Virenerkennung mit Sophos Anti-Virus: Ein technischer Überblick

Katherine Carr, Sophos, Oxford, UK

Oktober 2002

ÜBERSICHT

Dieses White Paper beschreibt die Hauptkomponenten von Sophos Anti-Virus und wie sie zueinander in Beziehung stehen. Es erläutert die Virenüberprüfung, Erkennungsmethoden und die Erstellung von Virenbeschreibungen. Nach einer Erläuterung, was bei einem Virenfund passiert, folgt eine Aufstellung der Vorteile der Sophos-Technologie.

Hinweis: Die exakten Arbeitsmethoden von Sophos Anti-Virus sind von Plattform zu Plattform verschieden. Sofern nicht anders angegeben, bezieht sich die in diesem White Paper erläuterte Technologie auf Windows 32-Plattformen.

Sophos Anti-Virus bietet plattformübergreifend Virenschutz, Virenerkennung und Desinfektion auf Servern, Desktops und Laptops. Mobile Geräte sind während der Synchronisation geschützt.

Hauptkomponenten von Sophos Anti-Virus

Sophos Anti-Virus basiert auf von Sophos eigens entwickelter Software.

Sophos Anti-Virus besteht aus zwei hauptsächlichen Komponenten, beide werden von Sophos entwickelt und gewartet:

- **Eine Virus Detection Engine**, die Dateien auf Viren, Trojanische Pferde und Würmer überprüft (in diesem White Paper wird weitestgehend der Begriff "Virus" für Malware jeglicher Art verwendet),
- **InterCheck-Technologie** filtert Dateien während des Zugriffs, um festzustellen, ob sie auf Viren überprüft werden müssen, und verfügt über Funktionen für zentrale Benachrichtigungen.

Virus Detection Engine

Die Sophos Virus Detection Engine bildet den Kern von Sophos Anti-Virus. Auf allen Plattformen wird dieselbe Virus Detection Engine verwendet, die eine eigens entwickelte Struktur ähnlich wie das COM (Component Object Model) von Microsoft besitzt und aus mehreren Objekten mit klar definierten Schnittstellen besteht. Das modulare Dateisystem der Engine basiert auf einzelnen abgeschlossenen Dynamic Libraries, wobei jede eine andere "Storage Class", d.h. einen anderen Dateityp, bearbeitet. Durch diese Methode können Virenüberprüfungen für generische Datenquellen, unabhängig vom Typ, durchgeführt werden.

Mit einer spezialisierten Technologie für das Laden von und das Suchen nach Daten kann die Engine hohe Geschwindigkeiten erreichen. Sie verfügt dabei über:

- einen kompletten Code-Emulator zum Erkennen von polymorphen Viren,
- einen Online-Dekompressor für die Überprüfung von Archivdateien,
- eine OLE2 Engine für die Erkennung und die Desinfektion von Makroviren.

Die Virus Engine ermöglicht umfassenden plattformübergreifenden Schutz.

In den meisten Versionen von Sophos Anti-Virus, MailMonitor und in allen Drittanwendungen ist die Virus Engine mit SAV Interface integriert. Sophos Anti-Virus für Windows, NetWare und DOS sprechen die Virus Engine derzeit direkt an.

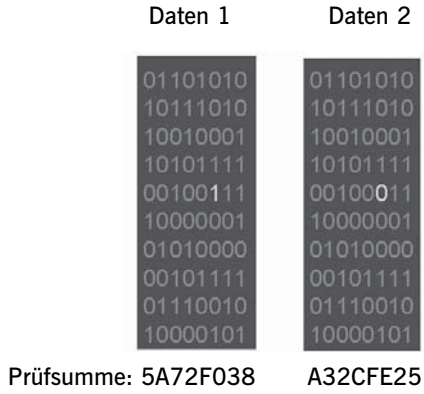
InterCheck-Technologie

Die einzigartige InterCheck-Technologie von Sophos ermöglicht On-Access-Überprüfungen.

