ERNW
Enno Rey Netzwerke GmbH

ERNW Newsletter 5 / September 2004

Liebe Partner, liebe Kollegen,

willkommen zur fünften Ausgabe des ERNW-Newsletters:

Neue Möglichkeiten Sicherheit durch Server 2003-basierte Gesamtstrukturen zu implementieren

(Von Friedwart Kuhn, fkuhn@ernw.de)

Der folgende Vortrag beschreibt neue Sicherheitsfeatures, durch die der Zugriff zwischen Server 2003-basierten Gesamtstrukturen (auch über Firewallgrenzen[1] hinweg) sicherer gemacht und feiner gesteuert werden kann.

Die hier behandelten Aspekte sind insbesondere für die folgenden Szenarien relevant:

- Neuerstellung eines sicheren Server 2003-basierten Active Directory-Designs
- Absicherung eines aus mehreren Server 2003-basierten Gesamtstrukturen bestehenden Active Directorys
- Umstrukturierung eines bestehenden Active Directory-Designs (z. B. durch die Integration oder den Zusammenschluß von Geschäftszweigen oder Tätigkeitsbereichen, die auf Gesamtstrukturen abgebildet werden; Umbenennungsszenarien, die die erste Domäne der Gesamtstruktur betreffen)
- Migration von Windows 2000-basierten Gesamtstrukturen auf Server 2003-basierte Gesamtstrukturen

Mit der Einführung von Active Directory unter Windows 2000 erweiterte Microsoft das Windows NT-Domänenmodell erheblich und stellte erstmals einen skalierbaren zuverlässigen Verzeichnisdienst zur Verfügung, der auch größeren und großen Unternehmen die Möglichkeit einer zentralisierten und einheitlichen Verwaltung bot.

Domänen innerhalb einer Gesamtstruktur sind darin über automatisch erstellte bidirektionale und transitive Vertrauensstellungen in einem hierarchisch organisierten Namensraum verbunden, und jede Domäne besitzt ihre (vordefinierte) Gruppe von Domänen-Administratoren[2] zur Verwaltung derselbigen.

Dieser in jeder Domäne spezifischen Administratoren-Gruppe ist eine zentrale Instanz pro Gesamtstruktur übergeordnet. Diese Instanz wird durch die Gruppe der Organisations-Administratoren[3] (*Enterprise-Admins*) repräsentiert.

Kennzeichen dieser Gruppe ist, daß sie die Gesamtstruktur und insbesondere in dieser Gesamtstruktur enthaltene Domänen und Domänencontroller vollständig verwalten darf.[4]

Damit wird hierarchisch organisierten Unternehmen und Organisationen eine zentralisierte Verwaltung ermöglicht, an deren Spitze eine oberste administrative Instanz steht, die sich für die Konfiguration und Administration gesamtstrukturweit-relevanter Komponenten wie der Multimasterreplikation, den Betriebsmasterrollen oder der Globalen Katalog-Server und in der Regel – in Abhängigkeit von deren Größe – auch für die Verwaltung der Forest-Root-Domäne verantwortlich zeichnet.[5]

Für einige Organisationen und Unternehmen ist es ein entscheidender sicherheitsrelevanter Faktor eines dergestalt zentralisierten administrativen Konzepts mit einer über nahezu unumschränkte Macht verfügenden Gruppe, daß die Macht eben dieser Gruppe (der Organisations-Administratoren) nicht ohne weiteres eingeschränkt werden kann.[6]

Immer dann, wenn eine Organisation oder ein Unternehmen ein Domänendesign wünscht, das Domänen enthält, in denen ein Organisations-Administrator nicht in die Administration einer Domäne eingreifen können darf, und auch immer dann, wenn ein Domänen-Administrator einer Domäne keinen Einfluß auf die Funktionstüchtigkeit einer anderen Domäne haben dürfen soll,[7] muß für den zu isolierenden Bereich eine eigene Gesamtstruktur erstellt werden.

Obwohl Microsoft vor der Einführung des Windows Server 2003-basierten Active Directory behauptete, eine Domäne sei eine Sicherheitseinheit, war dies nie der Fall (und ist es auch heute nicht). Diese Problematik führte in einigen Organisationen und Unternehmen zu der Herausbildung von mehreren getrennten (Windows 2000-basierten) Gesamtstrukturen mit manuell erstellten Vertrauensstellungen zwischen den Domänen (aus verschiedenen Gesamtstrukturen), in denen ein gegenseitiger Ressourcenzugriff notwendig war.

Ein solches Design löst zwar das Problem eines überlappenden administrativen Zugriffs und die mögliche Kompromittierung einer Gesamtstruktur durch die Kompromittierung einer einzelnen Domäne dieser Gesamtstruktur, bringt jedoch weitere sicherheits- wie auch administrative Probleme mit sich:

- Die Authentifizierung von Sicherheitsprincipals einer fremden Gesamtstruktur kann nicht gefiltert werden, so daß gesamtstrukturfremde Sicherheitsprincipals nach erstellter Vertrauensstellung automatisch Mitglieder der Gruppe *Authentifizierte Benutzer* in der vertrauenden Gesamtstruktur werden und damit – ohne daß ihnen irgendwelche zusätzlichen Zugriffsberechtigungen gegeben worden wären – durch die fremde Gesamtstruktur browsen können. Denn: Entweder wird die explizite Vertrauensstellung erstellt, und dann werden alle Sicherheitsprincipals der vertrauten Domäne authentifiziert, oder aber es wird keine Vertrauensstellung erstellt, dann kann aber auch kein Ressourcenzugriff zwischen Domänen verschiedener Gesamtstrukturen erfolgen.

