

Windows IT Pro

Das Magazin für den Windows-Administrator

Sonderdruck für H+H Software

Sicherheitslücken bei den Terminal Services

Es geht sicherer

von Alexander Vierschrodt

Von Microsoft zunächst als lästige Zusatzfunktion behandelt, haben sich die Terminal Services auf den Windows Servern inzwischen zu einer wichtigen Komponente in professionellen Netzwerken entwickelt. Aber auch auf dem Windows Server 2003 zeigen sich noch Schwachpunkte bei der Sicherheit dieser Dienste, sodass es zusätzlicher Lösungen bedarf.

Auf jedem Client-PC in Firmennetzwerken arbeiten heutzutage Virens Scanner, Spamfilter, Anti-Spyware-Tools und weitere Programme, die den Rechner funktionstüchtig halten und sicherer machen. Für den Administrator stellt eine derartige Konstellation besonders in großen Netzen sicher keine zufriedenstellende Lösung dar: Ständig muss er Sicherheits-Updates und Patches aufspielen, wobei dies oft genug von Hand oder mithilfe eigener Skripte geschieht, die zunächst einmal entwickelt werden müssen.

Eine Lösung: Programme weg vom Client. Diese Gründe veranlassen viele Firmen dazu, eine Lösung einzusetzen, die auf Server Based Computing basiert: Hier sind sämtliche relevanten Programme und Daten zentral auf dem Terminalserver gebündelt, der aus einem, mehreren oder gleich einer ganzen Farm von Servern bestehen kann. Der größte Vorteil für den

Administrator besteht darin, dass er alle Anwendungen zentral verwalten kann und so auch in der Lage ist, sicherheitsrelevante Updates vollständig und zeitnah einzuspielen. Viele Systembetreuer müssen allerdings bei genauerer Betrachtung der Terminal Services von Windows Server 2003 feststellen, dass diese Lösung noch Schwächen aufweist: So handhabt das Windows-Betriebssystem beispielsweise den Umgang mit den RDP-Dateien (Remote Desktop Protocol), die für eine Sitzung auf dem Terminalserver benötigt werden, sehr fahrlässig: Die Informationen in einer solchen Datei lassen sich mit einem beliebigen Text-Editor auslesen. Zudem versäumt es das Betriebssystem, deren Gültigkeitsdauer zu beschränken. Dadurch sind böswillige Anwender oder Angreifer in der Lage, die RDP-Daten mehrfach zu verwenden und auf dieser Weise eine Sitzung von einer nicht autorisierten Station aus zu starten.

Bei solchen Problemen soll der so genannte NetMan Desktop Manager (NDM) des Anbieters H+H Software Abhilfe schaffen und zugleich den Bedienkomfort für Administratoren und Anwender erhöhen. Die Software basiert auf zwei Grundkomponenten: Die Serverkomponente setzt auf dem Terminalserver auf und verwaltet in einer Datenbank sämtliche Netzwerkobjekte und -einstellungen, zu denen auch die Sicherheitskonfiguration gehört. Die Client-Komponente nimmt Anweisungen des Servers entgegen, stellt die Anwendungen dar und setzt die lokalen Zugriffsbeschränkungen durch.

Schwächen bekämpfen – RDP-Dateien im Griff. Um das zuvor geschilderte Problem mit den RDP-Dateien zu beheben, führt die Software ein Ticket-Verfahren ein. Dadurch kann der Administrator frei bestimmen, wie lange eine RDP-Datei gültig ist (Bild 1). Bereits diese Maßnahme hält die meisten Anwender von einem missbräuchlichen Serverzugriff ab, schützt aber nicht vor ausgefeilten „Man-in-the-middle“-Attacken. Mithilfe des Open-Source-Werkzeugs Ettercap können Systemverantwortliche testen, ob ihre Infrastruktur für diese Art von Angriffen anfällig ist. Diese Software erlaubt unter anderem auch die Überwachung des Datenverkehrs auf IP- und ARP-Basis, die Analyse einzelner Server oder des ganzen Netzwerks sowie das Filtern der transportierten Daten nach Inhalten. Aber die Terminal-Dienste des Windows Servers 2003 weisen neben den unbegrenzt gültigen RDP-Daten noch eine weitere gravierende Schwäche auf: Während sie dem Anwender den Zugriff auf lokale Laufwerke erlauben, geben sie gleichzeitig dem Administrator keine Möglichkeit an die Hand, diese wichtigen Zugriffsrechte

