

Automatische Virenschutzaktualisierung im Intranet

Nützlicher Zentralismus

von Dr. Henning Astheimer

Es besteht wohl kein Zweifel daran, dass auf jedem PC im Firmennetz eine Antivirus-Software installiert sein muss. Allerdings ist es wenig sinnvoll, wenn jedes einzelne dieser Systeme regelmäßig eine Internet-Verbindung aufbauen muss, um die aktuellen Virendefinitionen zu installieren. Unser Autor zeigt, wie man diesen Vorgang schnell und einfach zentralisieren kann.

Während sich Programme, die zur Bekämpfung von „Spyware“ und ähnlichen Bedrohungen dienen, noch weiter durchsetzen müssen, ist heute praktisch auf jedem PC eine Lösung zur Virenbekämpfung zu finden. Aber bei deren Einsatz ist es nicht mit der anfänglich erforderlichen Installation der Software im laufenden Betrieb getan, sondern es muss sicher gestellt werden, dass eine regelmäßige und zeitnahe Aktualisierung der Virendefinitionsdateien möglich ist. Relativ leicht ist es, diesen Vorgang auf einem einzelnen PC zu automatisieren, sofern dieser – zumindest gelegentlich – mit dem Internet verbunden ist. Bei einer mittleren bis großen Geräteanzahl sollte man aber die Bandbreite seiner Internetverbindung dadurch schonen, dass man sich ein eigenes lokales Verzeichnis mit den aktuellen Virendefinitionsdateien anlegt, aus dem sich dann alle PCs „bedienen“ können. Mit wenig mehr Aufwand kann man sogar die

Aktualisierung eines solchen „Repositories“ im Firmen-Intranet automatisieren. Dieser Artikel erläutert am Beispiel einer Windows-2003-Domäne und der Software NAI VirusScan Enterprise 8, wie dies einfach bewerkstelligt werden kann.

Ein ähnliches Szenario wurde vom Autor bereits in der Ausgabe 8/2003 des Windows 2000 Magazins auf den Seiten 22 und 23 am Beispiel einer Windows-2000-Domäne und der Software NAI VirusScan 4.51 beschrieben. Dabei erfolgte die Übertragung der Antivirendefinitionsdateien mithilfe einer DFÜ-Verbindung über eine serielle Schnittstelle. Auf diese Weise war es möglich, ein Datenvolumen von 3 MByte innerhalb von fünf Minuten in die Intranet-Domäne zu transportieren. Mittlerweile beträgt die Größe eines aktuellen Repositories fast 50 MByte, was die Übertragungszeit auf fast 90 Minuten erhöhen würde. Daher ist es sinnvoller, die beiden PCs mit je einer

weiteren Netzwerkkarte auszustatten, so dass sie dann über ein „Cross-Over-Netzwerkkabel“ verbunden werden können. Bei einer nominellen Netzwerkgeschwindigkeit von einem GBit/s dauert die Übertragung dann nur noch erträgliche drei bis fünf Minuten, wenn eine Aktualisierung erforderlich ist. Steht keine Aktualisierung an, so ist dies in weniger als 30 Sekunden erledigt.

Die im folgenden Abschnitt verwendete Bezeichnungen für die einzelnen Komponenten beziehen sich auf die im Bild 1 dargestellte Skizze: Dabei dient der „Antiviren-PC AV2“ im eigenen Internet-Bereich als einziger Empfänger der originalen Antivirendefinitionen. Er beherbergt das Repository „Repo2“ in einem beliebigen freigegebenen Verzeichnis wie beispielsweise „c:\Antivirus“ auf seiner Festplatte. Durch den „AutoMirrorTask 1“ werden die Daten vom Ursprungsrepository „Repo1“ auf dem Server AV1 der Firma Network Associates in das lokale Repository „Repo2“ dupliziert. Damit dies regelmäßig geschieht, muss man über die VirusScan Console zuerst den Task „AutoMirrorTask1“ per „Task / New Mirror Task“ einrichten und eine beliebige Häufigkeit einstellen, beispielsweise einmal täglich um 5 Uhr. Dabei wird dann auch gleich über den Button „Mirror Location“ der lokale Pfad zum „Repo2“ definiert.