InterCheck ist die patentierte Technologie von Sophos, die für eine optimale On-Access-Virenerkennung - speziell in Netzwerkumgebungen - entwickelt wurde. Da sie die Anzahl der notwendigen Virenüberprüfungen für jede Datei minimiert, ist sie einzigartig. Dabei werden alle Dateien, während auf sie zugegriffen wird, gefiltert und nur die Dateien zur Überprüfung an die Engine geschickt, die möglicherweise einen Virus enthalten. Das dabei von InterCheck angewandte Prinzip heißt Prüfsumme.

Prüfsumme

Beim Erstellen von Prüfsummen wird aus einer Bytefolge eine Zahl erzeugt. InterCheck errechnet diesen Wert mit Hilfe eines sicheren und eigens entwickelten Algorithmus. Mit der Prüfsumme für eine Datei kann diese eindeutig identifiziert und festgestellt werden, ob die Datei verändert wurde. Der Vorteil dieser Methode: Auch wenn sich nur ein einziges Bit in einer Datei ändert, verändert sich die Prüfsumme deutlich, wie das folgende Beispiel veranschaulicht:



Die Veränderung von 1 Bit führt zu verschiedenen Prüfsummenwerten.

Wenn auf eine Datei zugegriffen wird - von einem Benutzer, einem Betriebssystem usw. - fängt InterCheck die Zugriffsanfrage ab und errechnet eine Prüfsumme für die Datei. Wenn die Datei nicht verändert wurde, seit sie das letzte Mal von InterCheck gefiltert wurde, stimmt die vorhandene Prüfsumme mit der bereits vorhandenen überein und der Zugriff wird gewährt. Wenn die Datei **verändert wurde**, oder wenn es sich um eine neue Datei handelt, wird eine Kopie an die Virus Detection Engine zur Überprüfung gesendet. Sobald sich eine Datei ändert, ist ihre Prüfsumme ungültig und es wird eine neue erstellt, nachdem die Datei überprüft und festgestellt wurde, dass sie virenfrei ist.

Wenn in der Datei ein Virus gefunden wird, verhindert InterCheck, dass die Datei geöffnet wird. Wenn die Datei gerade geschlossen werden soll, wird sie geschlossen, wenn sie jedoch geöffnet werden soll, wird dies durch InterCheck verhindert. Zusätzlich erzeugt InterCheck beim Schließen der Datei eine Virenbenachrichtigung.

Die Prüfsummen werden in einer Datenbank gespeichert. Wenn eine neue Virenkennungsdatei (IDE) hinzugefügt wird (siehe unten), wird die Prüfsummendatenbank gelöscht. Dies ist eine reine Vorsichtsmaßnahme: Nehmen wir an, eine Datei mit einem neuen Virus wurde geöffnet, bevor die Virenkennungsdatei, die den Virus erkannt hätte, heruntergeladen wurde - die Datei wäre als virenfrei durchgegangen und es wäre eine Prüfsumme für diese Datei erstellt worden. Durch das Löschen der Prüfsummendatenbank stellt InterCheck beim nächsten Versuch die Datei zu öffnen fest, dass es keine übereinstimmende Prüfsumme gibt, und sendet die Datei dann erneut an die Virus Detection Engine, wo sie gegen alle neuen (und früheren) Virenkennungen geprüft wird. Wenn die Datei keinen Virus enthält, wird eine neue Prüfsumme erstellt und die Datei kann geöffnet werden.

Durch die hohe Geschwindigkeit, mit der Prüfsummen erstellt werden, wird die Systemleistung nicht beeinträchtigt.

Es sollte nicht unerwähnt bleiben, dass das Löschen und Neu-Erstellen der Prüfsummendatenbank extrem schnell vonstatten geht und nur einen geringen Einfluss auf die Leistung des Computers hat, so dass der Anwender gar nicht merkt, dass etwas passiert.

Mit Hilfe von Prüfsummen erkennt InterCheck, ob eine Datei verändert wurde - nicht, ob sie einen Virus enthält.

