tenfold

Best Practices im Berechtigungsmanagement in Microsoft-Umgebungen

Inhalt

1. Die Basics verstehen

1.1. Struktur

Berechtigungen haben den Zweck, den Zugriff auf Ressourcen (Verzeichnisse, Dateien, Postfächer und sonstige Objekte) zu regulieren. Die Berechtigungsstruktur in Microsoft-Umgebungen bietet sehr vieleGestaltungsmöglichkeiten. Entsprechend umfangreich und komplex können konkrete Umgebungen ausgestaltet werden. Darunter leiden sowohl die Verwaltbarkeit als auch die Möglichkeiten der Auswertung. Um die Best Practices in vollem Umfang verstehen zu können, ist es zunächst notwendig, die grundlegenden Konzepte zu verstehen, welche nachfolgend beschrieben sind.

1.2. Berechtigungsstufen

Grundsätzlich gilt in Microsoft-Umgebungen ein positives Berechtigungskonzept. Das bedeutet, dass alles verboten ist, was nicht explizit erlaubt ist. Somit wird bestimmten Benutzern oder Benutzergruppen durch das Berechtigungswesen der Zugriff auf eine Ressource erlaubt. Der Zugriff ist hierbei – abhängig vom zugrunde liegenden System – immer durch eine bestimmte Berechtigungsstufe definiert. Das bedeutet, dass eine Zugriffsberechtigung nicht einfach nur erteilt oder nicht erteilt wird, sondern dass nach unterschiedlichen Ebenen des Zugriffs unterschieden wird. Auf dem Fileserver kann beispielsweise zwischen rein lesendem Zugriff („Lesen & Ausführen“) oder schreibendem Zugriff („Ändern“) unterschieden werden. Andere Systeme, wie Microsoft Exchange Server oder Microsoft SharePoint Server, bieten hiervon abweichende Berechtigungsstufen zur Auswahl an. Innerhalb eines Systems kann es auch vorkommen, dass für unterschiedliche Objekttypen unterschiedliche Berechtigungsstufen vorgesehen sind. Beispielsweise sind die Berechtigungsstufen für Postfachberechtigungen im Exchange Server andere als jene für Postfachordnerberechtigungen.

1.3. Access Control Lists

Die Objekte, denen eine Berechtigung entsprechend der Berechtigungsstufe

zugeordnet wird, können sowohl Objekte aus dem Active Directory (Benutzerkonten, Gruppen, Computerkonten), als auch lokale Computerobjekte (lokale Benutzerkonten, lokale Gruppen) sein. Um die Berechtigung permanent zu speichern, werden, beispielweise im Dateisystem, Einträge in Form einer Liste – der Access Control List oder kurz ACL – gespeichert. Die einzelnen Einträge in der ACL werden als Access Control Entry (ACE) bezeichnet. Hinterlegt wird jeweils die Berechtigungsstufe, die interne Identifikation (SID; Security Identifier) des berechtigten Objekts und einige zusätzliche Verwaltungsinformationen, auf die später eingegangen wird.

1.4. Vererbung

In hierarchischen Strukturen (wie einer Ordnerstruktur auf einem Fileserver) können Berechtigungen von einem Objekt auf die untergeordneten Objekte vererbt werden. Das bedeutet, dass für einen Unterordner grundsätzlich die gleichen Berechtigungen gelten, wie für den Überordner. Voraussetzung ist, dass der oder die übergeordneten ACE so eingestellt sind, dass sie vererbt werden können (Vererbungseinstellungen des jeweiligen ACE) und, dass der untergeordnete Ordner so eingestellt ist, dass er übergeordnete ACE zur Vererbung akzeptiert (Aktivierung der Vererbung für den untergeordneten Ordner). Die ACL des untergeordneten Ordners umfasst somit grundsätzlich die gleichen ACE wie der übergeordnete Ordner. Jeder ACE wird hierbei speziell dahingehend gekennzeichnet, dass er von einem übergeordneten Objekt vererbt wurde. Vererbte ACE können auch über mehrere Ordnerebenen hinweg weitervererbt werden. Es ist nicht möglich, vererbte ACE aus der ACL zu verändern oder zu entfernen. Tatsächlich ist es jedoch möglich, die ACL des untergeordneten Objekts zu beeinflussen, in dem zusätzliche, nicht vererbte – somit initiale – Einträge hinzugefügt werden. Die Berechtigungen werden somit im untergeordneten Objekt erweitert und umfassen nunmehr einen größeren Benutzerkreis. Zusätzlich kann für ein untergeordnetes Objekt

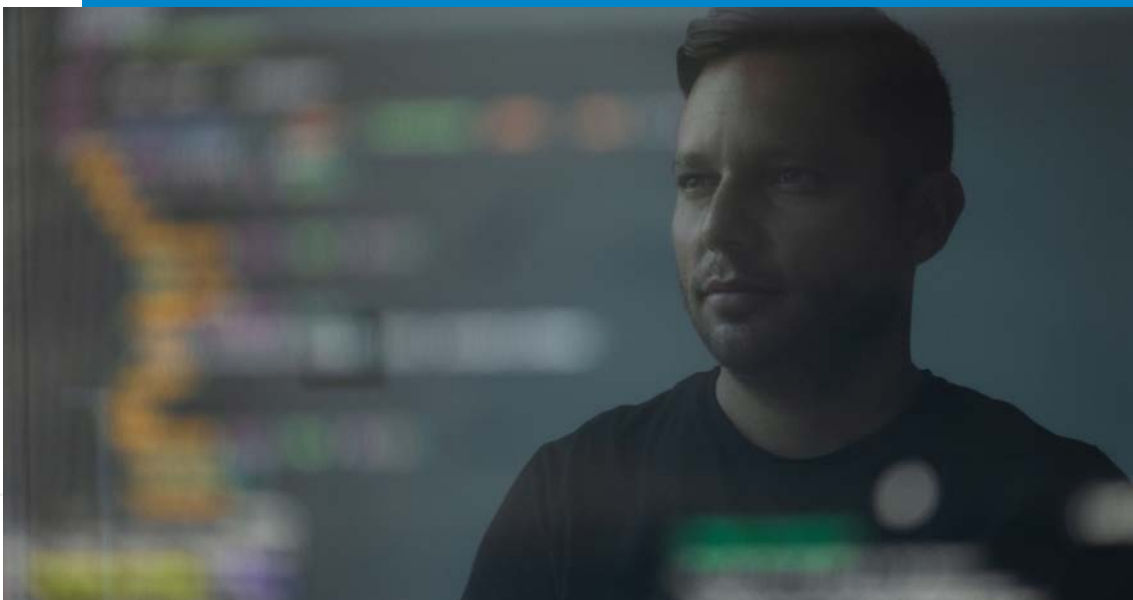
die Vererbung gänzlich deaktiviert werden. Das bedeutet, dass das Objekt nicht die ACL des übergeordneten Objekts erbt. Es gelten auf dem untergeordneten Objekt somit mitunter gänzlich andere Berechtigungen, als auf dem übergeordneten Ordner. Das Erweitern der ACL ist gängige Praxis und weitestgehend unproblematisch. Das Deaktivieren (oder auch „Aufbrechen“) der Vererbung führt jedoch zu einer Reihe von Problemen.

