Sicherheitsaspekte bei der Einsatzplanung von Microsoft Windows 2000

Matthias Hollick[1,2], Wolf Rosenow[2], Thomas Bormuth[2], Ralf Steinmetz[1,3]

[1] GMD Forschungszentrum Informationstechnik GmbH
IPSI – MOBILE, Dolivostrasse 15, D-64293 Darmstadt
[2] NFORMATION GmbH
Ober-Ramstädter-Strasse 96, D-64367 Mühltal
[3] Technische Universität Darmstadt
Institut für Prozess- und Systemkommunikation (KOM)
Merckstr. 25, D-64283 Darmstadt
matthias.hollick@darmstadt.gmd.de
wolf.rosenow, thomas.bormuth@nformation.de
ralf.steinmetz@kom.tu-darmstadt.de

Zusammenfassung: Die Einsatzplanung zur Integration moderner Betriebssysteme in bestehende Netze betrifft Universitäten und Forschungseinrichtungen aufgrund ihres innovativen Anforderungsprofils in besonderem Maße. Ein herausragender Bestandteil jeder Planung ist hierbei der Sicherheitsaspekt. Im folgenden stellen wir Ansätze vor, die bei Microsoft Windows 2000 Kernaspekte einer Sicherheitsplanung darstellen. Hierzu werden einleitend die Systemgrundlagen von Windows 2000 bzgl. Sicherheit geschildert. Anschließend wird ein Lösungsansatz erläutert, der die Planung einer Active Directory (AD) Struktur zur rollenbasierten Administration erläutert. Hierbei werden Planungshilfen gegeben und die zur Umsetzung verfügbaren Hilfsmittel vorgestellt. Abschließend stellt der Bericht eine Zusammenfassung der beschriebenen Bereiche dar.

1 Einleitung

Anwender im Universitäts- bzw. Forschungs-Bereich können als sehr innovativ bezeichnet werden. Ihre Anforderungen an die IT-Infrastruktur werden durch die Randbedingungen von Forschern festgelegt. Betriebsysteme stellen hierbei in vernetzten Umgebungen die Schnittstelle zwischen Informationsnetz und Benutzer dar. Diese Schnittstellenfunktion einerseits, der Verbund von Rechnern in administrativen Domänen andererseits bringt es mit sich, dass Sicherheit als Kernanforderung eines Netz-Betriebssystems gelten muss. In [Schneier2000] wird Systemsicherheit aus der Sicht des Praktikers geschildert, hierbei nehmen Betriebssysteme eine herausragende Rolle ein[1] (vgl. hierzu [Eckert2000] und [Tanenbaum2001]). Um vernetze Systeme sicher und effizient verwalten zu können, muss auf Basis einer sicheren Betriebssystemplattform der administrative Verbund von Systemen, die sog. Sicherheitsdomäne, einen weitreichenden Schutz bieten und optimal administriert werden können.

[1] An dieser Stelle soll nicht verheimlicht werden, dass in [Schneier2000] das Betriebssystem Windows 2000 aufgrund der nicht offengelegten Quelltexte und der Quellcodelänge von geschätzten 50 Millionen Zeilen als komplexes und nicht abzusicherndes System beschrieben wird.

Bereits bei der Einsatzplanung muss der Faktor Sicherheit angemessen berücksichtigt werden. Die Administration muss anhand von spezifizierten Richtlinien (Policies) erfolgen, möglichst mit Hilfe des zu verwaltenden Systems selbst. Um die Sicherheit im täglichen Einsatz zu gewährleisten, ist weiterhin ein fortlaufendes Risikomanagement durchzuführen.

Dieser Beitrag stellt einige Grundzüge der Sicherheitsplanung für das Microsoft Windows 2000 Betriebssystem dar[2] . Abschnitt 2 dient der Einführung in die grundlegende Systemstruktur sowie die Sicherheitsmechanismen des Windows 2000 Betriebssystems. Abschnitt 3 stellt die Grundlagen der Domänenplanung unter Berücksichtigung von Sicherheitsaspekten vor. Hierbei wird ausgehend von dem Prinzip der Delegation detailliert ein Entwurfsprozess für ein administratives Rollenkonzept beschrieben. In der Zusammenfassung erfolgt ein Ausblick der gleichzeitig die Thematik in einen umfassenderen Kontext eingebettet.

2 System- und Sicherheitsarchitektur von Microsoft Windows 2000

Im folgenden wird ein Überblick über die Systemstruktur von Windows 2000 mit dem Schwerpunkt Sicherheitsarchitektur dargestellt.