Es ist wichtig zu betonen, dass Sophos das Prüfsummenverfahren nur verwendet, um festzustellen, ob eine Virenüberprüfung für eine bestimmte Datei notwendig ist oder nicht, d.h. ob sie verändert wurde. Mit Prüfsummen wird nicht festgestellt, ob eine Datei einen Virus enthält oder nicht.

Die Beziehung zwischen Virus Detection Engine und InterCheck

In einer typischen Konfiguration befinden sich auf den einzelnen Desktops sowohl die Virus Detection Engine als auch InterCheck.

Wie bereits gesagt, führt die Virus Detection Engine den eigentlichen Überprüfungsvorgang bei den Dateien durch. Wenn sie eine On-Demand- oder eine zeitgesteuerte Überprüfung durchführt, überprüft sie alle in den Konfigurationseinstellungen angegebenen Dateien, InterCheck fängt diese Dateien während der Überprüfung nicht ab. InterCheck kommt erst ins Spiel, wenn versucht wird, die Datei zu öffnen, und InterCheck die Dateien zur Überprüfung an die Engine sendet. In dieser Funktion wird InterCheck auch “InterCheck-Client” genannt.

Der InterCheck-Client kann auch auf einem Server laufen, wo es besonders nützlich ist, sich vor Würmern zu schützen, die nach Windows-Netzwerkfreigaben suchen und sich dort speichern. Sophos empfiehlt den InterCheck-Client auf dem Server zu installieren, ihn aber aus Leistungsgründen standardmäßig auf “inaktiv” zu stellen. Wenn ein sich schnell verbreitender Wurm, wie z. B. Nimda, auftritt, kann InterCheck auf dem Server einfach auf “aktiv” gestellt werden.

Der InterCheck-Server ermöglicht Reports und Benachrichtigungen bei Virenvorfällen.

InterCheck kann sich auch als “InterCheck-Server” auf einem Server befinden. In dieser Funktion stellt er eine Kommunikationszentrale dar, die Reports über Virenvorfälle im gesamten Netzwerk empfängt und protokolliert sowie Alarmmeldungen an Administratoren und/oder Einzelne bzw. Gruppen sendet.

Sophos Anti-Virus für Unix verfügt nicht über den InterCheck-Client, aber über den InterCheck-Server für zentrale Meldungen und Benachrichtigungen.

Virenüberprüfungen

Der Dateityp legt fest, was und welcher Bereich einer Datei überprüft wird.

Verschiedene Virentypen verbergen sich auf unterschiedliche Weise und an unterschiedlichen Orten. Wo in einer Datei die Virus Detection Engine nach einem Virus sucht, hängt also von dem jeweiligen Dateityp ab. Wenn es sich bei der Datei beispielsweise um ein Programm handelt, untersucht die Engine den Header, in dem steht, wo der Programmcode beginnt, und sieht dort nach. Wenn es sich bei der Datei um ein Word-Dokument handelt, sucht die Engine nach den Makro Streams. Wenn es sich um eine MIME-Datei handelt, d.h. das Format, das für die Übertragung von E-Mails verwendet wird, sucht sie nach dem Ort, an dem das Attachment gespeichert ist.

