perComp Verlag GmbH

F-PROT Antivirus™ für Unix
Linux / BSD / Solaris / AIX

Kurzeinführung

perComp Verlag GmbH

F-PROT Antivirus für Unix - Kurzeinführung, 2. Auflage

perComp-Verlag GmbH, Hamburg

Satz: perComp-Verlag GmbH

Druck: Druckhaus Mölln

Informationen und Hotline-Service:

perComp-Verlag GmbH, Holzmühlenstr. 84, D-22041 Hamburg

Telefon: +49 40 69628160, Telefax: +49 40 69628169

Web: http://www.percomp.de/f-prot

Information: info@percomp.de, Hotline: support-f-prot@percomp.de

Inhaltsverzeichnis

Einleitung

Besonders die freien Unix-Dialekte Linux und BSD erfahren eine kontinuierlich wachsende Akzeptanz und bieten eine beliebte Alternative zu proprietären Betriebssystemen wie Windows. Aufgrund dieser Beliebtheit zielen Viren-Schreiber inzwischen auch auf Unix-Systeme.

Häufig wird Unix als Server in einem Netzwerk mit Windows- oder Macintosh-Rechnern eingesetzt und von vielen Menschen benutzt, oft ohne dass sie es wissen. Wenn ein Netzwerk mit Windows-Rechnern von Unix-Servern als einzigem Kontakt zum Internet umgeben ist, ist es besonders wichtig, diese Unix-Server zu schützen.

FRISK Software International bietet angepasste und erweiterte Versionen seines bewährten F-PROT-Scanners für Unix-Plattformen an. F-PROT für Unix benutzt primär die F-PROT Scanning-Engine, hat aber zusätzlich ein heuristisches System integriert, um auch unbekannte MalWare zu finden. F-PROT Antivirus schützt vor Viren, Makro-Viren, Würmern, Trojanischen Pferden, Backdoors etc., die unter dem Begriff MalWare zusammengefasst werden.

Die verschiedenen F-PROT Antivirus-Produkte für Unix wurden für die möglichst effektive Entfernung von MalWare, die Workstations und Server unter Unix bedroht, entwickelt.

Der Weg, auf dem sich Computer am häufigsten MalWare zuziehen, ist E-Mail. F-PROT für Mail-Server kann beispielsweise mit Programmen anderer Hersteller wie Anomy oder AMaViS eingesetzt werden. Diese Programme wurden entwickelt, um die E-Mails direkt auf dem Mail-Server nach MalWare zu durchsuchen.

Ein anderer Weg, auf dem sich MalWare verbreiten kann, ist über Datei-Server. Samba ist eine beliebte Methode, um Windows-Clients an Linux-Datei-Server anzubinden. F-PROT für Linux kann benutzt werden, um Infektionen über den Datei-Server zu verhindern, so dass die Benutzer keine bösartigen Dateien vom Server herunterladen können.

Es ist sehr effektiv, MalWare auf dem Server zu bekämpfen, damit diese die Workstations gar nicht erst erreicht. Außerdem kann MalWare auf dem Server einfacher bekämpft werden, als wenn sie einzelne Systeme bereits infiziert hat.

Durch das einfache Zusammenarbeiten von F-PROT für Unix und Programmen anderer Hersteller können Benutzer eine sichere, aber flexible Umgebung für ihre Computer und Netzwerke aufbauen.

Die Hauptmerkmale von F-PROT für Unix:

- Erkennt über 135.000 bekannten Viren und ihren Varianten. (Stand: Dezember 2004)
- Entfernt Viren sicher, wenn eine Entfernung möglich ist, und beschädigt die Originaldateien nicht.
- Durchsucht Festplatten, CDs, Disketten, Netzlaufwerke, Verzeichnisse und einzelne Dateien.
- Sucht nach Images von Boot-Sektoren, Makro-Viren, Würmern, Trojanischen Pferden und anderer MalWare.
- Durchsucht komprimierte Archive und komprimierte ausführbare Dateien.

Plattformen

F-PROT für Unix Workstations

F-PROT Antivirus für Workstations schützt Arbeitsplatzrechner schnell und einfach.