2.1 Systemarchitektur

Die Architektur von Windows 2000 basiert auf der von Microsoft für die Windows NT Versionen 3.1, 3.5, 3.51 und 4.0 entworfenen Architektur. Die Architektur von Windows 2000 sieht hierbei eine Trennung in Benutzer- und Kernelmodus vor. Im Benutzermodus befinden sich neben einigen fest verankerten System- und Dienstprozessen die Umgebungssubsysteme (Win32, POSIX, OS/2), die die nativen Betriebssystemfunktionen für die Applikationen zugänglich machen. Im Kernelmodus stellt die Windows 2000 Executive die grundlegenden Betriebssystemfunktionen wie Prozessverwaltung, Speicherverwaltung und sicherheitsrelevante Funktionen bereit. Der Windows 2000 Kernel beinhaltet die Betriebssystemfunktionen auf niedrigster Ebene (Interruptbehandlung, Scheduling). Gerätetreiber[3] übersetzen die Systemanfragen in gerätespezifische Anfragen (vgl. [SORU2000]).

2.2 Sicherheitsarchitektur

Der Ausgangspunkt für das Windows 2000 Sicherheitsmodell ist das von Windows NT 4.0. Dieses kann als eine solide Grundlage für ein sicheres Betriebssystem gelten. Eine detaillierte Sicherheitsanalyse von NT 4.0 zeigt jedoch Möglichkeiten zur Verbesserung auf, die im folgenden anhand einiger Schwachstellen und Problembereiche beschrieben werden:

[2] Die hierbei verwendeten Methoden wurden in Projekten der NFORMATION GmbH in Zusammenarbeit mit Beratern von Microsoft Deutschland entwickelt.

[3] Gerätetreiber und alle weiteren Komponenten des Kernelmodus sind insbesondere schutzbedürftig, da Windows 2000 bei deren Nutzung keine Sicherheitsüberprüfung durchführt, d. h. Windows 2000 vertraut den eigenen Komponenten im Kernelmodus, diese werden standardmäßig durch die Windows File Protection (WFP) geschützt.

– proprietäre Standards wie z.B. PPTP (vgl. hierzu [SM1999])
– mangelhafte Skalierbarkeit (z.B. Größenlimit der SAM-Datenbank, Beschränkung auf einfache Domänenstrukturen)
– fehlende Delegation administrativer Aufgaben durch unflexible Rechteverwaltung.

In Windows 2000 wurden, ausgehend von der NT 4.0 Sicherheit, viele Schwachstellen beseitigt und zusätzliche Funktionalität eingefügt. Im folgenden werden die Grundkomponenten der Windows 2000 Sicherheitsarchitektur dargestellt (vgl. Abb. 1):

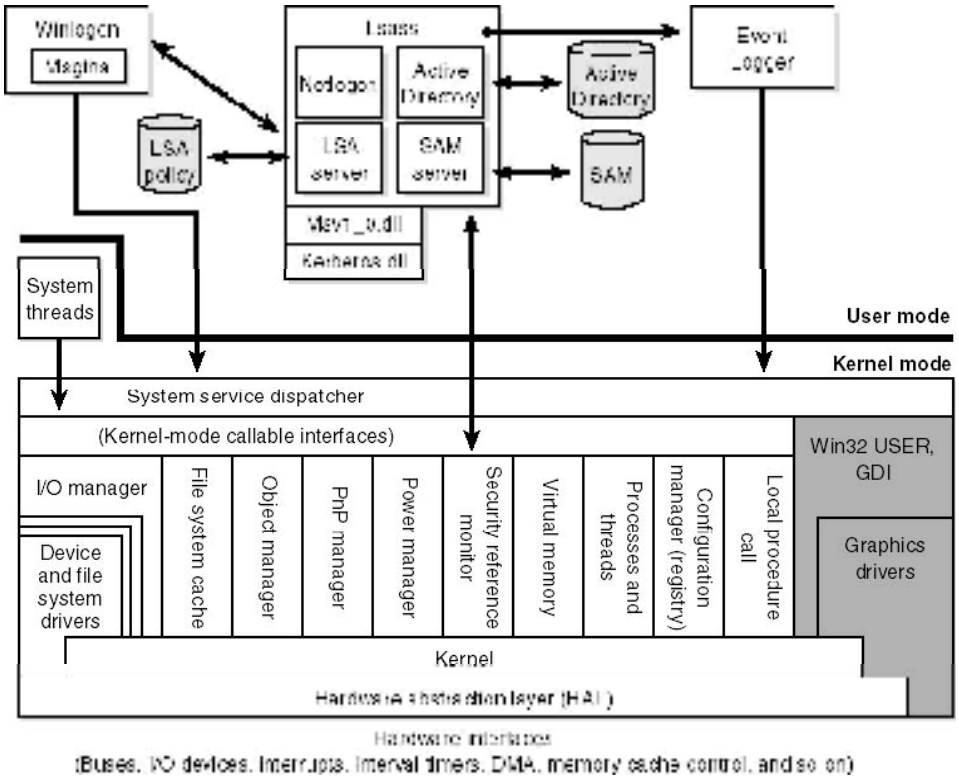

Abbildung 1. Die Windows 2000 Sicherheitsarchitektur [SORU2000]

