Windows NT für NetWare Administratoren

Funktionen, Begriffe, Vergleiche

Der Einsatz von WindowsNT als Server und Desktopbetriebssystem steigt auch dank leistungsfähiger Rechner. Für die Einbindung sind Kenntnisse der NT-Denkweisen, Konzepte und Programme notwendig.

Net at Work
Netzwerksysteme GmbH

Riemeke Straße 160
33106 Paderborn

http://www.netatwork.de

Stand: 27. August 2000

Autor: Frank Carius

ZUR BENUTZUNG DIESER DOKUMENTATION

Diese Dokumentation hält sich an folgende Formatierungen

Kennzeichnungen durch unterschiedliche Schriften

Neben der Standardschrift für diese Dokumentation kennzeichnen weitere Formatierungen wichtige Passagen oder Informationen

```
Sourcecode, Batchfiles und Listings werden in der Schriftart COURIER ausgedruckt,
damit die Ausrichtung erhalten bleibt und 80 Zeichen in einer Zeile passen
12345678901234567890123456789012345678901234567890123456789012345678901234567890
```

Eingaben durch das Keyboard sind mit **`Courier FETT`** gekennzeichnet und optional durch Tastenzeichen gekennzeichnet. Sondertasten wie **`[ENTER]`** oder **`[ESC]`** sind in eckigen Klammern gesetzt

Kennzeichnung durch Symbole

Zeichen	Bedeutung
	**Information** Dieser Abschnitt enthält zusätzliche Informationen zum Thema, Verweise auf andere Dokumentationen und Quellen
	**Hinweise** Bitte beachten Sie die Hinweise, da Sie wichtig für die Funktion sind.
	**STOP** Dieser Abschnitt ist außerordentlich wichtig. Die Mißachtung kann auch andere Dienste und Funktionen schwer beeinflussen.
	**Einschränkungen** Sie erhalten Hinweise auf nur eingeschränkt mögliche Funktionen
	**Frage** Wir stellen ihnen eine Fragen, welche sie für sich beantworten sollten, inwieweit dieser Aspekt ihre aktuelle Arbeit betrifft. Meist können Sie mit etwas zusätzlicher Arbeit die Funktion erweitern
	**Diskettenlaufwerk** Sie benötigen Disketten um die Aktionen auszuführen
	**CD-Rom** Sie benötigen die CD-Rom um diese Aktionen auszuführen
	**Maussteuerung** Die Folgenden Aktionen beschreiben die Bedienung mit der Maus
	**Tastatur** So können Sie die Funktion per Tastatur ausführen
	**Multimedia** Um voll die Funktion nutzen zu können muß ihr PC mit Multimediadaten umgehen können, d.h. zumindest eine Soundkarte haben.

INHALTSVERZEICHNIS

WindowsNT Workstation - Pro und Contra

Losgelöst von den Prospekten und allgemeinen Vergleichen sollte jeder Administrator abwägen, ob folgende Punkte unterm Strich eine positive Bilanz im Vergleich zu Windows 3.1 und Windows 95 für das Netzwerk ergeben:

- Höhere Anforderungen an Speicher und Prozessor
- zentral administrieren, Verhinderung eigenmächtiger Umbauten und Installationen der Benutzer.
- sehr stabil mit effektiven Speicherschutz und keine von Windows 3.x/95 bekannten Begrenzungen der Ressourcen
- Lokale Festplatten können geschützt werden, Benutzer können Ihre Daten fast nur auf dem Netzwerk ablegen, Schutz lokaler Anwendungen gegen Veränderung.
- Anmeldung am Netzwerk zwingend
- WindowsNT-Lizenzen sind noch teuer als Windows 3.1/95
- Skalierbarkeit (Verschiedene CPU-Plattformen)
- Eingeschränkte Treiber für Spezialhardware. Direkte Hardwarezugriffe nicht mehr möglich. Alte DOS-basierte Treiber nicht weiter verwendbar
- eingeschränkte PCMCIA-Unterstützung.
- Umfangreiche Netzwerkanbindung und gleichzeitiger Support mehrerer Netzwerkprovider (MS-Net, Novell, NFS, Banyan)

Dies dürften die für Administratoren und IT-Manager wichtigsten Punkte für und gegen Windows NT sein.

Festplatten unter NetWare und NT

Beide Betriebssysteme unterstützen die gängigen Festplatten und Kontroller. Auch mit RAID-Controllern kommen beide Systeme problemlos klar, solange passende Treiber existieren. Beide Betriebsysteme nutzen freien Speicher als Cache, um Zugriffe zu beschleunigen.

NetWare kann per Software Festplatten spiegeln, d.h. zwei oder mehr Festplatten an einem oder mehreren Kontrollern duplizieren. Dies erhöht den Datendurchsatz bei Lesen und die Fehlersicherheit. NetWare spiegelt dabei immer komplette Partitionen, welche die identische Größe haben müssen. In der Regel kann eine Festplatte genau eine NetWarePartition aufnehmen, in der dann mehrere Volumes definiert werden könnten. Volumes können dabei über mehrere Partitionen verteilt werden (Spawning), wodurch mit mehreren kleinen Festplatten auch große Volumes abgebildet werden können. Speziell beim Schreiben erhöht dies den Durchsatz. Die Fehleranfälligkeit nimmt jedoch auch zu, da ein Ausfall einer Festplatte das komplette Volume unbrauchbar ist, es sei denn, es existieren Spiegelfestplatten. NetWare bootet jedoch von einer DOS-Partition, welche nicht gespiegelt werden kann. Hier muß der Administrator zusehen, daß auf einer gespiegelten Platte (z.B. D:) die identischen Dateien liegen, damit beim Ausfall der primären Festplatte (mit dem DOS-Bootbereich) der Server wieder gestartet werden kann.

WindowsNT erlaubt neben Spiegel, Duplexing und StripeSets (=Spawing bei NetWare) auch ein Software-RAID, d.h. aus mehreren Festaplatten kann ein Software-RAID aufgebaut werden. Im Gegensatz zum Spiegeln sind mehr als 50% der Bruttokapazität nutzbar, Mit 3 Festplatten sind 2/3 erreichbar, mit 5 Festplatten auch 4/5 zu nutzen. Allerdings kostet dies Rechenzeit, da der Prozessor die Parityinformationen errechnen muß. WindowsNT kann sowohl NTFS als auch FAT-Partitionen spiegeln, wobei bei NT eine Partition bzw. ein Set immer auch ein Laufwerk darstellt. Allerdings kann WindowsNT von einfachen oder gespiegelten Partitionen gebootet werden, nicht von einem Software-RAID.

Beim Einsatz eines eigenständigen RAID-Controllers sind alle Arten von Partitionen bei beide Betriebssysteme abgesichert, da der Controller eigenständig den Zugriff organisiert und alle Betriebssysteme nur eine logische Festplatte sehen.

Beim Neustart eines Servers mountet NetWare zuerst alle Volumes. NetWare liest dabei alle Verzeichnisse mit den darin abgelegten Rechten und hält diese im Speicher. Dabei wird auch die Konsistenz der Einträge überprüft und bei Fehlern (z.B. mangels vorherigem DOWN) VREPAIR gestartet. Dies dauert in der Regel länger.

WindowsNT startet sehr viel schneller, da es auf das transaktionsgesicherte Dateisystem NTFS aufbaut und damit nur Fehler korrigiert werden. Das Einlesen der Informationen erfolgt erst im Moment des Zugriffs auf die Daten, wobei keine Unterscheidung nach Verzeichnissen, Dateieinträgen und den eigentlichen Nutzdaten gemacht wird. Erst nach und nach befinden sich die oft benutzten Verzeichnisse im Cache.