Der Antivirus für Workstations enthält einen On-Demand-Scanner für die Kommandozeile oder Shell-Skripts. Zeitplangesteuerte oder manuelle Scans über einzelne Dateien oder ganze Dateisysteme sind möglich. MalWare wird erkannt und wenn möglich entfernt. Nach jedem Scan wird ein detaillierter Bericht über Virenfunde angezeigt. Mögliche unbekannte Bedrohungen werden mit Hilfe der Heuristik erkannt.

Die in dem Antivirus für Workstations enthaltenen Komponenten sind der Kommandozeilen-Scanner und der Updater.

Die unterstützten Plattformen sind Linux x86, BSD x86, Solaris x86 und Solaris SPARC. Auf IBM eServer xSeries (Intel/AMD) mit Linux läuft die Version für Linux x86.

F-PROT für Unix File-Server

F-PROT Antivirus für File-Server schützt Datei- und Anwendungsserver sehr performant.

File-Server brauchen einen robusten und schnellen Antivirus-Schutz. F-PROT für File-Server bietet hohe Performance. Sogar unbekannte Bedrohungen werden mit Hilfe der Heuristik erkannt.

Die File-Server-Version enthält sowohl den Kommandozeilen-Scanner als auch den Dämon-Scanner. Der Dämon-Scanner ist speicherresident und daher schneller als der Kommandozeilen-Scanner. Er kann in andere Programme integriert werden. Außerdem sind der Updater und unter Linux der Preloadable Library Call Wrapper enthalten.

Als Plattformen werden Linux x86, BSD x86, Solaris x86 und Solaris SPARC unterstützt. Auf IBM eServer xSeries (Intel/AMD) mit Linux läuft die Version für Linux x86. Für Linux auf IBM eServer zSeries und AIX auf IBM eServer pSeries steht die Version für Mail-Server zur Verfügung, die die Version für File-Server einschließt.

F-PROT für Unix Mail-Server

F-PROT Antivirus für Mail-Server schützt sehr performant ein- und ausgehende E-Mails auf Mail-Servern. Es werden alle verbreiteten Mail-Server wie Sendmail, Postfix und Qmail unterstützt.

Die Version enthält sowohl den Kommandozeilen-Scanner als auch den Dämon-Scanner. Der schnelle Dämon-Scanner wird über den Mail-Scanner und ggf. Plugins für das in-transit Mail-Scanning integriert. Außerdem sind der Updater und unter Linux der Preloadable Library Call Wrapper enthalten.

F-PROT Antivirus für Linux auf zSeries und F-PROT Antivirus für AIX enthalten den Anomy Sanitizer, einen regelbasierten E-Mail Content-Filter.

Die unterstützten Plattformen sind Linux x86, BSD x86, Solaris x86, Solaris SPARC, Linux auf IBM eServer zSeries und AIX auf IBM eServer pSeries. Auf IBM eServer xSeries (Intel/AMD) mit Linux läuft die Version für Linux x86.

Die Version für Mail-Server enthält die volle Funktionalität der Version für File-Server.

Einsatz und Lizenzierung

	Einsatz auf Workstation	Einsatz auf File-Server	Einsatz auf Mail-Server
F-PROT für Workstations	x	-	-
F-PROT für File-Server	x	x	-
F-PROT für Mail-Server	x	x	x

Module

Kommandozeilen-Scanner

Kommandozeilen-Scanner sind die unter Unix zurzeit am häufigsten verfügbaren Antivirus-Programme. Zusätzlich zu den grundlegenden Funktionen eines Virus-Scanners kann der F-PROT Kommandozeilen-Scanner mit Hilfe von Cron-Jobs termingesteuerte Scans durchführen. Der Kommandozeilen-Scanner kann mit Programmen anderer Hersteller benutzt werden, ist aber nicht so schnell wie der Dämon-Scanner. Der Kommandozeilen-Scanner ist einfach und sicher

und damit die ideale Lösung für kleine Unternehmen und Einzelplätze.

Dämon-Scanner

Der Dämon-Scanner unterscheidet sich von dem Kommandozeilen-Scanner dadurch, dass er die ganze Zeit läuft. Deshalb ist der Dämon-Scanner die beste Lösung für die Kombination mit Programmen anderer Hersteller, die einen ständig aktiven Scanner erfordern.