Nun können die anderen PCs im eigenen Internet-Bereich unter vorrangiger Nutzung des Repositories Repo2 regelmäßige AutoUpdate-Tasks durchführen. Die voreingestellten NAI-Repositories dürfen dabei ebenfalls aktiviert bleiben, sollten aber in der Priorität hinter Repo2 verschoben werden. Allerdings ist es notwendig, diese Konfiguration an jedem PC einzeln händisch durchzuführen, will man nicht erheblich mehr Aufwand betreiben, indem die NAI-Komponenten „AutoUpdate Architect“ und eventuell „Installation Designer“ verwendet werden. Leider kann das System AV2 nicht

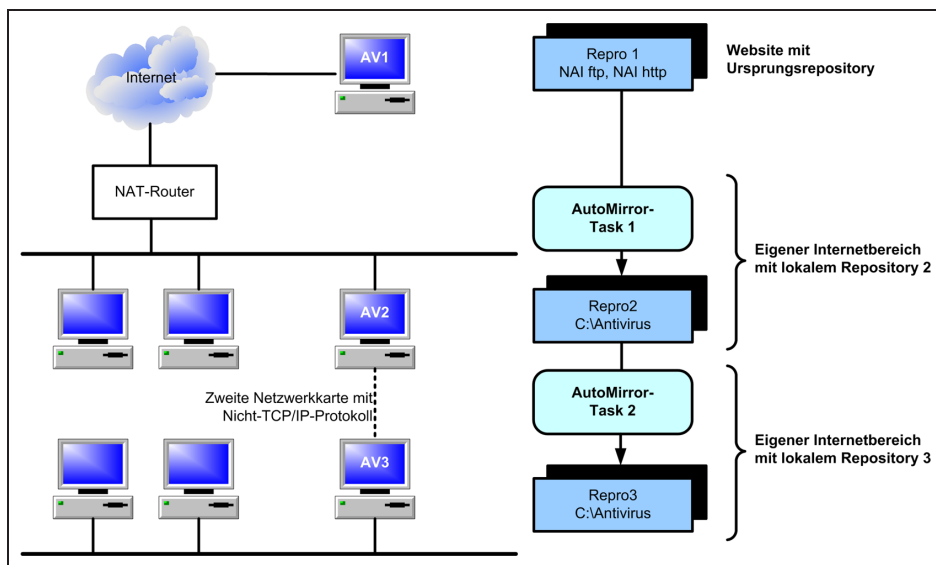


Bild 1. Die einzelnen Komponenten der im Artikel dargestellten Lösung: Dabei dient der „Antiviren-PC AV2“ im eigenen Internet-Bereich als einziger Empfänger der originalen Antivirendefinitionen.