NetWare nutzt jeden freien Speicher, der nicht für NLM‘s und andere Strukturen benutzt wird, als Cache. Der physikalisch vorhandene Speicher ist zugleich auch das Limit. WindowsNT nutzt hingegen auch virtuellen Speicher über eine Swapdatei auf einer Festplatte. Damit wird erst viel später ein Fehler aufgrund ”zuwenig RAM” auftreten. Allerdings wird so bei WindowsNT auch nicht sofort bemerkt, wenn der Cache schon unvernünftig gering geworden ist.

Beide Betriebssysteme (NT4 und NetWare 4.x) können mittlerweile Daten komprimieren. Bei NetWare kann je Volume die Kompression aktiviert werden. NetWare komprimiert in der Regel nachts selten benutzte Dateien. Die Funktion kann über Flags (Don’t Compress, Immediate compress) gesteuert werden. Bei häufigem Zugriff werden die Dateien automatisch wieder unkomprimiert gespeichert um den Zugriff zu beschleunigen.

WindowsNT komprimiert einzelne Dateien, wenn dies explizit gewünscht wird. Diese Funktion ist auf NTFS-Partitionen verfügbar. Ist ein Verzeichnis als ”komprimiert” gekennzeichnet, wird jede neu darin abgelegte Datei ebenfalls komprimiert. Wird eine Datei, ein Verzeichnis oder ein komplette Baum nachträglich auf ”komprimieren” umgestellt, dann ist in dem Moment der PC mit der Komprimierung beschäftigt.

Sicherheit und Rechte unter Windows NT

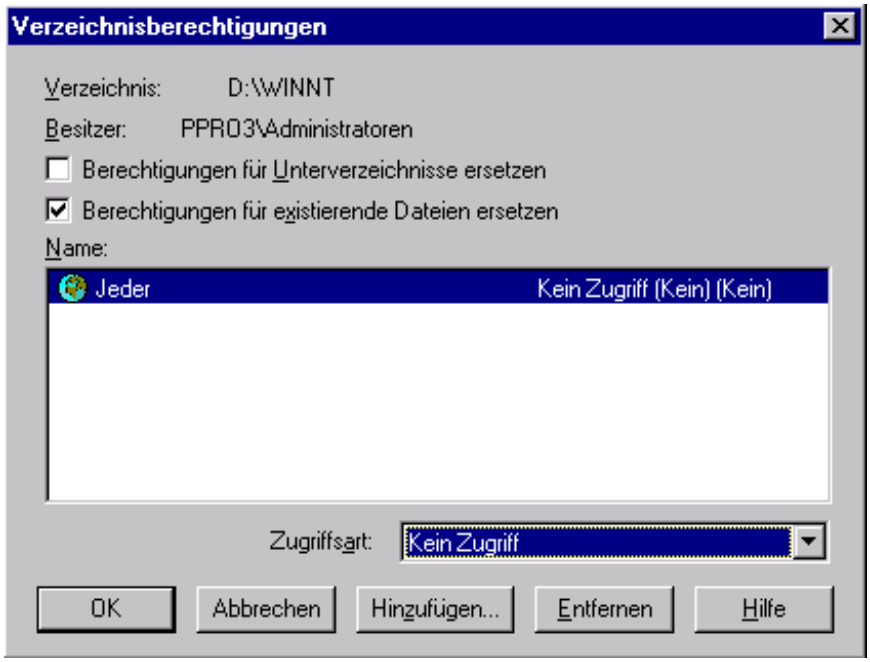
Die erste und wichtigste Regel: Gastzugang deaktivieren. Dies ist bei NT um vieles wichtiger als unter NetWare. Ein GUEST unter NetWare kann ihnen zwar das SYS-Volume auffüllen, indem er in SYS:MAIL\userid jede Menge Dateimüll ablegt, aber er kommt normalerweise nicht an Daten heran,

solange die Gruppe ”Everyone” keine weiteren Rechte bekommt. (Der GUEST ist per Default in EVERYONE !!)

Bei NT ist es ähnlich, bis auf daß die Tore um ein Vielfaches weiter geöffnet sind. Da z.B. JEDER Vollzugriff auf die lokale Festplatte besitzt, kann sich jeder als Gast ohne Paßwort anmelden und Schaden anrichten. Bei Arbeitsrechnern ist dies im Vergleich zu Windows 3.1 keine Verschlechterung. Kann sich dieser Benutzer aber auch auf dem NT-Server selbst anmelden, ist dies ein großes Loch. Auch ein Paßwort hilft nur, wenn unter WindowsNT ”Intruder detection” aktiviert ist, da sonst über das Netzwerk massive Attacken den scheinbaren Schutz aufbrechen. (Source z.B. bei http://www.somarsoft.com/ntcrack.htm). Generell sollten alle Festplatten des Servers auf Rechte von ”JEDER” geprüft werden. Vergleichbar zu NetWare ist das der User ”Not-Logged-In” bzw bei der NDS ”World”. ”Jeder” ist wirklich jedermann, während EVERYONE (NetWare) und ”DomainUsers” (WindowsNT; ACHTUNG! Lokalisierte Versionen nutzen andere Namen, z.B. „Domänenbenutzer) nur eingetragene Benutzer umfaßt.

Die Vergabe von Rechten unter Windows NT unterscheidet sich grundlegend von denen bei NetWare. NetWare speichert die vergebenen Rechte auf der Festplatte unter Verwendung der ObjektID ab. Dabei werden nur die wirklich vergebenen Rechte abgelegt. Beim Zugriff auf eine Datei bildet NetWare zur Laufzeit die effektiven Rechte des Benutzer aus seinen individuellen Rechten, Äquivalenten zu Benutzern und Gruppen und Vererbungsmasken. Die Vererbung und Berechnung erfolgt im Moment des Zugriffs. Daher muß NetWare beim Start auch erst das komplette Volume mounten um dabei die Verzeichnisse und die Rechte zu lesen.

Bei WindowsNT werden die Rechte zu jeder Datei und jedem Verzeichnis als ACL (access control list) bei dem Objekt direkt gespeichert. In dem Moment, in dem der Administrator die Rechte vergibt, wird die ACL jedes betroffenen Objekts verändert. Dabei gibt er an, ob diese Einstellungen für das aktuelle Verzeichnis gilt, oder auch die Zugriffslisten der darin enthaltenen Dateien und Unterverzeichnissen ersetzt werden.



Dies bedeutet, daß alle Dateien und Verzeichnisse auf einer NTFS-Partition ihre kompletten Rechteinformationen mitführen. Beim Zugriff auf eine Datei prüft WindowsNT nur die ACL der jeweiligen Datei, ob der Zugriff gestattet ist. Dies ist schneller, als die Berechnung bei NetWare, hat aber den Nachteil, daß nicht mehr direkt erkennbar ist, über welche Zuweisung die Rechte nun vorgenommen worden sind. Ebenso wird gerne übersehen, daß die ACL der Dateien und Verzeichnisse bei der Zuweisung ”gesetzt” und keineswegs nur verändert wird. Alle darunter eventuell vergebenen feineren Rechtestrukturen werden überschrieben. Hier ist NetWare ganz klar im Vorteil. Bei WindowsNT sollte daher am Anfang definiert werden, welche Gruppen wohin Rechte haben. Die Verteilung sollte von oben nach unten vorgenommen werden. Spätere Änderungen sind sonst sehr aufwendig. Die Vergabe von Rechten an Personen sollte dann über die Mitgliedschaft in Gruppen erfolgen.

Die Rechte sind bei NT nicht so fein einstellbar, wie dies ein NetWare-Administrator gewohnt ist. Aber für die meisten Situationen sind auch die Grundrechte von WindowsNT ausreichend.

Je Benutzer oder Gruppe eine Auswahl dieser Rechte sowohl für Dateien als auch Verzeichnisse individuell eingestellt werden. Die gängigen Grundrechte (Vollzugriff, Nur Lesen, kein Zugriff und einige andere) sind direkt zu verändern.

