Der *neue Aufenthaltsort* ist in der Aktionsseite der Konfigurationsoption definiert.

Der *neue Aufenthaltsort* ist in der Aktionsseite der Konfigurationsoption definiert.

Die Datei konnte nicht gelöscht / umbenannt / überschrieben / bewegt/ kopiert werden. Wenn die infizierte Datei auf einer Diskette gefunden wurde, stellen Sie bitte sicher, daß die Diskette nicht schreibgeschützt ist.

Die *Aktion* wird eine der folgenden sein:

```
Lösche Datei
Umbenennen in Dateiname
Überschreibe Datei
Bewege nach Ort
Kopiere nach Ort
```

Wichtig! Die infizierte Datei bleibt unverändert und kann weitere Disketten und Dateien infizieren.

SWEEP für Windows 95 kann automatisch Bootsektorviren auf Disketten desinfizieren oder bewegen, wenn die Option “desinfiziere Bootsektoren“ ausgewählt wurde. SWEEP für DOS wird zum Desinfizieren von Festplattenbootsektoren benötigt. SWEEP kann automatisch virulente Makros aus Dokumenten entfernen, Die einen Makrovirus enthalten.

SWEEP ist nicht dazu in der Lage den Bootsektor zu desinfizieren. Schauen Sie für eine Anleitung zum desinfizieren von Bootsektoren im Kapitel “Behandeln von Vireninfektionen“ nach.

Wichtig! Das infizierte Laufwerk bleibt unverändert und kann weitere Laufwerke und Dateien infizieren.

Ein Doppelklick auf die Zeile mit dem Virennamen zeigt nähere Informationen über den Virus an. SWEEP’s Mitteilung “Virenfragment gefunden“ beinhaltet den Namen und den Ort des Virusfragments.

SWEEP beseitigt keine Virenfragmente.

Bildschirmmeldungsfenster bei Fehlern

Die Datei mit dem Namen *Dateiname* befindet sich in der Liste der zu untersuchenden Dateien, konnte aber für eine nähere Untersuchung nicht geöffnet werden. Prüfen Sie, ob die Datei gerade in Benutzung oder anderweitig geöffnet ist.

Die Datei mit dem Namen *Dateiname* befindet sich in der Liste der zu untersuchenden Dateien, konnte aber nicht gelesen werden. Das kann ein Hinweis darauf sein, daß die Datei oder das Laufwerk beschädigt ist.

SWEEP prüft nur Laufwerkssektoren von 2k oder weniger. Es ist extrem ungewöhnlich, daß es irgendwann auf Sektorgrößen stößt, die darüber liegen.

Der Dateiname und das Verzeichnis der Reportdatei sind unter Report auf der Konfigurationsseite angegeben. SWEEP kann die Reportdatei nicht öffnen, wenn der Dateiname ungültig ist, oder das Verzeichnis oder die Datei nicht zugreifbar sind.

Der Aufenthaltsort der Log-Datei wird mit der Option *Protokollordner wählen* des *Datei* Menüs eingestellt. SWEEP kann die Log-Datei nicht öffnen, wenn das Verzeichnis oder die Datei nicht zugreifbar sind.

Der *Benutzer* war auf der Benachrichtigungsliste, konnte aber nicht erreicht werden. Es kann sein, daß der *Benutzer* nicht mehr in der Liste der bekannten Microsoft Exchange Benutzer eingetragen ist, oder es wurde ein Profil benutzt, daß die Eingabe eines Zugangspaßwortes erfordert.

SWEEP prüft nach, ob Microsoft Exchange installiert ist, bevor es den Zugriff auf die Benachrichtigungsoptionen erlaubt. Es kann vorkommen, daß SWEEP den Zugriff erlaubt, obwohl Microsoft Mail nicht korrekt installiert ist. Zum Beispiel, wenn das MAPI Mail Interface nicht korrekt installiert ist.

Wenn SWEEP sich nicht korrekt in das Mailsystem einloggen kann, dann ist möglicherweise der Profilname nicht korrekt.

