DocuWare

White Paper Sicherheit

DocuWare

Inhalt

1 Zielsetzung dieses White Papers 5

2 Einführung in DocuWare 6

3 Zugang zum DocuWare-System 7

3.1 Loginverfahren 7

3.2 Passwörter 7

3.3 Kommunikation der Komponenten 8

4 Authentizität: Echtheit der Dokumente 9

4.1 Systemeinträge zu Dokumenten 9

4.2 Elektronische Signaturen 9

5 Vertraulichkeit: Dokumentenzugriff nur für berechtigte Benutzer 10

5.1 Rechtesystem 10

5.1.1 Funktionale Rechte 11

5.1.2 Archivrechte 11

5.1.3 Benutzer- und Administratorrechte 12

5.2 Zuweisung der Rechte 12

5.2.1 Profile und Rollen 13

5.2.2 Vordefinierte Rollen und Profile 13

5.2.3 Benutzer und Gruppen 15

5.2.4 Ererbte und explizite Rechte 15

5.2.5 Zusammenspiel der Rechte und Berechtigungen 15

5.2.6 Dokumentzugriffe über Indexdaten einschränken 16

5.3 DocuWare als Hochsicherheitssystem 17

5.4 Dokumente verschlüsseln 17

5.5 Sensible Daten außerhalb von DocuWare schützen 18

6 Integrität von Daten und Dokumenten 19

6.1 Änderungen als neue Versionen speichern 19

6.2 Protokollierung von Benutzer-Ereignissen 20

7 Verfügbarkeit des DocuWare-Systems 21

8 Datensicherung 22

8.1 Komponenten für externes Backup 22

8.2 Backup von Dokument-Metadaten 22

Dieses Dokument wurde erstellt mit AuthorIT™, Total Document Creation (http://www.author-it.com).

Disclaimer

Dieses Dokument wurde mit größter Sorgfalt zusammengestellt und die Informationen darin sind Quellen entnommen, die als zuverlässig gelten. Dennoch kann keine Haftung übernommen werden für die Richtigkeit, Vollständigkeit und Aktualität der Informationen. Aus den in diesem Dokument aufgenommenen Informationen können keine Ansprüche hergeleitet werden. Die DocuWare GmbH behält sich das Recht vor, jegliche Informationen, die in diesem Dokument enthalten sind, ohne vorherige Ankündigung zu verändern.

DocuWare GmbH
Therese-Giehse-Platz 2
82110 Germering
www.docuware.com

1 Zielsetzung dieses White Papers

Dieses White Paper stellt die Sicherheitsmaßnahmen innerhalb der DocuWare Software dar. Sie erfahren, mit welchen Technologien und Methoden die Haupt-Sicherheitsziele umgesetzt werden können, wie sie unter anderem im Leitfaden IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik beschrieben werden.

Zu den Sicherheitszielen gehören:

- Vertraulichkeit: Dokumente und Daten sind nur für berechtigte Benutzer zugänglich
- Integrität: Dokumente und Daten können nicht unautorisiert geändert werden, Änderungen lassen sich nachvollziehen
- Verfügbarkeit: Dokumente und Dienste von DocuWare stehen jederzeit zur Verfügung
- Zugangs- und Zugriffssicherheit zum DocuWare-System
- Sicherung der in DocuWare gespeicherten Daten

Die dargestellten Sicherheitsmaßnahmen beziehen sich auf in DocuWare gespeicherte Dokumente und Daten.

Nicht Thema dieses White Papers sind die Einrichtung eines DocuWare-Systems, die Einbettung von DocuWare in die IT-Infrastruktur des Unternehmens, die Sicherung von Datenbanken und des Dateisystems außerhalb von DocuWare, der Schutz der lokalen Rechner sowie DocuWare als Service Provider (DocuWare Cloud).

Ziel des White Papers ist es, Ihnen zu ermöglichen, sich ein technisch fundiertes Urteil über die Sicherheit eines DocuWare On-Premises-System zu bilden.

Das White Paper richtet sich an technisch interessierte Leser, vor allem an technische Mitarbeiter bei Kunden, Vertriebspartnern und Beratungsunternehmen, sowie an Fachmedien. Vorausgesetzt wird lediglich ein technisches Grundlagenwissen über den Aufbau moderner Software-Anwendungen, idealerweise von Dokumenten-Management-Systemen.

2 Einführung in DocuWare

DocuWare ist die moderne Lösung für Dokumentenmanagement und Workflow-Automation. Mit DocuWare können Benutzer zu jedem Zeitpunkt und von jedem Ort aus auf ihre Dokumente und die wichtigen Informationen darin zugreifen.

Die Dokumente werden in Archiven zentral abgelegt. Zur Anzeige und Bearbeitung der Dokumente steht der browserbasierte DocuWare Client zur Verfügung. Auch ist es möglich, Dokumente aus DocuWare ins Dateisystem zu laden.

Durch die zahlreichen Indexierungsfunktionen werden alle Dokumentarten immer am richtigen Ort archiviert und mit wenigen Klicks wieder auf den Bildschirm geholt.

Diese und zahlreiche weitere Funktionen, zum Beispiel das Workflow-Management, machen DocuWare zu einer leistungsstarken Software, mit der Sie Ihre Geschäftsprozesse gezielt optimieren können. Über die verschiedenen Anwendungsfelder informiert Sie auch die DocuWare Webseite.

DocuWare folgt in seinem Sicherheitskonzept den Prinzipien der europäischen Datenschutz-Grundverordnung (DSGVO), die in Artikel 25 den Schutz personenbezogener Daten durch Technikgestaltung und datenschutzrechtliche Voreinstellungen fordert.

