Institut für Softwaretechnologie

Universität Stuttgart
Universitätsstraße 38
D–70569 Stuttgart

Prozessanalyse Nr. 7

Benutzer- und Rechteverwaltung eines Beratungsunternehmens

Marcel Lehwald, Michael Steffl, Niklas Schnabel

Studiengang:	Softwaretechnik
Prüfer/in:	Prof. Dr. rer. nat. Stefan Wagner
Betreuer/in:	Dipl.-Inf. Ivan Bogicevic
Beginn am:	1. Mai 2014
Beendet am:	31. Oktober 2014
CR-Nummer:	K.6.4, K.6.5

Kurzfassung

Im Rahmen dieser Arbeit wurde das Konzept einer einheitlichen Benutzerverwaltung in einem Unternehmensumfeld ausgearbeitet, welches aus verschiedenen unabhängigen Systemen besteht. Dazu wurden drei Lösungsansätze ermittelt und evaluiert. Als beste Lösung im Bezug auf das beteiligte Unternehmen hat sich ein Server mit einer zentralen Benutzerverwaltung durch LDAP (Lightweight Directory Access Protocol) ergeben. Das Konzept beinhaltet die dokumentierten und angepassten Unternehmensprozesse, die für diese Arbeit relevant sind, ein ausgearbeitetes Konzept für eine einheitliche Benutzer- und Rechtegruppenstruktur und Lösungsvorschläge im Bezug auf die Informationssicherheit.

Abstract

In this paper we evaluate the solution for a unified user administration approach in a company environment consisting of multiple independent systems. As possible solutions we identified three different approaches. After an evaluation of the different possibilities we chose the solution with a centralized LDAP (Lightweight Directory Access Protocol) server. The elaborated approach contains the documented business processes that are relevant for user administration, a concept for a unified user and rights structure and solutions for better information security.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. Einleitung

1.1. Das Unternehmen

Das beteiligte Unternehmen wird im Rahmen dieser Arbeit namentlich nicht genannt. Es handelt sich dabei um ein international tätiges Software- und Beratungsunternehmen. Der Aufgabenbereich umfasst unter anderem die Analyse von Geschäftsprozessen, der Entwurf und die Realisierung von Lösungen in Projekten, sowie das strategische Management, die Optimierung und Modernisierung von bereits vorhandenen Softwaresystemen.

1.2. Problemstellung

Zur Abwicklung der Projekte, internen Prozesse und Kommunikation betreibt das Unternehmen eine Reihe von Softwaresystemen. So wird unter anderem ein ERP-System, SVN-Repository, Wiki und Online-Kalender im täglichen Prozessablauf eingesetzt. Der Zugriff hierauf erfolgt sowohl im internen Netz als auch durch VPN über das Internet. Einige Systeme werden dabei durch das Unternehmen auf internen Servern betrieben und einige Systeme auf externen Servern. Jedes der eingesetzten Systeme besitzt dabei eine eigene Benutzerverwaltung und gegebenenfalls eine eigene Rechtestruktur, welche unabhängig voneinander verwaltet werden müssen. Diese getrennte Verwaltung führt dabei zu ineffizienten Prozessabläufen.

1.3. Zielsetzung

Im Rahmen der Prozessanalyse sollen durch das Konzept einer zentralen Benutzer- und Rechteverwaltung effizientere Prozessabläufe gestaltet werden. Das Konzept soll dabei die vorhandenen Benutzer- und Rechteverwaltungen der einzelnen Systeme berücksichtigen. Außerdem muss einerseits die Informationssicherheit berücksichtigt werden, andererseits soll das Konzept eine effiziente und reibungslose Nutzung ermöglichen und flexible Reaktionen auf ein dynamisches Umfeld erlauben. Im Rahmen des Konzepts sollen dabei auch mögliche Potenziale zur Verbesserung der Informationssicherheit identifiziert werden.

Für die Umsetzung müssen die vorhandenen unterschiedlichen Benutzergruppen, ihre typischen Aktivitäten und Zugriffsmuster und die hierfür nötigen Systemberechtigungen erfasst und dokumentiert werden. Des weiteren müssen die Prozesse, welche hauptsächlich zu Veränderungen in den Benutzergruppen und Rechten führen ermittelt werden.