SWEEP benötigt Speicherplatz für die Reportdatei, wenn sie zu Anwendern von der Benachrichtigungsliste gesendet werden soll. Wenn der Report zu groß ist, und SWEEP nicht in der Lage ist ihn in den Speicher zu lesen, kann er nicht gesendet werden. Die Reportdatei kann sehr groß werden, wenn sie so konfiguriert ist, daß sie alle Dateien listet, die untersucht werden (sehen Sie hierzu im Abschnitt “Reportmodus“ des Kapitels “Konfiguration“).

Pop-Up Mitteilungen

Spezifiziert das Laufwerk, Verzeichnis oder Dateiname das geprüft werden soll. Es können sowohl Gemappte, als auch UNC Pfadnamen eingegeben werden. Wildcards können problemlos eingefügt werden. *Durchsuchen* kann benutzt werden, um Dateien oder Bereiche auszuwählen.

Nur Dateien, die als ausführbar gekennzeichnet sind werden geprüft, es sei denn Sie haben die Option Alle Dateien angewählt.

Wenn diese Option ausgewählt ist werden Unterverzeichnisse mit durchsucht.

Der “Normale“ Sweep untersucht nur die Bereiche von Dateien, die normalerweise Viren enthalten, der “Ausführliche“ Sweep hingegen untersucht den kompletten Inhalt jeder Datei. Der “Ausführliche“ Sweep ist sicherer, weil er Viren entdecken kann, die sich unter anderem Kode verbergen, der an eine Datei angehängt ist, ebenso wie kleinere Virusmutationen und defekte Viren. Trotzdem ist der “Ausführliche“ Sweep wesentlich langsamer und für den üblichen Bedarf ist der “Normale“ Sweep der gebräuchlichere.

Um den Einfluß von SWEEP auf die Systemperformance zu minimieren, kann es so eingestellt werden, daß es mit einer “niedrigen“ Priorität läuft. Das erhöht die Zeit, das System zu untersuchen.

SWEEP ist in der Lage in Dateien nach Viren zu suchen, die mit PKLite, LZEXE und Diet komprimiert wurden. SWEEP kann nicht in Dateien schauen, die mit statischen Kompressionsprogrammen wie ARC, ZIP und ZOO komprimiert wurden. Diese Dateien müssen vor einer Durchsuchung entpackt werden. InterCheck bietet einen automatischen Schutz vor Viren in Dateien die komprimiert sind, da der Zugriff auf alle unregistrierten Dateien (z.B. neu entpackte Dateien) nur zugelassen wird, wenn sie auf Viren geprüft wurden.

SWEEP kann von Disketten die meisten Bootsektorviren entfernen. Normalerweise wird diese Option nur im Sofortstartmodus angewendet, da der zeitgesteuerte bis eine Bestätigung durch den Anwender erfolgt angehalten wird. SWEEP für Windows 95 desinfiziert keine Bootsektoren von Festplatten, da einige Bootsektorviren Tarnkappenmechanismen unter Windows 95 erfolgreich einsetzen können. Um einen Festplattenbootsektor zu desinfizieren, müssen Sie von einer sauberen Systemdiskette den Rechner neu booten und zum Desinfizieren die DOS Version Von SWEEP benutzen.

SWEEP kann alle virulenten Makros aus Dokumenten entfernen, die mit einem Makrovirus infiziert sind. Wenn die Desinfektion fehlschlägt, wird die infizierte Datei auf die gleiche Weise behandelt, wie jede andere infizierte Datei.

Wenn eine infizierte Datei gefunden wird, gibt es diverse Aktionen, die durchgeführt werden können um die Datei unschädlich zu machen. Das Umbenennen oder Bewegen einer ausführbaren Datei sollte sie vor einem Ausführen bewahren, während das Löschen oder Überschreiben sicherstellt, daß die Datei auch nicht aus versehen ausgeführt werden kann. Das Überschreiben ist eine sicherer Methode eine Datei zu löschen, da sie hierbei komplett überschrieben wird.

Wenn diese Option ausgewählt wird, wird jede Aktion, welche die Änderung infizierter Daten zur Folge hat (wie Desinfizieren von Bootsektoren, Desinfizieren von Dokumenten, das Umbenennen, Löschen, Überschreiben und das Bewegen infizierter Dateien) vor der Durchführung auf eine Bestätigung warten. Diese Option ist nur im Sofortstartmodus verfügbar, wo sie auch standardmäßig aktiviert ist.