Wenn Sie mehr über die technischen Aspekte von DocuWare erfahren möchten, finden Sie im DocuWare Knowledge Center und auf der DocuWare-Webseite weitere Informationen zu folgenden Themen:

- White Paper Systemarchitektur
- White Paper Integration
- White Paper Intelligent Indexing
- White Paper DocuWare Cloud
- Compliance und Zertifizierungen

3 Zugang zum DocuWare-System

Der Zugriff auf das DocuWare-System und die zentralen Archive ist durch ein Loginverfahren sowie durch einen sicheren Datenaustausch der Komponenten untereinander geschützt.

Im Rahmen der Authentifizierung wird die Identität des Benutzers, der sich anmeldet, geprüft und verifiziert. Dies gilt auch für IT-Komponenten oder Anwendungen, die auf das DocuWare-System zugreifen sollen.

Mehr Informationen zum Aufbau eines DocuWare-Systems im White Paper Systemarchitektur

3.1 Loginverfahren

Die Nutzung des Systems erfordert zunächst immer eine Anmeldung am Authentification Server. Der Authentification Server verwaltet sämtliche Benutzer, Lizenzen und Rechte des Systems.

Authentification Server unterstützt die folgenden Authentifizierungsmethoden:

- **DocuWare-Login**
  Der Benutzer muss sich über Namen und Kennwort, wie in DocuWare hinterlegt, als berechtigt ausweisen.
- **Trusted Login (Single Sign-On)**
  Der Client identifiziert sich ohne weitere Benutzereingabe über den Login-Namen des Windows-Betriebssystems. Der Authentication Server prüft den Login mittels der Benutzerverwaltung von Windows. Damit dieses Verfahren verwendet werden kann, müssen sich Client und Server im selben Windows Domain Netzwerk befinden.
- **Login Token**
  Login Tokens werden in der Regel nur für Single Sign-Ons zwischen DocuWare-Komponenten verwendet. Damit muss sich der Benutzer nur einmal bei DocuWare anmelden, auch wenn er beispielsweise zuerst den Web Client und dann die DocuWare Konfiguration aufruft. Authentification Server stellt dazu ein Login Token für einen Benutzer aus, wenn dieser sich für Anwendung A hinreichend authentifiziert hat, und übermittelt dieses verschlüsselt zur Anwendung B.

Die meisten DocuWare Komponenten kommunizieren über HTTP(S). Einmal verifizierte Anmeldedaten werden verschlüsselt vom Server an den Client gesendet, der diesen String zur Authentifizierung nachfolgender Anfragen benutzt. Dieses Cookie wird beispielsweise verwendet, um den Benutzer bei einem erneuten Öffnen des Browsers automatisch zu verifizieren.

3.2 Passwörter

Außer den Passwörtern der DocuWare-Benutzer werden auch das Datenbankserver-Passwort und das Passwort für den Mailserver kryptographisch sicher gespeichert, so dass nur die Serverkomponenten diese entschlüsseln können. Damit sind diese Daten sicher, auch wenn bestimmte Benutzer auf die für die Speicherung verwendeten Datenbanken zugreifen können, etwa für Backup-Zwecke.

Technische Umsetzung

Für die Verschlüsselung von Passwörtern wird der Algorithmus PBKDF2 (Password-Based Key Derivation Function 2) eingesetzt. Dabei wird eine Hashfunktion zusammen mit einem Saltwert auf das Passwort angewendet. Durch die Kombination mit einem Zufallswert entsteht auch bei zwei identischen Passwörtern nicht der gleiche Hashwert. Die Funktion wird danach mehrere tausend Male auf das Ergebnis angewendet. Dieses Verfahren erschwert es Hackern, durch Brute-Force-Attacken aus dem gehashten Wert auf das ursprüngliche Passwort zu schließen.

Passworteinstellungen

In der DocuWare Administration lässt sich festlegen, wie komplex Passwörter sein müssen. Sie definieren beispielsweise, ob ein Groß- oder Kleinbuchstabe, eine Ziffer oder ein Sonderzeichen in der Zeichenfolge enthalten sein müssen. Auch lässt sich die minimale Zeichenzahl eines Passworts festlegen, wie lange es gültig bleibt und ab wie vielen falschen Passworteingaben der Zugang gesperrt wird.

Der Organisationsadministrator kann zudem das Passwort-Zeitlimit für bestimmte Benutzer deaktivieren. Dies ist beispielsweise dann nützlich, wenn sich Dienste als Benutzer bei einem Server anmelden müssen.

Hat der Benutzer sein Passwort vergessen, kann er über den Anmeldedialog des Web Client ein automatisch generiertes Passwort anfordern. Damit ist es möglich, sich im Web Client einzuloggen und ein neues persönliches Passwort einzugeben.

Alternativ dazu kann auch der Organisationsadministrator das Passwort zurücksetzen. Dies ist für Benutzer mit der Sicherheitsstufe „Hoch" allerdings nicht möglich, siehe auch Kapitel DocuWare als Hochsicherheitssystem (auf Seite 17). Benutzer mit hoher Sicherheitsstufe können ihre Passwörter nur selber erneuern.

3.3 Kommunikation der Komponenten

Um einem Angriff von außen und damit dem unautorisierten Abgriff von Daten vorzubeugen ist es wichtig, die **Kommunikation per HTTP zwischen den webbasierten Client-Anwendungen und dem Platform Service mit SSL/TLS abzusichern** (HTTPS).