Herauszuheben sind hierbei insbesondere Komponenten, die mit der Authentifizierung des Benutzers gegenüber dem Betriebssystem verknüpft sind, da diese die Basis der Sicherheitsarchitektur des Betriebssystems bilden – in Windows 2000 getragen von dem Active Directory Verzeichnisdienst. Da eine detaillierte Darstellung der Funktionen und Interaktion aller Komponenten den Rahmen dieses Beitrages sprengen würde wird nachfolgend der Bereich Active Directory genauer bzgl. Einsatzplanung und Delegation von Rechten untersucht.

Das Active Directory ist ein Verzeichnisdienst, der in einer Datenbank Informationen über alle relevanten Objekte der Domäne verwaltet. Eine Domäne ist ein Bereich von Rechnern, die von der selben administrativen Autorität verwaltet werden. In der AD-Datenbank sind Benutzerobjekte, Gruppeninformationen, Privilegien, Kennwörter etc. abgelegt und werden zwischen den Domänencontrollern einer Domäne repliziert. Die Serverkomponente des AD ist hierbei als Komponente des Kernelmodus implementiert.

Neben der engen Systemintegration stützt sich Active Directory auf Dynamic DNS (DDNS) ab, der die bisherige NetBIOS-Namenstruktur und deren Umsetzung mittels WINS ablöst. Als Zugriffsmechanismen auf das Active Directory kommen LDAP und das Active Directory Service Interface (ADSI) zum Einsatz. Neben der Erweiterbarkeit kann als Vorteil von Active Directory insbesondere die feine Granularität der Rechtevergabe und die somit mögliche flexible Delegation von administrativen Rechten genannt werden. Weitere administrative Hilfsmittel stellen die Bereitstellung von flexiblen und weitreichenden Gruppenrichtlinien dar, die eine feingranulare Richtlinienstruktur für alle Domänenobjekte beinhaltet.

Das Active Directory ist die zentrale Instanz, um alle weiteren Mechanismen zur Gewährleistung von Sicherheit im System mit Informationen zu versorgen. Aus diesem Grund ist die Verfügbarkeit sowie die Integrität, Authentizität und Vertraulichkeit der enthaltenen Daten als Kernziel eines Sicherheitskonzeptes anzusehen.

Weitere wichtige Neuerungen der Sicherheitsarchitektur von Windows 2000 umfassen die Bereitstellung des Security Support Provider Interface (SSPI) und der CryptoAPI, die einheitliche Schnittstellen für Applikationen zur Nutzung der von der Betriebssystemplattform angebotenen Sicherheitsdienste anbieten. Der Einsatz von PKI wird systemweit unterstützt und proprietäre Standards der Vorgängerversion wurden durch offene Standards wie *Lightweight Directory Access Protocol (LDAP), Kerberos Version 5, Public Key Cryptography Standards (PKCS), PC and smart card integration (PC/SC), DNS Security sowie IP Security (IPSec)* ersetzt.

Die Abstützung auf offenen Standards steigert neben der Systemsicherheit (eine saubere Implementierung seitens Microsoft vorausgesetzt) gleichzeitig die Interoperabilität und ermöglicht den Austausch von Windows Komponenten durch andere standardkonforme Implementationen. Darüber hinaus unterstützt Windows 2000 aus Abwärtskompatibilitätsgründen ältere, proprietäre und oftmals unsichere Standards – dieser Aspekt sollte bei einer Migration unbedingt berücksichtigt werden.

3 Design einer sicherheitsbewussten Active Directory Infrastruktur unter administrativen Gesichtspunkten

Die Qualität eines Verzeichnisdienstes wird unter anderem an der Verfügbarkeit der Informationen und Ressourcen sowie dem Schutz derselben gemessen. Um dies optimal zu gewährleisten, stellt die Administration der Verzeichnisstruktur eine geschäftskritische Aufgabe dar. Im folgenden wird anhand der in Windows 2000 zur Verfügung gestellten Mechanismen beschrieben, wie administrative Rollen definiert und umgesetzt werden können. Als Hilfsmittel zur Organisation stehen hierbei Sicherheitsgruppen, Group Poli-

cy (GP) Objekte und eine Strukturierung der organisatorischen Einheiten (Organizational Unit – OU) zur Verfügung.