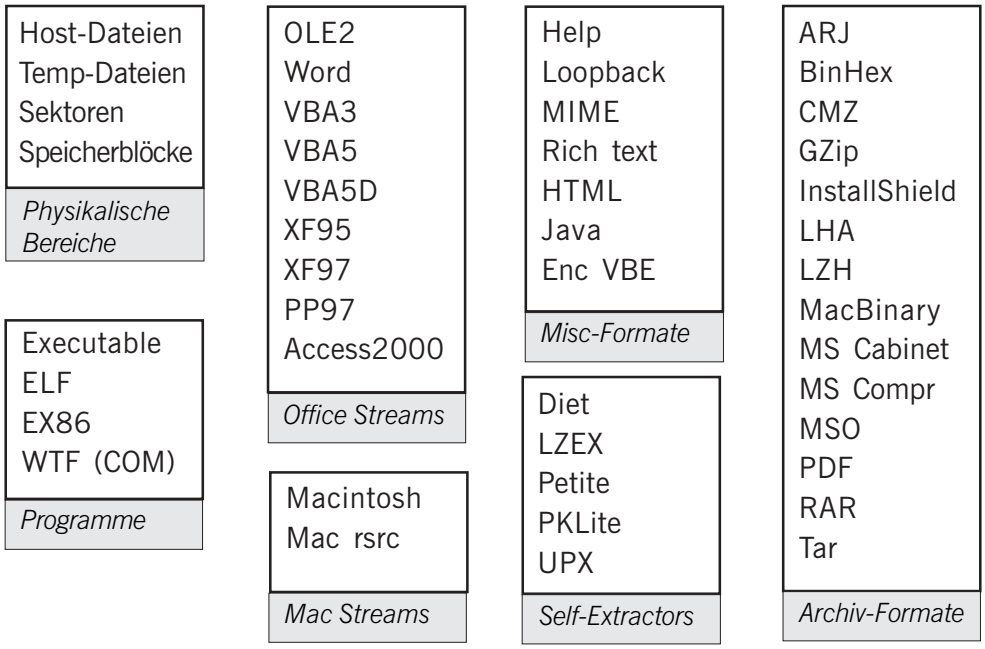
Die Überprüfungsfunktion der Engine wird von einer leistungsstarken Kombination aus zwei wichtigen Komponenten geregelt: einem Classifier, der weiß, wo er nachsehen muss, und der Virendatenbank, die weiß, wonach sie schauen muss. Die Engine klassifiziert die Datei nach dem Typ anstatt sich auf deren Erweiterung zu verlassen.

Was wird überprüft?

Die Virus Detection Engine kann annähernd eine unbegrenzte Zahl verschiedener Dateitypen überprüfen. In der Realität müssen aber nicht alle Dateitypen überprüft werden, da einige, z. B. ASCII-Textdateien, keine Viren enthalten können.

InterCheck analysiert die Dateiformate, um festzustellen, ob sie überprüft werden müssen, er verlässt sich dabei nicht auf die Dateierweiterungen. Dadurch wird ein Word-Dokument namens datei.inv als Word-Dokument überprüft.

Die Abbildung zeigt Beispiele für verschiedene Dateitypen, die die Engine überprüft.



Beispiele für Dateitypen, die von Sophos Anti-Virus überprüft werden

Die Liste der Dateitypen, die überprüft werden, wird kontinuierlich aktualisiert, da auch neue Dateitypen von Viren infiziert werden können. Im Konfigurationsfenster von Sophos Anti-Virus finden Sie eine Liste mit allen Dateitypen, die als potentielle Träger von Viren bekannt sind und in der Benutzer wählen können, welche Dateitypen in der Überprüfung eingeschlossen oder ausgeschlossen werden sollen.

Liste der Ausführbaren Dateien von Sophos Anti-Virus

Anwender können auch bestimmte Dateien **ausschließen**, um Konflikte zwischen der Überprüfung und anderen Anwendungen zu verhindern.

Überprüfung von anderen Objekten

Speicherüberprüfungen

Grundsätzlich überprüft Sophos Anti-Virus Dateien immer, wenn sie auf einem Datenträger geöffnet werden.

Sophos Anti-Virus kann auf DOS- und Windows 9x-Plattformen Speicherüberprüfungen durchführen. Die meisten Dateien werden auf Datenträgern gespeichert, so sind Anwender anderer Windows-Plattformen trotzdem geschützt, da InterCheck die Datei abfängt und zur Überprüfung schickt, sobald der Anwender die Datei speichern will. Auf Mac-, OS/2- und NetWare-Plattformen wird jeder Virus erkannt, sobald versucht wird, die gespeicherte Datei von dem Datenträger zu öffnen.