Gliederung

Im Folgenden wird eine Übersicht über den weiteren Aufbau der Arbeit aufgezeigt. In Kapitel 2 wird dabei zunächst der aktuelle Ist-Zustand bei dem Unternehmen analysiert und dokumentiert. In Kapitel 3 werden dann einige mögliche Lösungsansätze dargestellt und evaluiert. Schließlich wird die dabei ermittelte beste Lösung in Kapitel 4 genauer beschrieben und in Kapitel 5 werden dann abschließend die Ergebnisse zusammengefasst.

2. Analyse

In diesem Kapitel wird zunächst der Ist-Zustand des Unternehmens dargestellt. Dazu werden zu Beginn die einzelnen Systeme in einer Systemübersicht beschrieben und auf die Benutzergruppen der Systeme eingegangen, welche bei einer zentralen Benutzer- und Rechteverwaltung betrachtet werden müssen. Anschließend werden die relevanten Geschäftsprozesse dargestellt, die bei dem Unternehmen im Zusammenhang mit der Benutzer- und Rechteverwaltung stehen. Zum Schluss werden noch einige Probleme beschrieben, die im Bezug auf die Informationssicherheit des aktuellen Zustands stehen.

2.1. Systemübersicht

Das Unternehmen setzt eine Vielzahl von verschiedenen Systemen für verschiedenste Aufgaben ein. Abbildung 2.1 zeigt die Systeme und in welcher Umgebung diese eingesetzt werden. FTP, Subversion, OpenVPN und ein Samba-Server werden auf einem unternehmensinternen Server innerhalb des Unternehmensnetzwerks betrieben. E-Mail, OpenERP, StatusNet und MediaWiki werden über die Server des externen Anbieters der Strato AG betrieben. Alle extern gehosteten Systeme sind von überall über das Internet abrufbar. Die im Unternehmensnetzwerk betriebenen Systeme sind auch nur über das interne Netzwerk oder über eine VPN-Verbindung erreichbar. Eine Ausnahme stellt der FTP-Server dar, welcher auch frei über das Internet erreichbar ist. Im Folgenden werden die einzelnen Systeme genauer vorgestellt.