entsprechend zu steuern. Auch hier besteht die Gefahr eines Missbrauchs: Ein Anwender könnte leicht Daten aus einer Terminalserver-Sitzung heraus auf einen USB-Stick übertragen. Umgekehrt ist er so natürlich auch in der Lage, unerwünschte Dateien auf den Server zu kopieren. Die Lösung NDM ermöglicht es dem Administrator, die Lese- und Schreibrechte für sämtliche Verzeichnisse der Clients jeweils auch auf die Sitzung bezogen festzulegen (Bild 2). Dabei kann der Systembetreuer zudem auch die Zugriffsrechte für lokale USB-Wechselspeichermedien frei definieren. Die Software setzt dazu einen Filtertreiber ein, der sich in das Dateisystem des Clients einlinkt. Die dazu benötigten Informationen erhält der Filtertreiber vom Netman-Client-Service.

Wer darf was: Serverzugriff nur für bestimmte IP-Adressen. Weiterhin ist es dem Administrator auch möglich, durch den Einsatz der Software den Zugriff auf den Terminalserver anhand von IP-Adressen, IP-Adressgruppen und DNS-Namen zu reglementieren. Das Windows-System beherrscht diese Art der Zugriffssteuerung lediglich auf Nutzer- und Gruppenebene. So kann der Systemverantwortliche zum Beispiel für bestimmte IP-Adressen den Zugriff auf einzelne Anwendungen beschränken oder gänzlich untersagen. Gerade diese Art der Zugriffsregelung erweist sich in bestimmten Fällen als nützlich. Auf diese Weise kann der Verantwortliche auch anonymen Benutzern ohne großen Verwaltungsaufwand die Verwendung bestimmter Programme in seinem Netz gestatten. Jedem Systemprofil ist dabei aber klar, dass diese Art der Zugriffsbeschränkung keinen

weitergehenden Schutz vor Angriffen bieten kann. Fälscht beispielsweise ein Angreifer die Quelladresse in den Kopfdaten eines IP-Pakets, so überlistet er auf diese Weise die Authentifizierung auf IP-Basis. Diese Vorgehensweise wird als IP-Spoofing bezeichnet. Daten kann er auf diese Weise allerdings nicht empfangen, da die Antwortpakete ja an die gefälschte Adresse geschickt werden. Eine weitere Angriffsmöglichkeit bietet das DNS-Spoofing, bei dem die Zuordnung zwischen Rechnername und IP-Adresse gefälscht wird. Künftige Versionen der NDM-Lösung sollen nach Angaben des Herstellers auch über weitergehende Schutzmaßnahmen verfügen, die in der Lage sind, derartige Angriffe zu erschweren.

Nur einmal anmelden: Sicheres Single Sign On. Zusätzliche so genannte Komfortfunktionen sollen dabei helfen, die Akzeptanz der beschriebenen Sicherheitsmaßnahmen beim Anwender zu erhöhen. So ist beispielsweise ein einfacher Programmstart auf dem Terminalserver aus Anwendersicht sehr umständlich. Viele Benutzer empfinden bereits die Anmeldung beim lokalen Windows-Start als lästig. Müssen sie dann noch ein Programm auf dem Terminalserver starten, so wird erneut eine Anmeldung fällig – je

einem zusätzlichen Fenster. Erlaubt das Programm seinerseits noch mehrere zusätzliche Fenster, wie es in den meisten Fällen üblich ist, wird es für die meisten Anwender

