

Microsoft Office SharePoint Server

von

Dipl.-Ing. Thomas Simon
Dipl.-Ing. Lars Kuhl
Dipl.-Des. Alexandra Meyer
Dominik Zöller

4 Planungsaspekte

4.1 Architektur

Die SharePoint-Technologie basiert auf drei wesentlichen Komponenten, die jeweils eigene Dienste und Applikationen anbieten: Betriebssystemdienste, Windows SharePoint Services und MOSS 2007 Dienste.

Dabei ist es so, dass sich die Windows SharePoint Services der Dienste des Betriebssystems bedienen und selber Dienste für den MOSS 2007 bereitstellen. Die Dienste sind von Schicht zu Schicht immer mehr ausgerichtet auf die Unterstützung von Geschäftsprozessen.

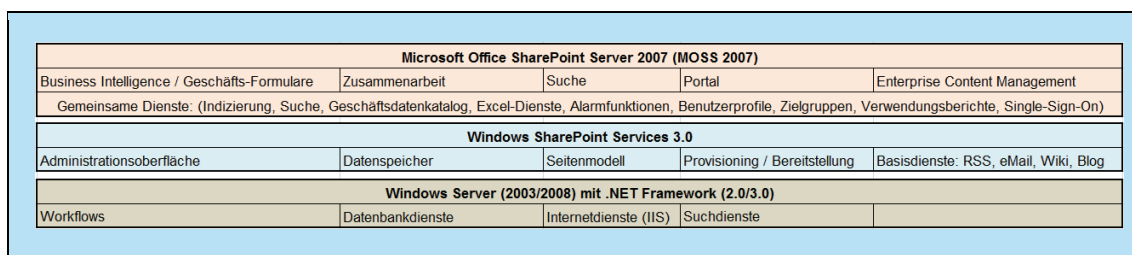


Abbildung 107: MOSS 2007 Architektur

Die Betriebssystemdienste stellen die unterste Ebene dar. Sie sind beispielsweise für die Bereitstellung der Tools zur Verwaltung der Hardware zuständig. Auch die Datenbankdienste (SQL-Server) sowie die Workflowdienste sind zu den Betriebssystemdiensten zu zählen.

Die Windows SharePoint Dienste in der Version 3.0 bilden die nächst höhere Ebene und stellen Features wie Blogs, Wikis, RSS, Dokumentenzusammenarbeit, Aufgabenmanagement sowie die E-Mail-Verwendung und die Kopplung zu den Office Applikationen zur Verfügung.

Die letzte Ebene bilden die MOSS 2007 Dienste, die als umfangreiche Erweiterung der Windows SharePoint Dienste zu verstehen sind. Als Beispiel kann hier die Lösung der Geschäftsprozess-Integration genannt werden: Über den Geschäftskundenkatalog kann auf Geschäftsdaten in LOB-Systemen (Line of Business) zugegriffen werden und Geschäftsprozesse können über die Forms Services sowie Workflows abgebildet werden. Weiterhin gehört zu den bereitgestellten Funktionen auch der „Anbieter für gemeinsame Dienste“ (Shared Service Provider, SSP). Der SSP ist als Sammlung von Diensten und Funktionen (Benutzerprofile, My Sites, Suche, Excel Dienste, Geschäftskundenkatalog) zu verstehen, die einmal zentral in der Farm konfiguriert werden und in allen Webanwendungen der Farm verwendet werden können.

4.2 Sicherheit im MOSS 2007

Bei der Entwicklung des MOSS 2007 wurde besondere Aufmerksamkeit auf die Verbesserung der Sicherheit gesetzt:

- Bei der Installation einer MOSS-2007-Farm werden für diverse Funktionen auf Farm-, SSP-, WSS-Such- und Anwendungspoolebene Dienstkonten benötigt (siehe Tabelle 3).