E-Mail-/Internet-Überprüfung

Die grundlegenden Prinzipien von Sophos Anti-Virus, die zuvor beschrieben wurden (die Virus Detection Engine überprüft Dateien auf dem Datenträger und InterCheck fängt Dateien ab, wenn sie von dem Datenträger geöffnet werden), gelten auch für E-Mails und Webseiten. Dabei handelt es sich ebenfalls um Dokumente, die auf den ersten Blick allerdings nicht "von einem Datenträger" geöffnet werden. Was passiert, wenn eine E-Mail geöffnet oder auf eine Webseite zugegriffen wird, bestimmt der Browser. Die meisten Browser schreiben alles auf einen Datenträger, wie z. B. den Inhalt einer Webseite, bevor sie geöffnet wird (auch wenn es für die Anwender scheint, dass sie lediglich E-Mail-Text oder eine Webseite lesen). Alle Viren, die von einem Skript abgelegt oder als Teil einer ActiveX-Steuerung heruntergeladen werden, werden von InterCheck aufgegriffen, sobald ein Zugriffsversuch erfolgt.

Bootsektorüberprüfung

Während des Bootens werden Bootsektorviren von On-Access-Scannern nicht gefiltert und aufgegriffen aus dem einfachen Grund, dass der Computer bootet, bevor alle anderen Programme, einschließlich InterCheck, gestartet werden. (Bootsektoren auf Festplatten und Disketten **werden überprüft**, wenn auf sie nach dem Bootvorgang zugegriffen wird.) Wenn der Computer von einer infizierten Diskette gebootet wird, wird er infiziert. Während der nächsten On-Demand- oder zeitgesteuerten Überprüfung wird der Virus dann entdeckt. Die Bedrohung ist nicht sehr groß, da sich Bootsektorviren nicht unter Windows NT verbreiten.

Überprüfungsmodus

Die Engine kann im ausführlichen oder im normalen Modus gestartet werden. Bei beiden Modi werden alle Dateitypen überprüft, die möglicherweise Viren in sich tragen können. Der normale Modus verwendet einen VDL-Interpreter (siehe unten), um die Bereiche zu durchsuchen, in denen es am wahrscheinlichsten ist, dass sich dort ein Virus aufhält. Der ausführliche Modus dauert ca. doppelt so lange wie der normale Modus. Er verwendet dieselben Methoden wie der normale Modus und kombiniert diese mit anderen Verfahren. In diesem Modus sucht die Engine beispielsweise nach strikten Mustern anstatt nach Dateitypen und deckt so auch Dateitypen ab, die keine wirkliche Bedrohung darstellen. Wenn ein bestimmter Dateityp einer Bedrohung durch Viren ausgesetzt ist, fügt Sophos diesen zu der Liste der im normalen Modus überprüften Dateien hinzu.

Erkennungsmethoden

Die Engine verwendet verschiedene Überprüfungsmethoden, abhängig vom Dateityp.

Wie Viren erkannt werden, hängt vom jeweiligen Dateityp ab. Während des Überprüfungsvorgangs analysiert die Engine jede Datei, identifiziert deren Typ und wendet dann die entsprechende Methode an. Allen Methoden liegt das Prinzip zugrunde, dass nach bestimmten Befehlstypen oder nach bestimmten Anordnungen von Befehlen gesucht wird.

Übereinstimmung von Mustern

Bei der Methode der übereinstimmenden Muster kennt die Engine die jeweilige Codefolge und sucht nach einer genauen Übereinstimmung, die den Code als Virus identifiziert. Meist sucht die Engine nach Codesequenzen, die den Sequenzen des Virencodes ähneln, aber nicht notwendigerweise identisch mit ihm sind. Beim Erstellen von Kennungen, mit denen Dateien während der Überprüfung verglichen werden, sind die Virenforscher bei Sophos bemüht, den Kennungscode so allgemein wie möglich zu halten, so dass - mit Hilfe von Heuristiken, wie unten erläutert - die Engine nicht nur den originalen Virus, sondern auch spätere Varianten entdecken kann.