Um die DocuWare-Komponenten für HTTPS (SSL/TLS) zu konfigurieren, müssen Sie im IIS Manager folgende Schritte vollziehen:

- Zertifikat bzw. Zertifikate einspielen ("Serverzertifikate", Aktion "Importieren")
- Bindung der Website anpassen und über SSL/TLS erreichbar machen
- Ggf. die HTTP - Bindung aus Sicherheitsgründen entfernen (optional)

4 Authentizität: Echtheit der Dokumente

Daten gelten als authentisch, wenn sie jederzeit ihrem Ursprung zugeordnet werden können. In DocuWare lässt sich die Herkunft der gespeicherten Dokumente anhand von unveränderbaren Systemeinträgen sowie elektronischen Signaturen nachweisen.

4.1 Systemeinträge zu Dokumenten

Bei der Ablage eines Dokuments in DocuWare werden automatisch Systemeinträge erstellt, die zu keiner Zeit von Benutzern in DocuWare geändert werden können. Folgende Systemeinträge zu Benutzer, Datum sowie Dokumentänderungen und -zugriffen geben Aufschluss über den Ursprung des Dokuments:

Abgelegt von	Abgelegt am
Letzte Änderung am	Letzte Änderung von
Letzer Zugriff am	Letzter Zugriff von
Dokument-ID	

Systemeinträge rufen Sie über das Kontextmenü eines Dokuments in der Ergebnisliste *Indexeinträge ändern* > *Systemeinträge* ab.

4.2 Elektronische Signaturen

Eine elektronische Signatur erfüllt den gleichen Zweck wie eine eigenhändige Unterschrift bei Papierdokumenten. Sie stellt weitgehend sicher, dass ein Dokument wirklich vom Urheber stammt. Auch lassen sich anhand von Signaturen Änderungen von Dokumenten nachprüfen und verifizieren.

Mit einer Angabe zum Urheber oder Absender ist ein Dokument bereits digital unterzeichnet, wobei eine einfache Signatur keinen besonderen Bestimmungen zur Fälschungssicherheit unterliegt. Eine in DocuWare per Stempel eingefügte gescannte Unterschrift kann als eine einfache elektronische Signatur fungieren.

Um sich eindeutig als Urheber von einem Dokument auszuweisen, haben Sie die Möglichkeit, für ein Dokument im PDF-A-Format beim Import in DocuWare ein Zertifikat auszuwählen. Das Zertifikat muss sich auf dem Client-Rechner im Windows-Zertifikat-Speicher befinden und nur der Benutzer darf darauf zugreifen.

Zertifikate sollten folgende Merkmale aufweisen:

- RSA-Zertifikat (empfohlen)
- Länge: mindestens 1024 Bit, empfohlen 2048 Bit
- Schlüsselverwendung: digitale Signatur

Ein mit Zertifikat importiertes Dokument kann in DocuWare mit Stempeln und Anmerkungen versehen, nicht jedoch bearbeitet werden.

5 Vertraulichkeit: Dokumentenzugriff nur für berechtigte Benutzer

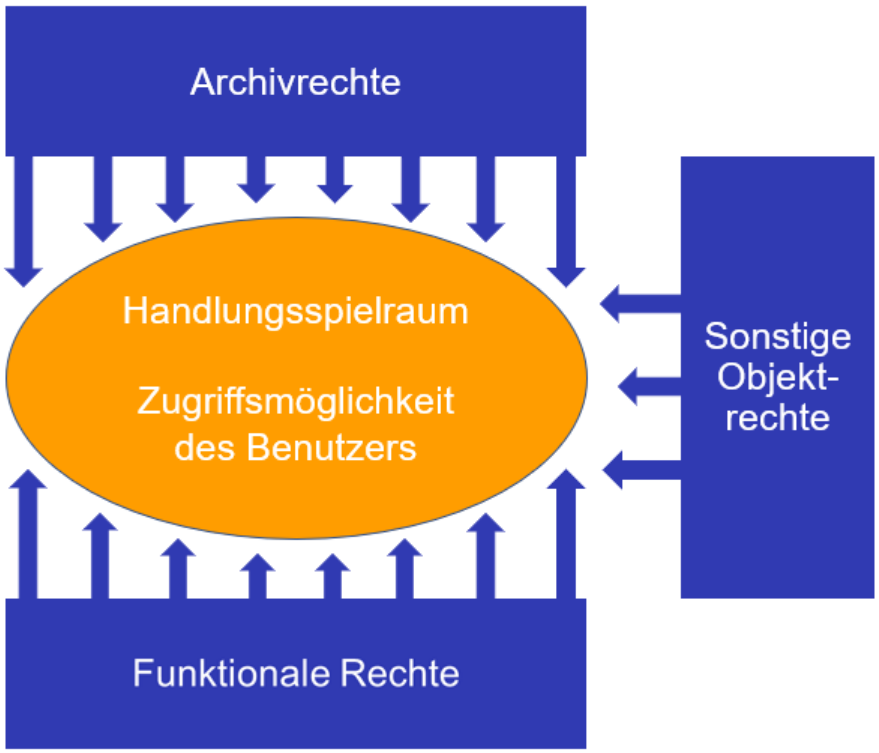
Mitarbeiter in großen Organisationen haben mit komplexen Abläufen zu tun und unterliegen vielen Regularien. Um ihre Aufgaben erfüllen zu können, benötigen sie Berechtigungen zur Benutzung vorhandener Ressourcen, z.B. Dokumenten- und IT-Funktionen.

Um das Sicherheitsziel "Vertraulichkeit" zu erreichen, sind jedoch auch Beschränkungen erforderlich. Bestimmte Befugnisse sollen nur berechtigten Personen erteilt werden. Dokumente und Daten dürfen nur von autorisierten Benutzern eingesehen beziehungsweise verändert werden.

DocuWare bietet ein Rechtekonzept, das solche komplexe Szenarien abbilden kann. Für jeden Anwender lässt sich der Handlungsspielraum detailliert definieren.