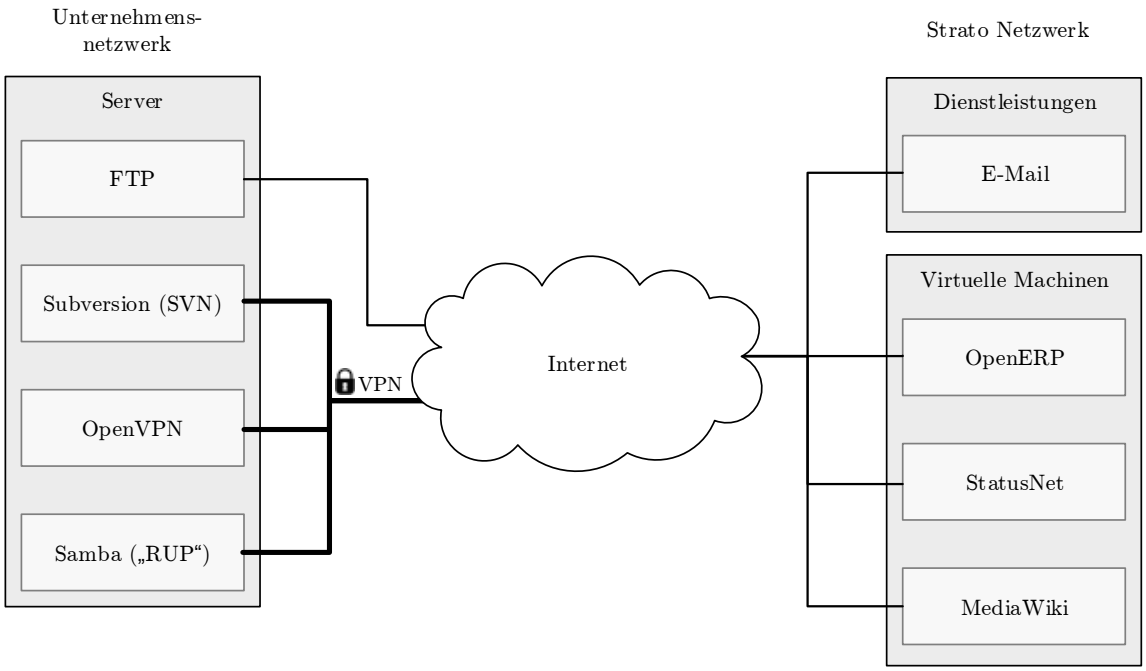

Abbildung 2.1.: Systemübersicht

E-Mail

Zum Anbieten von E-Mail Adressen für alle Mitarbeiter wird der externe Dienstleister der Strato AG verwendet [Str14]. Die E-Mail Adressen sind so an die Domain des Unternehmens gebunden. Es ist dabei nur möglich einzelne Benutzer und Postfächer über ein Webinterface zu verwalten. Der direkte Zugriff auf die Server und die Benutzerverwaltung ist nicht möglich, da der Dienst direkt von der Strato AG verwaltet wird. Ein Zugriff auf die E-Mails kann entweder über ein Webinterface, IMAP oder POP3 erfolgen.

FTP

Für den Austausch von Dateien stehen bei dem Unternehmen zwei FTP Server zur Verfügung. Ein FTP Server wird auf einem internen Server im Unternehmen direkt verwaltet. Der Zweite extern bei der Strato AG. So können unter anderem projektspezifische Daten zwischen dem Unternehmen und dem Kunden ausgetauscht werden.

OpenERP

OpenERP ist ein Enterprise-Resource-Planning-System (ERP-System). Es wird in Unternehmen eingesetzt um dort die vorhandenen Ressourcen wie unter anderem Kapital und Personal zu verwalten.

Durch individuell einbindbare Module kann OpenERP an die jeweiligen Bedürfnisse eines Unternehmens angepasst werden. Im Mai 2014 wurde eine Umbenennung von OpenERP zu Odoo vorgenommen, da das System zukünftig nicht nur klassische ERP-Aufgaben übernehmen soll [Odo14].

Bei dem Unternehmen wird das System hauptsächlich zur Erfassung und Planung der Projektabwicklung und des Personals eingesetzt. Auch die Zuordnung der Mitarbeiter zu den einzelnen Projekten wird dort abgebildet. Jeder Mitarbeiter benötigt einen Zugriff auf OpenERP, um dort unter anderem Arbeitszeiten und Ausgaben für einzelne Projekte einzutragen. Dabei ist das System auch extern erreichbar, um reisenden oder externen Mitarbeitern den Zugriff zu ermöglichen. Das OpenERP System stellt eine zentrale Rolle in der Verwaltung dar und ist im täglichen Prozessablauf bei dem Unternehmen tief verankert. Die Gruppenstruktur des OpenERP Systems muss daher auch zukünftig erhalten bleiben.

Subversion

Für die Verwaltung von Dateien wird bei dem Unternehmen Subversion verwendet. Das von der Apache Software Foundation entwickelte Open Source Projekt stellt dabei ein zentrales Werkzeug für die IT-Mitarbeiter dar. So wird dort die Software für die einzelnen Projekte verwaltet. Die Zugriffsverwaltung auf die einzelnen Projekte stellt dabei die in OpenERP abgebildete Zuordnung der Mitarbeiter zu den einzelnen Projekten dar. Diese Zuordnung wird jedoch manuell hergestellt. Die Rechteverwaltung in Subversion ist von zentraler Wichtigkeit für das Unternehmen und muss auch zukünftig erhalten bleiben.

MediaWiki

Für den internen Informationsaustausch wird unter anderem MediaWiki eingesetzt. MediaWiki ermöglicht es Inhalte in Form eines Wiki-Systems zu verwalten. Die Software ist als Open Source Projekt frei verfügbar. Das Wiki-System ist weit verbreitet und wird so unter anderem auch bei der Online-Enzyklopädie Wikipedia verwendet.

Bei dem Unternehmen wird das Wiki-System zum unternehmensweiten und projektspezifischen Informationsaustausch eingesetzt. Beim Eintritt in das Unternehmen erhält jeder Mitarbeiter ein MediaWiki-Konto mit Lese- und Schreibrechten. So können verschiedenste unternehmensinterne Informationen auf leichtem Wege festgehalten werden. Das MediaWiki selbst enthält keine Benutztergruppenstruktur und ermöglicht lediglich den Zugriff auf das gesamte Wiki oder keinen Zugriff.