Ebene	Konto	Besonderheiten
Farm	Benutzerkonto für die Installation	securityadmin, dbcreator, lokaler Administrator
	SQL-Server-Dienstkonto	
SSP	Serverfarmkonto	securityadmin, dbcreator, db owner
	Anwendungspoolkonto	db_owner für SSP-Inhaltsdatenbank
	SSP-Dienstkonto	kein Mitglied der lokalen Administratoren
	MOSS-Suchdienst-Konto	
	Inhaltszugriff Standard-Konto	benötigt Lesezugriff auf alle Ressourcen, die indiziert werden sollen
	Profilimport Standard-Konto	benötigt Lesezugriff auf den Verzeichnisdienst
Anwendungspool	Excel-Services Dienstkonto	
	ein Konto pro Webanwendung	db_owner

Tabelle 3: Dienstkonten für MOSS 2007

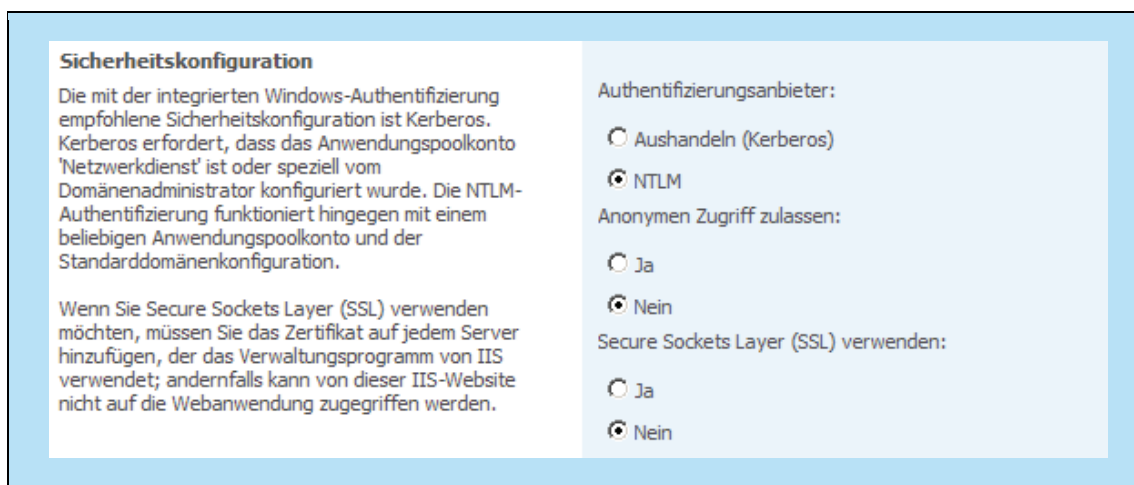


Abbildung 108: Authentifizierungsanbieter beim Erstellen einer Webanwendung

- Der IIS-Dienst übernimmt die Benutzerauthentifizierung in einer MOSS-2007-Farm. Nach der Authentifizierung erfolgt die Autorisierung – Bestimmung dessen, worauf der Benutzer Zugriff hat. Die Authentifizierung der Benutzer kann über verschiedene Mechanismen erfolgen. Bei der Erstellung einer Webanwendung kann man nur zwischen den folgenden Authentifizierungsanbietern wählen:
 - Integrierte Windows-Authentifizierung (Kerberos oder NTLM)
 - Anonyme Authentifizierung