1.5. Verweigern

Auf jedem Objekt gibt es neben der Möglichkeit, Objekten explizit den Zugriff zu erlauben, die Möglichkeit, den Zugriff einzelner Objekte zu sperren oder zu verweigern. Beispiel: Der Benutzer B ist Mitglied der Gruppe G. Die Gruppe G hat auf einem Ordner Leseberechtigungen. Durch seine Mitgliedschaft in Gruppe G hat auch Benutzer B diese Berechtigung. Ist nun zusätzlich ein ACE hinterlegt, in welchem Benutzer B der Lesezugriff explizit verweigert wird, hat der Benutzer effektiv keinen Zugriff auf den Ordner, da Verweigern-Einträge immer vor Zulassen-Einträgen ausgewertet werden. Dies wird dadurch sichergestellt, dass alle Verweigern-Einträge durch das Betriebssystem an den Beginn der ACL geschrieben werden und erst anschließend die Zulassen-Einträge folgen. Die Verwendung von Verweigern-Regeln erweitert die Komplexität um eine weitere Dimension. Im Rahmen eines guten Berechtigungskonzepts ist die Nutzung von Verweigern-Regeln nahezu nie erforderlich.

1.6. Berechtigungsprüfung

Wird nun von einem Benutzer zum Beispiel eine Datei geöffnet, so führt das Betriebssystem die Berechtigungsprüfung durch. Dabei werden die Einträge in der ACL der Datei der Reihe nach gelesen und es wird für jeden Eintrag überprüft, ob dieser dem Benutzer den Zugriff auf die Datei erlaubt oder explizit verweigert. Das ist dann der Fall, wenn ein ACE den Benutzer selbst – via dessen SID – enthält, oder wenn ein ACE eine



Gruppe beinhaltet, in welcher der Benutzer Mitglied ist. Es werden hierbei mehrstufige Mitgliedschaften berücksichtigt. Das bedeutet, der Zugriff ist auch dann zulässig, wenn im ACE eine Gruppe eingetragen ist, in welcher eine Gruppe Mitglied ist, in der dann letztendlich der Benutzer als Mitglied hinterlegt ist.

1.7. Zusammenfassung

Berechtigungen werden für Objekte in Verbindung mit bestimmten Berechtigungsstufen vergeben. Berechtigte Objekte können sowohl aus der lokalen Computerverwaltung, als auch aus dem Active Directory stammen. Gruppenmitgliedschaften werden bei der Berechtigungsprüfung genauso berücksichtigt, wie Regeln zur Vererbung oder Regeln zur expliziten Verweigerung von Zugriffen. Diese Möglichkeiten in Verbindung mit den Tausenden oder sogar Millionen von Ordnern und Dateien führen dazu, dass die IT-Organisation ein Konzept erarbeiten muss, nach welchem die Berechtigungen technisch strukturiert und vergeben werden sollen.

2. Strukturen richtig erstellen

2.1. Ein Benutzer soll eine Berechtigung bekommen

Wenn nun ein Benutzer beispielsweise auf einem Ordner mit Leseberechtigungen ausgestattet werden soll, gibt es mehrere Möglichkeiten, dies zu erreichen. Die naheliegende Variante ist selbstverständlich, den Benutzer in einen Access Control Entry mit der Berechtigungsstufe „Lesen & Ausführen“ zu berechtigen. Diese Vorgehensweise führt allerdings zu zwei groben Problemen:

- Sollte das Benutzerkonto im Active Directory (oder auf der lokalen Computerverwaltung) gelöscht werden, so bleiben alle ACL-Einträge, die auf das Objekt verweisen, ohne weitere Berücksichtigung zurück. Das Löschen eines Objekts aus dem Active Directory berücksichtigt nämlich nicht, wo das Objekt überall berechtigt ist (in ACE aufscheint) – um in Folge diese Einträge ebenfalls zu löschen. Im ACE ist ja lediglich die interne ID des Objekts – der sogenannte Security Identifier oder kurz „SID“ – eingetragen. Nach der Löschung des eigentlichen Objekts aus dem Active Directory ist die SID keinem Objekt mehr zugeordnet. Der Eintrag wird im Windows Explorer als „Unbekanntes Konto (S12345-12345678-12345)“ angezeigt. Die Zeichenkette beginnend mit „S“ stellt dabei die (ehemalige) SID des berechtigten Objekts dar. Diese als „verwaist“ bezeichneten Einträge haben negative Auswirkungen auf die Übersichtlichkeit, die Datensicherheit und die Performance des Systems.

- Durch die direkte Berechtigungsvergabe existiert beim Benutzerkonto im Active Directory selbst kein Hinweis auf die Ordnerberechtigung. Active Directory hat nämlich tatsächlich keine Kenntnis davon, wo die SIDs der beinhalteten Objekte überall eingetragen wurden. Die Berechtigung fällt somit aus jeglicher benutzerbasierten Berechtigungsbetrachtung hinaus.

2.2. Abhilfe für die bekannten Probleme

Beide vorher genannten Probleme können dadurch umgangen werden, dass Benutzer nicht direkt auf Ordnern berechtigt werden. Stattdessen wird eigens für den Ordner eine Gruppe eingerichtet, deren einziger Zweck die Berechtigungssteuerung für den Ordner ist. Diese Gruppe wird anschließend auf dem Ordner berechtigt. Mitglieder der Gruppe erhalten somit automatisch den Zugriff auf den Ordner, auf dem die Gruppe berechtigt wurde. Anschließend wird der zu berechtigende Benutzer in die Gruppe aufgenommen, wodurch der Zugriff auf den Ordner möglich ist.

Es müssen bei dieser Vorgehensweise vier Aspekte unbedingt berücksichtigt werden:

1. Für jede Berechtigungsstufe muss eine eigene Gruppe angelegt und auf dem Ordner berechtigt werden. Die Gruppen sollten „on-demand“ angelegt werden, also am besten dann, wenn der Zugriff zum ersten Mal eingerichtet werden soll. So kann verhindert werden, dass beispielsweise eine Lesen- Gruppe eingerichtet wird, wobei auf dem Ordner in weiterer Folge niemals Leseberechtigungen, sondern ausschließlich Schreibberechtigungen vergeben werden.

2. Eine Berechtigungsgruppe darf ausschließlich auf dem zugehörigen Ordner genutzt werden. Sie darf nicht in ACLs von anderen Ordnern oder Objekten (zum Beispiel in Exchange Server) genutzt werden. Durch die Mehrfachnutzung einer Berechtigungsgruppe entsteht nämlich ein Transparenzproblem: Es ist dann – ähnlich der Problematik bei verteilten, direkten Benutzerberechtigungen – nicht mehr nachvollziehbar, welche effektiven Zugriffe durch die Mitgliedschaft in der Gruppe erteilt werden.