OpenVPN

Durch OpenVPN kann eine verschlüsselte Verbindung zu dem unternehmensinternen Netzwerk aufgebaut werden [OT14]. Jeder Mitarbeiter hat dadurch die Möglichkeit auch von extern auf intern beschränkte Dienste wie zum Beispiel Subversion zuzugreifen. Der OpenVPN-Server läuft dabei auf einem der unternehmensinternen Server. Die Authentifizierung gegenüber dem Server wird alleinig über ein Zertifikat sichergestellt, welches nach einem Jahr abläuft. Zugang über den VPN-Server

erhalten nur fest angestellt Mitarbeiter und in Ausnahmefällen auch externe Partner. Studentische Mitarbeiter und Praktikanten erhalten jedoch keinen Zugang.

Samba

Um verschiedenste Daten innerhalb des Unternehmens für jeden verfügbar zu machen, existiert ein interner Linux Server der freien Software *Samba*. Samba ermöglicht es unter Nicht-Microsoft-Betriebssystemen, Windowsfunktionen wie den hier verwendeten Dateidienst bereit zu stellen.

StatusNet

StatusNet ist eine Open Source Kommunikationssoftware, welche in der Funktionalität mit Twitter vergleichbar ist. So lassen sich Kurznachrichten an alle Benutzer veröffentlichen.

Innerhalb des Unternehmens bietet der Dienst den Miterbeitern einen einfachen Weg sich den anderen Mitarbeitern mitzuteilen. Der Dienst besitzt einen untergeordneten Status gegenüber den anderen Diensten. StatusNet besitzt auch keine komplexe Benutzerverwaltung. Lediglich ein Benutzerkonto muss angelegt werden, um Zugriff auf den Dienst zu erhalten.

2.2. Benutzergruppen

Jedes der in Abschnitt 2.1 vorgestellten Systeme besitzt eine eigene Benutzerverwaltung und gegebenenfalls eine eigene Rechteverwaltung. Ein Teil dieser Benutzerverwaltungen setzt wiederum auf eine Kombination aus Benutzern und Benutzergruppen. Die komplexesten Benutzerstrukturen beinhalten dabei die Systeme OpenERP und Subversion. Die anderen Systeme besitzen nur eine einfache Benutzerkontenverwaltung, ohne eine tiefgreifende Gruppen-und Rechteverwaltung. Da OpenERP und Subversion die wichtigsten Systeme für das Unternehmen darstellen, werden beide Systeme im Folgenden genauer im Bezug auf die Benutzer-und-Rechteverwaltung betrachtet.

2.2.1. Subversion

Die Verwaltung der Rechte innerhalb von Subversion ermöglicht es den Zugriff auf bestimmte Repositories, Ordner oder Projekte einzuschränken. Dazu lassen sich Benutzer erstellen, die sich bestimmten Benutzergruppen zuordnen lassen. Benutzern und Gruppen können dabei Lese- und/oder Schreibrechte für ein gesamtes, oder ein Teil eines Repositories zugeteilt werden.

Beim Unternehmen reflektieren die Gruppen in Subversion zum Großteil die einzelne Abteilungen oder andere zusammengehörige Gruppen innerhalb der Unternehmensstruktur. So existieren unter anderem Gruppen für die Buchhaltung, Marketing, Softwareingenieure oder Studenten. Gruppen können dabei wiederum Teil einer anderen Gruppe sein. So sind z.B. die meisten Gruppen auch Teil der Gruppe Mitarbeiter. Die Tabelle 2.1 stellt die gesamte Struktur der Gruppen und deren Zusammenhänge innerhalb des Subversion Systems dar.

