Inhalt

F-Secure Anti-Virus anwenden

Überblick
F-Secure Anti-Virus Gatekeeper
Manuell nach Viren scannen
Desinfektions-Assistent

Benutzereinstellungen in F-Secure Anti-Virus

Einstellungen
Echtzeitschutz
Manuelles Scannen
Aktualisierungen
Statistiken

Technische Unterstützung

Technische Unterstützung

Über F-Secure Corporation

Unternehmensinformationen
Die Produktfamilie von F-Secure

Überblick

F-Secure Anti-Virus wurde für Unternehmens-Netzwerkumgebungen entwickelt. Die Funktionen zur Virenfeststellung werden nachvollziehbar und in Echtzeit ausgeführt. Das Programm wird weitgehend selbständig und ohne Benutzereingriff ausgeführt, wodurch weniger Schulungen und technische Unterstützung erforderlich sind. Die zentralen Verwaltungsfunktionen auf Richtlinienbasis stellen eine Anti-Virus-Lösung dar, die leicht zu bedienen und zudem kostengünstig ist.

F-Secure Anti-Virus Gatekeeper

Die Funktionsweise von F-Secure Anti-Virus Gatekeeper basiert auf der Technologie des dynamischen Virenschutzes. Im Rahmen dieser Technologie werden Gerätetreiber eingesetzt, die die Funktionsweise des Betriebssystems beim Öffnen von Dateien und Verwalten von Festplattenpartitionen überwachen.

Mit der von F-Secure Anti-Virus Gatekeeper bereitgestellten Funktion zum Echtzeitschutz werden die Dateien stets vor Viren geschützt, unabhängig davon, ob sie geöffnet, kopiert, verschoben, umbenannt oder vom Internet heruntergeladen werden.

Die Funktionen zum Echtzeitschutz werden nachvollziehbar im Hintergrund ausgeführt, und es wird stets dann nach Viren gesucht, wenn Sie auf der Festplatte, Disketten oder den Netzwerk-Laufwerken auf Dateien zugreifen. Wenn Sie versuchen, auf eine infizierte Datei zuzugreifen, wird ein Ausbreiten des Virus automatisch durch die Funktion zum Echtzeitschutz verhindert. Dies geschieht gemäß der Sicherheitsrichtlinie entweder durch Entfernen des Virus aus der Datei oder durch Anzeigen einer Warnmeldung.

F Um die Ausbreitung von Boot-Sektor-Viren zu vermeiden, werden auch die Disketten durch die Echtzeitschutz-Funktion überprüft, wenn der Computer heruntergefahren oder neu gestartet wird. Wenn keine Diskette im Diskettenlaufwerk eingelegt ist, ist unter Umständen ein Summton zu vernehmen. Dieser Summton ist normal.

Um zu überprüfen, ob die Funktion zum Echtzeitschutz aktiviert ist, doppelklicken Sie in der Task-Leiste in der unteren rechten Fensterecke auf das Symbol für die F-Secure-Einstellungen und –Statistiken. Wenn der Status von F-Secure Anti-Virus auf **Aktiviert** eingestellt ist, bietet die Funktion für den Echtzeitschutz fortwährenden Schutz.

Manuell nach Viren scannen

Es ist nicht erforderlich, Dateien manuell zu scannen. Durch den Echtzeitschutz von F-Secure Anti-Virus Gatekeeper ist der bestmögliche automatische Virenschutz gewährleistet. Die in diesem Abschnitt enthaltenen Informationen dienen lediglich als Referenz für den Fall, dass Benutzer manuell scannen möchten.

Das Scannen nach Viren kann auf eine der folgenden Weisen begonnen werden:

- Kontextmenü (Klicken Sie mit der rechten Maustaste auf eine Datei, einen Ordner oder ein Laufwerk.)
- Menü für F-Secure-Einstellungen und -Statistiken in der Task-Leiste (Klicken Sie mit der rechten Maustaste auf das F-Symbol [F-Secure] in der Task-Leiste.)
- Windows-Startmenü (Klicken Sie mit der rechten Maustaste auf das Menü.)

Während des Scan-Vorgangs wird im Dialogfeld **Manual Scanning Statistics** (Manuelle Scan-Statistik) eine Verlaufsanzeige und die Statistiken für den Scan-Vorgang angezeigt. Wenn der Scan-Vorgang abgebrochen werden soll, klicken Sie auf **Anhalten**. Nach Abschluss des Scan-Vorgangs wird ein Bericht erstellt. Sie können den Bericht in einem Web-Browser anzeigen lassen, indem Sie auf **Bericht anzeigen** klicken.