Eine Möglichkeit administrativen Aufwand zu minimieren ist, die dezentralen Aufgaben zu delegieren. Windows 2000 macht die Delegation einfacher als Windows NT. Es erlaubt die Verantwortlichkeit für die Verwaltung von Bereichen des Namensraumes an Benutzer oder Gruppen abzugeben. Der Empfänger der delegierten Berechtigungen kann die ausgewählten Teile der administrativen Kontrolle innerhalb des festgelegten Bereiches ausüben.

3.1 Rollen und Delegation

Kernpunkt unserer Konzeption ist die Organisation der Administration und die Einbindung der Services in die Active Directory Struktur. Die Definition administrativer Rollen dient zur Abgrenzung der Administration bzgl. verschiedener Bereiche ("need to know" Prinzip)[4] , um zusätzliche Sicherheit zu erreichen und die Grundlage einer erfolgreichen Delegation zu schaffen.

Administrative Rollen ordnen Tätigkeiten der Systembetreuung nach administrativen Aufgabengebieten ein. Durch eine derartige Gruppierung der Tätigkeiten, können Beziehungen zwischen ihnen und Benutzergruppen hergestellt werden. Auf der anderen Seite können anhand von Tätigkeiten die dafür benötigten Berechtigungen definiert werden. Schließlich kann durch die Definition von administrativen Rollen eine Beziehung zwischen benötigten Berechtigungen für administrative Tätigkeiten und Benutzergruppen hergestellt werden.[5] Die in Windows 2000 Active Directory verwendete Zugriffskontrolle (Access Control) enthält letztlich auf der Basis einer Mandatory Access Control (MDAC) zusätzlich Anleihen von rollen- (RBAC) und taskbasierten (TBAC) Ansätzen.

Windows 2000 mit einer Active Directory Infrastruktur erlaubt die differenzierte Vergabe von Rechten auf Netzwerkobjekte. Daher können die bisher oft nur organisatorisch verwendeten administrativen Rollen nun auch für die Verwaltung von Benutzergruppen und die Vergabe von Berechtigungen herangezogen werden.

Das Erarbeiten von administrativen Rollen ist stark abhängig von der Organisation, in der Windows 2000 eingeführt wird. Bei den Rollen kann vorab folgende grundlegende Unterscheidung getroffen werden: *Direkt auf das Active Directory bezogene Tätigkeiten vs. Tätigkeiten zur Bereitstellung von Diensten.* Eine weitere Unterscheidung ergibt sich durch die Abbildung eines physischen und oftmals vermaschten Systems in logische Administrationseinheiten. Hierzu kann zwischen *dezentralen und zentralen administrativen Tätigkeiten* unterschieden werden. Dies soll im folgenden anhand eines Beispiels erläutert werden:

[4] In vielen Windows Umgebungen ist es üblich, alle Administratoren mit den Standardrechten zu versehen. Dies stellt eine signifikante Verletzung des Grundsatzes "so viele Rechte wie nötig, so wenige Rechte wie möglich" dar.

[5] Auch in Windows NT 4.0 ist eine Definition von administrativen Rollen auf organisatorischer Ebene möglich. Durch die eingeschränkten Möglichkeiten der Differenzierung von Rechten ist die Zuordnung von administrativen Benutzergruppen über Rollen auf bestimmte Rechte nur schwer zu realisieren. Als Folge davon gibt es in NT 4.0 oftmals eine große Anzahl an Administratoren mit umfangreichen Rechten.

Infrastruktur AD-Tätigkeiten wie das Management der unternehmensweit verfügbaren Benutzer und Gruppen im AD werden üblicherweise zentral ausgeführt; delegierte AD-Tätigkeiten wie das Management von Benutzer, Gruppen und Services auf Arbeitsgruppen-Ebene erfolgen üblicherweise dezentral.

Diese Trennung von zentral und dezentral ist nicht statisch, sondern dynamisch und flexibel anpassbar an die Anforderungen. Prinzipiell sollte im Rahmen der Standardisierung der Ansatz eine zentrale Administration sein, der aber dezentrale Möglichkeiten offen lässt.

Eine detaillierte Definition administrativer Rollen erfolgt auf der Grundlage der im Unternehmen definierten Management-Funktionen (wie z.B. Operation-, Change-, Security-, Configuration-, Performance-, Problem- und Business-Management). Als zweiter Planungsbestandteil dient eine abstrahierte Darstellung der existenten administrativen Betriebsstruktur. Die Matrix aus den beiden Determinanten ist in Tabelle 1 dargestellt. Die sich ergebenden Rollen müssen hierbei genau definiert werden (leere Tabellenfelder sind erlaubt) und ergeben schließlich die weiter zu untersuchenden administrativen Rollen.