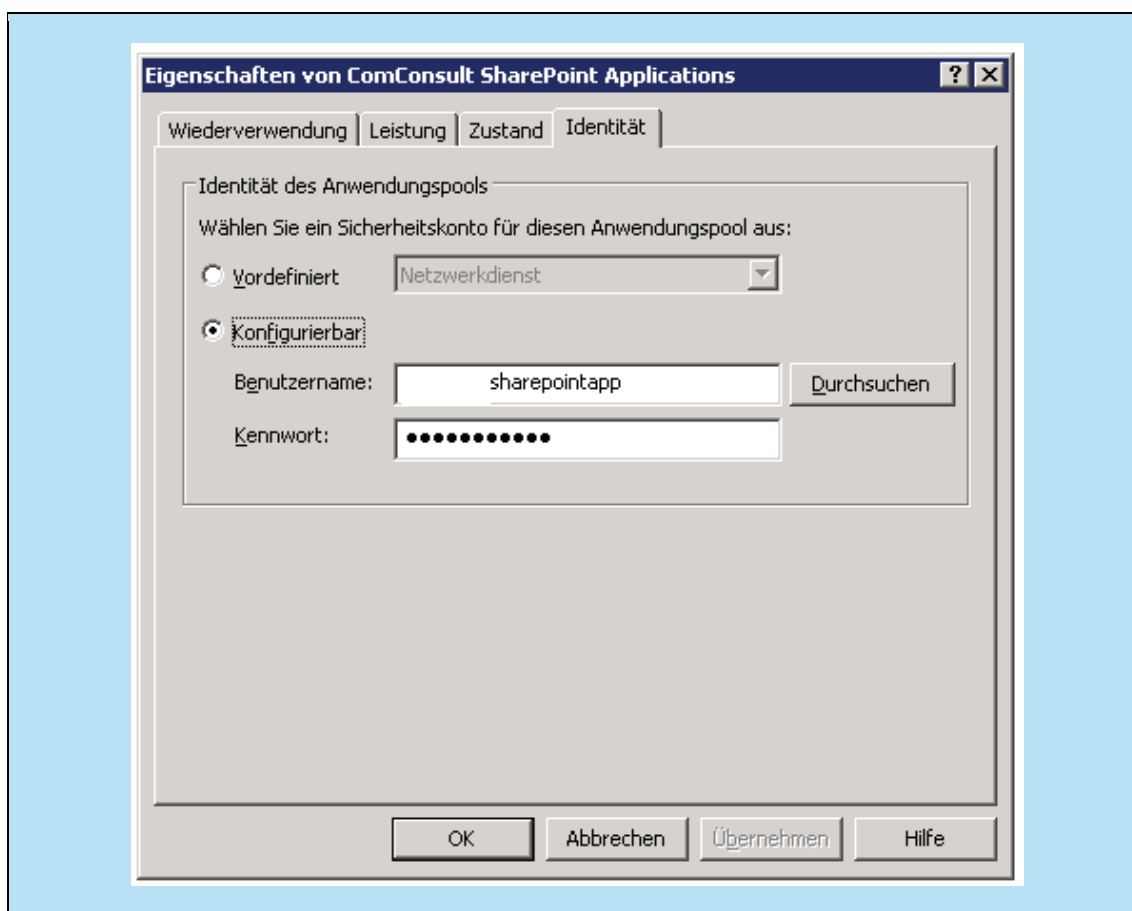


Abbildung 109: Identität des Anwendungspools

Integrierte Authentifizierung bedeutet, dass die Benutzer mit ihrem aktuell verwendeten Benutzernamen und Kennwort auf die MOSS 2007 Ressourcen zugreifen können, ohne diese Daten nochmals eingeben zu müssen. Hierbei kann NTLM oder Kerberos verwendet werden. Bei Wahl der NTLM Authentifizierung ist zu berücksichtigen, dass über HTTP gesendete NTLM-Kennwörter nur dann als sicher eingestuft werden können, wenn sie länger als 14 Zeichen sind. Somit ist Kerberos der bevorzugte Mechanismus und sollte direkt bei der Erstellung einer Webanwendung ausgewählt

werden. Hierzu ist zu erwähnen, dass nach Erstellen der Webanwendung manuell in der Kommandozeile noch ein SPN (Service Principal Name) für die Prozessidentität des Webanwendungspools erstellt werden muss (im nachfolgenden Code ist <Benutzername> die Identität des Anwendungspools):

```
Setspn.exe -A http/<Servername> <Domänenname>\<Benutzername>
```

Bei Verwendung der **anonymen Authentifizierung** können die Benutzer ohne die Eingabe von Benutzername und Kennwort auf die MOSS 2007 Inhalte zugreifen. Im Hintergrund wird für die anonyme Authentifizierung das Systemkonto IUSR_<computernamen> verwendet. Anonyme Authentifizierung wird bei öffentlichen Webseiten verwendet, aber nicht dort, wo Benutzern gezielt Inhalt zur Verfügung gestellt werden soll bzw. Kollaboration auf Team- oder Firmenebene betrieben werden soll. In der Standardeinstellung ist die anonyme Authentifizierung deaktiviert.

Nach Erstellung der Webanwendung stehen über die Zentraladministration umfangreichere Konfigurationsmöglichkeiten zur Verfügung:

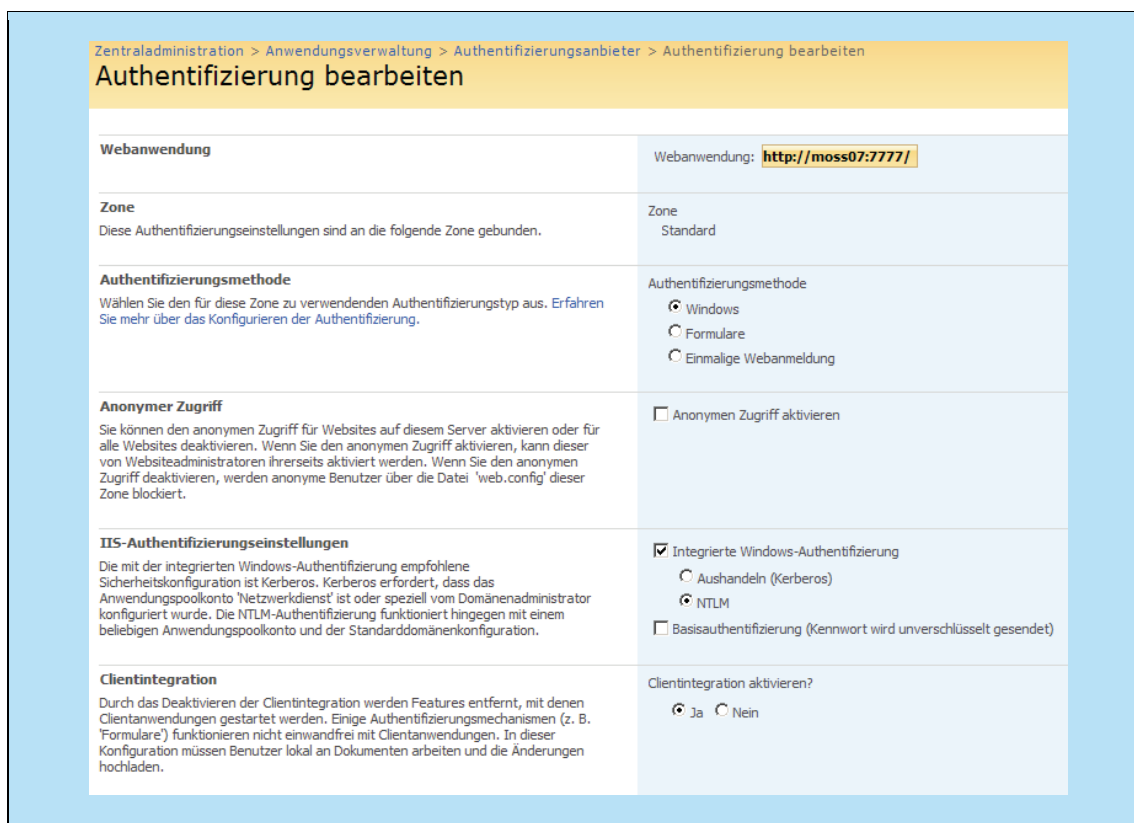


Abbildung 110: Bearbeiten der Authentifizierung

Bei der **Formularbasierten-Authentifizierung** können die Anmeldeinformationen in einem Active Directory, einem SQL-Server oder einem beliebigen LDAP-Verzeichnis gespeichert sein. Es öffnet sich ein Anmeldeformular, in das die Benutzererkennung eingegeben wird, die dann verifiziert wird.

Über einen Cookie kann die Identität für spätere Anmeldungen wiederhergestellt werden.

Bei der Authentifizierungsmethode „**Einmalige Webanmeldung**“ (auch SSO, Single-Sign-On) wird die Möglichkeit gegeben, mit einer Anmeldung einzigen Anmeldung aus dem SharePoint heraus auf andere Informationsquellen (z.B. eine Oracle Datenbank mittels einem Oracle-Webpart) zuzugreifen.

Weiterhin ist es möglich, die **Basisauthentifizierung** zu verwenden, bei der Benutzername und Kennwort im Klartext übertagen werden. Diese Variante könnte Verwendung finden, wenn Kerberos- oder NTLM- Authentifizierungen nicht möglich sind (Ports sind beispielsweise gesperrt), da ein Zugriff über das Internet erfolgt. Daher ist SSL bei der Verwendung der Standardauthentifizierung unumgänglich.