Weitere Informationen:

Kontextmenü

Menü für F-Secure-Einstellungen und -Statistiken in der Task-Leiste

Scannen vom Windows-Startmenü starten

Kontextmenü

Klicken Sie zum Scannen einer Datei, eines Ordners oder einer Diskette nach Viren mit der rechten Maustaste auf das entsprechende Symbol, und wählen Sie im Kontextmenü ***[Objekt]*** **nach Viren scannen** aus. Jede Datei, jeder Ordner und jedes Laufwerk kann unabhängig von der Erweiterung auf diese Weise gescannt werden.

Menü für F-Secure-Einstellungen und -Statistiken in der Task-Leiste

Klicken Sie mit der rechten Maustaste im Systemfeld der Windows-Task-Leiste auf das F-Symbol (F-Secure), damit das Menü für F-Secure-Einstellungen und -Statistiken angezeigt wird.

Wählen Sie im Menü eine der Scan-Aktionen aus, um den Scan-Vorgang einzuleiten.

Wenn Sie die Aktion **Ziel scannen** auswählen, müssen Sie anschließend den zu scannenden Ordner oder den zu scannenden Datenträger auswählen.

Scannen vom Windows-Startmenü starten

Von der F-Secure Anti-Virus-Programmgruppe aus kann man direkt das Scannen von Festplatten, Disketten und Ordnern veranlassen.

Klicken Sie im Menü auf einen der Scan-Befehle, um den Scan-Vorgang einzuleiten: **Alle lokalen Festplatten scannen**, **Diskette scannen** oder **Ordner scannen**. Wenn Sie die Option **Ordner scannen** auswählen, müssen Sie einen Ordner oder einen Datenträger auswählen.

Desinfektions-Assistent

Wenn ein Virus festgestellt wird, während Sie am Computer arbeiten, wird der Desinfektions-Assistent automatisch über F-Secure Anti-Virus ausgeführt.

1. Im ersten Fenster werden die Namen der festgestellten Viren angezeigt.

   Weitere Informationen zu einem Virus erhalten Sie, indem Sie auf den Namen und anschließend auf die Schaltfläche **Vireninfo** klicken. Auf der Vireninformationsseite wird eine Liste festgestellter Viren angezeigt.

   Durch Aktivieren des Kontrollkästchens können Sie die gesamte Vireninformationsdatenbank einsehen. Falls es sich um einen ganz neuen Virus handelt, ist dieser in der Datenbank unter Umständen noch nicht aufgeführt. Wenn Sie in der Datenbank keine Beschreibung zu diesem Virus finden, ist diese möglicherweise in der Virusinformationsdatenbank auf unserer Web-Site enthalten.

   Die Vireninformationsdatenbank von F-Secure ist eine umfangreiche Virendatenbank, die Informationen zu tausenden von Viren enthält. Die Datenbank wird täglich aktualisiert. Klicken Sie auf die Schaltfläche **Web Club**, um auf die Datenbank zuzugreifen.
2. Eine Liste mit infizierten Dateien wird angezeigt.

   Wählen Sie im Feld **Durchzuführende Aktion** die Aktion aus, die hinsichtlich der infizierten Dateien durchgeführt werden soll.
3. Die Dateien werden nun desinfiziert, und die Ergebnisse der Aktion werden angezeigt.
4. Ein Desinfektionsbericht wird erstellt. Wenn Sie nicht möchten, dass ein Bericht erstellt wird, deaktivieren Sie das Kontrollkästchen **Bericht erstellen**.

Der Desinfektionsbericht wird automatisch im Standard-Web-Browser angezeigt. Wenn das Programm zentral verwaltet wird, wird der Bericht an den Administrator geschickt.

> F Hinweis: Der Administrator kann F-Secure Anti-Virus so konfigurieren, dass Viren automatisch vom Computer entfernt werden, ohne dass eine entsprechende Aufforderung zum Handeln ausgesendet wird. In diesem Fall wird der Desinfektions-Assistent nicht ausgeführt.

Einstellungen

Sie können zur Ansicht und zum Ändern der Einstellungen in F-Secure Anti-Virus das Dialogfeld für F–Secure-Einstellungen und -Statistiken öffnen, indem Sie im Systemfeld der Windows-Task-Leiste auf das F-Symbol doppelklicken. Das Fenster für F–Secure-Einstellungen und -Statistiken mit einer Liste installierter F-Secure-Programme wird angezeigt.

Um das Dialogfeld für F-Secure Anti-Virus-Eigenschaften zu öffnen, doppelklicken Sie entweder auf die F-Secure Anti-Virus-Anwendung oder auf die Option **Eigenschaften**. Sie können im Dialogfeld für F–Secure Anti-Virus-Eigenschaften unterschiedliche Einstellungen für die drei Arten der Scan-Vorgänge festlegen: Echtzeitschutz, manuelles Scannen und Aktualisierungen. Das Dialogfeld für F-Secure Anti-Virus-Eigenschaften enthält außerdem Informationen über Scan-Statistiken.

Statistics (Statistiken)

Zeigt die Ergebnisse der Echtzeitsuche an.