Listing 1

```

echo off
echo AVupdate.cmd
rem H. Astheimer, UAE-Kinderonkologie, 19.09.2005
rem aufgerufen von VirusScanConsole/AutoUpdate nach erfolgreicher Mir-
ror-Aktualisierung
rem von NAI-site
rem C:\Batch\Antivirus\AVupdateGO!.cmd mit folgendem Inhalt
rem c:\Batch\Antivirus\AVupdate.cmd 1>c:\Batch\Antivirus\AVupdate.txt
2>&1
rem Verzeichnis fuer Protokolle
set LOG=%SystemDrive%\batch\Antivirus
set AV2=%COMPUTERNAME%
if not exist %LOG%\nul md %LOG%
cd /d %LOG%
echo.
echo %date%, %time%
echo Testen, ob eine neue SDAT angekommen ist ...
if not exist \\%AV2%\Antivirus\sdatt*.exe goto ERR1
dir /b \\%AV2%\Antivirus\sdatt*.exe > AVneu.dat
fc /l AVneu.dat AValt.dat >nul
if %errorlevel% neq 0 (
echo Neue Version angekommen:
type AVneu.dat
FOR /F „eol= tokens=1 delims=\\ „ %A IN ('dir \\%AV2%\Antivi-
rus\sdatt*.exe') DO echo %A >> AVdat.lst
net send %AV2% NAI-update angekommen! 1>nul 2>nul
rem SuperDat-Kommandozeilenoptionen
rem /logfile filename, /silent, /reboot, /prompt /e extract, /v dis-
play info, /f force update
echo SuperDAT-Datei ausfuehren...
FOR /F %A IN ('dir /b \\%AV2%\Antivirus\sdatt*.exe') DO \\%AV2%\Anti-
virus%%A /silent
copy AVneu.dat AValt.dat >nul
) else (
echo Keine Aktualisierung gefunden! Jetzige Version:
type AValt.dat
)
goto ENDE
:ERR1
echo keine SDAT gefunden!

```

Listing 1. Dieses Batch-Programm realisiert die Aktualisierung der Antivirendefinitionsdateien auf AV2 durch Nutzung des Programms „SDAT*.exe“.

mithilfe seines eigenen Repo2 über einen AutoUpdate-Task aktualisiert werden, da NAI nur eine einzige Repository-Liste vorgesehen hat, die gleichermaßen für Mirror-Aufgaben und damit auch für AutoUpdate-Tasks verwendet wird. So darf also das lokale Repository „Repo2“ am AV2 keinesfalls über „Tools Edit AutoUpdate Repository List“ einrichtet werden. Ein solcher Vorgang ist später nur noch am AV3 durchzuführen. Zur Aktualisierung des Systems AV2 konfiguriert man dort entweder einen Auto-

Update-Task 1, der die Antivirendefinitionen noch einmal direkt vom der NAI-Site abholt oder lässt gleich im Anschluss an AutoMirror-Task1 einen entsprechenden Batch-Job (C:\Batch\Antivirus\AVupdateGO!.cmd) ablaufen, der die mittlerweile in Repo2 befindliche „SDAT*.exe“ ausführt (siehe Listing 1). Diese Weg ist nach Ansicht des Autors zwar eleganter und schneller, das Resultat ist jedoch letztlich gleich. Die Batchdatei in Listing sollte sich durch die Kommentare einigermaßen selbst erklären. Der zweite der dort verwendeten FOR-Befeh-

fehle stellt eine etwas komplizierte Konstruktion dar, die aber leider erforderlich ist. Dies liegt daran, dass der Name der „SDAT*.exe“ sich natürlich mit jeder Versionsnummer wieder ändert und man der DOS-Shell keine EXE-Datei mit Platzhaltern zur Ausführung übergeben darf. Da es in dem angegebenen Verzeichnis aber immer nur ein Exemplar mit diesem Namensmuster gibt, kann man sicher sein, dass auch nur eines – und zwar das richtige – durch den FOR-Befehl ausgeführt wird. In der Datei „AVdat.lst“ wird eine Liste der eingetroffenen SDATs mit Datum und Uhrzeit geführt. Über einen längeren Zeitraum betrachtet, kann diese Liste sehr anschaulich die Aktualisierungshäufigkeit dokumentieren oder durch Lücken auf einen Übertragungsfehler aufmerksam machen. Eine weitere Anmerkung zu den Batch-Jobs betrifft deren Verschachtelung: Diese ist nur dann nötig, wenn man ein Protokoll des Ablaufs haben will, da die VirusScan-Console keine Befehlszeilenargumente zulässt, sodass „AVupdateGO!.cmd“ aufgerufen wird. Dort ist dann nur eine einzige Befehlszeile zu finden:

```

cmd /c c:\Batch\Antivirus\AVupdate-
te.cmd 1>c:\Batch\Antivirus\AVupdate-
te.txt 2>&1