	Problem-Management	**Security Management**	**...**
Help Desk	First Level Support (Rolle 1)		?
Operating		Audit Ereignisse überwachen (Rolle 3)	?
Anwendungen	Last Level Support Anwendungen (Rolle 2)	Security Anwendungen (Rolle 4)	?
...	?	?	?

Tabelle 1. Matrix zur Rollendefinition

Jeder definierten Rolle müssen nun die entsprechenden Tätigkeiten zugeordnet werden. In real umgesetzten System werden bspw. auftretende Probleme vom Kunden/Benutzer an den Help Desk eskaliert (First Level Support), der zur Betreuung von Benutzern bestimmte Berechtigungen benötigt. Dieser wiederum eskaliert das Problem an den Second Level oder Last Level Support, wenn er das aufgetretene Problem nicht alleine beheben kann.

3.2 Praxisanforderung

Die im Rahmen einer theoretischen Evaluation erarbeiteten Aspekte der Administration müssen schließlich in die Praxis überführt werden. Befolgt man die vorstehenden Überlegungen wird bei der Implementierung ein sehr großer administrativer Aufwand erzeugt. Dies resultiert unter anderem daraus, dass administrierende Mitarbeiter mehrere Rollen vereinen und die detaillierte Berechtigungsvergabe zusätzlichen administrativen Aufwand bedeutet. Es muss ein praktikabler Mittelweg gefunden werden, der die Sicherheit und Organisierbarkeit des Rollensystems mit den Anforderungen der Praxis vereint. Dies wird umgesetzt, indem eine Beschränkung auf geeignete Basisrollen erfolgt, mit der Option, bei Bedarf Erweiterungen vornehmen zu können. In einer von uns implementierten AD-Struktur erfolgte dies durch die Definition von vier Basisrollen, die aus vormals etwa 30

administrativen Rollen destilliert wurden (vgl. Abb. 2). Die Konten der Administratoren wurden hierbei in globale und lokale Sicherheitsgruppen abgebildet. Es existieren zusätzlich auf der höchsten Administrationsebene sogenannten Super Administratoren, die nahezu uneingeschränkte Berechtigungen besitzen.

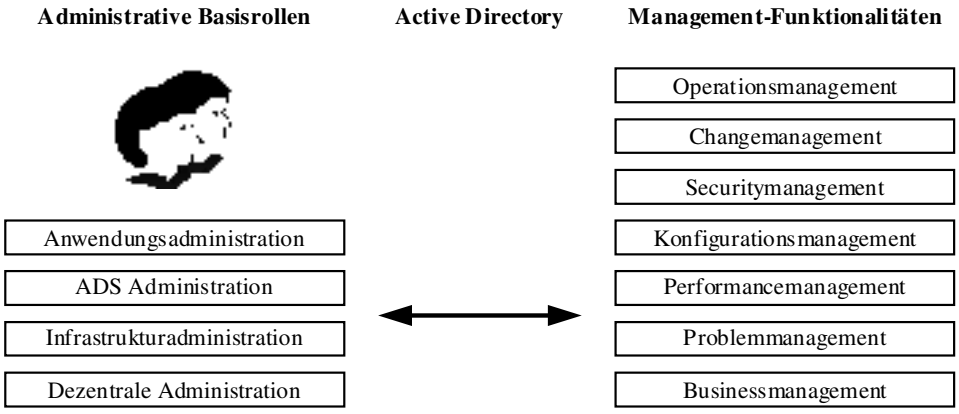

Abbildung 2. Die vier administrativen Basisrollen und die rollenübergreifenden Managementbereiche

3.3 Umsetzung der Rollen / Delegation

Um das beschriebene Konzept umzusetzen, ist es notwendig, eine der Organisation angepasste Active Directory Struktur zu entwerfen. Innerhalb von Domänen werden OUs genutzt, die eine hohe Flexibilität bieten. Die Konzeption von Sicherheitsgruppen und die Zuordnung der administrativen Rollen erfordert eine genaue Planung. Zur weiteren Vereinheitlichung der Administration sollten Gruppenrichtlinien implementiert werden

Es gibt Fälle, in denen die Organisationsstruktur des Unternehmens mehrere Domänen erfordert, weil eine zentrale Administrationsinstanz fehlt, die Berechtigungen an die Organisationseinheit eines Geschäftsbereichs delegieren kann. Bei einem solchen Entwurf werden strengere Sicherheitsbegrenzungen zwischen Geschäftsbereichen eingeführt, als dies bei einem Eindomänen Modell der Fall ist. Trotzdem ist eine zentrale Administration über Domänengrenzen hinweg möglich, deren Implementierung jedoch aufwendiger ist.