Echtzeitschutz

Einstellungen für den nachvollziehbaren, fortwährenden Schutz von F-Secure Anti-Virus. Dateien werden beim Öffnen vom im Hintergrund laufenden Programm gescannt.

Manuelles Scannen

Einstellungen für die Scan-Vorgänge, die manuell eingeleitet werden.

Aktualisierungen

Mit Hilfe der Einstellungen zur Aktivierung der automatischen Aktualisierung der Virusdefinitionsdatenbank wird zum manuellen Aktualisieren aufgefordert. Über die Schaltfläche **Jetzt aktualisieren** können Aktualisierungen sofort ausgeführt werden.

Das Echtzeit-Scannen sollte selten durchgeführt werden, damit nur geringe Systemressourcen in Anspruch genommen werden. Beim Scannen gepackter und sonstiger spezieller Dateien ist das Gegenteil der Fall.

Da manuelle Scan-Vorgänge nur bei Bedarf durchgeführt werden, können sie so eingestellt werden, dass größere Dateigruppen gescannt werden, wodurch mehr Systemressourcen in Anspruch genommen werden.

Echtzeitschutz

Um den Echtzeitschutz mit F-Secure Anti-Virus zu aktivieren bzw. zu deaktivieren, aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Schutz aktivieren**.

Weitere Informationen:

Durchzuführende Aktion bei infizierten Dateien

Scan-Optionen

Durchzuführende Aktion bei infizierten Dateien

Unter **Durchzuführende Aktion bei infizierten Dateien** können Sie festlegen, welche Aktion durch F-Secure Anti-Virus beim Feststellen einer infizierten Datei veranlasst wird. Wählen Sie eine der folgenden Aktionen aus:

Nach Scannen fragen

Der Desinfektions-Assistent wird gestartet, wenn eine infizierte Datei festgestellt wird.

Automatisch desinfizieren

Die Datei wird automatisch desinfiziert, wenn ein Virus festgestellt wird.

Automatisch umbenennen

Die Datei wird automatisch umbenannt, wenn ein Virus festgestellt wird.

Automatisch löschen

Die Datei wird automatisch gelöscht, wenn ein Virus festgestellt wird.

Scan-Optionen

Unter **Scan-Optionen** können Sie auswählen, welche Dateien in Echtzeit gescannt werden sollen. Folgende Optionen stehen zur Auswahl:

Alle Dateien

Alle Dateien werden unabhängig von der Dateierweiterung gescannt. Diese Option ist nicht empfehlenswert, da sie unter Umständen dazu führt, dass das System beträchtlich langsamer arbeitet.

Dateien mit diesen Erweiterungen

Dateien mit bestimmten Dateierweiterungen werden gescannt. Um Dateien ohne Dateierweiterungen festzulegen, geben Sie einen Punkt ein. Der Platzhalter '?' kann verwendet werden. Geben Sie alle Dateierweiterungen ein, und trennen Sie sie durch einen Leerschritt. Diese Option wird für den Echtzeitschutz empfohlen.

Dateien mit diesen Erweiterungen ausschließen

Es können Dateien angegeben werden, die nicht gescannt werden sollen.

Exclude objects (Objekte ausschließen)

Es können einzelne Dateien oder Ordner angegeben werden, die nicht gescannt werden sollen. Klicken Sie dazu auf die Schaltfläche **Auswählen**, und suchen Sie die Dateien und Ordner, die nicht gescannt werden sollen.

In komprimierten Dateien scannen

Aktivieren Sie dieses Kontrollkästchen, um komprimierte Dateien, wie beispielsweise .ZIP-, .ARJ- und .LZH-Dateien, zu scannen. Das Scannen umfangreicher komprimierter Dateien kann unter Umständen viele Systemressourcen in Anspruch nehmen und das System verlangsamen. Dies ist daher für den Echtzeitschutz nicht empfehlenswert.

Manuelles Scannen

Die Einstellungen für manuelles Scannen können auf der Seite für manuelles Scannen im Dialogfeld für F-Secure Anti-Virus-Eigenschaften festgelegt werden.

Weitere Informationen:

Durchzuführende Aktion bei infizierten Dateien

Scan-Optionen

Durchzuführende Aktion bei infizierten Dateien

Unter **Durchzuführende Aktion bei infizierten Dateien** können Sie festlegen, welche Aktion durch F-Secure Anti-Virus beim Feststellen einer infizierten Datei veranlasst wird.

Eine der folgenden Optionen kann ausgewählt werden:

Nach Scannen fragen

Der Desinfektions-Assistent wird gestartet, wenn eine infizierte Datei festgestellt wird.

Automatisch desinfizieren

Die Datei wird automatisch desinfiziert, wenn ein Virus festgestellt wird.

Automatisch umbenennen

Die Datei wird automatisch umbenannt, wenn ein Virus festgestellt wird.