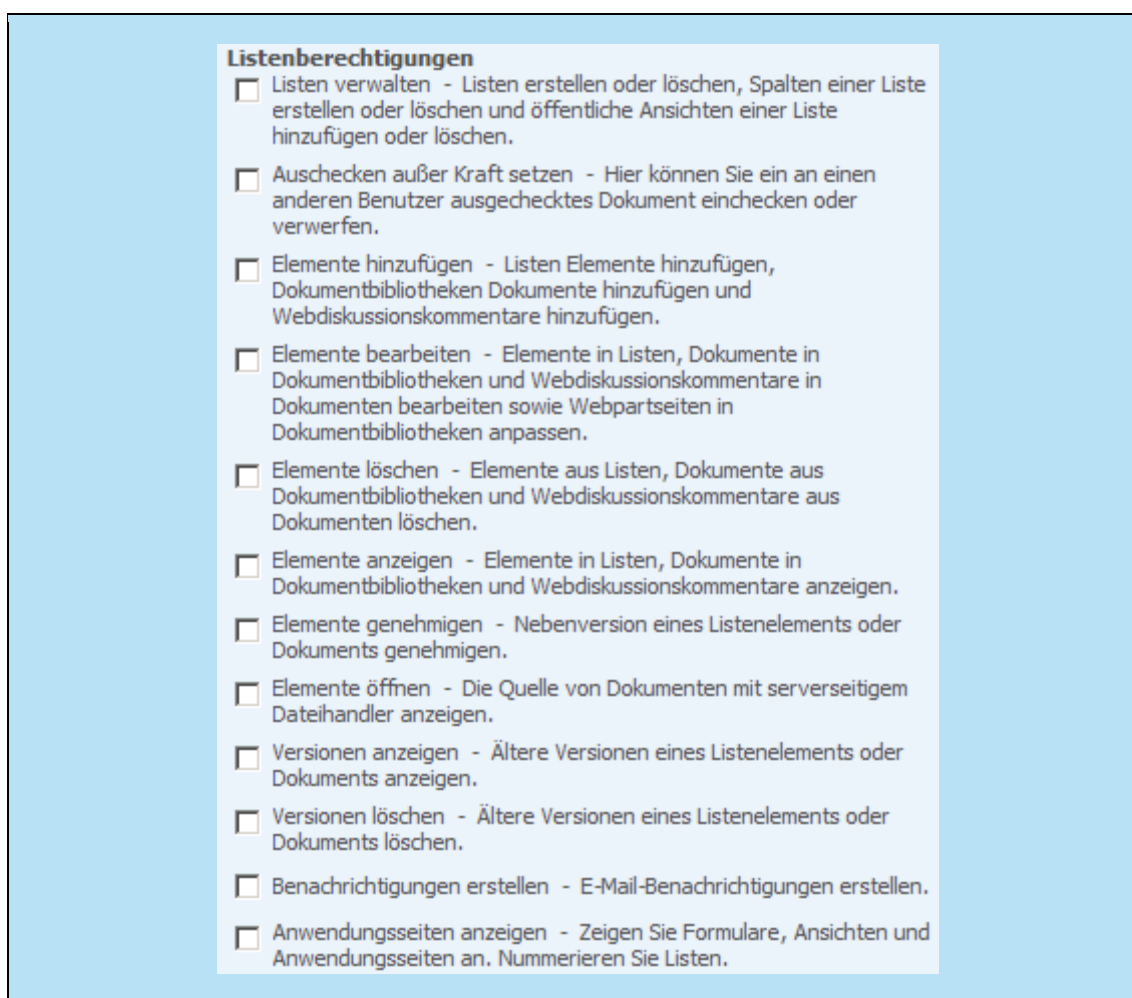


Abbildung 111: Listenberechtigungen

Websiteberechtigungen

- Berechtigungen verwalten - Berechtigungsstufen für die Website erstellen und ändern, und Benutzern und Gruppen Berechtigungen zuweisen.
- Verwendungsdaten anzeigen - Berichte über Websiteverwendung anzeigen.
- Unterwebsites erstellen - Unterwebsites wie Teamwebsites, Besprechungsarbeitsbereich-Websites und Dokumentarbeitsbereich-Websites erstellen.
- Website verwalten - Erteilt das Recht, alle Verwaltungsaufgaben für die Website wahrzunehmen sowie Inhalt zu verwalten.
- Seiten hinzufügen und anpassen - HTML- oder Webpartseiten hinzufügen, ändern oder löschen, und die Website in einem zu Windows SharePoint Services kompatiblen Editor bearbeiten.
- Designs und Rahmen anwenden - Design oder Rahmen auf die ganze Website anwenden.
- Stylesheets anwenden - Stylesheet (CSS-Datei) auf Website anwenden.
- Gruppen erstellen - Eine Gruppe von Benutzern erstellen, die überall in der Websitesammlung verwendet werden kann.
- Verzeichnisse durchsuchen - Dateien und Ordner in einer Website auflisten, die SharePoint Designer- und Web DAV-Schnittstellen verwenden.
- Self-Service Site Creation verwenden - Website mit Self-Service Site Creation erstellen.
- Seiten anzeigen - Seiten einer Website anzeigen.
- Berechtigungen auflisten - Berechtigungen für die Website, die Liste, den Ordner, das Dokument oder das Listenelement auflisten.
- Benutzerinformationen durchsuchen - Informationen über Websitebenutzer anzeigen.
- Benachrichtigungen verwalten - Benachrichtigungen für alle Benutzer der Website verwalten.
- Remoteschnittstellen verwenden - SOAP-, Web DAV- oder SharePoint Designer-Schnittstellen zum Zugreifen auf die Website verwenden.
- Clientintegrationsfeatures verwenden - Features zum Starten von Clientanwendungen verwenden. Ohne diese Berechtigung müssen Benutzer lokal an Dokumenten arbeiten und die Änderungen hochladen.