3. Berechtigungsgruppen müssen einen zumindest gleich langen Lebenszyklus aufweisen, wie der Ordner, dem sie zugeordnet sind. Wird die Berechtigungsgruppe zu einem Zeitpunkt gelöscht, zu dem der Ordner noch existiert, bleibt erneut ein Eintrag mit verwaister SID zurück (siehe oben). Eine Berechtigungsgruppe darf erst dann gelöscht werden, wenn vorher der zugehörige Ordner oder der betreffende ACL-Eintrag gelöscht wurde.

4. In der Praxis ist es notwendig, eine Konvention für die Gruppennamen zu vereinbaren. Der Name der Gruppe sollte – sofern dies möglich ist – auf den Ordnernamen und die Berechtigungsstufe hindeuten, für welche die Gruppe zuständig ist.

Beispiel: Eine Gruppe für Lesezugriff auf den Ordner \\srv1\doc\templates könnte den Namen fs_srv1_doc_templates_r tragen. Das Präfix „fs“ deutet darauf hin, dass es sich um eine Berechtigungsgruppe für Fileserver handelt. Der mittlere Teil repräsentiert den UNC-Pfad zum Ordner. Das Postfix „r“ steht für lesenden Zugriff („Read“). Zusätzlich muss beispielweise auch definiert werden, wie damit umgegangen wird, wenn der Ordnername Zeichen beinhaltet, die in einem Gruppennamen nicht vorkommen dürfen, oder wenn etwa der Pfadname die maximale Länge eines Gruppennamen (63 Zeichen) überschreitet.

2.3. Wie werden Personengruppen ordnungsgemäß berechtigt?

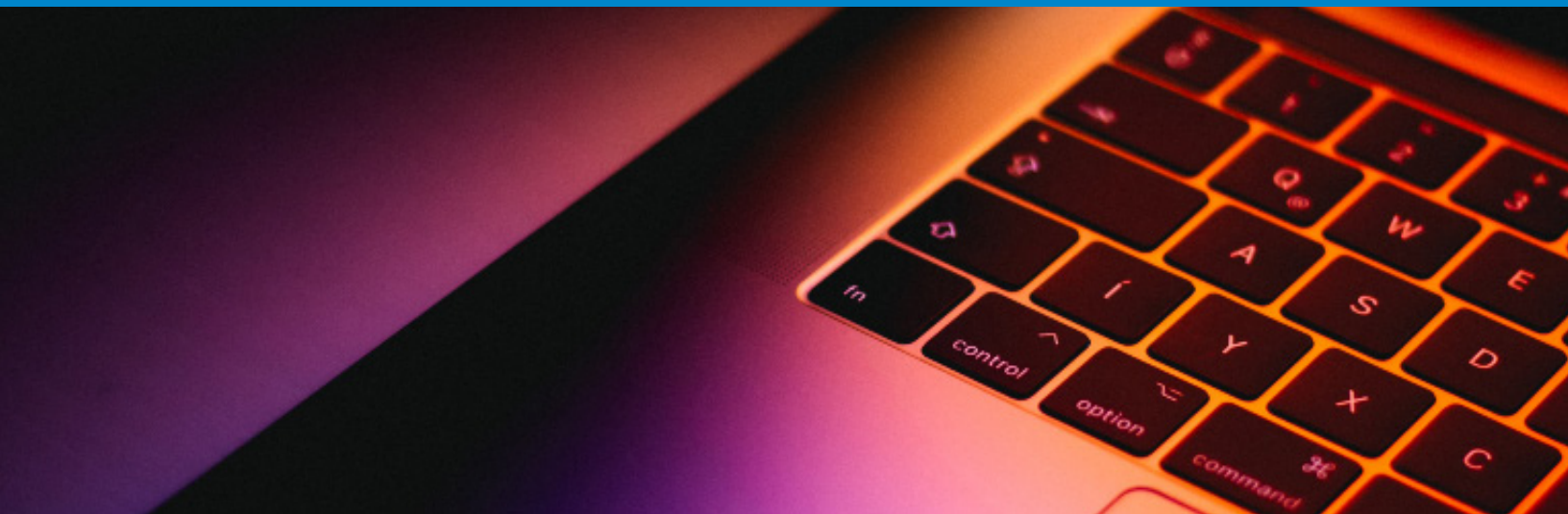
In der Praxis stellt sich relativ bald die Frage, wie eine ganze Gruppe von Personen auf einmal berechtigt werden kann. Müssten in jedem Einzelfall alle Mitglieder der jeweiligen Personengruppe einzeln berechtigt werden, entsteht dadurch einerseits ein enormer Arbeitsaufwand. Andererseits können neue Mitglieder der Personengruppe nicht auf einen Schlag überall dort berechtigt werden, wo bereits alle bisherigen Mitglieder berechtigt sind – stattdessen müssen die neuen Mitglieder wieder an allen Ordnern einzeln nachberechtigt werden.

Beispiel: Gehen wir davon aus, dass das Marketing im Unternehmen einen gemeinsam genutzten Ordner hat (\\srv\marketing). Es wurde eine Berechtigungsgruppe für Schreibzugriff erstellt (fs_srv_marketing_w). In diese Gruppe wurden alle Mitarbeiter der Marketingabteilung aufgenommen. Der Zugriff auf den Ordner funktioniert nun für alle Mitarbeiter der Abteilung.

Nun soll die gesamte Marketingabteilung, neben anderen Abteilungen, Zugriff auf die Daten des neuen Re-Branding-Projekts erhalten. Für das Projekt existiert ein eigener Ordner (\\srv\projects\rebranding). Nachdem nunmehr alle Marketingmitarbeiter bereits gruppiert sind (nämlich in der Gruppe fs_srv_marketing_w), ist die Verlockung groß, diese Gruppe einfach mit Ändern-Berechtigungen in der ACL des Projektordners einzutragen. Dies ist allerdings kein gültiger Ansatz und widerspricht den Best Practices ganz klar, denn – wie zuvor beschrieben – darf eine Berechtigungsgruppe nicht an zwei unterschiedlichen Ordnern berechtigt werden.