Automatisch löschen

Die Datei wird automatisch gelöscht, wenn ein Virus festgestellt wird.

Scan-Optionen

Unter **Scan-Optionen** können Sie auswählen, welche Dateien während des manuellen Scan-Vorgangs gescannt werden sollen.

Folgende Optionen stehen zur Auswahl:

Alle Dateien

Alle Dateien werden unabhängig von der Dateierweiterung gescannt. Diese Option ist nicht empfehlenswert, da sie unter Umständen dazu führt, dass das System beträchtlich langsamer arbeitet.

Dateien mit diesen Erweiterungen

Dateien mit bestimmten Dateierweiterungen werden gescannt. Geben Sie alle Dateierweiterungen ein, und trennen Sie sie durch einen Leerschritt. Der Platzhalter '?' kann verwendet werden.

Dateien mit diesen Erweiterungen ausschließen

Es können Dateien angegeben werden, die nicht gescannt werden sollen.

Exclude objects (Objekte ausschließen)

Es können einzelne Dateien oder Ordner angegeben werden, die nicht gescannt werden sollen. Klicken Sie dazu auf die Schaltfläche **Hinzufügen**, und suchen Sie die Dateien und Ordner, die nicht gescannt werden sollen.

In komprimierten Dateien scannen

Aktivieren Sie dieses Kontrollkästchen, um komprimierte Dateien, wie beispielsweise .ZIP-, .ARJ- und .LZH-Dateien, zu scannen. Da manuelle Scan-Vorgänge keinen Einfluss auf die Systemleistung haben, kann diese Option problemlos verwendet werden.

Die Schaltfläche **Jetzt scannen** kann verwendet werden, um einen Ordner zu beliebiger Zeit auf Viren zu durchsuchen.

Aktualisierungen

Die Seite **Aktualisierungen** enthält Informationen über installierte Scan-Module und Aktualisierungen der Virendatenbank. Über die Schaltfläche **Weitere Informationen** auf dieser Seite erhalten Sie eine direkte Verknüpfung zur F-Secure-Web-Site oder zu einer ISP-Site.

Weitere Informationen:

Installierte Scan-Module

Aktualisierungen der Virendatenbank

Zeitraum zum Auffordern für Aktualisierung

Jetzt aktualisieren

Aktualisierungsaufforderung

Weitere Informationen

Installierte Scan-Module

Im Feld **Installierte Scan-Module** finden Sie Informationen über zur Zeit installierte Scan-Modulnamen, über einzelne Datenbankdaten und ihre Versionsnummern. Die verwendeten Scan-Module lauten F-Secure F-Prot, F-Secure AVP bzw. F-Secure Orion.

Aktualisierungen der Virendatenbank

Im Abschnitt **Virus Database Updates (Aktualisierungen der Virendatenbank)** erhalten Sie Informationen über den aktuellen Status der Virusdefinitionsdatenbanken. Sie erhalten hier z. B. Informationen über sofort auszuführende Aktualisierungen, die ausgeführt werden sollten, wenn die Virusdefinitionsdatenbanken nicht mehr aktuell sind.

Zeitraum zum Auffordern für Aktualisierung

Im Kontrollkästchen **Zeitraum zum Auffordern für Aktualisierung** können Sie die automatische Aktualisierung der Virusdefinitionsdatenbank aktivieren. Sie können festlegen, wie oft das Dialogfeld zur Aktualisierung angezeigt wird, indem Sie im Feld **Days (Tage)** die Tage festlegen.

Die Verfügbarkeit der Funktion zur Aktualisierungsaufforderung wird durch die Richtlinieneinstellungen festgelegt. Wenn durch die Richtlinieneinstellungen die manuellen Aktualisierungen unterbunden sind, sind sowohl das Kontrollkästchen **Zeitraum zum Auffordern für Aktualisierung** als auch das Feld **[X] Days ([X] Tage)** nicht verfügbar. Der Administrator kann die Zugriffsrechte auf die Optionen von der F-Secure Administrator-Richtlinie aus ändern:

`FSAV\Data Fellows\F-Secure Anti-Virus\Einstellungen\Aktualisierungen der Virendatenbank\Aktualisierungsaufforderung\Aufforderungsstatus`

Der Standardstatus für den Einzelplatz-Modus ist **Allowed (Erlaubt)** und der Standardstatus für Zentralverwaltungsmodus ist **Not allowed (Nicht erlaubt)**.

Jetzt aktualisieren

Über die Schaltfläche **Jetzt aktualisieren** wird die manuelle Aktualisierung der Virusdefinitionsdatenbank ausgeführt. Ob diese Einstellung verfügbar ist oder nicht, wird von den Richtlinieneinstellungen festgelegt.

