aikux.com

Protokoll:

Migrations- & Berechtigungs-Workshop bei einem mittelständischen Unternehmen (2014)

Grundlage dieser Fallstudie ist ein vorbereitender Workshop für eine AD- und Fileservermigration in einem deutschen mittelständischen Unternehmen mit einigen tausend Usern. Konkret bestand die Aufgabenstellung darin, ein Konzept für die Migration der Fileserver aus einer Domäne in eine andere zu erarbeiten. Dabei handelte es sich um etwa 1500 User, die sich in sieben einzelnen Tochterfirmen befinden. Während der Migration sollte die Gelegenheit genutzt werden, die vorhandenen Verzeichnis- und Berechtigungsstrukturen auf der Basis eines domänenintegrierten DFS-Systems neu aufzubauen.

1. Einführung

Die aikux.com GmbH wurde vom Kunden beauftragt, in einem Workshop gemeinsam mit den IT-Mitarbeitern des Unternehmens ein Konzept für die Migration der Fileserver aus einer Domäne in eine andere zu erarbeiten. Dabei handelt es sich um ca. 1500 User, die sich in 7 einzelnen Unternehmen befinden. Die IT wird für alle 7 Unternehmen von einer gemeinsamen IT-Abteilung betreut.
Während der Migration sollen die vorhandenen Verzeichnis- und Berechtigungsstrukturen auf der Basis eines domänenintegrierten DFS-Systems neu aufgebaut werden. Die User werden von einem weiteren Dienstleister migriert. Zum Zeitpunkt des Workshops findet eine Replikation der User in die neue Domäne statt, diese Accounts werden permanent aktualisiert. Die User-Accounts bekommen in der neuen Domäne Anmeldenamen. Die SIDs der User werden erst zum letztmöglichen Zeitpunkt migriert.

2. IST-Zustand

Im Rahmen des Workshops fand eine umfassende Analyse der vorhandenen Verzeichnis- und Berechtigungsstrukturen mit dem Tool 8MAN statt, das als Teststellung von aikux.com zur Verfügung gestellt wurde. Dabei wurden folgende Tatsachen festgestellt:

- Es gibt eine hohe Anzahl von Shares, welche die Administration der Berechtigungen und Strukturen extrem erschweren.
- Auf Grund der fehlenden Prozesse für die Verwaltung der Strukturen und Berechtigungen wurden Shares in Hierarchien (Shares unterhalb von Shares) aufgebaut. Kaskadierte Share-Strukturen machen eine saubere Berechtigungsvergabe unmöglich.
- Es gibt keine übergreifende Logik für das Einbinden der Verzeichnisse beim User. Es wird für alle User nur das Home- und ein „Allgemein“- Verzeichnis eingebunden. Alle anderen Verzeichnisse werden von Usern immer selbständig und ganz individuell unter unterschiedlichen Laufwerksbuchstaben eingebunden. Das sorgt für Probleme in der Verknüpfung von Dateien untereinander.
- Die aktuellen Volumes sind weder thematisch noch nach rechtlichen Aspekten getrennt. User-Home-Verzeichnisse/ Shares sind vermischt mit Organisations- oder Projektdaten.
- Es gibt keinen definierten Prozess für die Einrichtung und Verwaltung von Verzeichnisstrukturen und Berechtigungen. Es sind zur Zeit einzelne User aus den Fachabteilungen auf den Verzeichnissen mit „Vollzugriff“-Berechtigungen ausgestattet.

Aktuell entspricht die Berechtigungslage nicht dem Optimum. Es ist zu befürchten, dass ungewollt hohen Userkreisen der Zugriff auch auf unternehmenskritische Daten möglich ist.