5.1 Rechtesystem

Grundlegend für die Rechteverwaltung in DocuWare ist die Unterscheidung in funktionale Rechte und Archivrechte.



Mit der komplexen Rechtestruktur vom DocuWare-System lässt sich der Handlungsspielraum eines Benutzers präzise festlegen.

5.1.1 Funktionale Rechte

Funktionale Rechte sind Rechte auf bestimmte Programmfunktionalitäten. Dazu gehört beispielsweise das Recht, einen Stempel oder eine Konfiguration für Briefkörbe anzulegen. Nur wenn ein Benutzer über das funktionale Recht *Briefkörbe* verfügt, wird ihm das Modul *Briefkörbe* in der DocuWare Konfiguration angezeigt.

Die funktionalen Rechte werden in der DocuWare Konfiguration unter *Benutzerverwaltung* vergeben.

Funktionale Rechte in einer Organisation

- Auswahllisten bearbeiten
- Benutzersynchronisierung
- Benutzerverwaltung
- Verwendung von Listen, Ergebnislisten, Suchdialogen. Ablagemasken oder Ordnerstrukturen
- Konfiguration von: Archiven, Auswahllisten, Autoindex, Briefkörben, Connect to Mail, Connect to MFP, Connect to Outlook, Dokumentverarbeitungen, E-Mail-Benachrichtigungen, Feldmasken, Formularen, Intelligent Indexing, Löschregeln, Protokollierung, Request, Smart Connect, Synchronisation, Texterkennung, Transfer
- SQL-Befehle verwenden
- Stempel

5.1.2 Archivrechte

Archivrechte sind auf ein Archiv und die darin gespeicherten Dokumente bezogen, wie das Ablegen und Suchen eines Dokuments, die Änderungen von Indexeinträgen oder den Export von Dokumenten oder eines Archivs in das Dateiverzeichnis. Für verschiedene Archive können verschiedene Archivrechte vergeben werden.

Archivrechte sind in administrative, allgemeine und Overlay-Berechtigungen sowie in Feldrechte unterteilt.

- **Administrative Berechtigungen** sind zum Beispiel: Berechtigungen verwalten, Dialoge verwalten oder die Migration von Dokumenten im Archiv.
- Unter **Allgemeine Berechtigungen** fallen unter anderem Ablegen, Suchen und Dokument löschen.
- **Overlay-Berechtigungen** beziehen sich auf Stempel, Anmerkungen und grafische Elemente.
- Zu den **Feldrechten** gehören unter anderem das Suchrecht, das Recht, Feldinhalte zu ändern, und das Recht, Einträge zu verwenden, die nicht in einer Auswahlliste vorhanden sind. Feldrechte können Sie für alle Felder eines Archivs oder für einzelne Felder vergeben.

Die Archivrechte werden im Archivbereich der DocuWare Konfiguration zugewiesen.

5.1.3 Benutzer- und Administratorrechte

Einige Objekte wie Briefkörbe, Archive oder Formulare können Benutzern und Rollen als Administrator oder Benutzer zugeordnet werden. Mit dem Benutzerrecht lässt sich das Objekt verwenden, das Administratorrecht enthält das Recht, das Objekt beziehungsweise die zugehörige Konfiguration zu ändern.

Damit ein Benutzer für ein Objekt das Benutzer- und Administratorrecht zuweisen kann, muss diesem Benutzer zunächst das funktionale Recht für das Objekt zugewiesen sein, wie etwa die Verwaltung von Briefkörben. Dann wird das entsprechende Modul in der DocuWare Konfiguration angezeigt, sobald der Benutzer sich anmeldet.

Objekte mit Benutzer- sowie Administratorrechten:

- Archive
- Autoindex-Jobs
- Briefkörbe
- Dokumentverarbeitungs-Konfigurationen
- E-Mail-Benachrichtigungen
- Konfigurationen für E-Mails aus Outlook
- Konfigurationen für E-Mails allgemein
- Formulare
- Intelligent Indexing
- Löschregeln
- Mailverbindungen
- Multifunktionsgerät-Konfigurationen
- Requests
- Synchronisationen und Spiegelungen
- Smart Connect-Konfigurationen
- Texterkennungs-Konfigurationen
- Transfer-Jobs

5.2 Zuweisung der Rechte

Die im vorigen Kapitel beschriebenen Rechte lassen sich mit Profilen, Rollen und Gruppen bequem den Benutzern zuweisen - insbesondere in Unternehmen mit vielen Mitarbeitern.

Gruppen – als Zusammenfassung von Benutzern – und Rollen – als Zusammenfassung von Rechten – sind verschiedene Sichtweisen auf dieselbe Sache. Einmal sind die Mitarbeiter und entsprechend die Benutzer der Ausgangspunkt, das andere Mal die Arbeitsabläufe beziehungsweise die Funktionen im DocuWare-System.

5.2.1 Profile und Rollen

Über Profile und Rollen ist es möglich, anstelle von vielen Einzelrechten in "Containern" zusammengefasste Rechte zu vergeben. Die Vergabe von Rechten über Profile und Rollen hat zwei Vorteile:

Erstens können detailliert zusammengestellte Rechte auf Knopfdruck an beliebig viele Benutzer vergeben werden, ohne dass ein Administrator pro Benutzer die komplexe Rechtestruktur anpassen muss.

Zweitens können Zusammenstellungen von Rechten auch ohne Benutzer existieren. Falls ein Mitarbeiter die Firma verlässt, kann ein Nachfolger - ohne großen Aufwand - die gleichen Rechte zugewiesen bekommen, unabhängig davon wie detailliert die Rechtezuweisung im Einzelnen ist.