3.4 Planung der Organisatorischen Einheiten

Die Zuweisung von Kontrolle auf Basis von OUs sollte bevorzugt verwandt werden, da die Vergabe von Berechtigungen auf Objekt Ebene schnell unübersichtlich wird und die Vergabe auf Domänen- oder Site-Ebene weitreichendere Auswirkungen haben kann, als ursprünglich vorgesehen war. [6]

[6] In jedem Fall sind Zuweisungen von Berechtigungen kritisch und sollten dokumentiert werden.

OUs sind die flexibelsten Active Directory-Entwurfselemente. Es handelt sich hier um Mehrzweckcontainer, mit deren Hilfe die meisten Objektklassen (wie z.B. Benutzer, Computer und Drucker) zu Administrationszwecken (z.B. Delegieren bestimmter Verwaltungsaufgaben und Anwenden von Gruppenrichtlinien) gruppiert werden können. Mit Hilfe von OUs wird die Infrastruktur des Unternehmens in der Active Directory-Infrastruktur abgebildet. Darüber hinaus können mit Hilfe von OUs Funktionen und Objekte abgebildet und gruppiert werden, die unter Windows NT Server 4.0 von dedizierten Ressourcendomänen bereitgestellt wurden. Organisatorische Einheiten sind weiterhin ein integraler Bestandteil bei der Erstellung eines Änderungs- und Konfigurationsverwaltungsprozesses, da Objekte nur aufgrund ihres Speicherorts in der Hierarchie vordefinierte Einstellungen annehmen können.

Entwurfsmodelle von Domänen und OUs werden in Hauptkategorien eingeteilt, da es keine einzelne optimale Methode gibt. Eine Hauptkategorie zur Organisation von OUs ist bspw. die Organisation nach Geschäftsbereichen, hierbei definieren die Geschäftsbereiche Domänengrenzen. Innerhalb dieser Geschäftsbereiche kann der physische Standort eine sekundäre Zuordnung darstellen. In diesem Fall ist der geografische Faktor das Organisationsmodell innerhalb einer Domäne.

Ein wichtiger Grundsatz für die Strukturierung der Organisatorischen Einheiten ist, dass die Existenz eines jeden Container rechtfertigbar sein muss. Obgleich es praktisch keine Begrenzung für die Verschachtelungstiefe von Organisationseinheiten gibt, wird empfohlen, nicht mehr als 5 Ebenen zu implementieren. Dies hat sich insbesondere bzgl. der Visibilität der Sicherheitskonfiguration als die optimale Vorgehensweise erwiesen.

3.5 Administrative Sicherheitsgruppen

Meist sind administrative Rollen auf verschiedene Gruppen innerhalb der IT-Organisation verteilt, hin und wieder auch innerhalb der Anwender sowie auf externe Berater und Fremdlieferanten/-zulieferer. Für eine Teamstruktur empfiehlt es sich, Rollen und Aufgaben genau zu definieren und ausdrücklich zuzuweisen, so dass die Ziele und Erwartungen für jeden klar sind.

Dies bedeutet, dass eine Struktur gefunden werden muss, die administrative Rollen abbildet und den Sicherheitsbestimmungen gerecht wird. Die empfohlene Vorgehensweise ‚Benutzer zu berechtigen, ist, sie in globale Domänen-Gruppen aufzunehmen, diese in lokale Domänen-Gruppen aufzunehmen und diese wiederum mit Berechtigungen auf Domänen Objekte zu versehen. Als Name von Sicherheitsgruppen wird ein aussagekräftiger Name gewählt, der die Aufgabe der Sicherheitsgruppe und die damit verbundenen Berechtigungen ausdrückt. Die Anzahl der administrativen Sicherheitsgruppen kann hierbei folgendermaßen unterteilt werden:

- Organisatorische Gruppen, um die Organisationsstruktur abzubilden
- Administrative Gruppen, um administrative Rollen abzubilden
- Dienste-Gruppen, um Dienste-Konten abzubilden

Die hier behandelten administrativen Sicherheitsgruppen stellen eine Hilfsstruktur dar. Pro Rolle eine Gruppe wäre eine zu starke Vereinfachung und würde dem Grundgedanken von

administrativen Rollen nicht gerecht werden. Daher ist die Anzahl der Gruppen sehr stark von den ausgeübten Tätigkeiten im Active Directory abhängig. Die Anzahl der Tätigkeiten ist wiederum von der Komplexität des Active Directory abhängig. Daraus ergibt sich eine große Anzahl an globalen Gruppen, da hier neben den ADS eigenen Tätigkeiten auch Tätigkeiten die mit Diensten zusammenhängen berücksichtigt werden müssen.