Die Benachrichtigungsmitteilung kann aus der kompletten Reportdatei bestehen, die am Ende eines jeden Scanjobs gesendet wird, und/oder einer Mitteilung für jede infizierte Datei, die gefunden wurde.

Die Benachrichtigungsliste enthält die Anwender, die benachrichtigt werden sollen. Das Betätigen der *Hinzufügen* Taste stellt eine Verbindung zu Microsoft Exchange her und eine Liste mit möglichen Anwendern wird angezeigt.

Die Einstellung Dateinamen auflisten bringt SWEEP dazu die Namen aller untersuchten Dateien und Bereiche in die Reportdatei aufzunehmen. Ansonsten werden nur infizierte Dateien oder Bereiche aufgelistet.

Die Reportdatei wird auf das Laufwerk gesichert.

Viren können sich selbst an COM und EXE Dateien anhängen; sie können den Masterbootsektor und den DOS-Bootsektor infizieren; Companionviren setzen sich in eine COM Datei, die den selben Namen erhält wie die EXE Datei; Linkviren Verbiegen Verzeichniseinträge, damit sie auf den Viruscode zeigen; und Windows Viren hängen sich an Windowsprogramme. Trojanische Pferde sind keine Viren, es sind Programme, die beim Ausführen unerwartete und unerfreuliche Nebeneffekte zeigen.

Speicherresidente Viren setzen sich nach der Programmausführung im Speicher fest und infizieren von dort andere Objekte, wenn bestimmte Bedingungen erfüllt werden.

Ein Häkchen ist in diesen Boxen enthalten, wenn die Viren von Disketten oder Festplatten entfernt werden können.

Viele Viren warten auf eine bestimmte Zeit, oder ein bestimmtes Datum, um die Seiteneffekte Wirksam werden zu lassen.

Die Option “Text in Beschreibung“ sucht nach einer Textfolge, die in der Information über den Virus vorkommen soll.

Was ist InterCheck?

SWEEP bietet mit der InterCheck-Technologie eine Virenaufspürung auf Zugriffsbasis, während SWEEP alleine eine Virenprüfung bei Bedarf bietet. InterCheck stellt sicher, daß unbekannte Dateien (z.B. Programme, Dokumente, Email-Anhänge oder Internet Downloads) und Laufwerke nicht benutzt werden können, bevor eine Virenprüfung erfolgt ist.

InterCheck teilt die Arbeit der Virensuche zwischen einem Client und einem Server auf. Der **InterCheck Client** entscheidet, welche Daten auf der Arbeitsstation nach Viren untersucht werden müssen, während in einer Netzwerkumgebung der **InterCheck Server** die Virenprüfungen, die für nötig erachtet werden, durchführt.

Es gibt zwei Unterarten des InterCheck Clients: Netzwerkbasiert und Standalone. Ein **Netzwerkbasierter InterCheck Client** läuft auf einem anderen Rechner, als der InterCheck Server und kommuniziert mit ihm durch das Netzwerk. Ein **Standalone InterCheck Client** braucht nicht mit einem angeschlossenen Server zu kommunizieren, er benutzt eine lokale Installation von SWEEP um nach Viren zu suchen.

Ein Netzwerkbasierter InterCheck Client ist einfacher zu administrieren und beansprucht auf der Client Arbeitsstation weniger Ressourcen. Ein Standalone InterCheck Client bietet normalerweise eine schnellere Autorisierung der Dateien, und kann auch auf Maschinen benutzt werden, die nicht immer mit dem Netzwerk verbunden sind. In beiden Fällen ist InterCheck die effizienteste Art den Anwender vor Viren zu schützen – alle Daten werden nur ein einziges Mal auf Viren untersucht, es sei denn, sie werden modifiziert. In diesem Fall werden sie erneut geprüft.

Wie arbeitet InterCheck?

Die InterCheck Software überwacht alle Datei und Laufwerkszugriffe. Wann immer ein Zugriff erfolgt, werden die Daten mit einer Liste autorisierter Daten verglichen. Wenn die Daten dabei identifiziert wurden, wird der Zugriff gestattet. Werden die Daten nicht erkannt, sendet der Netzwerkbasierte InterCheck Client eine Kopie der Daten zur Prüfung an den InterCheck Server, während der Standalone InterCheck Client die Prüfung mit einer lokalen Installation des SWEEP Programms vornimmt.