Stattdessen wird an diesem Punkt ein neuer Gruppentyp eingeführt: die Organisationsgruppe. Eine Organisationsgruppe dient lediglich dazu, Personen nach bestimmten Merkmalen zu gruppieren (zum Beispiel alle Mitarbeiter einer Abteilung oder eines Teams). Organisationsgruppen werden – wie Benutzerkonten – niemals direkt in einer ACL eingetragen. Soll eine Organisationsgruppe (im Beispiel die Marketingabteilung) auf einem Ordner berechtigt werden, so muss die Organisationsgruppe Mitglied der Berechtigungsgruppe des gewünschten Ordners und der gewünschten Berechtigungsstufe werden. In unserem Beispiel würde dies bedeuten, dass zuerst – bevor überhaupt Berechtigungen auf dem Marketingordner vergeben werden – eine Organisationsgruppe angelegt wird (beispielsweise abt_marketing). In diese Gruppe werden alle Mitarbeiter der Abteilung aufgenommen. Für die beiden Ordner, auf denen – mitunter – das Marketing berechtigt werden soll, werden zwei Berechtigungsgruppen angelegt (fs_srv_marketing_w und fs_srv_projects_rebranding_w). Anschließend wird die Gruppe abt_marketing in die beiden Berechtigungsgruppen aufgenommen. Durch die Verschachtelung der Gruppen entsteht eine Reihe von Vorteilen:

- Es existiert eine Gruppe, welche – unabhängig vom Kontext bestimmter Ordner – alle Mitarbeiter der Abteilung umfasst. Diese Gruppe kann überall zum Einsatz kommen, wo sich Berechtigungen auf die gesamte Abteilung beziehen sollen.
- Diese Gruppe wird nicht direkt auf Ordnern berechtigt – die Gefahr von verwaisten ACL-Einträgen ist somit neutralisiert.
- Es können neben der Marketingabteilung zusätzliche Objekte – einzelne Benutzer oder andere organisatorische Gruppen – auf beiden Ordnern ordnungsgemäß berechtigt werden, indem sie zur entsprechenden Berechtigungsgruppe hinzugefügt werden.



2.4. Die häufigsten Fehler

Oftmals sind die oben beschriebenen Best Practices nicht gänzlich unbekannt. Die Erfahrung zeigt allerdings, dass in der Praxis regelmäßig immer wieder die gleichen Fehler gemacht werden. Das hat mehrere Gründe:

- Die Administratoren agieren aus Dringlichkeit oder aus Bequemlichkeit heraus
- Die Administratoren verfolgen unterschiedliche Konzepte
- Die Administratoren verfügen über unterschiedliche Kenntnisse

Einige der Fehler, die regelmäßig auftauchen, sind nachfolgend beschrieben:

Fehler 1

Benutzer werden direkt berechtigt. Selbst wenn Berechtigungsgruppen genutzt werden, werden Benutzer zusätzlich fallweise – aus unterschiedlichen Gründen – in Einzelfällen direkt berechtigt. Diese Direktberechtigungen sind in weiterer Folge nicht mehr nachvollziehbar. Es besteht die Gefahr, dass die Berechtigungen auf die gesamte Lebenszeit des Benutzerkontos bestehen bleiben. Anschließend werden sie zu verwaisten Einträgen. Abhilfe: Auch in Einzelfällen oder bei Dringlichkeit dürfen Benutzer niemals direkt auf einem Ordner berechtigt werden. Es muss vorab die benötigte Berechtigungsgruppe erstellt und berechtigt werden.

Fehler 2

Berechtigungsgruppen werden mehrfach genutzt. Aus Bequemlichkeit oder Unwissenheit werden Berechtigungsgruppen eines Ordners auf einem anderen Ordner wiederverwendet – beispielsweise, weil der gleiche Personenkreis berechtigt werden soll. Abhilfe: Für den Personenkreis (die Abteilung, den Standort, die Projektgruppe) ist eine organisatorische Gruppe zu bilden und diese ist mittels zweier unabhängiger Berechtigungsgruppen auf den gewünschten Objekten zu berechtigen.

Fehler 3

Organisationsgruppen werden als Berechtigungsgruppen genutzt. Es wird häufig darauf verwiesen, dass bei der Berechtigungsvergabe Gruppen verwendet werden. Allerdings handelt es sich dabei um Gruppen des falschen Typs. Organisatorische Gruppen (häufig Abteilungsgruppen) dürfen niemals direkt in ACLs verwendet werden. Es droht die Gefahr von verwaisten Einträgen, wenn die Abteilung umorganisiert wird und die zugehörige Gruppe gelöscht wird. Außerdem ist in solchen Fällen die Vergabe von zusätzlichen, individuellen Benutzerberechtigungen nicht mehr möglich, da die entsprechende Berechtigungsgruppe fehlt (in die – fälschlicherweise als Berechtigungsgruppe zweckentfremdete – Abteilungsgruppe kann der einzelne Benutzer nicht aufgenommen werden, da er sonst alle Berechtigungen der Abteilung erhalten würde, nicht nur die Berechtigungen auf diesem einzelnen Ordner). Abhilfe: Es muss stets das Best Practice-Konzept, bestehend aus organisatorischen Gruppen und Berechtigungsgruppen, angewendet werden.

Fehler 4

Namenskonventionen werden missachtet. Wenn Gruppen angelegt werden, so muss dies anhand der Namenskonvention geschehen. Wird die Namenskonvention ignoriert oder existieren mehrere Konventionen parallel, so kann der Zweck der Gruppe eventuell nicht mehr zweifelsfrei nachvollzogen werden und es wird früher oder später zu fehlerhaften Berechtigungen kommen. Abhilfe: Die Namenskonvention muss klar kommuniziert werden und darf nicht außer Acht gelassen werden. Fehler müssen umgehend nachgebessert werden.

3. Technische Detailaspekte

3.1. Listberechtigungen verstehen und richtig anwenden

Bei Ordnerberechtigungen in Windows gilt eine Besonderheit, die vor allem Anfänger, aber auch Umsteiger von Novell, immer negativ überrascht: Hat ein Benutzer auf einem Ordner in der Ebene 2 (zum Beispiel \\srv\projects\rebranding) Berechtigungen, jedoch auf dem übergeordneten Ordner (in diesem Beispiel „projects“) nicht, so kann der Benutzer nicht mit dem Windows Explorer zum gewünschten Ordner navigieren. Je nach ABE-Einstellung (siehe unten), erhält der Benutzer entweder eine Fehlermeldung („unzureichende Berechtigungen“) beim Klick auf den „projects“-Ordner oder er kann den „projects“-Ordner im Explorer überhaupt nicht sehen. Nur wenn der Benutzer den exakten Pfad zum gewünschten Ordner kennt und im Explorer eingibt, kann er ihn öffnen. Es muss nicht erläutert werden, dass diese Art der Ordnerauswahl nicht benutzerfreundlich ist und auf heftigen Widerstand bei den Anwendern treffen wird.

Dieser Mangel liegt darin begründet, dass es in Windows erforderlich ist, zumindest die Berechtigungsstufe „Ordnerinhalt anzeigen“ auf einem Ordner zu besitzen, um diesen traversieren zu können (umgangssprachlich: um sich im Explorer „durchklicken“ zu können). Durch das oben beschriebene Konzept der Vergabe von Rechten über Berechtigungsgruppen auf den gewünschten Ordner wird diese, als „Listrecht“ bezeichnete, Berechtigung für übergeordnete Ordner nicht automatisch mitgesetzt.