- Es gibt keine Dokumentation über die tatsächliche Berechtigungssituation. Es ist nur mit erheblichem Aufwand möglich herauszufinden, welche Berechtigungen tatsächlich wo und für wen existieren. Das wird durch die vielen kaskadierten Shares erschwert.
- Es gibt kein einem Best Practice-Prinzip entsprechendes Berechtigungskonzept mit der Konsequenz, dass die Vererbungen oft unterbrochen sind und es keine Listberechtigungen gibt, dafür aber oft Berechtigungen für „Everyone“.
- Es gibt keine Übersicht über die tatsächliche Zuordnung und Nutzung der Daten auf den Servern: Welche Verzeichnisse/Shares werden tatsächlich von welchem Unternehmen/ Fachbereich genutzt bzw. bearbeitet?
- Es gibt keine DataOwner. DataOwner sind die Personen im Fachbereich, welche Verantwortung für die Daten und Berechtigungen übernehmen. Sie dienen der IT-Abteilung als direkte Ansprechpartner für die Klärung von Fragen im Umgang mit Daten und Berechtigungen.
- Die Datenmenge ist mit einigen zehn Terabyte ungewöhnlich hoch. Die hohe Datenmenge verursacht im Unterhalt extreme Kosten. Bei übersichtlicheren Strukturen wären es vermutlich wesentlich weniger Daten.
- Es gibt keine standardisierte Verzeichnisstruktur innerhalb von Bereichsverzeichnissen.
- Es befinden sich innerhalb der Filestruktur Verzeichnisse, die über FTP freigegeben werden. Das ist unzulässig, weil auf diesem Wege der Zugriff aus dem Internet auf den kompletten Fileserver erlangt werden kann!

3. Migration

a. Aus der Analyse ergeben sich zwei Möglichkeiten für die Migration in die neuen Domänen.

Möglichkeit 1 (‚dirty')
Aus den vorhandenen Strukturen werden lediglich die User-Home-Verzeichnisse neu strukturiert und auf einzelnen, neuen Shares getrennt nach Unternehmen aufgebaut. Die restlichen Unternehmensdaten müssen komplett in ihrer Struktur in die neue Domäne überführt werden. Die Überführung kann immer nur in der Form von kleineren Blöcken erfolgen. Es ist zu prüfen, ob der Server als Ganzes in die neue Domäne überführt werden kann. In diesem Fall werden alle Berechtigungen auf den Verzeichnissen gelassen. Neben der Überführung der User müssen auch alle Gruppen, die für Berechtigungen genutzt werden, in die neue Domäne migriert werden. Die Berechtigungen werden dann auf der Basis der alten SID in der SID-History ermöglicht. Dieses Verfahren verdoppelt die Größe des Security-Tokens für alle User.

Möglichkeit 2 (empfohlen)
Wenn man die Daten während der Migration in das neue DFS überführen will, müssen umfangreiche strukturelle Anpassungen vorgenommen werden. Außerdem verlangt die Frage der zukünftigen Administration (als Prozess verstanden) nach Antworten: Wenn man das Ziel verfolgt, langfristig korrekte Fileserver- und Berechtigungsstrukturen zu haben, muss ein Tool für die zukünftige Administration eben dieser Strukturen eingeführt werden.

Während der Migrationsphase ist Zeit für die Schulung der Helpdesk-Mitarbeiter einzuplanen, um die neue Struktur adäquat weiterzuführen und nicht wieder „verfallen" zu lassen.

b. Folgende Fragen sind im Vorfeld zu klären:

- Welche Shares/ Verzeichnisse werden von wem genutzt?
- Wer sind die DataOwner für die einzelnen Bereiche?
- Welche Abhängigkeiten gibt es innerhalb der Verzeichnisstrukturen?
- Welche Applikationen schreiben direkt in die Verzeichnisse und sind auf die Erreichbarkeit angewiesen?
- Auf welche Daten kann während der Migration verzichtet werden?