- Öffnen - Ermöglicht Benutzern das Öffnen einer Website, einer Liste oder eines Ordners und das Zugreifen auf im Container enthaltene Elemente.
- Persönliche Benutzerinformationen bearbeiten - Benutzern das Ändern ihrer eigenen Benutzerinformationen ermöglichen, z. B. Hinzufügen eines Bildes.

Abbildung 112: Websiteberechtigungen

- Berechtigungen können derart auf MOSS 2007-Objekte gesetzt werden, dass nur einzelne Benutzer oder Benutzergruppen Zugriff auf die Elemente haben. Standardmäßig findet eine Vererbung der Berechtigungen statt, die selbstverständlich auch deaktiviert werden kann. Eine im Hinblick auf die

Vererbung hierarchisch geordnete Liste der Objekte ist nachfolgend dargestellt:

- Websitesammlungen,
- Websites / Arbeitsbereiche,
- Listen / Bibliotheken,
- Ordner,
- Elemente / Dokumente.

Pro Objekt werden die Berechtigungen in Form von „Berechtigungsstufen“ für Benutzer oder Gruppen gesetzt (siehe Abbildung 111 bis Abbildung 113). Dabei ist eine Berechtigungsstufe als Zusammenfassung von Einzelberechtigungen zu verstehen. Diese Einzelberechtigungen kommen aus den Kategorien Listenberechtigungen, Websiteberechtigungen und Persönliche Berechtigungen. Durch den Administrator können eigene neue Berechtigungsstufen als Kombination aus Einzelberechtigungen erstellt werden und vorhandene Berechtigungsstufen können editiert oder gar gelöscht werden.

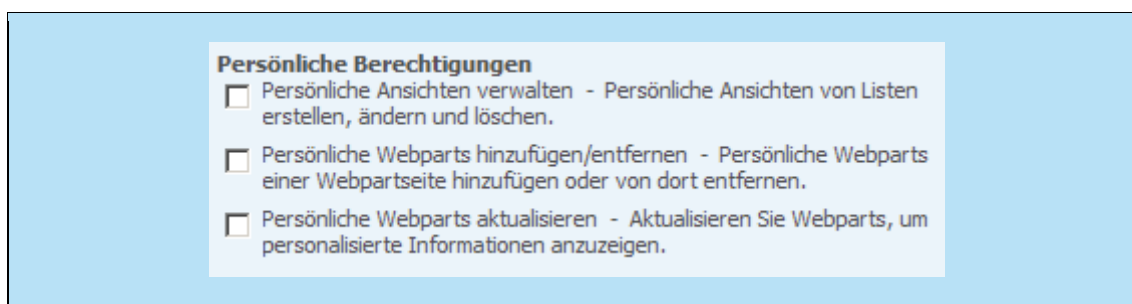


Abbildung 113: Persönliche Berechtigungen

- Ähnlich des bereits von Windows Fileservern bekannten Features ABE (Access Based Enumeration) werden auch bei der Anzeige von MOSS 2007 Inhalten die Rechte des zugreifenden Benutzers berücksichtigt und nur die Inhalte angezeigt, auf die er berechtigt ist.
- Die Administration einer MOSS 2007 teilt sich in drei Bereiche auf, für die es auch dedizierte Administratoren geben kann:
 - Shared-Service-Provider-Administratoren,
 - Websitesammlungsadministratoren,
 - Farmadministratoren.