Ähnlich der NetWareID werden auch bei Windows NT den verschiedenen Objekten eindeutige Werte zugewiesen. Diese SID ist einmalig und bleibt auch bei Umbenennungen erhalten. Wird ein Benutzer gelöscht und mit dem gleichen Namen neu angelegt, wird eine neue SID vergeben. Die Rechte der alten SID bleiben an den verschiedenen Stellen bis zu manuellen Löschung erhalten, wirken sich aber nicht weiter aus.

Ähnlich zu NetWare lassen sich auch bei WindowsNT verschiedene Zugriffe protokollieren (Accounting) um Zugriffe, Veränderungen und unerlaubte Zugriffe feststellen zu können. Dabei landen alle Datensätze im zentralen Eventlog, welches NT je Maschine führt. Das Eventlog kann ist mit dem Eventviewer gelesen werden und diverse Sharewareutilities erlauben den

Export in Datenbanken oder die Ausführung bestimmter Aktionen bei einem vorgegebenen Event. Eine intensive Überwachung erzeugt sehr schnell viele Einträge, die nur schwer wieder auszuwerten sind. Bei NetWare 4 wurde das Auditing soweit verbessert, daß eine Gewaltenteilung möglich ist, d.h. der Überwachende muß nicht der Administrator sein und der Administrator selbst kann sich bei geeigneter Einrichtung nicht der Überwachung entziehen oder diese abschalten. Diese Trennung kennt WindowsNT nicht.

Wie bei NetWare gibt es auch bei WindowsNT Besitzer der Verzeichnisse und Dateien. Diese Besitzer haben fast alle Rechte auf die Dateien oder Verzeichnisse. Administratoren können selbst jede Datei in ihren Besitz übernehmen. So können auch ”tote” Zweige wieder aktiviert werden. Damit ist aber ebenso klar, daß der Administrator ähnlich wie der Supervisor volle Zugriffsrechte hat und nicht zu überwachen ist.

Mit Windows NT 4.0 ist nun auch der Policyeditor verfügbar, der mit Windows 95 schon einigen Administratoren eine zentrale Steuerung von Zugriffsrechten möglich machte. Der Policyeditor von WindowsNT erlaubt ebenso, bestimmte Aktionen und Einstellungen von Benutzern zu verbieten.

Bei NetWare werden Einstellungen an Rechten für Verzeichnisse, Dateien und Drucker, Gruppenzuordnungen und Accounteinstellungen ”sofort” gültig ohne daß der Benutzer sich neu anmelden muß. Bei WindowsNT ist für einige Einstellungen ein Neuanmelden erforderlich.

Beim Anlegen einer Datei oder eines Verzeichnisses wird die Rechteeinstellung des übergeordneten Verzeichnisses übernommen. Das gleiche Verhalten ist übrigens auch bei Ordnern in Microsoft Exchange zu finden.

Wird auf solche eine Festplatte über das Netzwerk zugegriffen, so erfolgt dies über Freigaben, denen wiederum Rechte zugegeben werden können. Diese Rechte werden ”UND”-verknüpft, d.h. enthält die Freigabe nur das Leserecht, dann kann ein Anwender ”maximal” Lesen. Das gleiche Verzeichnis kann mit mehreren Freigabenamen und unterschiedlichen Rechten veröffentlicht werden. Die Sharerechte betreffen auch den Admin!. Allerdings kann der Administrator die Basisverzeichnisse der Laufwerke über die versteckten Freigaben C$, D$ etc. direkt nutzen, wenn dieser Standardfreigaben nicht abgeschaltet wurden..

Die wichtigsten Unterschiede:

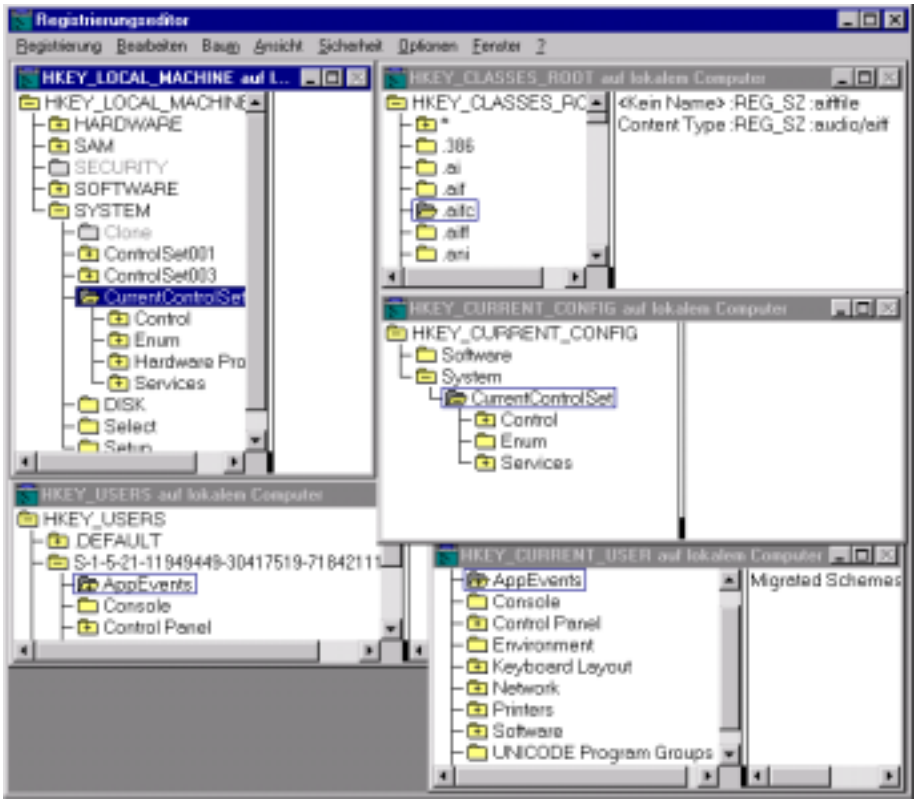
- Wenn ein Benutzer in einem Unterverzeichnis Rechte hat, so gewährt im NetWare auch auf dem Pfad dorthin das filecan-Recht, damit er das Verzeichnis auch finden kann. Dies ist bei NT nicht so. Hat ein Benutzer in einem darüber befindlichen Verzeichnis keine Rechte, kann er nicht per ”CD Verzeichnis” an die Stelle gelangen. Tip: Vor der Installation der Gruppe „Domänenbenutzer“ das Leserecht auf den kompletten Baum geben und dann je Unterverzeichnis entziehen bzw. richtig zuweisen.
- Auf Verzeichnisse gibt es das ”eXecute”-Recht. Dieses ist Notwendig, um einen ”Change directory” zu machen. ”Read” reicht nicht alleine aus.
- Es ist möglich, daß auf ein Verzeichnis niemand mehr Rechte hat. Da Rechte nicht vererbt werden, kommt damit auch der Administrator mit allen Rechte auf die Wurzel nicht mehr hin. Dieses Verzeichnis ist trotzdem kein ”toter Zweig”, denn der ”Besitzer” kann die Rechte ändern, auch wenn er zu dem Zeitpunkt keine hat.
- Bei NetWare kann jedes Verzeichnis vom Klient mittels ”MAP” zugeordnet werden. Das Verzeichnis kann mit MAP ROOT auch als

Basisverzeichnis genutzt werden. Bei WindowsNT können nur Freigaben zugeordnet werden. Diese sind automatisch die Wurzel. Die Nutzung eines Unterverzeichnisses als Wurzel ist nicht möglich.

Auch WindowsNT erlaubt die Rechte per Kommandozeile zu verändern. Parallel zu den Novellbefehlen Grant, Remove, Revoke, Tlist und Rights bzw. “RIGHTS alleine bei NetWare 4 heißt das Programm unter WindowsNT “CACLS”. Im Gegensatz zum Explorer können hiermit auch Rechte “verändert” werden, d.h. die Rechte werden nicht zwingend “ersetzt”.