Die Lösung für das Problem besteht darin, dem Benutzer für alle übergeordneten Ordner dieses Listrecht zuzuordnen. Selbstverständlich darf auch diese Berechtigungszuordnung nicht direkt auf dem Benutzer oder auf der Organisationsgruppe durchgeführt werden. Auch für das Listrecht muss eine entsprechende Berechtigungsgruppe angelegt werden. Angelehnt an das vorangegangene Beispiel mit dem Re-Branding-Projekt würde also eine Gruppe fs_srv_projects_li (das Postfix „li“ steht für „List“) angelegt werden und mit der Berechtigungsstufe „Ordnerinhalt anzeigen“ auf dem Ordner \\srv\projects\ berechtigt werden. Der Benutzer, oder die Gruppe, welche die Schreibberechtigung auf dem „rebranding“-Ordner erhalten soll, muss somit Mitglied der erzeugten Listgruppe werden.

Damit man aber nicht jedem Benutzer, der Schreibberechtigungen auf dem „rebranding“-Ordner bekommen soll, die zusätzliche Listgruppe manuell zuordnen muss, wird die Berechtigungsgruppe für den „rebranding“-Ordner ganz einfach Mitglied der Listgruppe. Der Benutzer erhält dann – angelehnt an das Beispiel – über die Marketingabteilung die Mitgliedschaft in der Berechtigungsgruppe für den „rebranding“-Ordner (über die Gruppe fs_srv_projects_marketing_w) und über diese wiederum die Mitgliedschaft in der übergeordneten Listgruppe, und damit das Listrecht für den „projects“-Ordner. Werden Berechtigungen auf tieferer Ebene als zwei vergeben, so müssen entsprechend mehrere Listgruppen angelegt werden. Die Berechtigungsgruppe für den Schreibzugriff ist dann Mitglied in allen Listgruppen der übergeordneten Ordner. Es ist jedoch zu beachten, dass Berechtigungen nicht tiefer als in der Ebene 3 gesetzt werden sollten, da ansonsten die Übersichtlichkeit leidet und auch die Anzahl der Gruppen stark zunimmt, da ja für jede Ebene zusätzliche Listgruppen benötigt werden. Es ist insbesondere zu beachten, dass bei älteren Versionen von Windows-Servern eine übermäßige Anzahl an Gruppenmitgliedschaften zu Problemen bei der Benutzeranmeldung führen kann. Dies ist dann der Fall, wenn die Anzahl der Gruppen die maximale Größe des Login-Tokens überschreitet (siehe dazu auch http://www.msxfaq.de/verschiedenes/kerberosticketsize.htm).

Vorsicht! Ein Detail muss beim Setzen der Berechtigung für die Listgruppe noch beachtet werden: Die Standardeinstellung für die Weitervererbung der Berechtigungsstufe „Ordnerinhalt anzeigen“ muss auf „Nur dieser Ordner“ geändert werden. Andernfalls würde das auf oberer Ebene gesetzte Listrecht via Vererbung auf alle Verzeichnisse mit aktivierter Vererbung am Fileserver angewendet werden und der Benutzer könnte fälschlicherweise mitunter den gesamten Fileserver im Explorer durchsuchen. Das Listrecht wird anschließend – je nach Windows-Version – nicht mehr als „Ordnerinhalt anzeigen“, sondern entweder als „Speziell“ oder als „Lesen & Ausführen“ angezeigt. Dies lässt sich nicht vermeiden, da für die Qualifizierung des Rechts „Ordnerinhalt anzeigen“ Windows-seitig die Voreinstellungen hinsichtlich der Vererbung zwingend erforderlich sind.

3.2. Ordnersichtbarkeit über ABE steuern

Windows erhielt mit der Version 2003 R2 eine sehr nützliche neue Funktion mit dem Namen „Access Based Enumeration“ (zu Deutsch „berechtigungsgesteuerte Aufzählung“). Diese Funktion bewirkt, dass der Benutzer im Windows Explorer nur noch Ordner zu sehen bekommt, auf denen er zumindest die oben beschriebene Listberechtigung hat. Ordner, auf denen der Benutzer keinen Zugriff hat, werden automatisch ausgeblendet. Diese Funktion sollte auf jeden Fall aktiviert werden. Eine Liste von vielen Ordnern zu sehen, und dabei nicht zu wissen, auf welche Ordner man Zugriff hat, ist für die Anwender unzumutbar. ABE erhöht insofern die Übersichtlichkeit für den Benutzer wesentlich.

Ein weiterer Vorteil besteht darin, dass Verzeichnisstrukturen zukünftig flacher gehalten werden können. Vormals mussten Ordner mitunter in tieferen Ebenen „versteckt“ werden, damit unbefugte Benutzer den Ordner nicht zu sehen bekamen und aufgrund der Ordnerbezeichnung bereits bestimmte Rückschlüsse ziehen konnten, die unerwünscht waren. Nunmehr können diese Ordner durchaus in einer höheren Ebene angesiedelt werden, und müssen nicht mehr versteckt werden – hat der Benutzer keinen Zugriff auf den Ordner, so sieht er ihn auch nicht – selbst, wenn er auf dem übergeordneten Ordner das Listrecht hat. Zur Aktivierung der ABE siehe: https://technet.microsoft.com/de-de/libRAry/dd772681(v=ws.10).aspx. Inzwischen haben auch Anbieter von Storage-Systemen mit integriertem CIFS-Server diese Funktion implementiert, sodass sie auch bei Einsatz dieser Systeme genutzt werden kann. Siehe dazu auch: https://library.netapp.com/ecmdocs/ECMP1196993/html/GUID-A6676E82-2E89-48C8-A014-369C58854113.html

4. Reporting

Ein wichtiger Aspekt ist die Etablierung von brauchbaren Reportmöglichkeiten. Ohne entsprechende Auswertungen fällt auch die Verwaltung der Berechtigungen schwer. Schnell wird die Situation undurchschaubar. Leider sind die Funktionen, die Microsoft für Reporting zur Verfügung stellt, sehr eingeschränkt. So ist lediglich Folgendes mit vertretbarem Aufwand umsetzbar:

4.1. Ressourcenauswertung

Um herauszufinden, welche Benutzer über effektive Berechtigungen auf einem Ordner verfügen, muss zuerst mit dem Windows Explorer festgestellt werden, welche Objekte (im Optimalfall lediglich Berechtigungsgruppen) auf dem Ordner berechtigt sind. Anschließend müssen diese Gruppen bis auf die Ebene der einzelnen Mitglieder aufgelöst werden. Hierfür steht lediglich das Werkzeug „Active Directory-Benutzer und -Computer" zur Verfügung. Die Vorgehensweise ist mit folgenden Nachteilen verbunden:

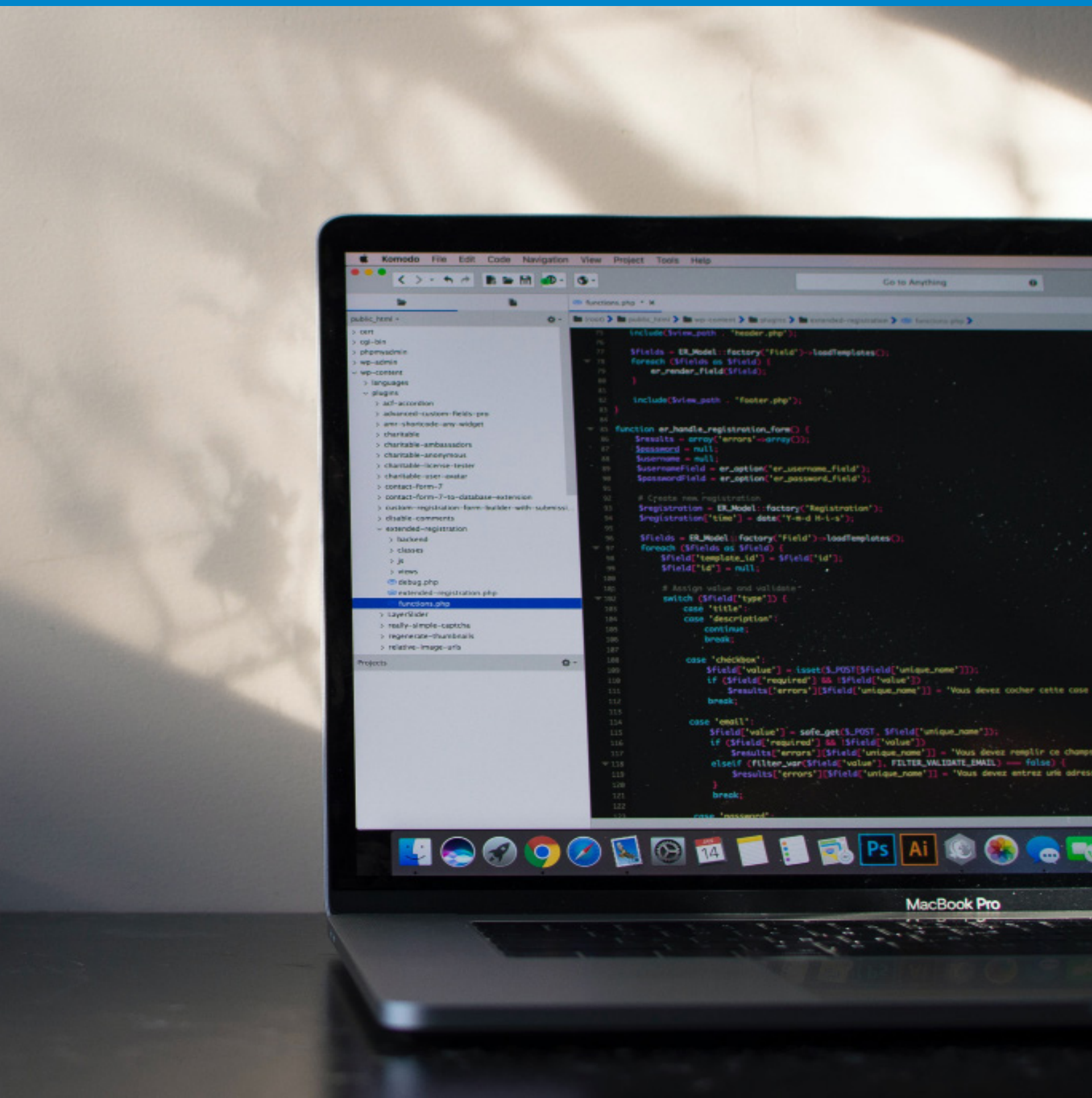
- Die manuelle Auflösung der Gruppen ist mit enormem manuellen Aufwand verbunden. Speziell wenn Gruppen – wie in AGDLP vorgesehen – verschachtelt sind, steigt der Aufwand für die Auflösung exponentiell an.
- Die Auswertung sagt nichts über etwaige Veränderungen in Unterordnern aus. Es kann nicht davon ausgegangen werden, dass jeder Unterordner exakt die gleiche Rechtestruktur aufweist. Es können einerseits zusätzliche Objekte auf Unterordnern berechtigt werden – andererseits können über eine Vererbungsunterbrechung (siehe oben) gänzlich abweichende Berechtigungen gesetzt werden.

4.1. Benutzerauswertung

Die Berechtigungen eines Benutzers können nur anhand der Gruppenmitgliedschaften des Benutzers abgelesen werden. Hierbei müssen die Gruppen nunmehr in umgekehrter Richtung aufgelöst werden, sodass am Ende die Ebene der Berechtigungsgruppen erreicht wurde. Anhand der Bezeichnungen kann nun hoffentlich abgelesen werden, wo der Benutzer berechtigt ist. Auch hier existieren signifikante Nachteile:

- Wurde die Namenskonvention der Gruppen nicht exakt eingehalten, ergeben sich mitunter Doppeldeutigkeiten

- Wurde der Benutzer – eventuell auch vor langer Zeit – auf einem Ordner direkt berechtigt, so ist diese Berechtigung nicht sichtbar
- Die manuelle Auflösung der Gruppen ist mit enormem manuellen Aufwand verbunden.



5. Organisatorische Elemente

Über die technische Architektur hinaus müssen für die Umsetzung eines Berechtigungsmanagementsystems auch einige organisatorische Elemente berücksichtigt werden. In den folgenden Abschnitten werden diese ansatzweise beschrieben. Da eine Abbildung mit Standardwerkzeugen nicht praktikabel ist, wird für die detaillierte, konkrete Umsetzung auf unsere weiterführende Literatur zu diesen Themen verwiesen.

5.1. Genehmigungsworkflows konzipieren und umsetzen

Für die Vergabe von Berechtigungen sind entsprechendes Know-how, Administrationsberechtigungen und die notwendigen Werkzeuge erforderlich. Daher ist der Vorgang primär eine Aufgabe der IT Abteilung. Der Auslöser des Vorgangs ist jedoch im Normalfall ein Mitarbeiter aus einem Fachbereich außerhalb der IT, der Zugriff für sich oder einen Mitarbeiter auf bestimmte Ressourcen anfordert. Die Entscheidung über die Vergabe der Berechtigungen sollte beim fachlich Verantwortlichen für die Daten liegen, auf die der Zugriff beantragt wurde. Dies ist im Normalfall ebenfalls ein Mitarbeiter aus einem Fachbereich außerhalb der IT. Somit liegt sowohl Beauftragung, als auch Entscheidung außerhalb der IT-Abteilung. Die IT ist lediglich für die eigentliche Durchführung verantwortlich.