```

Der „Antiviren-PC AV3“ im eigenen Intranet-Bereich vermittelt seinen „Kollegen im Intranet“ die Antivirendefinitionsdateien, die er aus dem „Repo2“ über seinen „AutoMirrorTask2“ in sein eigenes lokales „Repo3“ transportiert. Wegen der privaten Gigabit-Netzwerkverbindung zwischen AV2 und AV3 geht dies in Sekundenschnelle. Daher ist es sinnvoll, dass der AV3 seine eigene Aktualisierung ebenfalls auf diesem Wege durchführt, nämlich aus dem Repo2. In seiner Liste der Repositories darf nur Repo2 mit oberster Priorität aktiviert sein; die Ursprungs-Repositories bei NAI (Repo1) sind ohnehin für keinen PC im Intranet erreichbar. Die Handhabung der VirusScan-Console bei diesem Konfigurationsteil ähnelt den zuvor für AV2 geschilderten Vorgängen. Die Ausnahme besteht darin, dass jetzt ein so genannter AutoUpdate-Task definiert werden muss. Außerdem soll in diesem Zusammenhang noch beispielhaft die Zeittafel der benötigten Tasks (Tabelle auf der Seite 31) erläutert werden. Ein Blick auf diese Auflistung zeigt unter anderem den bislang noch nicht angesprochene Task „AVaufraeum.cmd“. Dieser Aufgabe wurde deshalb eingeführt, weil im Logfile des „AutoMirrorTasks2“ im Netzwerk des Autors immer wieder Fehlermeldungen der folgenden Form aufgetaucht sind: „Error

occurred while verifying file SK_det.msc“. Diese Meldungen blieben erst aus, nachdem ein weiterer Batch-Job in Betrieb genommen wurde. Dieser hat die Aufgabe, nach jedem erfolgreichen AutoUpdate auf AV3 das dort vorhandene Verzeichnis „Repo3“ komplett zu leeren, bevor der AutoMirror-Task2 das Verzeichnis erneut füllt. Dies ist nach unseren Erfahrungen bisher die stabilste Konfiguration, wobei allerdings ungeklärt bleibt, weshalb während der Aktualisierung des Repo2 durch den AutoMirror-Task 1 keine derartigen Fehlermeldungen auftraten. Eine ähnliche Fehlermeldung mit dem Inhalt „File SK_det.mcs is corrupt. Downloading complete file again.“ tritt gelegentlich auch beim AutoUpdateTask auf, scheint aber ohne weitere Folgen zu bleiben.

Die Häufigkeit der ScanAllFixedDisks-Tasks sollte in der Regel der Einschätzung des Systemadministrators überlassen bleiben. So kann es durchaus ausreichen, wöchentliche Scans durchzuführen, da die PCs im laufenden Betrieb ja durch den „On-Access-Scan“ geschützt sind. Die Dauer dieser Tasks hängt natürlich von der Anzahl der Dateien auf den lokalen Festplatten ab. Der Scan sollte jedoch möglichst beendet sein, bevor der PC wieder für interaktive Nutzung zum Einsatz kommt.