Die Registrierung von Windows NT

Die Registrierung (Registy)gibt es schon seit Windows 3.1. Mit Windows95 und OLE-Verknüpfungen wurde die Mehrzahl der Anwender erstmalig darauf aufmerksam. Bei WindowsNT ist die Registrierung die wichtigste Konfigurationsdatei und alle INI-Dateien ablösen. Die Registrierung bietet einen sehr schnellen Zugriff auf die Daten, da sie keine sequentielle auf 64kByte begrenzte Textdatei ist. Die Registrierung bei WindowsNT spaltet sich in verschiedene Unterschlüssel auf, die in eigenen Dateien unter %Systemroot%\System32\CONFIG abgelegt sind. Diese Dateien sind transaktionsgesichert, so daß auch plötzliche Ausfälle keinen Schaden hinterlassen sollten. Es ist möglich, den vom Benutzer abhängigen Teil der Registrierung auf einem Server zu plazieren und beim Anmelden einzubinden.



Die Schlüssel der Registrierung bedeuten im einzelnen:

HKEY_LOCAL_MACHINE

Dieser Zweig beschreibt den Rechner und besteht aus dem Zwei SYSTEM, SAM, SECURITY, welche intern als eigene Dateien existieren und dem Zweig HARDWARE, der bei jedem Start neu gebildet wird. In SYSTEM sind alle Dienste, Kartenparameter etc. hinterlegt. Der Teilbaum SOFTWARE beschreibt die installierte Software

HKEY_USERS

Dieser Teilbaum enthält die Einstellungen aller lokalen Benutzer, wenn welche angelegt sind. Der jeweilige Teilbaum mit der SID des angemeldeten Benutzers wird auf HKEY_CURRENT_USER zugeordnet. Beim Einsatz eines serverbasierten Profils ist dieser Zweig nicht genutzt.

HKEY_CURRENT_USER

Hier sind die eigentlichen Einstellungen für den Benutzer abgelegt. Dies ist entweder ein Teil von HKEY_USERS oder das serverbasierte Profil.

HKEY_CURRENT_CONFIG

Dies ist eine Teilmenge von HKEY_LOCAL_MACHINE und beschreibt die aktuelle Konfiguration. Dieser Zweig ist erst bei NT4 verfügbar, da ab hier verschiedene Hardwareprofile benutzt werden können

HKEY_CLASSES_ROOT

Dieser Teilbaum vom HKEY_LOCAL_MACHINE/SOFTWARE/Classes beschreibt die Dateiverknüpfungen.

Wichtig ist dabei zu wissen, daß Schlüssel überlagert werden. Wenn eine Anwendung z.B. unter SOFTWARE\Herstellername einen bestimmten Wert sucht, dann wird in der Registrierung zuerst in HKEY_CURRENT_USER gesucht. Ist dieser Wert dort nicht vorhanden, wird in HKEY_LOCAL_MACHINE/SOFTWARE gesucht. Damit können Einstellung in HKEY_LOCAL_MACHINE als Defaultwerte angenommen werden, wenn die jeweilige Anwendung für den Benutzer noch keine eigene Einstellungen gemacht hat.

Dies hat z.B. den Vorteil, daß Anwendungen vom Administrator lokal installiert werden können, und die Parameter (Pfade zu Programmen etc.) für alle Benutzer gelten, sofern diese keine eigenen Einstellungen durchgeführt haben. Leider legen einige Installationsprogramme noch nicht alle Werte global ab, sondern schreiben einige Parameter direkt in die Benutzereinstellungen des installierenden Benutzers. Ein anderer Benutzer an diesem Rechner wird dann nicht alle Funktionen des Programms nutzen können. Umgekehrt sind Probleme zu erwarten, wenn Anwendungen auf verschiedenen Rechnern in verschiedenen Pfaden installiert sind. Ideal ist der Start einer Anwendung vom Server mit immer dem gleichen Pfad.

Änderungen an der Registrierung können mit REGEDT32.EXE lokal als auch über das Netzwerk ausgeführt werden. Ebenso gibt es Hilfsprogramme (REGINI.EXE) um batchgesteuert Veränderungen auszuführen, sofern die notwendigen Rechte dazu vorhanden sind. Ähnlich dem Dateisystem können auch auf Zweige der Registrierung Rechte gegeben und genommen werden. Dies kann bis zur Unbrauchbarkeit von WindowsNT führen.

Um die Veränderung der Registrierung über das Netzwerk auf Administratoren zu beschränken, reicht es, den Schlüssel HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipe Servers\winreg einzutragen. Bei NT3.51 sollte dazu der Gruppe Everyone

die Rechte auf HKEY_LOCAL_MACHINE (aber nicht darunter !!) auf lesen beschränkt werden.

Domain vs. NDS

NetWare 3.x speicherte Benutzer, Gruppen und Zuordnungen in der Bindery. Diese ist Serverbasiert, d.h. jeder Server führt seine eigene Datenbank mit eigenen Benutzern. Eine Synchronisation findet nicht statt. Nur die ebenfalls in der Bindery abgelegten dynamischen Einträge (Server etc.) werden per SAP's verteilt und so auf allen Servern eingetragen. Einige Zeit gab es von Novell den "NetWare Name Service", welche aus einem Satz Programme (NETCON etc.) bestand, welche die alten Administrationsprogramme (SYSCON) ablösten. Der Administrator hat dann beim Anlegen neuer Benutzer diese an allen Servern der Domäne angelegt.

Diese Ansicht ist mit dem Domänenmodell von WindowsNT vergleichbar. Mehrere Server und Workstations können in einer Domäne zusammengefaßt werden und nutzen die gleiche Sicherheitsdatenbank. Ein NT-Server ist dabei der primäre Domänenkontroller (PDC), während andere NT-Server als Backupdomainkontroller (BDC) zur Lastverteilung und Sicherung dienen können oder "nur Server" sind. Dies ist vergleichbar mit einer Replikation der NDS, bei der ein Server die MASTER-Replikation der [ROOT] trägt und andere Server eine Read/Write-Replika tragen oder keine.

Beim Windows NT Domänen besteht jedoch nicht die Möglichkeit einer "ReadOnly"-Replika und auch eine Untergliederung in verschiedene Teile (Partitionierung der NDS) ist nicht möglich. Repliziert wird alles oder nichts. Alle Benutzer und Drucker einer Domäne sind damit in der gleichen "Liste". Es können mehrere Domänen in einem Netzwerk eingerichtet werden, welche gegenseitig eine Vertrauensstellung erhalten. So können Benutzer in Domänen gruppiert werden, und trotzdem auf Ressourcen in anderen Domänen zugreifen. Ein NT-Server kann aber immer nur in einer Domäne sein, so daß mindestens genauso viele NT-Server existieren müssen, wie Domänen geplant sind während bei NetWare die NDS auf dem gleichen Server mehrere verschiedene Partitionen tragen kann. Zur Ausfallsicherheit sollten zudem Backupdomaincontroller vorgesehen werden, die aber ebenfalls nur eine Domäne sichern können. Bei der Anmeldung eines Benutzer oder Änderung eines Paßwortes wird immer der primäre Domänencontroller angefragt, wodurch WAN-Verbindungen entsprechend kostenintensiv werden. Die NDS bietet hier den besseren Ansatz, da die Replikation serverbasiert zu bestimmten Zeiten passiert und mit aktuellen Routern auch auf bestimmte Zeiten einstellbar ist. Ein Anwender kann sich auch an jedem Server mit einer R/W-Replika anmelden kann und sucht nicht den Master. Auch bei WindowsNT reicht ein BDC zur Authorisierung aus, die Suche nach dem PDC bleibt jedoch bestehen.