- **Profile**
  Rechte können zu funktionalen Profilen, Archivrechte zu Archivprofilen zusammengefasst werden. Sie lassen sich einzelnen Benutzern und Rollen zuteilen.
  Archivrechte werden in jedem Fall zu Profilen zusammengefasst. Es ist nicht möglich, Archivrechte direkt einzeln Benutzern zuzuweisen. Nur die Archivprofile können Benutzern bzw. Rollen zugewiesen werden.
  Genauso wie die funktionalen Rechte sind auch die Archivprofile additiv. Das heißt, werden einem Benutzer mehrere Archivprofile eines Archivs zugewiesen, erhält er alle Rechte, die in diesen Profilen enthalten sind. Weiterhin bedeutet dies, dass Rechte nicht eingeschränkt, sondern nur erweitert werden können. Dieses Verhalten wird im Kapitel Zusammenspiel der Rechte (auf Seite 15) näher erläutert.
- **Rollen**
  Mehrere Profile lassen sich zu einer Rolle zusammenfassen. Eine Rolle kann sowohl Profile mit funktionalen Rechten als auch Profile mit Archivrechten umfassen. Rollen können Gruppen und einzelnen Benutzern zugewiesen werden.

5.2.2 Vordefinierte Rollen und Profile

Bei der Installation eines DocuWare Systems werden vordefinierte Rollen mit vordefinierten Profilen angelegt. Dies ermöglicht einen schnellen Start mit DocuWare und bindet zudem die Verwaltungsaufgaben in das Berechtigungskonzept ein.

Die vordefinierten Rollen und Profile können verschiedenen Benutzern oder Benutzergruppen zugewiesen werden.

Systemadministrator

Der Systemadministrator verwaltet das System aus Sicht der generell benötigten Basiskomponenten und der Hardware. Der Systemadministrator kann so definiert werden, dass er keinen Zugriff auf einzelne Organisationsinformationen hat und insbesondere nicht in die detaillierte Benutzerverwaltung eingreifen kann. Allerdings kann nur er die Rolle „Systemadministrator" anderen Benutzern zuweisen. Dies ist nicht in der Benutzerverwaltung der Organisation, sondern nur im Systembereich der DocuWare Administration möglich.

Nach der Installation von DocuWare übernimmt er gleichzeitig die Rolle des Organisationsadministrators für alle Organisationen. Mit jeder neu erzeugten Organisation erhält der Systemadministrator zunächst auch die Rolle des Organisationsadministrators, die dann aber einer anderen Person zugewiesen werden kann.

Aufgaben eines Systemadministrators

- Bereitstellung und Wartung von Hardware, Betriebssystem und Datenbanken
- Installation der DocuWare-Server-Module
- Konfiguration systemweiter Einstellungen für Server, Verbindungen für Datenbanken und Dateiverzeichnisse, Speichersysteme und Benutzerverzeichnisse
- Einsicht in die Protokollierung auf Systemebene

Organisationsadministrator

Ein DocuWare System kann eine oder auch mehrere Organisationen mit jeweils eigenem Organisationsadministrator umfassen. Der Organisationsadministrator verwaltet insbesondere die Rechte, Benutzer und Benutzergruppen seiner Organisation. Die Rolle beinhaltet keine Zugriffsrechte auf Archive und deren Verwaltung.

Zur Übernahme dieser Rolle ist kein technisches Detailwissen der IT-Umgebung erforderlich. Der Organisationsadministrator kann die Rolle auch anderen Benutzern zuordnen oder entziehen. Insbesondere kann die Rolle auch einem Systemadministrator entzogen werden.

Aufgaben eines Organisationsadministrators

- Zuweisung der Lizenzen
- Anlegen von Benutzern und Gruppen,
- Konfiguration von Clients, Viewer und Briefkörben, Stempeln und Signaturen, Auswahllisten
- Einsicht in die Protokollierung auf Organisationsebene

Standard-Archivprofile

Der Zugriff auf die Archive und Dokumente wird über die Archivprofile geregelt. Nach der Installation von DocuWare sind vier Archivprofile vorderfiniert, die sich Benutzern und Gruppen zuweisen lassen.

- Besitzer
- Bearbeiten
- Lesen
- Löschen

Zusätzlich können Sie in den Archiveinstellungen eigene, benutzerdefinierte Profile erstellen.

Details zu den Berechtigungen der Archivprofile

5.2.3 Benutzer und Gruppen

Die einzelnen DocuWare-Benutzer können zu verschiedenen Gruppen zusammengefasst werden. Dabei ist es auch möglich, dass ein Benutzer Mitglied mehrerer Gruppen ist.

- **Benutzer**
  Für jeden Mitarbeiter, der DocuWare verwenden soll, wird mindestens ein Benutzer angelegt. Das Rechtespektrum erhalten Benutzer über die Zuweisung einzelner Rechte oder Rechtebündelungen in Form von Profilen und Rollen.
  Benutzer können Gruppen angehören.
- **Gruppen**
  Benutzer, die über die gleichen Funktionalitäten verfügen und die gleichen Archivrechte besitzen sollen, lassen sich zu Gruppen zusammenfassen. Entsprechende Rechte erhält der einzelne Benutzer über die Zugehörigkeit zu der Gruppe, der die entsprechende Rolle zugewiesen ist.

5.2.4 Ererbte und explizite Rechte

Bei der Zuweisung von Rechten zu Benutzern unterscheidet DocuWare zwischen ererbten und expliziten Rechten.

- **Ererbtes Recht**
  Rechte, die ein Benutzer über die Zugehörigkeit zu einer Gruppe oder über eine Rolle bzw. ein Profil erhalten hat, sind ererbte Rechte.
- **Explizites Recht**
  Rechte, die ein Benutzer direkt erhält und nicht über Rolle, Profil oder Gruppe, sind explizite Rechte. Es können nur funktionale Rechte als explizite Rechte vergeben werden.