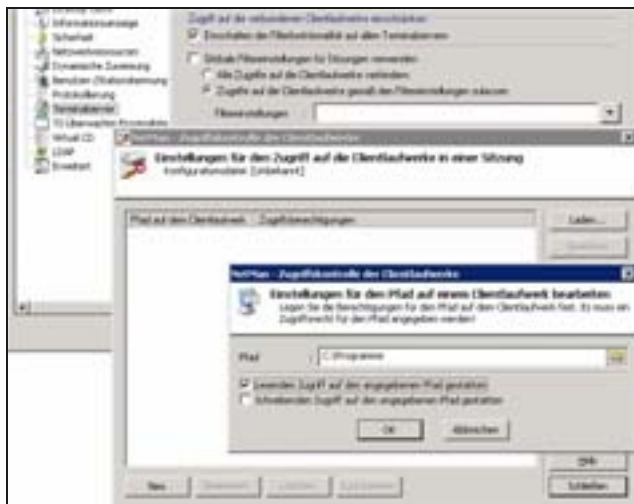


Bild 2. Wenn die Nutzer nicht alle lokalen Verzeichnisse verwenden sollen: Die Software ermöglicht die Lese- und Schreibrechte für sämtliche Verzeichnisse der Clients sitzungszugangsbezogen festzulegen. (Quelle H+H Software)

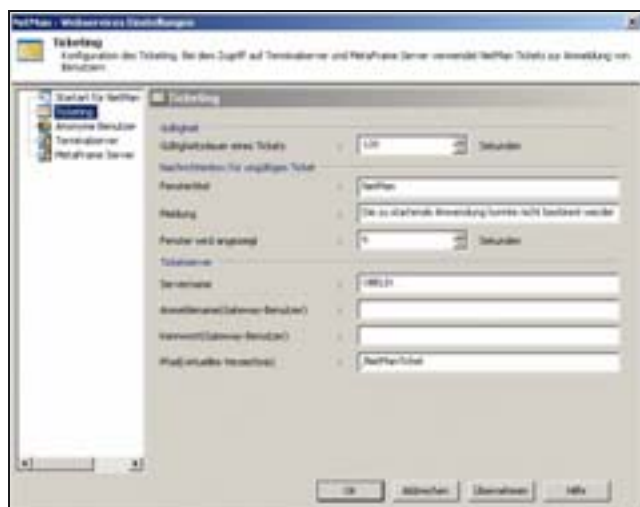


Bild 1. Keine Probleme mehr mit den RDP-Dateien auf dem Terminalserver: Der Administrator kann in diesem Menü die Gültigkeitsdauer einer RDP-Datei beschränken. (Quelle: H+H Software)

nach Konfiguration möglicherweise sogar mit anderen Login-Daten. Der NDM unterstützt aus diesem Grund auch Single Sign On, verwendet also auf Wunsch die lokalen Anmeldedaten auch für den Terminalserver. Diese Funktion kann der Administrator global oder auch für jeden Client individuell aktivieren. Die Daten werden vom Programm mit starker Verschlüsselung in der Registry abgelegt. Standardmäßig unterscheidet sich eine Terminal-Anwendung von lokalen Anwendungen: Der Windows Server 2003 zeigt dieses Programm in

schwierig, die Übersicht auf ihrem Desktop zu behalten. Durch den Einsatz der vorgestellten Lösung kann der Systemadministrator erreichen, dass sich die lokalen und die Terminal-Anwendungen optisch gleichen: Der Anwender findet alle Programme wie gewohnt im Desktop oder Startmenü und kann sie direkt aufrufen. Normalerweise müsste der Administrator diese Verknüpfungen manuell erstellen – bei mehreren Dutzend oder Hunderten von Anwendern und Programmen eine undankbare Aufgabe, die aufgrund der Komplexität auch leicht zu Fehlkonfigurationen führen kann. Das Programm veröffentlicht hingegen automatisch diejenigen Terminal-Programme und -Dokumente, für die der Benutzer oder die Gruppe eine Berechtigung besitzt. Zusätzlich kann der Administrator nutzer- und gruppenspezifische Rahmenbedingungen festlegen, deren Einhaltung die Lösung vor dem Programmstart sicherstellt. Dabei kann es sich beispielsweise um eine Laufwerkszuweisung handeln. (fms)

Der Autor:

Alexander Vierschrodts ist als Produktmanager bei der Firma H+H Software in Göttingen tätig.