Mit dem Microsoft Client und dem alten Novell Client für Windows NT kann auf einen DomainController nicht ohne Einbußen verzichtet werden, da ansonsten alle Benutzer auf allen NT-Workstations und Servern lokal eingerichtet werden müßten. Erst der neue NT-Client von Novell erlaubt es, NetWare als "Security Provider" zu nutzen und auch Registry Werte in der NDS zu speichern. Bei der Anmeldung wird der Benutzer automatisch als lokaler NT-Benutzer angelegt und mit den notwendigen Rechten versehen. Die Einstellungen werden ebenfalls aus der NDS gelesen, womit eine zentrale Administration über die NDS möglich wird. Allerdings sind einige Funktionen der MS-Produktserie (z.B. MS Exchange) nur nutzbar, wenn eine NT-Domäne vorhanden ist. So muß sich jeder Administrator Gedanken

machen wie der die Benutzer eines gemischten Netzwerks einfach administriert.

Windows NT Server und NetWare

WindowsNT Server verfolgt andere Ziele, als NetWare. Während Novell NetWare primäre Datei- und Druckdienste anbietet, und Drittdienste wie E-Mail, Datenbankserver, Jobsserver extra als NLMs entwickelt werden mußten, ist WindowsNT die bessere Plattform für Anwendungsserver, wenn es nach Microsoft geht. Ein echter Fileserver benötigt z.B. keinen ”virtuellen” Speicher, sondern sollte selbst möglichst wenig Speicher benutzen und alles übrige als Cache den angeschlossenen Systemen zugänglich machen. Für einen Anwendungsserver ist dies fatal, da erst virtueller Speicher, Paging, Swapping etc. die Entwicklung und den Einsatz bestimmter Anwendungen zulassen. Diese Auslagerung von Speicherseiten benötigen aber Zeit und belasten die Festplatten, wodurch die reine ”Fileservertauglichkeit” des Systems abnimmt. Ein Anwendungssserver muß auch in der Disziplin Speicherschutz und Multitasking anderen Anforderungen genügen. Die zusätzliche Stabilität, die NT durch eben diese Kontrollmechanismen erreicht, gehen zu Lasten der Geschwindigkeit. Ein NetWare-Server, der einfach das tut, wofür er primär entwickelt wurde, ist ebenso stabil aber schneller, allerdings durch unsaubere NLMs sehr viel einfacher zum Absturz zu bringen. Umgekehrt verleitet die ”DosBox” von Windows NT oft dazu, Programme zu starten und damit auch NT zu schwächen. Angriffe auf den NetWare-Server können in der Regel nur vom LAN aus geführt werden.

Bei zwei gleich ausgestatteten Systemen wird NetWare im Bezug auf Dateidienste immer schneller sein. Allerdings nehmen Speicher- und Prozessorleistung beinahe täglich zu. Daher finden Sich in großen Netzwerken immer mehr Mischformen, bei denen beide Systeme nebeneinander dafür eingesetzt sind, wofür diese am besten geeignet sind. NetWare als Datei und Druckserver, WindowsNT als Anwendungsserver. Eine große Herausforderungen sind die grundlegend anderen Ansichten der Rechtevergabe, wodurch die Administration erschwert wird.

Administrator, Supervisor, Admin, root - wer darf was ?

Die Rechteteilung bei WindowsNT ist ab besten mit NetWare 3.x vergleichbar. Analog zum ”SUPERVISOR” gibt es unter WindowsNT einen ADMINISTRATOR. Die Gruppe EVERYONE unter NetWare entspricht in etwa der Gruppe ”Domainbenutzer” unter WindowsNT. Zusätzlich gibt es unter WindowsNT Gruppen (Domainadministratoren, Sicherungsadministratoren etc.), deren Mitglieder weitreichende Rechte haben. Sie können z.B. Eigentümer fremder Dateien werden und so auf diese zugreifen. Ebenso kann hier die Übersetzung in die Landessprache ein Schnippchen schlagen, da einige Anwendungen die englischen Namen erfordern. Eine verteilte Rechtevergabe auch für Administratoren, wie diese mit der Novell NDS möglich ist, ist mit NT schwer möglich. Die Unterteilung in verschiedene Domänen erlaubt eine Untergliederung.

Einen Unterschied zwischen WindowsNT und NetWare gibt es auch beim Paßwort. Die Paßworte bei NT sind sensibel im Bezug auf Groß und

Kleinschreibung, was bei NetWare nicht zutrifft. Dafür bietet NetWare einige Optionen mehr, um Benutzer zu Paßwortänderungen und sicheren Paßworten zu zwingend. Einstellungen für die Passwortlänge und Verfallszeiten sind bei NetWare je Benutzer einstellbar, während WindowsNT dies global je Domäne handhabt.

Protokolle im LAN

Windows NT Workstation als auch Server sind sehr flexibel, was die Nutzung möglicher Protokolle angeht. Dabei basiert die komplette Netzwerkkommunikation letztlich auf den von NetBios bekannten Protokollen. Auch wenn IPX oder TCPIP statt das originäre NetBEUI benutzt werden, dienen diese Protokolle immer nur als Transportmittel. Die Abkürzung NBT, welche bei einigen Programmen vorkommt (z.B. NBTSTAT) deutet auch darauf hin, daß damit ”NetBios über TCPIP” gemeint ist. Dies ist aber nicht unbedingt als ”Mangel” zu betrachten, da auch NetWare eigentlich das Protokoll IPX ”nur” als Transportdienst nutzt und die eigentlichen Netzwerkanfragen (NetWare Core Protocol, NCP) ebenfalls in IPX eingepackt werden. Beim Einsatz von TCP/IP werden dabei die Sockets 137 bis 139 genutzt. Mit diesem Wissen ist es einfach, Wählverbindungen für diesen Verkehr zu blockieren. Mit IPX werden daraus die berühmten Typ 20-Pakete, die Multiprotokollrouter schon lange filtern können.

NetBEUI selbst ist ein ”nicht routbares” Protokoll und beschränkt sich auf ein Netzwerksegment. Bridges und Switches sind dabei keine Hindernisse. Einige Router erlauben es, NetBEUI, IPX Typ 20 oder NBT-Pakete zu forwarden, damit Microsoft Netzwerke über Router hinweg funktionieren. Besonders der bei NetWare oft eingesetzte MPR for ISDN erlaubt hier sehr individuelle Einstellungen. Die einstellbare Filterung von NetBios Paketen bezieht sich in der Version 3.1 gleichzeitig auf IPX und TCPIP. Frühere Versionen filterten nur NetBios über IPX. Ist heute das getrennte Filtern von NetBios über IPX und IP notwendig, muß dies mit FILTCFG konfiguriert werden.

Aber auch ohne diese Fähigkeit kann ein Microsoft Netzwerk über Router hinweg funktionieren, wenn entsprechende Hilfsmittel (Wins, LMHOSTS, DNS etc.) zur Verfügung stehen. Gerade der Einsatz eines WINS-Servers ist in größeren Netzwerken wichtig, da damit die Anzahl der Broadcasts stark reduziert wird und das Antwortverhalten zunimmt.

TCPIP-Sicherheit

Sofern der NT-Server am Internet erreichbar ist und nur als HTTP oder FTP-Server dienen soll, gibt es einige einfache Regeln, um Angriffe abzuwehren. Über TCPIP arbeitet NetBios mit den Ports 137,138, und 139. Sperren Sie diese beim Router, damit diese Zugriffe nicht möglich sind. Weiterhin sollten sie eine eigene Netzwerkkarte für die offizielle IP-Seite haben. Dann ist es möglich, Services (WINS, DHCP, SERVER etc.) an dieser Netzwerkkarte zu deaktivieren.

Unter WindowsNT 4.0 können auch auf dem Server selbst einfache Filter auf PORT-Basis gesetzt werden. Erlauben Sie z.B. nur eingehende Verbindungen auf den notwendigen Ports. (20/21=FTP, 25=SMTP, 42/53 für

DNS, 70=Gopher, 80 HTTP) Sie reduzieren damit effektiv die möglichen Schwachpunkte.