Wenn die folgende F-Secure Administrator-Richtlinieneinstellung

`FSAV\Data Fellows\F-Secure Anti-Virus\Einstellungen\Aktualisierungen der Virendatenbank\Manuelle Aktualisierungen ermöglichen`

auf **True (Wahr)** eingestellt ist, kann die Schaltfläche **Jetzt aktualisieren** verwendet werden. Wenn F-Secure Anti-Virus mit der Zentralverwaltungs-Konfiguration installiert wurde, startet es eine normale Aktualisierung, wobei die Abfrage entweder vom Management Server oder vom Speicherort der Virusdefinitionsdatenbanken erfolgt. Mit Hilfe des Einzelplatz-Modus werden neue Datenbanken von der F–Secure-Web-Site oder von einer IPS-Site heruntergeladen.

Während des Herunterladevorgangs wird ein Dialogfeld angezeigt. Sie können die Aktualisierung abbrechen, indem Sie auf die Schaltfläche **Cancel Update (Aktualisierung abbrechen)** klicken.

Aktualisierungsaufforderung

Wenn manuelle Aktualisierungen der Virusdefinitionsdatenbank zugelassen sind, sind Aktualisierungsaufforderungen aktiviert. Wenn das Dialogfeld **Zeitraum zum Auffordern für Aktualisierung: [X] Tage** aktiviert ist und X Tage seit der letzten Aktualisierung bzw. seit der letzten Aktualisierungsaufforderung verstrichen sind, wird ein Dialogfeld angezeigt.

Wenn Sie auf die Schaltfläche **Jetzt aktualisieren** klicken, wird die manuelle Aktualisierung der Virusdefinitionsdatenbank gestartet. Wenn Sie auf die Schaltfläche **Später auffordern** klicken, wird die Aktualisierung um die Tage verschoben, die als Aufforderungsintervall gewählt wurden. Wenn Sie auf die Schaltfläche **Aktualisierungsoptionen** klicken, wird das Dialogfeld für F-Secure Anti-Virus-Eigenschaften angezeigt, wobei die Registerkarte zur Datenbankverwaltung aktiviert ist.

Weitere Informationen

Über die Schaltfläche **Weitere Informationen** wird ein Standard-Web-Browser entweder mit der F-Secure-Web-Site von der IPS-Site gestartet. Die URL kann in F-Secure Administrator an folgender Stelle geändert werden:

`FSAV\Data Fellows\F-Secure Anti-Virus\Einstellungen\Aktualisierungen der Virendatenbank\Informationsseite`

Beachten Sie, dass die URL das Protokoll und den Site-Namen enthalten muss: http://www.unternehmen.com.

Statistiken

In der Registerkarte für Statistiken im Dialogfeld für F-Secure Anti-Virus-Eigenschaften werden die Ergebnisse der Echtzeitsuche der aktuellen Sitzung angezeigt.

Technische Unterstützung

F-Secure bietet technische Unterstützung via E-Mail und über die F-Secure-Web-Site an. Sie können diese Web-Site in F-Secure Anti-Virus oder über Ihren Web-Browser aufrufen.

Weitere Informationen:

Web Club

Virenbeschreibungen im Internet

Unterstützung per E-Mail

Web Club

Der F-Secure Anti-Virus Web Club bietet Unterstützung für die Benutzer von F-Secure Anti-Virus. Um auf den Web Club zuzugreifen, wählen Sie im Menü **Hilfe** den Befehl **Web Club** aus. Wenn Sie diese Option zum ersten Mal verwenden, müssen Sie Ihren Standort sowie Pfad und Namen Ihres Web-Browsers angeben.

Wenn Sie eine Verbindung direkt mit Ihrem Web-Browser herstellen möchten, rufen Sie folgende Web-Site auf:
http://www.F-Secure.com/webclub/

Für ausführliche Unterstützung steht Ihnen das Support Center für F-Secure Anti-Virus unter folgender Adresse zur Verfügung:
http://www.F-Secure.com/support/

Virenbeschreibungen im Internet

F-Secure Corporation unterhält auf seiner Web-Site eine umfangreiche Sammlung von Vireninformationen. Wählen Sie zum Öffnen der Virusinformationsdatenbank im Menü **Hilfe** den Befehl **Virus Descriptions On the Web** (**Virenbeschreibungen im Internet**) aus.

Sie können die Virusinformationsdatenbank aber auch unter folgender Adresse einsehen:
http://www.f-secure.com/vir-info/

Unterstützung per E-Mail

Wenn Sie noch Fragen über F-Secure Anti-Virus haben, die im Benutzerhandbuch oder online unter *www.F-Secure.com* nicht behandelt wurden, wenden Sie sich an Ihren F-Secure-Händler vor Ort oder direkt an F-Secure Corporation.