Der Ort von administrativen Sicherheitsgruppen liegt im zugehörigen OU-Container. Zugehörig heißt in diesem Zusammenhang, dass dort die Benutzerkonten oder die zu administrierenden Objekte liegen. Globale Gruppen liegen dort wo die administrativen Benutzerkonten liegen. Lokale Gruppen liegen dort, wo die zu administrierenden Objekte liegen. Wichtig ist die Einhaltung von Regeln zur Einteilung von allgemeinen Sicherheitsgruppen, um die Übersichtlichkeit zu erhalten. Regeln beinhalten Dokumentation und Namenskonvention. Wichtig ist auch, dass nur lokalen Gruppen, lokalen Domänen-Gruppen oder lokalen Gruppen eines Mitgliedservers Berechtigungen zugewiesen werden. Aus Gründen der Performance, aber vor allem aus der fehlenden Notwendigkeit heraus sollte es keine universellen Sicherheitsgruppen zur Administration geben.

3.6 Administrative Konten

Für die Konzeptionierung der Benutzerkonten für administrative Zwecke müssen verschiedene Gesichtspunkte berücksichtigt werden:

- Trennung; administrative Tätigkeiten sollen von allgemeinen Tätigkeiten getrennt werden
- Nachverfolgbarkeit; welcher Benutzer hat wann welche Tätigkeit mit welchen Ergebnissen durchgeführt

Daraus ergibt sich, dass jeder Benutzer mit administrativen Aufgaben über zwei Konten verfügen sollte. Der Administrator wird davon in der Art profitieren, dass er einerseits Problematiken von Benutzer mit seinem eigenem Konto nachvollziehen kann. Andererseits werden administrative Tätigkeiten bewusster durchgeführt, da sie eine Vor- und Nachgeschichte, speziell die An- und Abmeldung, haben.[7] Das System ist sicherer, da der Zeitraum der Anmeldung mit dem administrativen Konto und damit auch die Zeit für einen potentiellen Angriff verkürzt ist.

In einer Windows 2000 Active Directory Netzinfrastruktur, stellt sich die Frage des Containers, in dem dieses zweite Benutzerkonto abgelegt werden soll. Zur Beantwortung dieser Fragen müssen Überlegungen zur Struktur des Active Directory angestellt werden. Grundsätzlich kann jedoch die Aussage getroffen werden, dass die administrative Benutzerkonten in der Struktur dort liegen sollten, wo die zu administrierenden Objekte eingeordnet sind.

[7] Ziel der Regulierung von Administration soll nicht die Entmündigung von Administratoren sein. Der Begriff des Administrators muss in Windows 2000 Umgebungen auf Grund der enorm gestiegenen Möglichkeiten viel weiter gefasst werden, als das noch in Windows NT 4.0 Netzwerken der Fall war.

3.7 Gruppenrichtlinien

Um standardisierte Richtlinien durchzusetzen, verwendet der Active Directory Verzeichnisdienst die sog. Group Policy (Gruppenrichtlinien). In ihrer Implementierung und Wirkungsweise unterscheiden sie sich maßgeblich von den Systemrichtlinien unter Windows NT 4.0. Gruppenrichtlinien werden zur Gestaltung und Reglementierung aller Aspekte der Benutzerumgebung verwendet. Es können Einstellungen für registrierungsbasierende Richtlinien, Sicherheitsrichtlinien, Softwareinstallationen, Skripte und Ordnerumleitung vorgenommen werden.

Die Daten zu Gruppenrichtlinien sind in Gruppenrichtlinien-Objekten (Group Policy Objects, GPO) gespeichert. GPO werden an zwei Orten abgelegt: Die Konfigurationsdaten (Group Policy Configuration, GPC) sind im Active Directory abgelegt und die Vorlagen (Group Policy Template, GPT) sind in dem Systemverzeichnis abgelegt. Die GPOs sind Instanzen im Active Directory (für das Beispiel security.nformation.de) unter:

LDAP://CN=Policies,CN=System,DC=security,DC=nformation,DC=de

Gruppenrichtlinien können auf Sites, Domänen und Organisatorische Einheiten angewandt werden. Gruppenrichtlinien, die mit einer Domäne verknüpft sind, sind nicht automatisch in anderen Domänen des AD bekannt. Um eine Gruppenrichtlinie einer Domäne in einer anderen Domäne zu aktivieren, muss sie explizit verknüpft werden. Eine Verknüpfung bedeutet aber, dass bei jeder Anwendung der Richtlinie ein Zugriff auf die Ursprungsdomäne der Richtlinie erfolgt. In einem solchen Fall sollte aus Leistungsgründen ein neues GPO mit den gleichen Einstellungen in der Zieldomäne erstellt werden.

In Windows 2000 können administrative Privilegien zentral auf allen Rechnern in der Domäne über Gruppenrichtlinien verwaltet werden. Diese können zwar nicht auf Sicherheitsgruppen angewandt werden, aber man kann Sicherheitsgruppen verwenden, um Gruppenrichtlinien zu filtern.