Rechte sind immer additiv. Das heißt, die Summe der ererbten Rechte und der expliziten Rechte eines DocuWare-Benutzers bilden den Handlungsspielraum dieses Benutzers.

5.2.5 Zusammenspiel der Rechte und Berechtigungen

Ist ein Benutzer Mitglied mehrerer Gruppen, hat er alle Rechte, die über diese Gruppen und ihre Rollenzuteilung verfügbar sind.
Sind einem Benutzer mehrere Rollen oder Profile zugewiesen, hat der Benutzer alle Rechte zusammen, die über diese Rollen beziehungsweise Profile zugeteilt werden.

Beispiele:

- Ein Benutzer hat sein Rechtespektrum über eine Rolle erhalten. Weist man diesem Benutzer eine weitere Rolle mit weniger Rechten zu, ändert sich für den Benutzer nichts, da die Rechte additiv sind. Um ihm die Rechte einzuschränken, muss man ihm die ursprüngliche Rolle entziehen. Entsprechendes gilt auch für Gruppen.
- Ein Benutzer ist Mitglied zweier Gruppen und hat über die Rollen dieser Gruppen sein Rechtespektrum erhalten. Entzieht man ihm die Mitgliedschaft einer Gruppe, so verliert er nicht automatisch alle Rechte, die ihm über die Rollen dieser Gruppe zugewiesen sind, sondern nur diejenigen, die über die andere Gruppe nicht zugeteilt werden.

Die Möglichkeiten, die ein Benutzer in einem Archiv hat, resultieren aus den Archivrechten sowie dem Zugriff auf die Dialoge.

Beispiel:

- Das Menü einer Ergebnisliste enthält standardmäßig den Button *Als PDF mit Anmerkungen herunterladen*. Ein Benutzer hat nun Zugriff auf diese Ergebnisliste sowie das Archivrecht *Export*. Damit kann er diese Option verwenden. Ein anderer Benutzer hat ebenfalls Zugriff auf die Ergebnisliste, jedoch nicht das Export-Recht, weshalb der Button zum Herunterladen eines PDF mit Anmerkungen nicht verfügbar ist. Er kann also diese Funktion nicht nutzen.

Die Einstellungen zu den einzelnen Archivfeldern in den Dialogen und die zugewiesenen Archivrechte überschneiden sich in einigen Bereichen. So ist es möglich, ausgewiesenen Benutzern spezielle Rechte zur Verfügung zu stellen, während die Benutzerrechte generell über die Feldeinstellungen in den Dialogen gesteuert werden.

Beispiel:

- Ein Archivfeld im Ablagedialog ist als *Fester Wert* belegt. Ein Benutzer hat wiederum das allgemeine Archivrecht, Indexeinträge zu bearbeiten sowie das Feldrecht *Ändern*. Dieser Benutzer ist demnach berechtigt, den festen Feldeintrag direkt bei der Ablage oder auch im Nachhinein über *Indexeinträge ändern* zu editieren.

Die Archivrechte eines Benutzers haben also Vorrang gegenüber den Feldeinstellungen in den Dialogen.

5.2.6 Dokumentzugriffe über Indexdaten einschränken

Um innerhalb eines Archivs Rechte nach Indexeinträgen vergeben zu können, stehen zudem Indexwertprofile zur Verfügung. Die Limitierung der Dokumentenzugriffe über Indexdaten bietet sich insbesondere dann an, wenn Dokumente sensiblen Inhalts in einem Archiv zusammengefasst werden.

Beispiel:

- In einem Personalarchiv sind die Dokumente der Mitarbeiter gespeichert. Als Indexeintrag steht unter anderem der Mitarbeitername zur Verfügung. Mitarbeiter der Personalabteilung haben Zugriff auf alle Dokumente, während der einzelne Mitarbeiter nur auf die Dokumente Zugriff hat, die mit seinem Namen in den Indexdaten abgelegt sind.

5.3 DocuWare als Hochsicherheitssystem

Wenn ein DocuWare System auf die Stufe Hochsicherheitssystem gesetzt wird, kann der Organisationsadministrator die Eigenschaft „Hochsicherheit" bestimmten Benutzern und Archiven zuteilen. Nur ein Benutzer mit dieser Eigenschaft kann auf ein Hochsicherheits - Archiv zugreifen. Folgende Unterschiede gibt es zu einem System ohne die Eigenschaft „Hochsicherheit":

- Der Organisations-Administrator kann nicht für einen Hochsicherheits-Benutzer das Passwort zurücksetzen. Das kann nur der Hochsicherheits-Benutzer selbst.
- Für solche Benutzer ist es auch nicht möglich, sich über ein Trusted Login (auf Seite 7) anzumelden, da beim Trusted Login die Sicherheit nicht über DocuWare gewährleistet wird.
- Es ist nicht möglich für ein Hochsicherheits-Archiv die Archivprofile einer Rolle zuzuweisen. Diese Archivprofile müssen Benutzern direkt zugewiesen werden und diese Benutzer ebenfalls über die Eigenschaft „Hochsicherheit" verfügen. Somit ist ausgeschlossen, dass für besonders sensible Bereiche ein Zugriff ungewollt über Gruppen- und Rollenzuweisungen erfolgen kann.

5.4 Dokumente verschlüsseln

Um sicherzustellen, dass selbst Administratoren nicht unautorisiert sensible Dokumente lesen können, lassen sich in DocuWare Dokumente verschlüsselt speichern.

Mit dieser Option können Sie den Zugriff auf Dokumente auch im Dateisystem zuverlässig unterbinden.