Heuristik

Die Virus Detection Engine kann grundlegende Methoden der Musterübereinstimmung mit Heuristik - eine Methode, bei der anstelle von bestimmten Regeln, allgemeine Regeln verwendet werden - kombinieren, um mehrere Viren derselben Familie zu erkennen, auch wenn Sophos-Forscher eventuell erst einen Virus dieser Familie analysiert haben. Mit dieser Methode kann eine einzige Virenkennung erstellt werden, die mehrere Varianten eines Virus erkennen kann. Sophos kombiniert seine Heuristik mit anderen Methoden und minimiert so die Anzahl von Fehlalarmen.

Emulation

Emulation ist ein Verfahren, das die Virus Detection Engine bei polymorphen Viren anwendet. Der Emulator innerhalb der Virus Detection Engine wird in DOS- und Windows-Programmen verwendet, während polymorphe Makroviren durch Erkennungscode entdeckt werden, der in der von Sophos entwickelten Virus Description Language (VDL) geschrieben ist (siehe unten).

Polymorphe Viren sind verschlüsselte Viren, die sich selbst verändern, um sich so zu verbergen. Es gibt keinen sichtbaren konstanten Virencode und der Virus verschlüsselt sich bei jeder Verbreitung anders. Wenn er gestartet wird, entschlüsselt er sich. Erst nach der Entschlüsselung zeigt sich der **wirkliche** Virencode, der von der Sophos Virus Detection Engine nach dem Start des Emulators erkannt wird.

Programme, die an die Engine zur Überprüfung gesandt werden, werden in dem Emulator gestartet, der die Entschlüsselung des Virenstamms speichert, wenn sie in den Speicher gelesen wird. Normalerweise befindet sich der Eintrittspunkt für einen Virus am vorderen Ende eine Datei und startet als erstes. In den meisten Fällen muss nur ein kleiner Teil des Virus entschlüsselt werden, damit er erkannt wird. Die meisten virenfreien Programme stoppen den Emulator nach nur ein paar Anweisungen, wodurch die Systembelastung eingeschränkt wird.

Da der Emulator in einem begrenzten Bereich läuft, wird der Computer nicht infiziert, sollte sich der Code als Virus entpuppen.

Virenbeschreibungen

Sophos tauscht jeden Monat Viren mit anderen vertrauenswürdigen Antiviren-Herstellern aus. Außerdem senden Kunden uns jeden Monat tausende verdächtiger Dateien, von denen ca. 30 % tatsächlich Viren enthalten. Jede verdächtige Datei wird einer strengen Analyse in den sicheren Virenlaboren unterzogen, um festzustellen, ob es sich um einen Virus handelt oder nicht. Für jeden neu entdeckten Virus oder jede neue Virengruppe erstellt Sophos eine Kennung.

Analyse einer verdächtigen Datei

Die komplexe Aufgabe der Virenanalyse wird von Virenexperten bei Sophos ausgeführt.

Viren können - abhängig von dem jeweiligen Virus - auf verschiedenen Wegen analysiert werden. Es gibt viele von Sophos entwickelte Standard-Tools, mit deren Hilfe Virenforscher eine Datei auseinander nehmen, aber der wichtigste Faktor ist immer noch das Fachwissen unserer Forscher. Allgemein gesprochen werden folgende Schritte, häufig in Kombination, ausgeführt:

1. Der Virus wird repliziert und die Replikanten auf Standard-"Goat"-Dateien gestartet (der Begriff bezieht sich auf "sacrifical goat"=Opferlamm), deren Inhalt und Betriebsart bekannt sind.
2. Der Code wird analysiert.
3. Es wird eine Virenkennungsdatei für die Erkennung/Desinfektion erzeugt, wie nachfolgend erläutert.
4. Funktionstüchtigkeit von Erkennung und Desinfektion wird auf allen Plattformen und unter allen Bedingungen getestet. Im Falle von polymorphen Viren erzeugt der Forscher tausende infizierter Testdateien, um sicher zu prüfen, dass die Erkennung korrekt funktioniert.