Für grundlegende technische Unterstützung wenden Sie sich bitte an Ihren F-Secure-Vertragspartner vor Ort. Senden Sie eine E-Mail an:

Anti-Virus-<Land>@F-Secure.com

Beispiel: Anti-Virus-Germany@F-Secure.com

Wenn es keinen autorisierten F-Secure Anti-Virus-Vertragspartner in Ihrem Land gibt, erhalten Sie unter folgender Adresse grundlegende technische Unterstützung:

Anti-Virus-Support@F-Secure.com

Geben Sie in Anfragen um Unterstützung Folgendes an:

Versionsnummer von F-Secure Anti-Virus (einschließlich Build-Nummer).

Name und Version des Betriebssystems (DOS, Windows); einschließlich Build-Nummer.

Genaue Beschreibung des Problems, inklusive aller angezeigten Fehlermeldungen, sowie andere Details, die uns beim Nachvollziehen des Problems hilfreich sein könnten.

Wenn Sie sich telefonisch an die F-Secure-Unterstützung wenden, können Sie uns hiermit helfen, Zeit zu sparen:

Sie sollten sich an Ihrem Computer befinden, um die Anleitungen des Technikers umsetzen zu können. Falls dies nicht möglich ist, sollten Sie die Anleitungen notieren.

Ihr Computer sollte eingeschaltet sein und sich möglichst in dem Zustand befinden, in dem er sich befand, als das Problem auftrat. Ist dies nicht möglich, sollten Sie in der Lage sein, das Problem auf dem Computer mit geringem Aufwand nachstellen zu können.

Stellen Sie im Fall einer Virusinfektion sicher, dass das neueste F-Secure-Update verwendet wurde. Das F-Secure-Update kann aus dem Web Club heruntergeladen werden.

Unternehmensinformationen

F-Secure Corporation (ehem. Data Fellows) ist eines der weltweit führenden Unternehmen bei der Entwicklung von Produkten für die Datensicherheit. Das Unternehmen entwickelt, vermarktet und unterstützt Anti-Virus-, Datensicherheits- und Verschlüsselungs-Software für die Computernetzwerke von Firmenkunden. Die F-Secure-Hauptniederlassungen befinden sich in San Jose, Kalifornien und Espoo, Finnland. Tochtergesellschaften befinden sich u. a. in Großbritannien, Frankreich, Deutschland, Japan, Hong Kong und Kanada. F-Secure Corporation ist in über 80 Ländern mit Geschäfts- und Vertragspartnern sowie sonstigen Händlern vertreten. F-Secure-Produkte werden in mehr als 20 Sprachen übersetzt.

Software-Produkte von F-Secure haben international zahlreiche Auszeichnungen erhalten und wurden lobend erwähnt. In ihrer Ausgabe vom September 1998 zählte die Zeitschrift "Red Herring" F-Secure zu den Top 100-Technologieunternehmen der Welt. Die Computerzeitschrift "SECURE" bewertete F-Secure Workstation Suite 4.0 in der Ausgabe vom Juli 1999 mit fünf Sternen, der höchsten zu vergebenden Auszeichnung. In der Ausgabe vom Juli 1999 der deutschen Zeitschrift "PC Professionell" erhielt F-Secure Anti-Virus die Empfehlung der Redaktion. Zu den weiteren Auszeichnungen gehören: "Hot Product of the Year 1997" (Data Communications Magazine), "Best Anti-Virus Product" (SVM Magazine, Mai 1997) sowie der "European Information Technology Prize" 1996.

F-Secure Corporation verfügt über zehntausende Kunden in über 100 Ländern. Dazu zählen viele der weltweit größten Unternehmen und bekannte Telekommunikationsgesellschaften, wichtige internationale Fluggesellschaften, mehrere europäische Regierungen, Postunternehmen und Verteidigungsinstitutionen sowie mehrere Großbanken. Zu unseren Kunden gehören: NASA, die US-Luftwaffe, die medizinische Abteilung des US-Verteidigungsministeriums, US Naval Warfare Center, San Diego Supercomputer Center, Lawrence-Livermore National Laboratory, IBM, Unisys, Siemens-Nixdorf, EDS, Cisco, Nokia, Sonera (früher Telecom Finland), UUNet Technologies, Boeing, Bell Atlantic und MCI.

Die Produktfamilie von F-Secure

Alle F-Secure-Produkte sind im F-Secure-Verwaltungsrahmen integriert. Dieser bietet eine dreistufige, skalierbare Infrastruktur für die Verwaltung auf Richtlinienbasis, wodurch sich die Kosten der Sicherheitsverwaltung minimieren lassen.

F-Secure Workstation Suite bietet die Feststellung und Entfernung von Viren und bösartigen Codes, problemlose Datei- und Netzwerkverschlüsselung sowie persönliche Firewall-Funktionen – alles integriert in eine Verwaltungsarchitektur auf Richtlinienbasis.