Die dann erlaubten Dienste sollten ebenfalls beschränkt werden. Die Internetsuite bei WindowsNT 4 legt dazu einen eigenen Benutzer IUSR_servername an. Wenn Sie einen anderen Webserver nutzen, sollten sie ebenfalls ein eigenes Benutzerkonto anlegen und diesem nur die absolut notwendigen Rechte geben. Aktuelle Service Packs sollten Windows NT auch gegen bekannte Bugs standfest machen (”Ping of Death”). NetWare ist hier von Hause aus sicherer, da z.B. keine eigenen Programme auf dem Server gestartet werden können und die meisten Dienste ohne TCP/IP auskommen. Erst beim Einsatz von NetWareNFS, FlexIP, NetWareIP oder anderen IP-Produkten ist eine genauere Betrachtung notwendig.

Browser, WINS, DNS und LMHOSTS

In jedem Netzwerk muß es Mechanismen zur Suche und Anzeige von Ressourcen geben. Bei NetWare werden meist Server, Festplatten und Drucker gesucht. Da Novell Server dedizierte Rechner sind, kann in solchen Netzwerken davon ausgegangen werden, daß diese Server die aktiven Systeme kennen und bereitwillig Auskunft geben. Der Klient braucht dann nur den nächsten Server zu fragen.

Bei Microsoft Netzwerken gibt es mehrere Möglichkeiten der Namensauflösung. Mit einem NT-Server kann der WINS- Dienst aktiviert werden, welcher ebenso ”Bekanntmachungen” der Systeme sammelt und auf Anfragen antwortet. Ohne diesen Service suchen Rechner andere Dienste per Broadcast. Namensauflösungen können auch über die Datei LMHOSTS (analog zur /etc/hosts bei UNIX oder NetWare) oder per DNS (nur mit TCPIP) durchgeführt werden. Ohne WINS sind komplexere Netzwerke (z.B.: über Router hinweg) nur bedingt realisierbar oder sehr aufwendig zu pflegen.

Unabhängig von der angeforderten Auflösung nach Namen arbeitet der Browserdienst. Vergleichbar zu ”SLIST” oder ”NLIST SERVER” bei NetWare kann über den Browser eine Liste der aktiven Dienste ausgewählt werden. Der Browser erhält seine Informationen durch Broadcasts, die jeder Dienst regelmäßig (3,6,9,12 Min Rhythmus) absendet. Dies ist vergleichbar zu den Novell ”SAP’s”. Während bei NetWare jeder Server automatisch diese Daten vorhält, ist bei Microsoft dies nicht immer vorbestimmt. Historisch aus einem ”Windows for Workgroups”-Netz entstanden, kann auch eine normale Arbeitsstation ”Browser” sein, d.h. für andere Arbeitsstationen Informationen anbieten. Je häufiger PCs neu gestartet werden, desto öfter wechseln sich die Rollen. Erst mit einem NT-Server kommt mehr Ruhe in dieses Spiel, da die verschiedenen Betriebssysteme (WFW, WindowsNT WindowsNT-Server, Domaincontroller) verschiedene Wertigkeiten haben. Läuft im eigenen Netzwerk ein Domaincontroller, so wird dieser automatisch zum Masterbrowser. Dazu kommen für je 32 Stationen im Netzwerk weitere Backupbrowser und potentielle Browser. Dies können auch normale Arbeitsstationen sein. Wichtig ist zu wissen daß Browser bei TCPIP immer nur im eigenen Subnetz arbeiten, d.h. wer mehrere IP-Subnetze plant, und keinen NT-Server als Browser hat, wird sich damit anfreunden müssen, daß normale Workgroupsrechner zum Browser werden. Da so nicht immer eine serverbasierte Datenbank vorliegt, ist es möglich, daß Dienste bis fast eine Stunde nach ihrem Abschalten noch angezeigt werden, Umgekehrt tauchen neue Dienste nicht sofort auf. Oftmals ist ein Arbeitsplatzrechner mit wenig Speicher nicht schnell genug, um alles zu verarbeiten. Wer letztlich zum

Browser wird, legt ein Auswahlverfahren (Election) fest, welches manchmal auch von Clients initiiert wird, und dadurch einige Zeit lang Namen nicht mehr aufgelöst werden können.

Eine Besonderheit gilt es zu beachten, wenn WindowsNT auch DNS zur Namensauflösung in Kombination mit NetWare verwendet: Wird z.B. ein Laufwerk auf einen Server zugeordnet (NET USE), so muß WindowsNT den Namens auflösen. Unabhängig, welcher Netzwerkprovider (NetWare oder LanMan) in der Prioritätenliste oben steht, erfragt WindowsNT den Namen per DNS. Ist nun auch der NetWare-Server in der DNS eingetragen (z.B. weil er als WWW-Server oder NFS-Server Dienste für TCPIP-basierte Clients erbringt), so findet NT diesen Eintrag und versucht per NetBios über TCPIP eine Verbindung aufzubauen. Auf diesem Ohr ist NetWare allerdings taub (sofern kein SAMBA für NetWare installiert ist), so daß WindowsNT erst nach einem Timeout diese Versuche abbricht und dann per IPX/NCP erneut aufsetzt. Je nach Einstellung sind Verzögerungen bis zu 45 Sekunden möglich.

Teilweise werden auch ohne DNS verlängerte Antwortzeiten beim Zugriff auf NetWare-Server beobachtet. Obwohl NetWare als erster Netzwerkprovider eingetragen ist, läßt WindowsNT es sich nicht nehmen, per Broadcast doch nach einem NT-Server des gleichen Namens zu suchen. Eine Verbindung zu NetWare wird erst danach (und nicht parallel dazu) versucht. Dies kann ebenfalls bis zu 4 Sekunden dauern. All dies passiert nur, wenn ein neuer directory handle zugeordnet werden muß. Beim Zugriff auf bestehende Laufwerke gibt es keine Verzögerung. Dadurch wird ein NetWare Server natürlich subjektiv langsamer, obwohl er gar nichts dazu kann.

Installationen unter WindowsNT

Die Installation von Programmen unter WindowsNT verläuft etwas anders als unter Windows 3.x. Abhängig von den Rechten und der Rechtevergabe kann ein Anwender keine Programme installieren oder die Installation schlägt fehl. Da ein Anwender in der Regel auch ein Laufwerk für seine Nutzdaten hat, kann er dieses zur Installation von Programmen angeben. Aber die meisten Programme versuchen ebenfalls DLL's, Schriften etc. in das Windows Systemverzeichnis zu kopieren. Bei einer ordentlichen Installation wird aber gerade dies im Sinne eines Schutz gegen Veränderungen nicht erlaubt sein. Ebenso sind Veränderungen an der Registrierung notwendig, die nicht immer von Anwendern durchgeführt werden dürfen. Leider ist bei einer Standardinstallation von WindowsNT der Teilschlüssel HKEY_CLASSES_ROOT für Anwender veränderbar. Dort finden sich die Verkettungen von Dateierweiterungen zu Programmen. Und diese gelten für jeden Anwender auf diesem System, d.h. sind nicht benutzerabhängig. Während bei Windows 3.1 Programme entweder serverbasiert oder auf dem Arbeitsplatz installiert werden konnten, muß der Administrator bei WindowsNT andere Techniken anwenden. Entweder er tritt selbst den Marsch durch alle Räume an, um Anwendungen unter seiner Administratorkennung zu installieren, oder er läßt für sich arbeiten. Microsoft SMS, Intel LanDesk und einige andere sollen hier dem Administrator helfen. Auf Interesse dürfte hier auch der "Zero Administration Kit (http://www.microsoft.com/windows/zak) von Microsoft stoßen. Am Ende läuft es darauf hinaus, daß der Administrator analysieren muß, welche Einstellungen und Dateien ein Programm zur Funktion benötigt. So könnten systemweite Dateien z.B. per Replikationsdienst vom Server auf die lokalen Festplatten kopiert werden. Der Replikationsdienst kann dabei andere

Rechte besitzen, als der Anwender selbst. Ein weiterer Schritt betrifft die Einträge der Registrierung, welche auf dem lokalen Rechner zu aktualisieren sind. Entsprechende Hilfsmittel wie REGINI sind im Resource Kit zu WindowsNT enthalten, damit Einträge batchgesteuert verändert werden können.