Als zentrale Anlaufstelle gerät die IT-Abteilung damit in die Rolle des Vermittlers, der den Vorgang koordinieren muss. Diese Aufgabe ist zeitaufwändig und mit Verantwortung verbunden. Jeder Vorgang sollte deshalb zwecks Nachvollziehbarkeit detailliert dokumentiert werden.
Die Vergabe „auf Zuruf“ ohne Kontrolle und Dokumentation ist mittlerweile verpönt und sollte in jedem Fall vermieden werden. Es besteht sowohl die Gefahr interner Konfliktsituationen („Wieso und seit wann hat dieser Mitarbeiter Zugriff auf meine Daten?“), als auch die Gefahr entsprechender Findings bei Audits. Workflows im Berechtigungsmanagement zählen mittlerweile zweifelsfrei zum Stand der Technik (siehe hierzu zum Beispiel auch die Regelungen der ISO 27000) und müssen auch im Rahmen der EUDatenschutzgrundverordnung umgesetzt werden.

5.2. Dokumentation zur Nachvollziehbarkeit pflegen

Die Dokumentation der einzelnen Berechtigungsanträge ist aus mehreren Gesichtspunkten erforderlich:

- Als unternehmensinterner Nachweis darüber, wie Berechtigungen zustande gekommen sind
- Gegenüber Auditoren als Nachweis über die kontrollierte Vergabe von Berechtigungen im Rahmen des geltenden Stands der Technik

Zu jedem Vorgang sollten zumindest folgende Daten hinterlegt werden:

- Wann ist der Antrag eingelangt?
- Wer hat den Antrag gestellt?
- Welcher Benutzer soll Berechtigungen erhalten?
- Auf welchen Ordner sollen die Berechtigungen erteilt werden?
- Welche Berechtigungsstufe soll gesetzt werden? (Lesen, Ändern)
- Soll die Berechtigung unbefristet gelten oder per bestimmtem Datum ablaufen?
- Wann wurde der Antrag genehmigt?
- Wer hat den Antrag genehmigt? (unbedingt mit Nachweis, z.B. entsprechende E-Mail)
- Achtung: Gegebenenfalls ist mehr als eine Freigabe erforderlich (4-Augen-Prinzip)
- Welcher Administrator hat die Berechtigungen tatsächlich gesetzt?
- Wann wurden die Berechtigungen gesetzt?
- Wann wurden Antragsteller und berechtigter Benutzer über die Durchführung informiert?

Aus der Liste der zu dokumentierenden Daten geht bereits hervor, dass die Anlage der Dokumentation ein umfangreicher und zeitaufwändiger Vorgang ist. Für die ordnungsgemäße Durchführung führt allerdings kein Weg daran vorbei. In den „Tipps für die Umsetzung“ werden Empfehlungen gegeben, wie sich Workflows und Dokumentation zuverlässig, und mit möglichst geringen manuellen Aufwänden, realisieren lassen.

6. Tipps für die Umsetzung

In den Abschnitten oberhalb wird beschrieben, mit welchen Herausforderungen die Etablierung eines Berechtigungsmanagementsystems in Microsoft-Umgebungen verbunden ist. Es wird herausgestrichen, dass in vielen Bereichen klare Defizite bei den Werkzeugen existieren, die vom Hersteller standardmäßig bereitgestellt werden. Manche Funktionen werden überhaupt nicht betrachtet, wie etwa die Abbildung von Workflows. Für andere Aufgaben wird der Administrator nur mit rudimentären Werkzeugen versorgt und ist weitestgehend sich selbst überlassen. Dies gilt insbesondere für das Setzen von Berechtigungen und das Reporting.

Um diese Unwägbarkeiten zu überwinden, hat die tenfold Software GmbH eine Lösung entwickelt, die sich ganzheitlich der beschriebenen Schwierigkeiten annimmt. In den nachfolgenden Kapiteln wird beschrieben, welche Erleichterungen durch den Einsatz der Software tenfold für den Administrator, den IT-Sicherheitsverantwortlichen sowie die gesamte Organisation erzielt werden.

6.1. Berechtigungsvergabe

Die Vergabe von Berechtigungen mit Hilfe der Standardwerkzeuge ist geprägt von der manuellen Verwaltung der benötigten Berechtigungsgruppen. In tenfold wurde versucht, die Administration hiervon zu entkoppeln, um sich weitestgehend auf Benutzer, Ordner und Berechtigungsstufen konzentrieren zu können.

tenfold erlaubt dem Administrator, Berechtigungen auf Fileservern für Benutzer und Organisationsgruppen über die Weboberfläche ganz einfach per Drag & Drop zu vergeben. Die notwendige Gruppenstruktur wird dabei automatisch erzeugt und verwaltet. Der Berechtigungsmodus (A-G-DL-P, A-G-P, etc.), Namenskonventionen, Speicherorte im Active Directory und andere Einstellungen können dabei je Fileserver individuell festgelegt werden. tenfold ist sowohl in Single- als auch in Multi-Domain- Umgebungen einsatzfähig und kann beliebig viele Fileserver verwalten. Es werden sowohl native Windows Fileserver, als auch andere SMB/CIFS-basierte Lösungen (NetApp, EMC und weitere) unterstützt.

tenfold kümmert sich darüber hinaus von selbst um die Erzeugung entsprechender Listgruppen für das Browsing durch die Benutzer. Gruppen, die erzeugt wurden und nicht mehr benötigt werden, werden automatisch wieder entfernt. Durch die vollautomatische Verwaltung der Best-Practice-Strukturen können enorme Einsparungen bei der benötigten Arbeitszeit erzielt werden. Das Aufkommen typischer Fehler sinkt dabei gleichzeitig auf null. Die Administratoren können sich auf die wesentlichen Aufgaben des Geschäfts konzentrieren.

6.2. Reporting

Wie zuvor beschrieben, ist es out-of-the-box nur möglich, zwei Typen von Auswertungen mit vertretbarem Aufwand zu erstellen. Darüber hinaus sind die Möglichkeiten und vor allem die Zuverlässigkeit dieser Auswertungen wesentlich eingeschränkt. Mit einem IT-Sicherheitsmanagementsystem nach dem Stand der Technik sind diese Einschränkungen nicht vereinbar. Zurückzuführen ist diese Schwäche vordergründig darauf, dass es für entsprechende Reports keine geeignete Datenquelle gibt. Die Daten in Active Directory und auf den Ressourcen sind nur sehr lose (über Eintragung der SID) verknüpft. Active Directory weiß nicht darüber Bescheid, auf welchen Ressourcen die unterschiedlichen SIDs eingetragen wurden. Um dies herauszufinden, müssten die entsprechenden Ressourcen für den Report überprüft werden. Ein Echtzeitzugriff auf große Mengen von Ressourcen (zum Beispiel von 100.000 Ordnern auf dem Fileserver) ist jedoch aus Performancegründen ausgeschlossen.