F-Secure Anti-Virus, mit verschiedenen Scan-Modulen wie F-PROT und AVP, ist das umfassenste Echtzeitsystem zum Viren-Scannen und Viren-Schutz für alle bekannten Desktop- und Server-Plattformen. Diese dreistufige Lösung ist auf Firmenkunden zugeschnitten und umfasst zahlreiche Funktionen zur Netzwerkverwaltung und zur zentralen Nutzung von Ressourcen.

F-Secure Content Scanner schützt Netzwerke vor Viren, die über E-Mails, beim Herunterladen aus dem Internet und über die Verbreitung von Datenbanken in das Netzwerk gelangen. Das Programm kann mit Microsoft Exchange Server, Lotus Domino und Firewall-Programmen von Check Point und anderen führenden Herstellern betrieben werden.

F-Secure VPN+ bietet eine Software-basierte, IPSec-kompatible Lösung für virtuelle private Netzwerke im Rahmen von großen und kleinen Unternehmensnetzwerken sowie Fernnetzwerken. Durch die Kombination von F-Secure VPN+-Produkten können Unternehmen aller Größen mit Hilfe kostengünstiger Netzwerke oder des Internets sichere virtuelle private Netzwerke erstellen, ohne spezielle Hardware installieren zu müssen.

F-Secure FileCrypto ist das erste und bislang einzige Produkt, das eine zuverlässige Echtzeitverschlüsselung direkt in das Windows-Dateisystem integriert. Es verschlüsselt Daten automatisch, bevor sie auf der Festplatte gespeichert werden, und schützt dadurch wichtige Daten auch in heiklen Situationen. Mit Hilfe von FileCrypto können die Benutzer außerdem verschlüsselte, selbstextrahierende Pakete per E-Mail an andere Benutzer senden.

F-Secure SSH ermöglicht sichere Fernanmeldungs- sowie Terminal- und andere Verbindungen über ungesicherte Netzwerke. Es ist das am weitesten verbreitete Werkzeug für sichere Fernverwaltung.

F-Secure NameSurfer ist die Lösung für Internet- und Intranet-DNS-Verwaltung von einem entfernten Standort aus. Seine einfach zu verwendende WWW-Benutzerschnittstelle automatisiert und vereinfacht die DNS-Verwaltung.

F-Secure Distributed Firewall ist ein Software-basiertes Firewall-Programm, das von einer zentralen Arbeitsstation aus vollständigen Schutz für eine weitgehende dezentralisierte, mobile Arbeitswelt bietet.

Glossar

AUTOEXEC.BAT
BAT-Datei
BIOS
Bit
Booten
Boot-Sektor
Byte
CMOS
COM-Datei
CONFIG.SYS
CounterSign
CPU
CRC
DOS
Echtzeitscanner
EXE-Datei
Hintergrundaufgaben
HPFS
Kaltstart
Kilobyte
LAN
MBR
Megabyte
Modem
Multipartite-Virus
Mutationsvirus
NFS
NTFS
On-Access-Scanner
On-Demand-Scanner
Prüfsumme
RAM
Zugriffssteuerung
Zurücksetzen

Zugriffssteuerung

Verfahren, bei dem Benutzern oder Abläufen Zugriff auf das System gewährt oder verwehrt wird. Hierzu gehört gewöhnlich die Autorisierung des Benutzers, Überprüfung von Zugriffsrechten, Überwachung und Anmeldung.

AUTOEXEC.BAT

Die Befehlsdatei, die automatisch beim Systemstart in DOS ausgeführt wird.

Hintergrundaufgaben

Aufgaben, die ausgeführt werden, aber nicht im aktiven Fenster angezeigt werden.

BAT-Datei

Datei, in der DOS-Befehle verwendet werden, um sich wiederholende Aufgaben zu automatisieren.

BIOS

Basis-Eingang/Ausgang-System *(Basic Input/Output System)*. Der Teil des Betriebssystems, in dem die Mehrzahl der Hardware-spezifischen Aufgaben ausgeführt werden. Auf den meisten Computern ist das BIOS im ROM gespeichert.

Bit

Die kleinste Speichereinheit, die vom Computer erkannt werden kann. Mehrere Bits ergeben ein Byte. Sie werden in sequentiellen Mustern angeordnet, um Text, Zahlen oder andere detaillierte Informationen darzustellen.

Booten

Den Computer neu starten.

Boot-Sektor

Booten. Bereich, auf der ersten Spur einer Diskette oder eines logischen Datenträgers. Über Boot-Sektor-Informationen kann der Computer das Betriebssystem (beispielsweise MS-DOS) lesen.

Byte

Kleine Einheit einer Speichergröße, die zum Speichern eines Buchstaben oder einer Zahl ausreicht. Jedes Byte setzt sich aus Bits zusammen. Bits sind binäre Einheiten, die gruppiert werden (z. B. 00101101) und in denen die kleinsten Bruchteile an Informationen gespeichert werden.