Wenn die Daten als sauber erachtet werden, werden sie der Liste mit den autorisierten Daten hinzugefügt, und die Fortführung des Zugriffs auf die Daten wird sofort gestattet. Jeder weitere Zugriff auf die Daten findet dann ohne jede weitere Autorisierung statt, bis die Daten modifiziert wurden. In diesem Fall wird automatisch eine erneute Autorisierung angefordert.

Immer, wenn ein Virus gefunden wird, verhindert InterCheck den Zugriff auf die infizierten Daten, so, daß die Arbeitsstation nicht infiziert werden kann.

Merkmale

Kompletter Schutz

Für das Netzwerk: InterCheck bietet einen kompletten Virenschutz für das gesamte Netzwerk bei minimalem Speicherbedarf und geringem Einfluß auf die Performance, dabei unterstützt es die größte Bandbreite an Client und Serverplatformen.

Für die Arbeitsstation: InterCheck überwacht den Zugriff zu allen Programmen, Bootsektoren, Dokumenten, Emailanhängen, Internet Downloads und CD-ROMs.

Performance

Wenn etwas autorisiert ist, entfällt die Notwendigkeit einer weiteren Überprüfung. Dies ist solange unnötig, bis sich die Daten ändern oder eine neue SWEEP Version erschienen ist. Der Prozeß, der überprüft ob etwas autorisiert ist oder nicht, ist wesentlich schneller, als die Durchführung einer kompletten Virensuche.

Automatische Benachrichtigung

Viele Virenvorfälle sind schwerwiegender, als sie sein müßten, nur weil die Anwender die Virenmeldungen nicht an die zuständigen Personen weiterleiten. Wenn ein InterCheck Client Zugang zu einem Netzwerk hat und ein Virus gefunden wird, so kann automatisch eine Nachricht an den Netzwerkadministrator gesendet werden.

Einfache Administration

InterCheck Clients können zentral überwacht, kontrolliert und upgedatet werden. Netzwerkbasierte InterCheck Clients können in vielen Fällen automatisch über ein Netzwerk installiert werden.

Portable PCs

InterCheck Clients bieten den gleichen Sicherheitsstatus auch an, wenn der Rechner keine Verbindung mehr zum Netzwerk hat.

Überblick über InterCheck Installation und Konfiguration

Netzwerkbasierte InterCheck Clients benötigen einen separaten InterCheck Server. Dies beinhaltet das Installieren von SWEEP und der InterCheck Software auf dem Datenserver, und das Starten von SWEEP im InterCheck Servermodus. Netzwerkbasierte InterCheck Clients sind zur Zeit für DOS, Windows 3.x, Windows für Workgroups, Windows 95 und Macintosh Arbeitsstationen verfügbar.

Standalone InterCheck Clients benötigen keinen InterCheck Server. Im Falle von Windows 95 und Windows NT, wird der Standalone InterCheck Client als ein Teil des SWEEP Installationsprozesses installiert. Standalone InterCheck Clients sind derzeit verfügbar für Windows 3.x, Windows für Workgroups, Windows 95 und Windows NT Arbeitsstationen.

Die InterCheck Serverfunktionalität ist derzeit in SWEEP für NetWare, Windows NT (Intel & Alpha), OpenVMS, DOS, OS/2 und Banyan VINES integriert. SWEEP für DOS kann aber auch angewendet werden, um die Serverfunktionalität für andere Betriebssysteme zur Verfügung zu stellen.

InterCheck Server Installation und Konfiguration

Windows NT, NetWare, OpenVMS, OS/2 & Banyan VINES

Schauen Sie hierzu in die SWEEP für Windows NT, NetWare, OpenVMS, OS/2 und Banyan VINES Benutzerhandbücher (oder die InterCheck Server Benutzerhandbücher).

DOS

Schauen Sie hierzu ins SWEEP für DOS Handbuch ins Kapitel InterCheckServer.

Standalone InterCheck Clientinstallation

Windows 3.x & Windows für Workgroups

Schauen Sie hierzu ins Kapitel “Installieren des InterCheck Clients“ des InterCheck Server Benutzerhandbuches.

Windows 95 & Windows NT

Schauen Sie hierzu ins Kapitel “Installieren von SWEEP“ im SWEEP für Windows 95 und SWEEP für Windows NT Benutzerhandbuch nach.