Bleiben zuletzt noch die Einträge der benutzerabhängigen Schlüssel (HKEY_CURRENT_USER) und dessen Desktop. Hier könnte das Anmeldeskript weiterhelfen. Einen passenden Interpreter findet sich im Internet unter dem Begriff KIXTART (http://netnet.net/~swilson/kix.html). Mittlerweile findet sich dieses hilfreiche Programm auch im NT4-ResourceKit und dient dazu, Registrierungswerte, INI-Dateien und Symbole und Gruppen auf dem Desktop zu verändern und Parameter der Netzwerkumgebung auszulesen. Aber all dies bedeutet, daß der Administrator die Anwendungen ”verstehen” muß. Nur sehr wenige Programme restaurieren die Umgebung beim Start nahezu alleine (positives Beispiel: Visio 4.1)

Es ist natürlich immer noch möglich, daß wir von festen Benutzern an festen Arbeitsplätzen ausgehen, und jeder Anwender für seinen PC selbst verantwortlich ist. Dann muß dieser auch die Rechte auf die lokale Festplatte haben, und sich selbst um die Software kümmern. Aber dies entspricht eher nicht der Vorstellung eines guten Netzwerks, denn die Anwender werden nicht für die Aktualisierung ihrer Arbeitsmittel bezahlt und die Anzahl der Mitarbeiter am Helpdesk muß auch begrenzt bleiben.

Wandernde Benutzer - Roaming profiles

Mit NetWare und Windows 3.x und Windows95 ist es möglich, wandernde Benutzer zu realisieren, d.h. Benutzer, die sich dauernd an anderen Rechnern anmelden oder Rechner an denen abwechselnd andere Benutzer arbeiten. Dabei ist es notwendig, daß die wichtigen Daten und Einstellungen serverbasiert abgespeichert werden. Dies ist dann realisierbar, wenn das Betriebssystem erst nach der Anbindung des Netzwerkes gestartet werden kann oder selbst erst nach der Anmeldung auf die notwendigen Einstellungen zugreift.

Auch WindowsNT erlaubt eine Trennung der Benutzereinstellungen von den Systemdaten, indem die Registrierung schon diese Trennung vorsieht. Bei NT 3.51 liegen dabei die kompletten Einstellungen in einer *.USR-Datei im WindowsNT-Share \\servername\NETLOGON. Bei Windows NT4 liegt das Profil und der Desktop in einem Verzeichnis mit dem Benutzernamen unter diesem Share oder einen entsprechend im Benutzermanager angegebenen Pfad. Bei der Anmeldung überprüft WindowsNT nun, ob das Profil auf dem Netzwerk aktueller ist als eine eventuell alte Kopie lokal und kopiert dieses bei Bedarf lokal. Gearbeitet wird immer mit dem lokalen Profil. Wird dabei ein WindowsNT-Rechner unvermittelt ausgeschaltet, werden die Einstellungen nicht wieder auf den Server zurückkopiert. Heikel ist dies dann, wenn Dokument auf solche einem ”Desktop” abgelegt werden. Diese bleiben lokal liegen und landen nicht auf dem Server, sind nicht im Backup und bei FAT-Partitionen nicht mal gegen fremde Zugriffe geschützt.

Besondere Beachtung bei WindowsNT 4.0 verdienen die früheren Programmsymbole. Nach der Ablösung des Programm Managers tauchen die Einträge zum Start von Programmen im Startmenü auf. Die Programmsymbole für ”alle Benutzer” sind lokal hinterlegt während ”private” Symbole mit dem Profil gespeichert werden. Dies hat aber die Folge, daß diese Programme nur dann aufrufbar sind, wenn der Pfad auf dem aktuellen

Rechner vorhanden ist. Dies ist jedoch nur dann gewährleistet, wenn das Programm entweder vom Server gestartet wird, oder der lokale Pfad bei allen Rechnern identisch ist. Eine entsprechende Planung muß daher bei der Installation der Clients vorgesehen werden. Ebenso sind die NTFS-Rechte auf diesen Baum relevant, um die Programmicons auch starten zu können.

Ein weiteres Problem ist die Ablage von Dateien. Mit Windows NT 4.0 können auf dem Desktop die Daten selbst oder nur Links auf die Dateien abgelegt werden. Während die Links auf Netzwerklaufwerke verweisen können und nur wenige Bytes groß sind, nehmen Nutzdaten mehr Speicherplatz ein. Daten auf dem Desktop werden bei jeder An- und Abmeldung zwischen lokaler Festplatte und Server transferiert. Dies kostet Zeit und belastet Netzwerk und Server. So sollten den Anwendern der kleine Unterschied ausführlich erklärt werden.

Leider sind die Profile von Windows NT nicht kompatibel zu Windows95. Ein Parallelbetrieb ist daher nicht einfach möglich. Auch eine einfache Übernahme der Windows 95-Einstellungen auf NT ist schwer möglich.

Viren mit Windows NT

Die meisten Viren bauen auf den Schwächen von DOS auf, indem sie Programme oder Startbereiche von Festplatten infizieren und dabei bei jedem Neustart aktiv und virulent werden.

Auch WindowsNT ist nicht gegen Viren und deren Schäden geschützt, da auch NT nicht im ROM des Rechners residiert, sondern von der Festplatte gebootet wird. Viren, die sich z.B. im Bootsektor einklinken, werden vor dem Start von WindowsNT aktiv und können einige Zeit lang ihr zerstörerisches Wert tun. Nachdem jedoch der WindowsNT gestartet wurde, werden alle BIOS-Funktionen des Rechners im protected mode nicht mehr genutzt, da passende 32bit-Treiber geladen werden. Viren klemmen sich in der Regel in diese Biosaufrufe ein, welche unter WindowsNT nicht mehr benutzt werden. Damit sind diese Viren ausgeschaltet.

WindowsNT selbst schützt zum Teil gegen Viren, da keine Programme direkt auf die Festplatte zugreifen können. Auch befallene Programme einer DOS-Box können nur innerhalb ihrer Umgebung arbeiten und keine anderen laufenden Programme erreichen. Dies gilt natürlich nur insoweit, wie der Benutzer am NT-System keine Schreibrechte auf die Programme hat. Leider hat der Benutzer im Standardsetup einige Rechte mehr, als dies sinnvoll erscheint. Ein Hilfsprogramm zum Anzeigen der Rechte bietet www.somarsoft.com mit dem Programm DUMPACL an.