Für das Datenmanagement wurde bei tenfold deshalb Neuland beschritten: Um die Auswertungsfähigkeit der Daten zu garantieren, werden diese regelmäßig in eine relationale Datenbank synchronisiert. Dabei werden sowohl alle Objekte des Active Directory, als auch die Ordner (und ACL) der Fileserver, gegebenenfalls die Objekte aus Exchange Server als auch die Objekte aus SharePoint Server über entsprechende Agents ausgelesen und in die tenfold Datenbank übertragen. Diese Vorgehensweise bringt zwei Vorteile mit sich:

1. Sind die Daten erst in der relationalen Datenbank angelegt, sind jegliche Abfragen wesentlich einfacher und mit unvergleichbarer Performance zu realisieren. Es werden interessante Berechtigungskonstellationen sichtbar, die vorher im Verborgenen geblieben sind.

2. Die Daten können in der tenfold Datenbank historisiert werden. Das ermöglicht Auswertungen nicht nur nach dem aktuellen Stand, sondern auf Basis jedes Zeitpunkts in der Vergangenheit. Voraussetzung ist, dass tenfold zu diesem Zeitpunkt bereits im Einsatz war – Datenbestände vor dem Einsatz von tenfold können nicht reproduziert werden.

Auf Basis der tenfold Datenbank können anschließend sowohl online als auch offline (PDF, Excel) in Sekundenschnelle übersichtliche Auswertungen erstellt werden:

- Zugriff auf einen Ordner am Fileserver (oder ein Postfachordner in Exchange Server oder ein Objekt in SharePoint Server): Gruppen werden automatisch aufgelöst und grafisch dargestellt, Änderungen auf Unterordnern (zusätzliche Berechtigungen, aufgebrochene Vererbung) sind sofort sichtbar, alle Änderungen an den Berechtigungen können im zeitlichen Verlauf dargestellt werden, und vieles mehr.
- Zugriff eines Benutzers: Alle Zugriffsmöglichkeiten des Benutzers, unabhängig, ob direkt oder über Berechtigungsgruppen in allen beteiligten Systemen, werden auf Objektebene und Berechtigungsstufe aufgelöst und angezeigt.
- Alle Berechtigungsänderungen eines Benutzers oder einer Ressource können im zeitlichen Verlauf visualisiert werden.
- Für alle Auswertungen kann auf historische Daten zugegriffen werden.

6.3. Workflows und Dokumentation

Im Standardumfang ist keine Workflowunterstützung vorhanden, weshalb häufig auf Ausweichlösungen zurückgegriffen wird. Im einfachsten Fall werden die Workflows manuell bearbeitet und die Ergebnisse in einem E-Mail-Postfach oder einer Excel-Liste abgelegt. Aufwändigere Lösungen basieren auf Ticketsystemen, IT-Service-Management-Lösungen oder Dokumentenmanagementsystemen. Für alle Umgehungslösungen stellt sich die zusätzliche Aufgabe, dass sowohl die Workflows (Schritte, Vier-Augen- Prinzip, Eskalationsregeln) als auch die einzelnen für die Ressourcen verantwortlichen Personen extern dokumentiert und verwaltet werden müssen. Derartige Medienbrüche machen Fehler und Unklarheiten sehr wahrscheinlich.

Allen Lösungen ist darüber hinaus eines gemeinsam: Der Fokus liegt darauf, die Daten in das System hineinzubekommen. Dagegen wird wenig Augenmerk darauf gelegt, wie die Daten anschließend vernünftig ausgewertet werden können. Weder eine Excel-Liste, noch ein Ticketsystem bieten hierfür den richtigen Ansatz. Die Möglichkeiten werden dem Stand der Technik nicht gerecht.

Workflows sind ein integrierter Bestandteil von tenfold. Jegliche Änderung an Benutzerkonten oder Berechtigungen sind nur über entsprechende Requests (Anträge) möglich. Über die Requests steuert tenfold automatisiert die Workflows. Die Modellierung der Workflows erfolgt grafisch auf Basis des einheitlichen Standards „BPMN“ (Business Process Model and Notation). Für die unterschiedlichen Ressourcen können auf der Oberfläche die Verantwortlichen definiert werden, auf welche in den Workflows referenziert wird. Beteiligte werden automatisch von tenfold informiert, wenn ein Antrag zur Freigabe ansteht – eine Anmeldung in tenfold ist nicht notwendig.

7. Fazit und Zusammenfassung

Viele Organisationen stehen vor den gleichen Herausforderungen. Dass man sich als Organisation heute mit der Thematik auseinandersetzen muss, ist Fakt – sei es aufgrund interner Anforderungen oder externer Faktoren, wie etwa Audits oder neuer gesetzlicher Grundlagen wie der EU-DSGVO. Die verfügbaren Handlungsalternativen sind in vielen Fällen unzureichend oder werfen für sich neue Probleme auf. Mit tenfold wird Berechtigungsmanagement auf Microsoft-Plattformen nach dem Stand der Technik überhaupt erst ermöglicht. tenfold bietet dabei eine ganzheitliche Lösungsplattform – von der technischen Abwicklung bis zu Workflows, Dokumentation und letztendlich Compliance hinsichtlich der relevanten Standards.

Über den Autor

Michael Ugrinovich

Senior Products & Services Manager

Michael Ugrinovich ist Senior Manager Products & Services beim Software Hersteller tenfold. Mit seinem hochgradigen technischen Know-how setzt der diplomierte IT-Experte ununterbrochen neue Maßstäbe beim Benutzer- und Berechtigungsmanagement sowie Identity- und Access Management. Er war richtungsweisend an der Entwicklung des Standard-Softwareprodukts tenfold beteiligt.

tenfold unterstützt mittelständische und große Unternehmen beim systemübergreifenden Berechtigungsmanagement. Das bedeutet, dass alle Produkte, in denen Berechtigungen verwaltet werden, in den tenfold Workflow integriert werden können. Das sind unter anderem Active Directory, File Server (Ordnerfreigaben), Exchange, SAP oder branchenspezifische Anwendungen. tenfold überwacht und verwaltet dabei den gesamten Lebenszyklus der Benutzer und kann dabei automatisiert auf Ereignisse wie Eintritt, interne Wechsel oder Ausscheiden von Mitarbeitern reagieren. Daten können dabei aus dem Personalsystem automatisch übernommen werden – tenfold ist mit allen namhaften Anbietern kompatibel. Durch die Automatisierung dieser Prozesse wird die Datensicherheit wesentlich erhöht. Das ist darauf zurückzuführen, dass Benutzerkonten zuverlässig gesperrt werden, wenn Mitarbeiter das Unternehmen verlassen. Die automatische Anpassung der Berechtigungen beim Abteilungswechsel sorgt für zusätzliche Sicherheit und löst nebenbei das weithin bekannte „Azubi-Problem“. Der Entfall von Routinetätigkeiten im Benutzer- und Berechtigungsmanagement schafft wieder freie Ressourcen für die wirklich wichtigen Aufgaben der IT.

info@tenfold-security.com
www.tenfold-security.com