Mit anderen Programmen kommuniziert der Dämon-Scanner über normale, standardisierte HTTP-Requests über ein lokales TCP/IP-Socket und antwortet auf jeden Scan-Auftrag mit einem detaillierten, XML-formatierten Bericht über Virenfunde.

Technische Informationen

Der Dämon bindet sich an einen Loopback-Port. Um den Dämon aufzufordern, eine Datei zu scannen, wird ein HTTP-GET-Request an den aktiven Port geschickt. Dieser Request enthält den kompletten Pfad der zu scannenden Datei. Der Scanner kennt die meisten Parameter so wie der Kommandozeilen-Scanner. Die Parameter müssen aber als ordnungsgemäße HTTP-Requests kodiert sein, gefolgt von einem Fragezeichen und dem Dateinamen.

Der Dämon aktualisiert sich selbst, indem er sein eigenes Binary ausführt, wenn eine neue Version eingetroffen ist. Die neu ausgeführte Kopie muss sich einen neuen Port nehmen, weil der alte Prozess noch etwa eine halbe Minute auf dem alten Port weiterarbeitet, damit immer mindestens ein Dämon verfügbar ist. Die Clients müssen ausprobieren, auf welchem der angegebenen Ports ein Dämon arbeitet, wenn der bisher benutzte nicht mehr verfügbar ist.

Updater

Der Updater dient dem automatischen Aktualisieren der Virus-Definitionen.

Ein Skript prüft über das Internet, ob neue Virus-Definitionen verfügbar sind. Wenn dies zutrifft, lädt es diese herunter und installiert sie.

Normalerweise wird der Updater bei der Installation in die Cron-Tabelle eingetragen.

Preloadable Library Call Wrapper

Dieser Wrapper ergänzt unter Linux den Dämon-Scanner. Er verpackt bestimmte Bibliothekaufrufe zum Öffnen von Dateien, um die Dateien vor dem Zugriff zu scannen.

So kann beispielsweise ein Echtzeitschutz für einen Samba- oder FTP-Server mit dem Wrapper realisiert werden.

Technische Informationen

Der Wrapper exportiert Symbole für verschiedene Funktionen, die zum Öffnen von Dateien benutzt werden können. Diese Symbole scannen die Dateien mit dem Dämon-Scanner. Es wird für jede Datei ein Socket geöffnet und eine Verbindung mit dem Dämon-Scanner hergestellt. Nach dem Scannen wird je nach Ergebnis die Originalfunktion aufgerufen oder der Zugriff auf die Datei nicht gewährt, indem EACCES (Zugriff verweigert) zurückgegeben wird. Eine Protokollierung erfolgt über den syslogd.

Der Zweck des Wrappers ist, dass Dateien, auf die das System zugreift, gescannt werden. Entweder alle Programme oder auch nur einzelne können so geschützt werden. Für den Betrieb des Wrappers müssen die Programme dynamisch gelinkt sein.

Mail-Scanner

Der Mail-Scanner scannt E-Mails auf einem Mail-Server. Er unterstützt alle verbreiteten Mail-Server wie Sendmail, Postfix und Qmail.

Das Skript benutzt die Anomy Mailtools, um E-Mails zu verarbeiten. Es extrahiert den Nachrichtenkörper und die Attachments und scannt sie mit Hilfe des Dämon-Scanners.

Wenn eine Infektion entdeckt wird, versucht der Mail-Scanner, die Bedrohung zu neutralisieren. Falls desinfiziert werden kann, wird die gereinigte Mail zugestellt. Nicht desinfizierbare Teile werden entfernt und eine entsprechende Nachricht an die Mail angehängt.

Der folgende Header wird in saubere E-Mails eingefügt:

"X-Antivirus: Scanned by F-Prot Antivirus (http://www.f-prot.com)".

Plugin

Zusätzlich zu dem Mail-Scanner werden für einige Mail-Server Plugins für das in-transit Mail-Scanning geliefert.