- Wie groß sollen/ müssen die neuen Volumes sein?
- Wie können die Strukturen/ Zugriffe für die User vereinheitlicht werden?
  -> Standardisierung!
- In welchen Blöcken können die aktuellen Shares in Abhängigkeit mit der neuen Zielstruktur überhaupt migriert werden?
- Wie geht die Archivierungslösung mit den migrierten Daten um? Werden sie wiedererkannt?
- Welche gemappten Shares sind notwendig für welche User?

c. notwendige Schritte:

- Behandlung der Verlinkungen innerhalb von Dateien
- neue Zielstruktur in Abstimmung mit Fachabteilung erarbeiten
- Replikationsmapping in Abstimmung mit Fachabteilung erstellen
- neue Berechtigungs- und Verzeichnisstrukturen im Zielsystem aufbauen
- Daten replizieren
- Mapping der Shares für User einrichten
- Links fixen
- User migrieren

d. mögliche Verzeichnisstruktur:

Orgadaten:	Share für ‚XXXXX'\Unternehmen\Abteilung/Leitung\Team
Projektverzeichnisse:	Share für ‚XXXXX'\Projekte\Projekt_1
Public:	Share für ‚XXXXX'\Public\Thema

Die User können immer erst unterhalb der erwähnten Ordner selbst Verzeichnisse erstellen und Daten bearbeiten. Das setzt voraus, dass in Zukunft alle Verzeichnisse bis zu der entsprechenden Ebene durch den Helpdesk erstellt und berechtigt werden. Es wird nur 3-4 Shares geben, die für alle User über alle Unternehmen hinweg gleich sind und so einen Standard für eine unkompliziertere Zusammenarbeit zu schaffen. ABE sorgt dafür, dass den Usern immer nur die für sie wichtigen/ notwendigen Verzeichnisse angezeigt werden. In Zukunft werden keine Vererbungen mehr unterbrochen.

e. Für beide Varianten relevante Aufgaben:

- Unnötige/ alte User identifizieren und bereinigen – weder die Accounts noch die Daten sollten migriert werden.
- Verwaiste Homeverzeichnisse identifizieren und eliminieren.
- Verwaiste Daten in den Organisationsdaten identifizieren und archivieren/ eliminieren.
- Von der Unternehmenspolicy abweichende Daten identifizieren und vom Fileserver eliminieren (z.B. Multimediadaten in den Homeverzeichnissen).

f. Beispiel: Tochterfirma

Es gibt schon eine gute Struktur im Share. Allerdings sind aktuell „EveryOne“ mit Leserechten ausgestattet. Aus diesem Grund müssen die kompletten Berechtigungen für alle Verzeichnisse abgefragt werden. -> DataOwner müssen ermittelt und kontaktiert werden.

Zu jedem Abteilungsverzeichnis wird ein weiteres Verzeichnis parallel für die Leitung eingerichtet und explizit berechtigt.

Die Dateiverlinkungen werden mit Linkfixer vorbereitet.

Verzeichnissberechtigungen werden mit migRaven definiert und in der neuen Domäne aufgebaut, die Verzeichnisse auf dem neuen Fileserver erzeugt und direkt berechtigt. Die Berechtigungsgruppen werden direkt in der neuen Domäne erzeugt. Das verhindert, dass gleich in der neuen Domäne Gruppen und Berechtigungen auf der Basis der SID-History erzeugt werden.

Die Daten werden dann repliziert.

Die Shares müssen neu verbunden werden. Die Konfiguration für das Mounting der userspezifischen Laufwerke erfolgt direkt in der neuen Domäne auf der Basis von GPOs.

Wenn die Replikation abgeschlossen ist, können die User-Accounts vollständig in die neue Domäne migriert werden. Ab diesem Zeitpunkt melden sich die User in der neuen Domäne an und arbeiten auf dem neuen Fileserver.