Netzwerkbasierte InterCheck Clientinstallation

DOS, Windows 3.x, Windows für Workgroups, Windows 95 & Macintosh

Schauen Sie hierzu ins Kapitel “Installieren des InterCheck Clients“ des InterCheck Server Benutzerhandbuches.

Standalone InterCheck Clientkonfiguration

Windows 3.x, Windows für Workgroups & Windows 95

Schauen Sie hierzu ins Kapitel “Installieren des InterCheck Clients“ des InterCheck Server Benutzerhandbuches, und im SWEEP für Windows 95 Benutzerhandbuch.

Windows NT

Schauen Sie hierzu ins Kapitel “Konfigurieren von SWEEP“ im SWEEP für Windows NT Benutzerhandbuch.

Netzwerkbasierte InterCheck Clientkonfiguration

DOS, Windows 3.x, Windows für Workgroups & Windows 95

Schauen Sie hierzu ins Kapitel “Konfigurieren des InterCheck Client“ im InterCheck Server Benutzerhandbuch.

Über Sophos Plc

Sophos Plc wurde 1980 gegründet, 1985 begann Sophos seine Aktivitäten in dem Bereich Datensicherheit und ist nun ein weltweit führender Entwickler für Software im Bereich Datensicherheit und Antivirensoftware. Im Mittelpunkt dieses Erfolges steht das Einstehen für innovative und fortschrittliches Produktdesign unterstützt durch einen hochwertigen Support. Sophos exportiert mit einem internationalen Distributionsnetzwerk zur Zeit in 27 Länder.

Alle Sophos Produkte werden in der Firmenzentrale nahe Oxford entworfen, hergestellt und supported. Diese Produkte sind:

- "SWEEP" Virenaufspürungssystem.
- "D-FENCE" Autorisierungssoftware.
- "VACCINE" Prüfsummenvirenaufspürungssystem.
- "EDS" Datenverschlüsselungstool für DOS und Windows.

Kontaktliste Sophos

Email

Allgemeine Anfragen:
enquiries@sophos.com

Verkaufsfragen:
sales@sophos.com

Technischer Support:
support@de.sophos.com

Kommentare über Handbücher, Online-Hilfe, usw.:
publications@sophos.com

Sophos GmbH, Deutschland

Phone: +49-6136-91193

Fax: +49-6136-911940

Sophos GmbH
Am Hahnenbusch 21
55268 Nieder-Olm
Deutschland

Sophos Plc, UK

Phone +44 1235 559933

Fax +44 1235 559935

Sophos Plc
The Pentagon
Abingdon Science Park
Abingdon
OX14 3YP
England

Sophos Inc, USA

Phone +1 781 932 0222

Fax +1 781 932 0251

Sophos Inc
18 Commerce Way
Woburn
MA 01801
USA

WWW http://www.sophos.com/

FTP ftp.sophos.com

BBS +44 1235 559936

Was ist ein Computervirus?

Ein Computervirus infiziert Programme und Laufwerke, indem es Kopien von sich darin plaziert:

- Ein Bootsektorvirus infiziert den Bootsektor von Laufwerken.
- Parasitäre-, Begleit-, Link- und Makroviren infizieren Dateien.
- Multi-Partite Viren können sowohl Dateien als auch Bootsektoren infizieren.

Einen PC oder ein Laufwerk kann man als infiziert bezeichnen, wenn es einen infizierten Bootsektor und/oder ein oder mehrere infizierte Dateien enthält. Der Speicher eines PC's wird als infiziert bezeichnet, wenn er einen speicherresidenten Virus enthält.

Es gibt drei Möglichkeiten, durch die ein PC und der Speicher eines PC's infiziert werden können:

- Der PC wurde von einer Diskette gebootet, die mit einem Bootsektorvirus oder einem Multipartite Virus infiziert ist.
- Ein infiziertes Programm wurde ausgeführt, z.B. durch Eingabe seines Dateinamens an der Kommandozeile, oder durch Anklicken des Programmicons unter Windows.
- Eine Datei, die mit einem Makrovirus infiziert ist wird von einer Applikation geladen, die die entsprechende Makrosprache ausführen kann.

Weitere Informationen über Viren finden Sie im Sophos' *Data Security Reference Guide*.