Der Schlüssel ist standardmäßig 256 Bit lang. Zusätzlich stehen Schlüssellängen von 192 oder 128 Bit zur Verfügung. Je länger der Schlüssel, desto sicherer ist das Verfahren, aber desto mehr Zeit benötigen Ver- und Entschlüsselung und damit Ablage und Suche.

Es ist zu beachten, dass verschlüsselte Ablagen für autorisierte Nutzer nur bei Verfügbarkeit des entsprechenden Schlüssels nutzbar sind. Die Dokument-Schlüssel werden über ein asymmetrisches Verfahren mit einem in der Datenbank gespeicherten Schlüssel entschlüsselt. Da die Dokumente ohne den Schlüssel in der Datenbank nicht entschlüsselt werden können, muss bei verschlüsselter Ablage darauf geachtet werden, dass von den DocuWare-System-Tabellen ein regelmäßiges Backup erstellt wird, um bei Verlust der Datenbank insbesondere die Schlüssel-Tabellen wieder herstellen zu können.

Zusätzliche Hinweise:

- Volltext-Dateien können nicht durch DocuWare verschlüsselt werden. Die Indexdaten in der Datenbank sind ebenfalls nicht verschlüsselt. Enthalten diese Daten sensible Informationen, ist auf die Sicherungsmöglichkeiten des Datenbank-Anbieters zurückzugreifen - siehe dazu auch das folgende Kapitel.
- DWX-Dateien sind nicht verschlüsselt. In DWX-Dateien lassen sich Metadaten zum Dokument zusätzlich zu der Speicherung am Archiv-Speicherort sichern.

5.5 Sensible Daten außerhalb von DocuWare schützen

Bestimmte für DocuWare relevante Daten lassen sich nicht mit DocuWare-Sicherheitsmaßnahmen schützen. Dazu gehören die Indexdaten zu den Dokumenten und der extrahierte Volltext, die in den jeweiligen Datenbanken abgelegt werden. Jeder Systemadministrator mit ausreichenden Rechten kann diese Daten einsehen. Zudem ist der Volltext in einem separaten Index gespeichert. Dieser wird vom Volltext Server gesteuert, der auf der weit verbreiteten Volltextengine Apache SoLR basiert.

Wenn in diesen Daten sensible Informationen enthalten sind, muss der Zugriff zu den Datenbanken, zum Speicherort vom Volltextindex sowie der Zugang zum Volltext Server – die URL ist standardmäßig http://machinename:9012/solrt - vom Administrator mit den allgemein üblichen Maßnahmen geschützt werden, wie beispielsweise Access Control Lists für Dateiverzeichnisse oder Datenbanken sowie einer transparenten FileSystem-Verschlüsselung (EFS) für den Volltext-User.

6 Integrität von Daten und Dokumenten

Das Sicherheitsziel Integrität besagt, dass Daten und Dokumente nicht unautorisiert geändert werden dürfen. Alle Änderungen an einem Dokument müssen nachvollziehbar sein.

DocuWare gewährleistet die Integrität der archivierten Dokumente mit folgenden Maßnahmen:

- Es ist über das Berechtigungssystem möglich, Dokumente für Benutzer generell zu sperren, beziehungsweise nur für autorisierte Benutzer zugänglich zu machen. Auch können Sie den Zugriff auf Dokumente generell zulassen, aber einschränken, beispielsweise indem Sie Benutzern das Leserecht, aber nicht das Bearbeiten-Recht an Dokumenten zuteilen.
  Dies wurde bereits im Kapitel Vertraulichkeit > Rechtesystem (auf Seite 10) dargestellt.

- Mit der Archivfunktion *Automatisches Versionsmanagement (auf Seite 19)* lässt sich jederzeit nachvollziehen, ob ein Dokument geändert wurde.

- DocuWare kann alle benutzerbezogenen Vorgänge innerhalb eines DocuWares System transparent protokollieren (auf Seite 20).

6.1 Änderungen als neue Versionen speichern

Wenn für ein Archiv die Funktion *Neue Versionen automatisch erstellen* aktiviert ist, wird ein Dokument, sobald es geändert wird, als neue Version im gleichen Archiv gespeichert. Das heißt, jede Änderung führt automatisch zu einer neuen Dokumentversion.

Bei aktiviertem Versionsmanagement befinden sich in einem Archiv also neben der aktuellen auch ältere Versionen. Ältere Versionen können in der Versionshistorie betrachtet werden. Angezeigt werden unter anderem die Versionsnummern, Status, Speicherdatum, Kommentare sowie der Nutzer, der das Dokument gespeichert hat.

Das in Bearbeitung befindliche Dokument wird aus DocuWare ausgecheckt und gesperrt. Andere Benutzer können das Dokument zwar ansehen, aber nicht selber bearbeiten, bis das Dokument als neue Version wieder eingecheckt ist. Es kann jeweils nur die aktuelle Version bearbeitet werden.

Es ist auch möglich, das Versionsmanagement so einzurichten, dass einzelne Dokumente manuell ausgecheckt und als neue Version gespeichert werden. Dann ist natürlich nicht die Integrität für alle Dokumente eines Archivs gewährleistet.

Mehr Informationen zum Thema Versionsmanagement

6.2 Protokollierung von Benutzer-Ereignissen

DocuWare verfügt über eine transparente Protokollierung aller Benutzer-Ereignisse in einem DocuWare-System. Mit dem entsprechenden Funktionsrecht sehen Sie auf Dokument-, Archiv-, Organisations- oder Systemebene, wer wann welche Einstellungen geändert oder Dokumente abgelegt hat.

Alle Protokollierungen können Sie in der DocuWare Konfiguration im universellen CSV-Format herunterladen und für Auswertungen in vielen Programmen verwenden.