Als krönenden Abschluss der hier vorgestellten Konfiguration wird jetzt noch die Verbindung zwischen den beiden PCs AV2 im Internet- und AV3 im Intranet-Bereich benötigt, da ansonsten die gesamte Lösung nicht funktionieren kann. Nach erfolgter Installation passender zusätzlicher Netzwerkkarten gibt man den beiden LAN-Verbindungen am besten leicht zu identifizierende Namen. In der von uns betriebenen Konfiguration heißt das System, das über einen NAT-Router Verbindung zum Internet besitzt, dann „InternetLAN“. Es verwendet natürlich das Netzwerkprotokoll TCP/IP mit privaten IP-Adressen aus dem Bereich 172.x.x.x. Die Direktverbindung zwischen AV2 und AV3 haben wir „AntiVirusLAN“ getauft und dafür zusätzlich das Novellprotokoll IPX/SPX installiert, wobei jedes andere, am besten ein „nicht geroutetes“ Protokoll für diesen Zweck ebenso geeignet wäre. Damit eine zusätzliche Sicherheit zur geforderten Trennung von Inter- und Intranet gegeben ist, muss unter „Netzwerkeigenschaften / Erweitert / Erweiterte Einstellungen“ das Protokoll TCP/IP für das „AntiVirusLAN“ deaktiviert werden. Stattdessen wird das NWLink-Protokoll an die erste Stelle verschoben, wie in Bild 2 gezeigt wird. Das Windows-2003-Betriebssystem fügt die Häkchen ohne jegliche Fehlermeldung

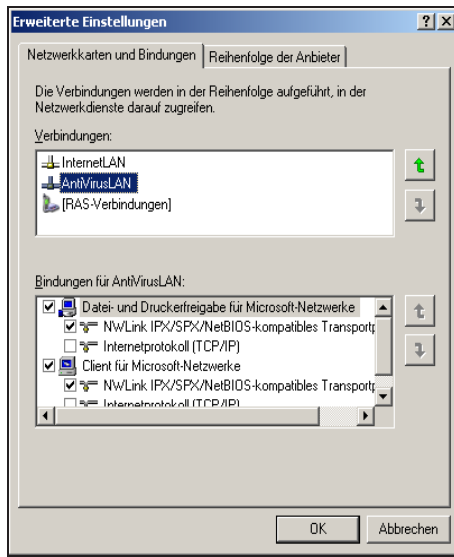


Bild 2. Die Netzwerkeinstellung für das AntiVirusLAN: Das NWLink-Protokoll wird dabei an die erste Stelle verschoben, um eine sichere Trennung zwischen Intra- und Internet zu erreichen.

wieder hinzu, wenn man sie bei der Internet-LAN-Verbindung entfernt hatte. So konfiguriert, können freigegebene Verzeichnisse auf AV2 und AV3 zwar von dem jeweils anderen Partner aus, nicht aber von den Clients des anderen Netzes genutzt werden. Die Freigabeberechtigung sollte dabei folgendermaßen lauten: Jeder /Voll-

zugriff, die NTFS-Berechtigungen („Sicherheit“): Administratoren und System/Vollzugriff; Benutzer/Lesen, Auflisten, Ausführen. In der Netzwerkumgebung von AV2 und AV3 kann man sich davon überzeugen, dass die Freigaben nutzbar sind. Nach Aufwurf eines Ping-Befehls wird dann nur noch die Meldung „Zeitüberschreitung der Anforderung“ angezeigt.

Man könnte natürlich auch bei dieser Konfiguration mit einer (langsameren) DFÜ-Verbindung auskommen, wenn man nur die „SDAT*.exe“ weitergeben wollte. Man müsste dann aber auch die Clients mithilfe einer Batch-Datei aktualisieren, wie sie in Listing 1 dargestellt ist. Man kommt jedoch nicht um eine schnelle Netzwerkverbindung herum, wenn man das gesamte Repository transportieren will, so wie es von NAI zusammengestellt wird. Ungelöst bleibt dann noch die Frage, ob man den Client-Systemen die Lage des aktuellen, vielleicht gerade erst auf einen anderen Server verschobenen, Repositories auf besonders ökonomische Weise mitteilen kann, ohne selbst auf jedem Gerät tätig werden zu müssen. In größeren Installationen wäre sicher der Einsatz der oben genannten NAI-Tools sinnvoll, in kleineren bringen diese Lösungen dann aber doch zuviel Overhead mit sich.