Wichtige Randbedingungen beim Einsatz von Group Policy sind die einfache Pflege und Administration und die schnelle Anwendung aller Richtlinien, so dass keine Behinderungen für den Benutzer entstehen. Vor diesem Hintergrund können gewisse Richtlinien für die Implementierung von GPO aufgestellt werden: Zum einen muss die Anzahl von angewandten Richtlinien minimal gehalten werden, da die Dauer des Anmeldevorgangs stark von der Anzahl der abgearbeiteten Gruppenrichtlinien abhängig ist. Eine Empfehlung zur maximalen Anzahl von Gruppenrichtlinien kann nicht generell gemacht werden, da zu viele Faktoren die annehmbare Verarbeitungsgeschwindigkeit bestimmen. Beginnend mit der Leidensfähigkeit der Benutzer, über die Leistungsfähigkeit der Server und Workstations bis hin zur Netzwerkperformance.

4 Zusammenfassung

Der erfolgreiche Einsatz von Windows 2000 hängt von vielen Faktoren ab; grundlegend ist einerseits die Sicherheit des Betriebssystems selbst, andererseits die Sicherheit der durch das Betriebssystem verwalteten administrativen Domäne mittels eines an die Organisation angepassten Designs des Active Directory.

Um die Sicherheit innerhalb von Windows 2000 gewährleisten zu können, muss das System selbst vertrauenswürdig sein. Diese Systemintegrität geht von den Kernelkomponenten in Windows 2000 aus. Für sämtliche Arbeiten am System (Wartungsarbeiten, Service-Packs, Bugfixes) die nach der Auslieferung stattfinden, müssen vertrauenswürdige Strukturen eingesetzt werden, um eine kontinuierliche Integrität des Systems zu gewährleisten. Dies kann nur durch sinnvoll gestaltete administrative Maßnahmen erfolgen.

Diese Administration in einem Windows 2000 Umfeld gestaltet sich durch die Einführung des Active Directory als globalen Verzeichnisdienst komplexer, als dies in Windows NT 4.0 Umgebungen der Fall war. Daneben ergibt sich jedoch auch die Möglichkeit, mit zusätzlichen Funktionen und detaillierteren Berechtigungsstufen die Administration zu delegieren und somit die Sicherheit zu erhöhen ohne wichtige Kontrollfunktionen abzugeben.

In diesem Beitrag konnte ein Ansatz gezeigt werden, der ausgehend von diesem Prinzip der Delegation eine optimale Definition der administrativen Rollen erlaubt. Die beschriebene Vorgehensweise vereinfacht gleichzeitig den Entwurf einer Active Directory Verzeichnisstruktur unter Berücksichtigung von Sicherheitsaspekten. Die hierbei zum Einsatz kommenden Hilfsmittel wie Organisationseinheiten, Sicherheitsgruppen, administrative Konten und Gruppenrichtlinien wurden motiviert und ausführlich beschrieben. Weitergehend wurden praktische Überlegungen zur Einsatzplanung berücksichtigt.

Ausgehend von der in diesem Beitrag beschriebenen Planung stellt die Implementierung des Konzeptes und die Erhöhung des Detaillierungsgrades den nächsten Schritt bei der Einführung eines Windows 2000 Systems dar, um zu einer konkreten Definition von Aufgaben und Berechtigungen der einzelnen Services zu kommen. Für die tägliche Administration muss weiterführend eine konkrete Prozessdefinition erfolgen, um den Grundgedanken administrativer Rollen zur Delegation von Aufgaben umzusetzen.

Literatur

[Eckert2000] Claudia Eckert; IT-Sicherheit Konzepte – Verfahren – Protokolle, Oldenburg Verlag, 2000, ISBN: 3-486-25298-4

[Schneier2000] Bruce Schneier; Secrets and lies: digital security in a networked world, John Wiley and Sons, 2000, ISBN 0-471-25311-1

[SM1999] Bruce Schneier, Mudge, Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2), CQRE '99, Springer-Verlag, 1999, pp. 192-203.

[SORU2000] D. Solomon, M. Russinovich; Inside Microsoft Windows 2000 Third Edition, Microsoft Press, ISBN 0-7356-1021-5

[Tanenbaum2001] Andrew S. Tanenbaum, Modern Operating Systems – 2nd Edition, Prentice Hall, 2001, ISBN: 0-130-31358-0

Webadressen

http://www.cert.dfn.de CERT des Deutschen Forschungsnetzwerkes

http://www.microsoft.com/technet/security/bpentsec.asp Microsoft – Sicherheit in Unternehmensstrukturen

http://www.sans.org SANS – System Administration, Networking, and Security