Sophos Anti-Virus-Updates auf der Cisco Security Appliance unterscheiden sich von den auf der Sophos-Website verfügbaren Aktualisierungen.

Inhalt

[Einführung](#)
[Voraussetzung](#)
[Hintergrund](#)
[Konfigurieren](#)

Einführung

In diesem Dokument wird erläutert, warum sich die Sophos Anti-Virus-Updates auf der Cisco Security Appliance von denen auf der Sophos-Website unterscheiden.

Voraussetzung

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco E-Mail Security Appliance (ESA)
- Alle Versionen von AsyncOS

Hintergrund

Es gibt zwei Arten von Updates: Aktualisierungen der Sophos Anti-Virus-Engine und Aktualisierungen der Sophos-Virenidentitätsdateien (Integrated Development Environment (IDE)-Dateien).

Die Sophos Anti-Virus-Engine ist vollständig in das AsyncOS-Betriebssystem integriert. Sophos generiert etwa jeden Monat eine neue Version seiner Antivirus-Scan-Engine. Die neue Version enthält sowohl die aktuellen Virendefinitionen als auch alle Codeänderungen, die erforderlich sind, um neue Virentypen zu erkennen und bekannte Probleme zu beheben. Wenn weitere Viren entdeckt werden, veröffentlicht Sophos Virenidentitätsdateien, die als IDE-Dateien bezeichnet werden. Diese werden mit Motoren funktionieren, die weniger als 90 Tage alt sind.

Sophos-Updates werden automatisch von Cisco AsyncOS in der Appliance der C-Serie verwaltet. Wenn Sophos neue Versionen seiner Engine herausbringt, qualifiziert Cisco diese durch einen

Qualitätssicherungsprozess und platziert sie dann auf den Cisco Update-Servern, sodass diese automatisch von der Appliance der C-Serie heruntergeladen und aktualisiert werden. Wenn IDE-Virendefinitionsdateien veröffentlicht werden, werden sie automatisch über den Dienst übertragen und innerhalb weniger Minuten nach ihrer Veröffentlichung durch Sophos auf den Cisco Update-Servern gespeichert.

Sophos IDE-Virensignaturen sind gültig und funktionieren mit den vorherigen Motorenversionen. Alle aktuellen IDEs werden geladen und funktionieren mit der Engine-Version, die in der Appliance der Cisco C-Serie ausgeführt wird.

Konfigurieren

Manchmal scheinen die Dateien auf der Cisco ESA nicht mit den Dateien abzustimmen, die direkt von Sophos verfügbar sind. Dies kann durch den Zeitzonenunterschied zwischen Sophos und den meisten nordamerikanischen Kunden noch komplizierter werden. Die Sophos-Website wird von der Sophos-Zentrale in der Nähe von Oxford in Großbritannien verwaltet. Die Posts auf der Website werden mit der lokalen Zeitzone GMT datiert. Es ist etwas verwirrend, Sophos IDE-Dateien zu korrelieren. Der große Zeitunterschied bewirkt nicht nur, dass die Daten oft einen Tag voneinander getrennt erscheinen, sondern Cisco verwendet auch ein anderes Nummerierungsschema für die IDE-Dateien. Sie können versuchen, diese Dateien abzugleichen, indem Sie die Sophos IDE-Site überprüfen, um festzustellen, wann eine IDE veröffentlicht wurde und wie viele andere am Tag und am Tag davor veröffentlicht wurden. Da Cisco jedoch häufig inkrementelle Änderungen übernimmt, die nicht auf dieser Website veröffentlicht wurden, ist dies nicht die effizienteste Methode. Cisco fragt alle 10 Minuten die Sophos-Website ab. Die Standardeinstellung für eine Appliance ist, die Cisco Download-Site alle fünf Minuten abzufragen. Im schlimmsten Fall wird es eine Verzögerung von 15 Minuten geben.

Das Nummerierungsschema für die IDE-Dateien ist das Datum. Beispiel: "Sophos IDE Rules 2004121402 Tue 14 06:27:14 2004" korreliert mit dem dritten Update (beginnend mit der Zählung von Null) am 14. Dezember, veröffentlicht hier.

Cisco empfiehlt, das automatische Aktualisierungsintervall von Sophos auf die Standardeinstellung von 15 Minuten einzustellen. Stellen Sie sicher, dass Sie über die webbasierte Benutzeroberfläche auf der Seite **Security Services > Anti-Virus** kontinuierliche Updates von Cisco erhalten. Diese Informationen sind auch über den Befehl **antivirusstatus** CLI verfügbar, z. B.:

```
mail3.example.com> antivirusstatus
    SAV Engine Version        4.03
   IDE Serial                2006031503
   Last Engine Update        Tue Mar 14 01:01:49 2006
   Last IDE Update           Thu Mar 16 06:33:50 2006
   Last Update Attempt       Thu Mar 16 09:18:51 2006
   Last Update Success       Thu Mar 16 06:33:50 2006
```

Wenn Ihre Updates nicht erfolgreich sind (Sie erhalten in diesem Fall eine Warnmeldung), können Sie eine manuelle Aktualisierung mit der Schaltfläche **Update** in der GUI oder dem Befehl **antivirusupdate** CLI versuchen. Der Status der Aktualisierung wird in der Virenschutzprotokolldatei angezeigt. Beispiel:

```
smtp.example.com> tailCurrently configured logs:
```

```
1. "antivirus" Module: thirdparty Format: Anti-Virus
2. "avarchive" Module: mail Format: Anti-Virus Archive
3. "bounces" Module: bounces Format: Bounces
4. "brightmail" Module: thirdparty Format: Symantec Brightmail Anti-Spam
5. "cli_logs" Module: system Format: CLI Audit Logs
6. "error_logs" Module: mail Format: IronPort Text
7. "ftpd_logs" Module: ftpd Format: IronPort Text
8. "gui_logs" Module: gui Format: IronPort Text
9. "mail_logs" Module: mail Format: IronPort Text
10. "rptd_logs" Module: rptd Format: IronPort Text
11. "sntpd_logs" Module: sntpd Format: IronPort Text
12. "status" Module: mail Format: Status Logs
13. "system_logs" Module: system Format: IronPort Text
Enter the number of the log you wish to tail.
[]> 1Press Ctrl-C to stop.
Thu Mar 16 09:08:50 2006 Info: Current IDE serial=2006031503. No update needed.
Thu Mar 16 09:13:50 2006 Info: Checking for Sophos Update
Thu Mar 16 09:13:50 2006 Info: Current SAV engine ver=4.03. No engine update needed
Thu Mar 16 09:13:50 2006 Info: Current IDE serial=2006031503. No update needed.
Thu Mar 16 09:18:50 2006 Info: Checking for Sophos Update
Thu Mar 16 09:18:50 2006 Info: Current SAV engine ver=4.03. No engine update needed
Thu Mar 16 09:18:50 2006 Info: Current IDE serial=2006031503. No update needed.
Thu Mar 16 09:23:50 2006 Info: Checking for Sophos Update
Thu Mar 16 09:23:50 2006 Info: Current SAV engine ver=4.03. No engine update needed
Thu Mar 16 09:23:50 2006 Info: Current IDE serial=2006031503. No update needed.
^C
smtp.example.com>
```