Es ist auf jeden Fall etwas unglücklich, dass man für Update- und Mirror-Tasks nicht auf verschiedene Quellen – also Reposito-

Listing 2

```

echo Testen, ob neue DAT angekommen ...
if not exist \\<AV2>\Antivirus\sdatt*.exe goto ERR1
dir /b \\<AV2>\Antivirus\sdatt*.exe > AVneu.dat
fc /l AVneu.dat AValt.dat >nul
if %errorlevel% neq 0 (
echo Neue Version angekommen:
type AVneu.dat
FOR /F „eol= tokens=1 delims= \ „ %A IN ('dir \\<AV2>\Antivirus\sdatt*.exe') DO echo %A >> AVdat.lst
net send %COMPUTERNAME% NAI-update angekommen! 1>nul 2>nul
echo Antivirus-Verzeichnis leeren...
rd c:\Antivirus\Current /s /q
echo.
del c:\Antivirus\*. * /q /f
echo.
echo %date%, %time%
copy AVneu.dat AValt.dat >nul
) else (
echo Keine Aktualisierung gefunden! Jetzige Version:
type AValt.dat)
    
```

Listing 2. Dieser Auszug aus einem weiteren Batch-Programm zeigt das Leeren des Repository 3 auf AV3 vor jedem neuen AutoMirrorTask 2.

Zeittafel der benötigten Tasks

Laufende Nummer	PC	Uhrzeit (täglich)	Task	Dauer
1	AV2	05:00	AutoMirror1	0,5-5 Minuten
2	AV2	Anschließend	AVUpdate.cmd	6 Sekunden
3	AV2	05:30	ScanAllFixedDisks	50 Minuten
4	AV3	05:15	AutoUpdate	20 Sekunden
5	AV3	Anschließend	AVaufraeum.cmd	1 Sekunde
6	AV3	05:45	AutoMirror2	3 Minuten
7	AV3	06:00	ScanAllFixedDisks	30 Minuten

ries – zurückgreifen kann. Dann würden die hier dargestellten Batch-Jobs nicht mehr benötigt werden. Hier bleibt wohl nur die Hoffnung auf eine Folgeversion der Software.

Die „VirusScan-Console“ bietet allerdings noch eine weitere Möglichkeit der Verwaltung von Clients über das Netzwerk: So ist es über „Tools / Open Remote Console“ möglich, den Netbios-Namen des gewünschten Clients einzugeben. Leider

funktioniert diese Möglichkeit jedoch nur, wenn auf den Clients exakt die gleiche Softwareversion installiert ist.

Abschließend soll nicht verschwiegen werden, dass während der Arbeit an diesem Artikel bei unserer Installation ein Fehler auftrat: Aus unerklärlichem Grund begann die VirusScan-Console an unserem System AV2 auf einmal abzustürzen, wenn man über „Tools/Edit AutoUpdate Repository List“ die Liste der Repositories einsehen

wollte. Die Fehlermeldung lautete: „Fehlgeschlagene Anwendung mcconsole.exe, Version 8.0.0.912, fehlgeschlagenes Modul unknown, Version 0.0.0.0, Fehleradresse 0x008401bd“. Der Fehler wurde dann auch per E-Mail an NAI weitergeleitet. Zum Glück liefen die Hintergrunddienste trotzdem einwandfrei weiter, sodass der Virenschutz weiter bestand; der AutoMirrorTask1 blieb jedoch stehen. Eine Reparaturinstallation brachte keine Abhilfe, sodass eine Deinstallation mit anschließender Neuinstallation durchgeführt wurde. Durch die umfangreiche Dokumentation in diesem Artikel sollte aber für derartige Fälle gut vorgesorgt sein. (fms)

Der Autor

Dr. Henning Astheimer leitet als Medizininformatiker die EDV-Arbeitsgruppe der Kinderkrebsklinik am Universitätskrankenhaus Hamburg-Eppendorf. Er ist per E-Mail unter astheimer@uke.uni-hamburg.de erreichbar. Die Webadresse der Klinik lautet <http://www.uke.uni-hamburg.de/kliniken/haematologie>.