Beispiele für Ereignisse, die auf den einzelnen Ebenen protokolliert werden, jeweils mit Datum, Zeit und Benutzer:

Dokument: Ablage, Indexänderung mit altem und neuem Wert, Anzeige, Druck, Anfügen von Anmerkungen etc

Archiv: Neue Indexfelder, Änderungen bei Such- und Ablagedialogen sowie Ergebnislisten, neue Archivprofile etc. Zudem alle Dokumentereignisse innerhalb des Archivs.

Organisation: Neue Konfigurationen sowie alle Änderungen an Bestehenden, An-und Abmeldung der Benutzer

System: Änderungen an Server-Einstellungen, Änderung an Zeitplänen für automatische Prozesse wie Transfer, Löschregeln, Synchronisation

7 Verfügbarkeit des DocuWare-Systems

Um die Geschäftskontinuität zu gewährleisten, sollen ein DocuWare-System und seine Services durchgängig betriebsbereit sein. Benutzer können jederzeit auf Dokumente, Daten und Anwendung zugreifen.

Da ein Dokumentenmanagement-System meist in eine heterogene IT-Infrastruktur eingebettet ist, kann es aus Gründen, die zunächst nichts mit dem DMS zu tun haben, dennoch zu einem Ausfall kommen - beispielsweise durch einen Hardwarecrash oder durch eine Infizierung von Client-Rechnern im Unternehmen mit Schadsoftware. Beidem kann DocuWare durch seine spezielle Architekur vorbeugen:

- **Skalierbarkeit:** Server und andere Komponenten können mehrfach installiert werden, so dass redundante Komponenten die im Falle eines Hardwarecrashs ausgefallenen Funktionen nahtlos übernehmen können.

- **DocuWare als Hybrid-System:** Neben Ihrem On-Premises-System kann DocuWare Cloud als redundantes Backupsystem dienen und die Geschäftskontuinität auch im Falle eines Crashs nahezu ohne Ausfallzeit sicherstellen.

  Um nahtlos auf das redundante System wechseln zu können, müssen die Dokumente und Indexdaten regelmäßig mit dem Modul Synchronisation gespiegelt werden. Dabei werden alle neuen und geänderten Dokumente in das Ziel übertragen, auch können in der Quelle gelöschte Dokumente im Ziel entfernt werden.

  Von einer Spiegelung ausgenommen sind die Dokumentversionen, Workflow-Historie und Protokollierungsdateien.

  Der Spiegelungsprozess erfolgt über sicheres HTTPS.

- **Schutz vor Schadsoftware:** Kryptoviren beispielsweise verschlüsseln Dateien in einem Dateisystem, so dass sie danach nicht mehr verwendet werden können. Wenn ein Benutzer mit seinem infizierten Rechner auf einen synchronisierten Cloud-Speicher wie DropBox oder Onedrive oder auf einen Filesharing-Server zugreift, besteht die Gefahr, dass der Virus den kompletten Inhalt des Cloud-Speichers verschlüsselt.

  Bei in DocuWare archivierten Dokumenten kann dies nicht passieren. Die Dateien auf dem Dateispeicher werden ausschließlich von DocuWare-Server-Komponenten gelesen und geschrieben. Nur das Konto für die DocuWare-Dienste benötigt Schreibzugriff. Da also keine bidirektionale Synchronisation mit dem Dateisystem stattfindet, kann ein Kryptovirus auf einem Client-Rechner keinen Schaden in dem verwendeten DocuWare-System anrichten.

8 Datensicherung

Für die Daten und Dokumente im DocuWare-System sollten Sicherungsläufe etabliert sein, damit sich die Daten im Falle eines Hardwarecrashs unverzüglich wieder einspielen lassen.

Die Sicherung der DocuWare-Datenbanken und -Speichorte ist in der Verwantwortung der Unternehmens-IT. Es gibt keinen DocuWare-Mechnismus, der die Datenbanken und Speicherorte automatisch sichert.

8.1 Komponenten für externes Backup

Folgende DocuWare-Komponenten müssen für ein Backup extern gesichert werden, damit Sie im Falle eines Hardwarecrashs wieder zur Verfügung stehen:

Datenbanken

- DWSYSTEM: system- und organisationsrelevante Daten

- DWDATA: systeminterne Informationen für das Suchen und Finden von Dokumenten

- DWNOTIFICATION: E-Mail-Benachrichtigungen

Weitere Informationen zu den Datenbanken im White Paper Systemarchitektur

Speicherort-Inhalte

Ein Speicherort ist ein Dateiverzeichnis im Netzwerk oder in einem Content Addressed Storage, in dem Dokumente und Dateien aus Archiven und Briefkörben gespeichert werden.

Volltext-Katalogdateien

Der Volltextserver speichert die Textshots in Katalogdateien und nutzt sie für die Suchanfragen. Sie sind standardmäßig auf dem Rechner gespeichert, auf dem auch der Volltext Server installiert ist. Diese Katalogdateien können ebenfalls im Rahmen eines Backups gesichert werden und lassen sich ohne großen Aufwand wieder herstellen.

8.2 Backup von Dokument-Metadaten

Die kompletten Metadaten der Dokumente wie Indexdaten, Anmerkungen, Stempel und Signaturen werden automatisch in der Datenbank gespeichert und können nach einem Hardwareschaden über ein externes Datenbankbackup wiederhergestellt werden.

Zusätzlich besteht die Möglichkeit, die Metadaten im ZIP-basierten Format DWX im Speicherort des Archivs zu sichern. Dazu aktivieren Sie in den Archiveinstellungen unter *Allgemein > Informationen für Administratoren* die Option *Indexdaten-Backup im Speicherort.* Mit der Konsolenapplikation *Indexdaten wiederherstellen* lassen sich diese redundant gespeicherten Metadaten wieder einspielen.