

# Viren im Visier

Die neue Scan-Technologie von Sybari mit Antigen 5.5 für Microsoft Exchange Server ist bisherigen MAPI-Scannern überlegen. Im Gegensatz zu anderen Produkten aus dem Bereich der Virens Scanner für Exchange geht Antigen völlig neue Wege, da es kein MAPI-basierender Virens Scanner ist.

## Potentielles Sicherheitsrisiko

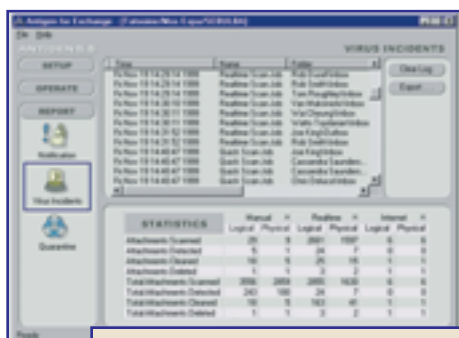
Messaging API (MAPI) ist das meistverwendete API heutzutage, und fast jedes Antivirus-Produkt verwendet diesen Ansatz, um den Information Store (IS) zu überwachen. Der Virens Scanner meldet sich an jedem Postfach an, wartet auf die Ankunft

Mailanhänge zu überwachen, wenn diese in den IS gelangen oder den IS verlassen, und falls notwendig, einen Virus aus dem Anhang zu entfernen.

## Intelligenter Virens Scanner

Antigen benützt damit einen zentralen Ansatzpunkt zum IS, statt sich an jedem einzelnen Postfach anzumelden. Wenn ein virenverseuchter Mailanhang erkannt wird, muss Antigen lediglich einmal auf diesen zugreifen und erst danach erfolgt die Weiterverteilung der nun ungefährlichen Mail samt Anhang. Dadurch ist die zusätzliche Belastung durch Scanprozesse geringer und der Anwender kann nicht vor einer Überprüfung auf seine eMails zugreifen. Durch Beachtung der Exchange Single Instance Storage Architektur wird eine Mail an mehrere Empfänger nur einmal überprüft und nicht bei jedem Postfach erneut. Eine SMTP-Mail wird bereits am Internet Mail Connector (IMC) gescannt.

- Überprüfung von Mails im Hauptspeicher
- Remote Installation und Administration
- Scannen von MIME Mails
- Microsoft Cluster Server Support
- Automatischer Schutz von neuen Postfächern
- Überprüfung und Säuberung von verschiedenen ZIP Varianten durch binäre Identifikation der Dateiart
- Filterung der Mailanhänge durch Bestimmung des Dateinamens oder der Dateiart
- Benachrichtigung und Bericht bei gefundenen Viren
- Support für länderspezifische Exchange Versionen



Antigen erkennt und säubert virenverseuchte Mailanhänge. Jeder Scan Job wird protokolliert und kann in der Reportansicht eingesehen werden.

einer neuen eMail und überprüft jeden Mailanhang auf Viren.

Diese Methode stellt beim Empfangen vieler Mails ein potentielles Sicherheitsrisiko dar, da ein Anwender möglicherweise eine Mail öffnen kann, bevor diese überprüft wurde. Eine zusätzliche Belastung der Systemressourcen, speziell der CPU und des Hauptspeichers, ist bei dieser Scanmethode unumgänglich.

Sybari's Produkt Antigen 5.5 benutzt das Extensible Storage Engine (ESE) API anstatt MAPI, um einen Zugriff auf den Information Store auszuführen. ESE ist der Basisdienst, auf dem der Information Store (IS) aufgesetzt ist. Antigen benützt ESE um

## Die wichtigsten Fakten:

- Echtzeit-Überprüfung aller ein- und ausgehenden Mails im Information Store sowie Exchange Internet Mail Service (IMC)
- Scant SMTP in- und outbound und Public Folders in Echtzeit
- Integriert Scan Engines von Norman Data Defense, McAfee und Sophos
- Trusted Scanning zwischen Internet Mail Connector und Mailboxen verhindert doppeltes Scannen von Mails
- Kein Logon auf Mailbox
- Unterstützt Exchange Single Instance Storage Architektur

## info



### InfoWAN Datenkommunikation GmbH

Frankfurter Ring 193a  
80807 München  
Tel. 089 - 3247560  
Fax 089 - 32475699  
info@infowan.de  
www.infowan.de



### Sybari Software Europe

C/ Diego de Leon, 11  
28006 Madrid, Spain  
Fon. +34 - 91 - 5621617  
Fax +34 - 91 - 5629697