- Die Authentifizierung zwischen Domänen verschiedener Gesamtstrukturen kann nicht über Kerberos, sondern muß über das vergleichsweise unsichere und ineffizient arbeitende NTLMv2-Protokoll erfolgen.[8]

- Es gibt keine Firewallunterstützung für Vertrauensstellungen zwischen Domänen unterschiedlicher Gesamtstrukturen, so daß ein ganzer RPC-Portbereich freigeschaltet und mit zu definierenden Regeln versehen werden muß.[9]

- Manuell zwischen Domänen unterschiedlicher Gesamtstrukturen erstellte Vertrauensstellungen sind unidirektional und nicht transitiv, so daß der Extremfall zweier Gesamtstrukturen, in dem jede Domäne der einen jeder Domäne der anderen Gesamtstruktur vertrauen soll, schon bei je drei Domänen in zwei Gesamtstrukturen die Verwaltung von 18 Vertrauensstellungen verlangt.[10]

Alle angeführten und weitere damit assoziierte Probleme können auf elegante Weise durch die Implementierung von Server 2003-basierten Gesamtstrukturen gelöst werden. Zwar stellt eine Domäne auch innerhalb einer Server 2003-basierten Gesamtstruktur nie eine Sicherheitseinheit, sondern – neben einer Verwaltungs- und Replikationseinheit – höchstens immer nur einen autonomen Sicherheitsbereich dar, doch kann nun nicht nur der Zugriff auf Ressourcen in isolierten Bereichen mit feinster Granularität gesteuert werden, sondern auch die Verwaltung von zu isolierenden Bereichen gestaltet sich deutlich sicherer, effizienter und auf einfachere Weise als unter Windows 2000.

Für Fragen und weitergehende Beratung steht Ihnen unser Team gern zur Verfügung,

Herzlichst,

Ihr

Friedwart Kuhn, fkuhn@ernw.de.

ERNW Enno Rey Netzwerke GmbH - Zaehringerstr. 46 - 69115 Heidelberg
Tel. +49 6221 480390 - Fax 6221 419008 - Mobil +49 173 6745902
www.ernw.de

Anmerkungen

[1] Der Einbezug von IPSec wird in einem späteren Dokument erfolgen.
[2] Oder *Domänen-Admins* wie die korrekte Bezeichnung im Deutschen lautet.
[3] Oder *Orga-Admins*, wie die in den Tools zu verwendende deutschsprachige Bezeichnung lautet.
[4] Dies geschieht über die standardmäßige *Vollzugriffs*-Berechtigung auf jedes Domänenobjekt der Gesamtstruktur und durch die standardmäßige Mitgliedschaft in der domänenlokalen Guppe der *Administratoren* einer jeden Domäne der Gesamtstruktur. Die Reichweite dieser Gruppe hängt – anders als die bei manuell erstellten lokalen Gruppen in einer Domäne der Fall ist – nicht von dem Modus, bzw. der Funktionsebene, in der die Domäne betrieben wird, ab.
[5] Ein Organisations-Administrator kann zwar auch das Kennwort eines beliebigen Benutzerkontos in seiner Gesamtstruktur zurücksetzen, jedoch ist das nicht seine Aufgabe.
[6] Dem Verfasser liegt eine von einem Kunden bei Microsoft in Auftrag gegebene Studie des *Microsoft Supportability Review Centers* vor, in der es um die Beschränkung der Rechte der Organisations-Administratoren geht. Die darin beschriebene Verfahrensweise zur Erreichung einer sinnvollen Beschränkung der Organisations-Administratoren ist nicht trivial. Das von J. Barrett verfaßte und wohl wegen seiner Singularität auf diesem Gebiet immer noch häufig referenzierte Paper *Windows 2000 Active Directory Design: Restricting the Enterprise Administrators Group* berücksichtigt nicht alle zu beachtenden Aspekte (z. B. wird u. a. das *AdminSDHolder*-Objekt nicht berücksichtigt – vgl. dazu den auch für Server 2003 relevanten KB-Artikel 232199).
[7] Dieser Aspekt wird von Barrett und seinem Workaround gar nicht berücksichtigt; ihm geht es ausschließlich um die Einschränkung der Organisations-Administratoren.
[8] Es gibt sogar Szenarien, in denen höchstens NTLM verwendet wird.
[9] Es sei denn, es wird IPSec verwendet. Ein Szenario mit Gesamtstrukturen, die sich in durch eine Firewall getrennten Netzwerksegmenten befinden, ist nicht ungewöhnlich.
[10] Bei zwei Windows 2000-basierten Gesamtstrukturen, wobei die eine über *m*, die andere über *n* Domänen verfügt, erfordert ein kompletter Vertrauensverbund die Erstellung und Verwaltung von (*n* x *m*) x 2 unidirektionalen, nicht transitiven Vertrauensstellungen. Handelt es sich um *i* Gesamtstrukturen mit insgesmat *n* Domänen, muß das Produkt entsprechend über alle *i* Gesamtstrukturen summiert werden, so daß die Anzahl der zu erstellenden und zu pflegenden unidirektionalen und nicht transitiven Vertrauensstellungen *C* durch die folgende Formel beschrieben wird: $C = N^2 - \sum_i (n_i)^2$ mit $N = \sum_i n_i$.