Beispiel für eine Virenbeschreibung

Die Virenbeschreibung enthält den Namen des Virus, Eigenschaften, Kommentare und eine komplette Definition darüber, wie der Virus und/oder seine Varianten erkannt und desinfiziert werden können. Sie kann außerdem die Auslösebedingungen enthalten. Unter Umständen sind mehrere Kennungen notwendig, wenn der Virus verschiedene Formen annehmen kann. Die Virenbeschreibung kann auch nur aus einer einfachen Folge von Hexadezimalbytes bestehen, die ein Muster darstellen, mit dem der Virus identifiziert wird. Andere wiederum können weitaus komplizierter sein.

So könnte eine einfache Virenbeschreibung aussehen:

Name	`#Bleah-C ; Bleah-c, cmg970206`
Segmentstart	`{ ;MBR,DBR`
	`<identity code inserted here>`
Segmentende	`}`
Virentyp	`W { MRIi }`
Muster	`P { bb00 0283 f901 757b 0af6 7577 3d01 0374 593d 0102 756d 9cff }`
Entdeckungs-datum	`D { Nov 1996 }`

VDL und Virenkennungsdateien (IDEs)

VDL

Virenbeschreibungen werden in einer von Sophos entwickelten Programmiersprache geschrieben.

Virenbeschreibungen werden in der von Sophos entwickelten, vorkompilierten Programmiersprache VDL (Virus Description Language) geschrieben. Die Engine führt das VDL-Programm auf einem virtuellen Computer aus. Die Vorteile von VDL liegen in ihrer Erweiterbarkeit und Flexibilität.

Die Beschreibungen aller Viren werden in eine Datendatei namens VDL.DAT geschrieben, die jeden Monat neu erstellt wird. Derzeit gibt es ca. 30.000 kompilierte Beschreibungen, die mehr als doppelt so viel Viren erkennen. VDL.DAT ist komprimiert, verschlüsselt und befindet sich innerhalb einer eigenen Datenbankstruktur.

IDEs

Wenn der Virus als ernsthafte Bedrohung angesehen wird (wenn er sich "in the wild" befindet, oder wenn eine Datei mit diesem Virus von einem Kunden an Sophos gesandt wurde), wird eine einzelne Virenkennungsdatei (IDE) erstellt. Die IDE enthält in einfachem ASCII-Format kodierte VDL für einen Virus oder eine Virenfamilie. Zum Beispiel erkennt die IDE für W32/Frethem-Fam 14 E-Mail-fähige Würmer einer Virenfamilie. IDEs können in den Sophos Anti-Virus Programmordner des Anwenders manuell oder automatisch durch Enterprise Manager von Sophos hinzugefügt werden. Sie ermöglichen Erkennung und Desinfektion des entsprechenden Virus oder der entsprechenden Virenfamilie, bis die nächste VDL.DAT erstellt wurde. Dann sind dort die Daten der IDE enthalten.

IDEs können auch als druckbarer Hexadezimalcode erstellt und per Fax oder Telefon übertragen werden. Normalerweise aber werden IDEs von der Sophos Website heruntergeladen.

VDL-Daten im Speicher

Das Prinzip, mit dem die Virus Detection Engine die VDL-Daten im Speicher organisiert und durch das ein Maximum an Effizienz erreicht wird, sind verschiedene standardmäßige Hashing-Methoden.

Durch die verwendeten Methoden - kombiniert mit der Effizienz der InterCheck-Technologie - ist die Anzahl der Viren, die Sophos Anti-Virus verarbeiten kann, nicht strukturell begrenzt. Sie stellen außerdem sicher, dass auch mit einer zunehmenden Anzahl Viren die Überprüfungsgeschwindigkeit konstant bleibt.

Wenn ein Virus gefunden wird

Sophos Anti-Virus verhindert, dass infizierte Dateien geöffnet werden, desinfiziert diese oder löscht sie - je nachdem, was der Anwender angegeben hat.