4. Fazit

Die ungewöhnlich hohe Menge von Daten stellt nicht nur die Administration vor erhebliche Herausforderungen: Gleichzeitig verhindert sie ein effektives Arbeiten der User mit den Daten. Wenn man wesentlich mehr Daten in seinen Verzeichnissen findet, als benötigt werden und diese auch schon seit vielen Jahren nicht mehr in Benutzung sind, dann wird es schwer, produktiv zu sein. Die Datenmenge ist letztlich auch Folge und Ausdruck einer fehlenden Struktur und fehlender Ansprechpartner, welche die Daten kennen und bewerten können (DataOwner). Die Lösung für den User ist dann oftmals naheliegend: Er schafft sich eigene Strukturen z.B. in seinem Home-Laufwerk. Die bevorstehende Migration gibt eine einmalige Chance, diese alten Zöpfe abzuschneiden und nur diejenigen Daten zu migrieren, die wirklich gebraucht werden und sie mit Rechten zu versehen, die genau den richtigen Usern den Zugriff darauf ermöglichen – und niemandem sonst. Man kann ganz klar sagen, dass die aktuelle Situation nicht den aktuellen Anforderungen nach sauberen Fileserver-Strukturen und Berechtigungen entspricht. Diese Situation erschwert die Migration erheblich.

Falls es im Fileserverbereich Daten gibt, die schützenswert sind und nicht allen Mitarbeitern (aktuell ca. 6000 User-Accounts) des Unternehmens zugänglich sein sollen, dann müssen schnellstens bzw. während der Migration die geeigneten Schritte ergriffen werden. Außerdem ist sicherzustellen, dass nach der Migration die bereinigten Strukturen „sauber“ bleiben. Dafür empfiehlt sich die Etablierung von DataOwner-Strukturen in den Fachabteilungen. Diese stellen entweder nur die Schnittstelle zwischen Fachabteilung und IT dar oder können mit geeigneten Tools die Administration der Verzeichnisse und Berechtigungen eigenständig übernehmen. (Auf keinen Fall mit Microsoft Bordmitteln arbeiten lassen!) Das ist inzwischen Standard und gelebte Kultur in vielen Unternehmen – darüber hinaus aber auch die einzige Möglichkeit, Strukturen und Berechtigungen dauerhaft sauber zu halten. Der DataOwner ist der einzige, der wirklich weiß, wie es sein sollte!

Unter der Maßgabe der Sicherheit empfiehlt es sich, gleichzeitig zu den technischen Maßnahmen die User in die Lage zu versetzen, die wichtigen Anforderungen an Sicherheit und Ordnung zu verstehen. Das ist nur durch regelmäßige Sensibilisierung möglich. Die User müssen ‚abgeholt‘ werden!

Dieses Vorgehen garantiert ein Verständnis für den verantwortungsvollen Umgang mit Daten und führt zu gelebter aktiver Sicherheit durch jeden.

Sicherheit besteht immer aus einem Set von technischen Maßnahmen und erfolgter Weiterbildung. Das sollte in einer Sicherheitspolicy zusammengefasst werden. Diese Sicherheitspolicy enthält den Maßnahmenkatalog für die Vielzahl der Systeme, die sich im Unternehmen befinden und ganz unterschiedlichen Sicherungsanforderungen unterliegen.

Aktionen zur Vorbereitung für das Pilotprojekt:

- Planungsmatrix für den zukünftigen Fileserver: Darstellung der Volumes mit den aufzunehmenden Daten
- Matrix über die zu erwartenden Datenmengen für User und Organisationsdaten (TreeSize)
- vorbereitete Verzeichnis- und Berechtigungsstruktur für eine Tochterfirma
- Identifizierung der Abteilungs- und Teamleiter
- Übersicht über alle User, die zu den einzelnen Unternehmen gehören

Entsprechende Vorlagen können von aikux.com zur Verfügung gestellt werden.

aikux.com GmbH
Alt Moabit 59-61
10555 Berlin

Geschäftsführer: Thomas Gomell
Tel.: +49 (30) 8095010-40
Fax: +49 (30) 8095010-41
Email: info@aikux.com

www.aikux.com