Makroviren, wie sie immer mehr für Word und Excel auftauchen sind unter WindowsNT natürlich ebenso aktiv, wie unter Windows 3.x und Windows 95. Auch wenn WindowsNT mehr Schutzmechanismen bietet, besteht weiterhin die Gefahr einer Ansteckung, so daß die üblichen Regeln auch bei NT angewendet werden müssen. Mittlerweile gibt es auch Virenscanner, die auf NT-Servern mitlaufen und direkt Alarm schlagen, Das Booten von Disketten sollte wie bisher möglichst vermieden oder abgeschaltet werden und der Schreibschutz auf Programme kann mit WindowsNT auch auf die lokale Festplatte ausgedehnt werden. All dies gilt natürlich nur, bis ein findiger Programmierer eine Lücke entdeckt. Eine ausführlichere Quelle ist z.B. http://www.symantec.com/avcenter/reference/vbnt.html

Remote Boot, Update der Clients, Autoinstallation

WindowsNT Workstation ist im Gegensatz zu Windows 3.x und Windows 95 nicht fernstartfähig, d.h. das Betriebssystem kann nicht von einem Server bezogen werden. Allerdings kann ein Bootrom in der Workstation das Leben des Administrators immer noch vereinfachen. Auch wenn WindowsNT viele Schutzmechanismen mitbringt, ist es denkbar, daß die lokale Installation nicht mehr funktionstüchtig ist. Dann ist per Remotebootrom immer noch ein Fernstart möglich, so daß vom Server erneut eine Installation erfolgen kann. Dazu gibt es Programme, welche z.B. eine Festplatte als Dateiimage ablegen und wieder restaurieren können. So kann sehr schnell und automatisch eine Arbeitsstation wieder aktiviert werden, wenn keine lokalen Daten darauf liegen. Allerdings kann ein Rechner, der mit DOS gebootet worden ist, nur eingeschränkt auf NTFS-Partitionen zugreifen. (http://www.ntinternals.com/ntutil.htm) Wird daher NTFS eingesetzt, bleibt im Fehlerfall nur die Möglichkeit ein neues Setup durchzuführen. Wird hingegen FAT als Dateisystem genutzt kann der Administrator ohne Windows NT zumindest eine Prüfung auf Viren und veraltete oder veränderte DLL's vornehmen und gegebenenfalls aktualisieren. Ein Neustart sollte dann aber direkt von der Festplatte erfolgen.

Sicherheitslöcher in NT

Wie jedes Betriebssystem hat auch NT einige Löcher, die es zu stopfen gilt. Denn die Standardinstallation ist bei weitem nicht so, wie es wünschenswert erscheint, auch wenn von NT3.51 auf NT 4.0 einige Werte schon enger gefaßt wurden. Gute Quellen bietet auch hier das Internet, z.B. unter http://www.it.kth.se/~rom/ntsec.html oder http://www.somarsoft.com/security.htm.

1.1 Rechte auf Verzeichnisse

WindowsNT gibt dem normalen Anwender einige Rechte auf die lokale Festplatte. Zum Teil sind diese absolut notwendig (TEMP, Profilpfad), zum Teil aber auch gefährlich. Zum einen besteht die Gefahr, daß Programme verändert werden und dem nächsten Benutzer schaden, zum anderen legen einige Anwendungen (z.B. Terminalemulation) mit automatischer Anmeldung auch Paßworte in Konfigurationsdateien oder Skripten ab. Ein Zugriff anderer Benutzer hierauf sollte daher unterbunden werden. Am besten ist es, wenn Daten überhaupt nicht lokal landen.

1.2 Rechte auf die Registrierung

Ähnlich zu den Rechten auf Dateien können auch Rechte auf die Registrierung vergeben werden. Dabei haben Benutzer standardmäßig Rechte auf Zweige, die besser geschützt sein sollten. Die Zuordnung von Dateierweiterungen zu Programmen ist nur eine davon. Wer hindert einen Anwender sonst daran, z.B. die Erweiterung *.TXT mit einem Batchfile in C:\TEMP zu assoziieren, in welchen ganz andere Programme gestartet werden, ehe am Ende NOTEPAD %1 %2 %3 aufgerufen wird. Aus diesem Grund sollte dieser Teilbaum auf READONLY gesetzt werden. Diese Lücke trifft aber auf alle Schlüssel zu, die mit dem Start eines Programmes etwas zu tun haben und durch Benutzer veränderbar sind. Diese Probleme treten bei NetWare nicht auf, da der Schwerpunkt Datei und Druckdienste sind.

1.3 Die Sicherheit von NTFS

Jeder, der sich mit WindowsNT auseinandersetzt, wird mittlerweile von NTFSDOS gehört haben um unter Umgehung der Zugriffsmechanismen auf NTFS-Partitionen lesend zuzugreifen. Voraussetzung ist aber der physikalisch Zugriff auf den NT-Rechner und der Start mit DOS. Auch NetWare bietet gegen diesen Anschlag keinen Schutz, da die Daten auf den Festplatten beider Systeme nicht verschlüsselt werden. Letztlich sollten diese Hilfsmittel einem Administrator erlauben, Daten einer korrupten NT-Installation, die nicht mehr bootfähig ist, zu retten. Und ein physikalischer Zugangsschutz zu Servern durch Türen, Schlösser und dergleichen ist immer eine gute Idee. Racksysteme oder besondere Serversysteme zeichnen sich hier aus.

Ebenso gibt es eine Rechtekombination unter NTFS, welches unter bestimmten Umständen Benutzern erlaubt, Dateien zu löschen auf die sie durch Filerechte überhaupt keine Rechte haben dürften. Wird einem Benutzer oder einer Gruppe auf ein spezielles File das Rechte ”No Access” gegeben, dann können diese Anwender nicht darauf zugreifen, aber unter bestimmten Umständen trotzdem löschen. Genau dann, wenn der Anwender auf den höheren Ordner Vollzugriff hat. Per Default hat aber die Gruppe ”JEDER” auf eine lokale NTFS-Partition Vollzugriff. Der Anwender hat dann zwar keinen Zugriff auf die Datei aber doch auf die Verzeichniseinträge.

1.4 Der Papierkorb unter Windows NT

Der Papierkorb unter WindowsNT ist nur für den lokalen Rechner vorhanden. Werden Dateien auf einem Netzwerklaufwerk gelöscht, sind diese wirklich gelöscht, wenn kein Backup zur Verfügung steht. Im Gegensatz zu Netware gibt es bei WindowsNT kein ”Salvage” zum Restaurieren gelöschter Dateien. Wird lokal eine Datei gelöscht, landet diese im Papierkorb. Erst mit dem Einsatz von NTFS ist aber auch sichergestellt, daß jeder Anwender ”seinen” Papierkorb besitzt. Wird hingegen FAT eingesetzt, so kann später ein anderer Anwender die Daten der vorigen Benutzers restaurieren. Dies ist ein weiterer Grund, Daten nur auf Netzwerklaufwerken abzulegen und lokal möglichst keine Daten zu halten, oder NTFS einzusetzen.

1.5 WINS-Server braucht Rechte für Everyone

Teilweise sind es auch Systemdienste, die Dateizugriffe einer allgemeinen Gruppe benötigen. Im Artikel Q158865 der Microsoft Knowledgebase (http://www.microsoft.com/kb) wird beschrieben, daß der recht wichtige WINS-Server-Dienst nicht richtig startet, wenn die Gruppe Everyone (oder Domainbenutzer) nicht die Rechte ”Full Control” auf das Verzeichnis %Systemroot%\System32\WINS besitzt. Ein Anwender, der sich auf dem Server anmeldet, kann dann auf diese Datenbank zugreifen. Daher sollten sich auf den NT-Servern keine Anwender anmelden können, bzw. ein Server nicht als Workstation genutzt werden.

Resümee

WindowsNT Workstation wird aufgrund vieler Vorteile in nächster Zeit eine starke Durchdringung bei Arbeitsplätzen finden. Im Gegensatz zu Windows 3.x und Windows 95 bietet es erweiterte Sicherheitsfunktionen und Möglichkeiten für den Administrator. Aber es besitzt in der Grundausstattung auch einige Löcher, die gestopft werden müssen, damit sich die Vorteile

auch in höherer Funktionssicherheit und einfacher Pflege niederschlagen. Jedem Administrator von NT sei geraten, die gängigen Diskussionslisten, Zeitschriften und Informationsquellen (z.B. http://www.microsoft.com/kb) zu nutzen. Am breiten Einsatz von Windows NT Workstation führt in der nächsten Zeit kein Weg vorbei. Die Lizenzpolitik von Microsoft und natürlich auch das Potential von Windows NT Server wird auch serverseitig zu einem Umschwung führen.