Wie schon im Abschnitt über InterCheck oben beschrieben, verhindert Sophos Anti-Virus, dass bei einem Virenfund die infizierte Datei geladen, geöffnet oder aktiviert werden kann. Neben obligatorischen Funktionen, wie zu verhindern eine Datei zu öffnen, gibt es viele Optionen, z. B. wer benachrichtigt werden soll, ob desinfiziert werden soll oder nicht, die am besten über die Sophos Anti-Virus GUI eingestellt werden können.

Desinfektion

Wenn die automatische Desinfektion aktiviert ist, säubert Sophos Anti-Virus jede Datei, in der ein Virus gefunden wurde. Die Datei kann ohne Gefahr geöffnet werden. Welche Maßnahme dann ergriffen wird, hängt von dem jeweiligen Virus ab. Im Falle eines Makrovirus entfernt die Engine lediglich das Makro. Wenn InterCheck dann die Vorlage erhält, d. h. wenn der Anwender ein neues Dokument öffnet/erstellt, werden andere Makros in der Vorlage ebenfalls entfernt.

Bei der Desinfektion kann es jedoch Grenzen geben, da es nicht immer möglich ist, eine Datei wieder in ihren Ursprungszustand zu bringen. Einige Viren überschreiben Teile des Ausführungsprogramms, die nicht wiederhergestellt werden können. In diesem Fall ist es am sichersten, wenn der Anwender das Programm von einem Backup neu lädt.

Erstellen von Reports

Sophos Anti-Virus protokolliert jeden Virenvorfall und alarmiert den Netzwerkadministrator. Einzelne Benutzer und Gruppen können ebenfalls als Empfänger angegeben werden.

Reports werden in einer einfachen Textprotokolldatei erstellt, die in einem Texteditor, wie z. B. Notepad geöffnet werden können. Alarme werden über InterCheck sowie über andere Mechanismen, wie SMTP Mail, Network Logging, SNMP und Event Logging gesendet. Auf Unix-Systemen werden Benachrichtigungen auf dem gleichen Weg mit Hilfe von syslog versendet.

Sophos' Design

Das Design und die Architektur von Sophos Anti-Virus, die in diesem White Paper erläutert worden sind, haben verschiedene Vorteile, die plattformübergreifend Gültigkeit haben.

AIX (PowerPC)	OpenVMS (Alpha)
Digital Unix (Alpha)	OpenVMS (VAX)
DOS	OS/2
FreeBSD (Intel)	SCO OpenServer (Intel)
HP-UX (HP-PA)	SCO UnixWare (Intel)
Linux (Alpha)	Solaris (Intel)
Linux (Intel)	Solaris (SPARC)
Lotus Notes	Windows 3.1x
Macintosh	Windows 95/98/Me
Microsoft Exchange	Windows NT/2000 (Intel)
NetWare	Windows NT (Alpha)

Von Sophos Anti-Virus unterstützte Plattformen

Die gesamte Technologie, auf der Sophos Anti-Virus basiert, ist eigens von Sophos entwickelt worden. Dies bringt bedeutenden Nutzen gegenüber Lösungen, die auf Dritt-Libraries basieren, da sie keinen Entwicklungsbeschränkungen ausgesetzt ist. Vielmehr stellt die Erweiterbarkeit der VDL-Programmiersprache sicher, dass die Engine auch mit neuen, zukünftigen Virentypen umgehen kann.

Die hohe Überprüfungsgeschwindigkeit der Engine wird von InterCheck ergänzt, der mit der Prüfsummentechnologie die einmalige Dateiüberprüfung möglich macht. Dieser Leistungsvorteil wird beim Update-Prozess noch weiter verbessert. Da nur die Daten und nicht der Code aktualisiert werden, sind Updates für Sophos Anti-Virus relativ klein.

Die Qualität der Sophos-Technologie wird unterstützt von hochkarätiger Forschung und umfassendem Support, die alle einen Teil der kompletten Gesamtlösung eines Virenschutzes für Unternehmenskunden darstellen.