Anomy Sanitizer

Der Anomy Sanitizer ist ein freier, regelbasierter E-Mail Content-Filter. Informationen hierzu finden Sie unter

http://mailtools.anomy.net

Installation

Die minimalen Systemvoraussetzungen sind die folgenden:

	Linux x86	BSD x86	Solaris x86	Solaris SPARC
Prozessor	Intel Pentium- oder AMD K5			SPARC
Betriebs-system	SuSE, Red Hat, Debian etc.	FreeBSD, NetBSD oder OpenBSD	Solaris 9.0	
Speicher	10 MB freier Speicher auf der Festplatte			
Perl-Interpreter	Perl-Interpreter 5.8			

Zur Installation können Sie das mitgelieferte Installationsskript aufrufen oder je nach Plattformen die folgenden Installationspakete verwenden:

- RPM-Paket
- DEB-Paket
- GZIPptes TAR-Archiv

Eine spezifische Beschreibung der Installation finden Sie in dem HTML-Handbuch (s. u.)

Es wird sehr empfohlen, das HTML-Handbuch und die Text-Dateien README und CHANGES zu beachten, unter anderem auch die aktuellen Hinweise und Änderungen.

Aktualisierung der Virus-Signaturen

Für einen möglichst umfassenden Schutz vor Viren ist es nicht nur wichtig, dass stets die aktuelle Version von F-PROT eingesetzt wird, sondern auch, dass die Virus-Signaturen immer aktuell gehalten werden.

Die Virus-Signaturen können mit Hilfe des Updaters automatisch aktualisiert werden. Wenn dieses Skript neue Virus-Signaturen findet, lädt es diese herunter und installiert sie.

Eine englische Beschreibung der Aktualisierung finden Sie unter

http://www.f-prot.com/support/unix/updating.html

Weitere Informationen

Wir empfehlen Ihnen unbedingt, sich mit der Dokumentation zu den Produkten, die Sie einsetzen möchten, vertraut zu machen.

Handbücher

Die englischen Handbücher für alle Unix-Versionen finden Sie unter

http://www.f-prot.com/support/helpfiles/unix

Zusätzlich finden Sie das jeweilige Handbuch auf der CD und in dem Installationspaket unter

/doc_xx/index.html

Man-Pages

Die aktuellen englischen Man-Pages für die Komponenten Kommandozeilen-Scanner, Dämon-Scanner, Updater, Mail-Scanner, Plugins für den Mail-Scanner und Preloadable Library Call Wrapper- finden Sie unter

http://www.f-prot.com/support/unix/unix_manpages

Text-Dateien

Diese Text-Dateien finden Sie im Stammverzeichnis der CD und in dem Installationspaket.

- README – Anweisungen für die Programmversion
- CHANGES – Letzte Änderungen und behobene Fehler
- LICENSE – Lizenzinformationen

Häufige Fragen (FAQ)

Die englische FAQ des Herstellers ist erreichbar unter

http://www.f-prot.com/support/unix/unix_faq

Virus-Datenbank

Die Virus-Datenbank des perComp-Verlags ist die umfangreichste deutschsprachige:

http://www.percomp.de/virinfo

Die englische Virus-Datenbank des Herstellers:

http://www.f-prot.com/virusinfo

Support

Informationen und News finden Sie auf der Website des perComp-Verlags unter

http://www.percomp.de

Technische Informationen zu F-PROT für Unix finden Sie unter

http://www.percomp.de/f-prot

oder auf englisch beim Hersteller unter

http://www.f-prot.com/support/unix

Bei allgemeinen Fragen wenden Sie sich bitte per E-Mail an

info@percomp.de

oder telefonisch

+49 40 696 28 16 - 0

oder per Fax

+49 40 696 28 16 9

Wenn Sie F-PROT für Linux direkt oder indirekt über den perComp-Verlag bezogen haben, können Sie bei technischen Fragen direkt die F-PROT-Hotline des perComp-Verlags am besten per E-Mail unter

support-f-prot@percomp.de

oder telefonisch unter

+49 40 696 28 16 – 16

erreichen. Sonst wenden Sie sich bitte an Ihren Händler.

Wir wünschen Ihnen viel Erfolg beim Einsatz von F-PROT für Linux.