Prüfsumme

Identifizierungsnummer, die aufgrund der Dateicharakteristika erstellt wird. Werden auch nur die geringsten Veränderungen an der Datei vorgenommen, ändert sich auch diese Nummer.

CMOS

Komplementärer Metalloxid-Halbleiter *(Complementary Metal Oxide Semiconductor)*. Der batteriebetriebene Speicher eines PCs. Dieser Speicher hat gewöhnlich eine Größe von zwischen 32 und 50 Byte. CMOS enthält Informationen über externe Informationen, wie beispielsweise Disketten, Daten und Peripheriegeräte. Solange die Batterie geladen ist, wird dieser Speicher beim Ausschalten des Computers nicht geleert.

Kaltstart

Neustart des Computers durch Aus- und Einschalten des Computers.

COM-Datei

Ausführbares DOS-Programm mit einfacher Struktur. Die maximale Größe beträgt 64 Kilobyte.

CONFIG.SYS

Über die Konfigurationsdatei wird das Programm beim Systemstart in DOS automatisch ausgeführt.

CounterSign

Kombination verschiedener Scan-Module, um den Schutz auf verschiedenen Ebenen und für alle denkbaren Komprimierungs- und Verschlüsselungsschemata zu gewährleisten, wodurch Unternehmen ein praktisch 100-prozentiger Virenschutz in einer einzigen Schnittstelle zur Verfügung steht.

CPU

Zentraler Prozessor *(Central Processing Unit)*. Das "Gehirn" des Computers. Er befindet sich normalerweise an einer Stelle, die unter Umständen nicht Teil des Monitors ist.

CRC

Zyklische Redundanzprüfung *(Cyclic Redundancy Check)*. Eine der beliebtesten Prüfsummenmethoden. Bei dieser Methode wird aus dem Dateiinhalt eine 32-Bit-Signatur berechnet.

DOS

Betriebssystem der Festplatte *(Disk Operating System)*. Die einfachste Systemart, die normalerweise für alle PCs verwendet wird.

EXE-Datei

Ausführbare Datei oder Programmdatei. Im Gegensatz zu Dokumenten- oder Datendateien eine Dateiart, die ausgeführt wird.

HPFS

Hochleistungs-Dateisystem *(High Performance File System)*. Dateisystem, das von OS/2 verwendet wird.

Kilobyte

1.024 Byte

LAN

Lokales Netzwerk *(Local Area Network)*. Kleines Netzwerk innerhalb eines Raums, Gebäudes oder einer Gruppe, das an das größere, weltweite Internet angeschlossen werden kann.

MBR

Haupt-Boot-Bereich *(Master Boot Record)*. Bereich, der sich auf der Nullspur von physischen Festplatten befindet. In ihm befindet sich das Haupt-Boot-Programm und die Partitionstabelle. Der Haupt-Boot-Bereich ist betriebssystemunabhängig und wird immer zuerst ausgeführt, sobald der Computer den Betriebsselbsttest durchgeführt hat (POST; *Power-On-Self-Test*). Die Größe des Haupt-Boot-Sektors beträgt 512 Byte. Das Haupt-Boot-Programm wandelt die Partitionstabelle, die Informationen zur Teilung (Partition) der physischen Festplatte enthält, in logische Einheiten um. Anschließend führt das Haupt-Boot-Programm den Boot-Sektor der aktiven Partition aus.

Megabyte

1.024 Kilobyte (eine Million Byte)

Modem

Hardware aus dem Bereich der Telefonie, das zum Anschluss eines Computers oder eines lokalen Netzwerks an ein größeres Netzwerk, wie beispielsweise das Internet, verwendet wird.

Multipartite-Virus

Virus, der aus mehreren Teilen besteht. Jeder Teil eines Multipartite-Virus muss bereinigt werden, um zu gewährleisten, dass keine Infektion mehr vorhanden ist.

Mutationsvirus

Virus, der sich von einer Host-Datei zur nächsten selbst verändert (mutiert), wodurch die Desinfektion zu einer ernsthaften Herausforderung wird.

NFS

Netzwerk-Dateisystem *(Network File System)*, das für viele UNIX-Systeme verwendet wird.

NTFS

Windows NT File System.

On-Access-Scanner

Echtzeitscanner, der im Hintergrund läuft und einen ständigen Virenschutz gewährleistet.

On-Demand-Scanner

Manuell zu startender Virusscanner.

RAM

Speicher mit Zugriff nach Wahl *(Random Access Memory)*. Ein dynamischer, von Prozessoren verwendeter Speicher.

Echtzeit-Scanner

Scanner, der im Hintergrund arbeitet, wodurch der Benutzer in normaler Geschwindigkeit weiterarbeiten kann und es zu keiner beträchtlichen Verlangsamung kommt.

Zurücksetzen

Warmstart des Systems.