Gruppe	Beinhaltete Gruppen	Beschreibung
Gf	-	Geschäftsführung
itadmin	Gf	IT Administration
bu	Gf	Business Unit
topic	Gf	Topic Leader
administrators	Gf	Administratoren
swengineers	Gf	Softwareingenieure
hr	Gf	Human Resources
marketing	Gf, hr, backoffice	Marketing
buchhaltung	-	Buchhaltung
sales	-	
backoffice	-	
mitarbeiter	Gf, swengineers, hr, marketing, buchhaltung, sales, backoffice	Mitarbeiter
account	-	Kontoverwaltung
dsb	-	Datenschutzbeauftragte
fo	-	Function Owners
students	-	Studenten
hob	-	Head of Branch
hot	-	Head of Team

Tabelle 2.1.: Ist-Zustand der Gruppenstruktur in Subversion

2.2.2. OpenERP

Innerhalb des OpenERP Systems gibt es verschiedene Kategorien die jeweils über die Menüführung des Systems erreichbar sind. Bei den Kategorien handelt es sich beispielsweise um „Accounting and Financing“ (Buchhaltung), „Human Ressources“ (Personalwesen) oder „Project Management“ (Projektmanagement). Zusätzlich lassen sich Rechtegruppen erstellen, zu denen sich die einzelnen im OpenERP System angelegten Benutzer hinzufügen lassen. Wird eine Gruppe einer Kategorie zugewiesen, so haben alle Benutzer dieser Gruppe die Möglichkeit, die zugeordnete Kategorie mit den entsprechenden Funktionen aufzurufen. In Tabelle 2.2 ist die Struktur des Unternehmens in Form einer Matrix zu sehen. Hierbei stellen die Reihen die einzelnen Kategorien und die Spalten die Rechtegruppen dar. Ein „x“ bedeutet, dass die Gruppe der entsprechenden Kategorie zugeordnet ist. So ist zum Beispiel die Gruppe „HR Manager“ der Kategorie „Human Ressources“ zugeordnet. Somit sind alle Benutzer der Gruppe „HR Manager“ dazu berechtigt, die Funktionen dieser Kategorie auszuführen.

		Gruppe																					
		Manager	Invoicing & Payments	Accountant	User	HR Manager	HR Officer	Employee	Configuration	Access Rights	Supplier Staff	User - One Leads Only	User - All Leads	Admin	Access	Technical Features	Analytical Accounting	Multi Companies	Product Variant	Product UoS View	Extended View	Survey / User	Partner Manager
Kategorie	Purchase Management	X			X																		
	Warehouse Management	X			X																		
	Commision Management	X																					
	Inventory Management	X			X																		
	Project Management	X			X									X									
	Sales Management	X										X	X										
	Accounting & Finance	X	X	X																			
	Humand Resources					X	X	X															
	Administration								X	X													
	Extra Tools	X			X																		
	Usability															X	X	X	X	X			
	Temp														X								

Tabelle 2.2.: Ist-Zustand der Gruppenstruktur in Open-ERP

2.3. Relevante Prozesse

Im Folgenden werden die relevanten Unternehmensprozesse beschrieben. Dabei werden nur die Prozesse betrachtet, welche Veränderungen in der Benutzer-und-Rechteverwaltung bewirken. Dies betrifft unter anderem Prozesse in denen Benutzer oder Rechte angelegt, gelöscht oder verändert werden. Es werden dabei teilweise nur Ausschnitte aus dem gesamten Prozessablauf abgebildet. Alle Prozesse sind nochmals in vollständiger Ausführung als Anhang A angehängt.

2.3.1. Mitarbeiter Eintritt in das Unternehmen

Tritt ein neuer Mitarbeiter in das Unternehmen ein, so gibt es eine Reihe von Aufgaben die realisiert werden müssen um dem neuen Mitarbeiter das Arbeiten zu ermöglichen. Neben Einführungsgesprächen und Schulungen gilt es vor allem Zugänge zu den Systemen des Unternehmens einzurichten.

Innerhalb der einzelnen Systeme müssen zwei Wochen vor Arbeitsbeginn des neuen Benutzers Benutzerkonten angelegt und die für den neuen Benutzer passenden Rechte vergeben werden. Die Accounts für E-Mail, MediaWiki und StatusNet werden vom Backoffice eingerichtet. Die IT muss zusätzlich einen SVN und OpenERP Account anlegen, einen Zugang zu RUP (Samba-Server) einrichten und ein personenbezogenes VPN Zertifikat für den OpenVPN-Client erstellen.

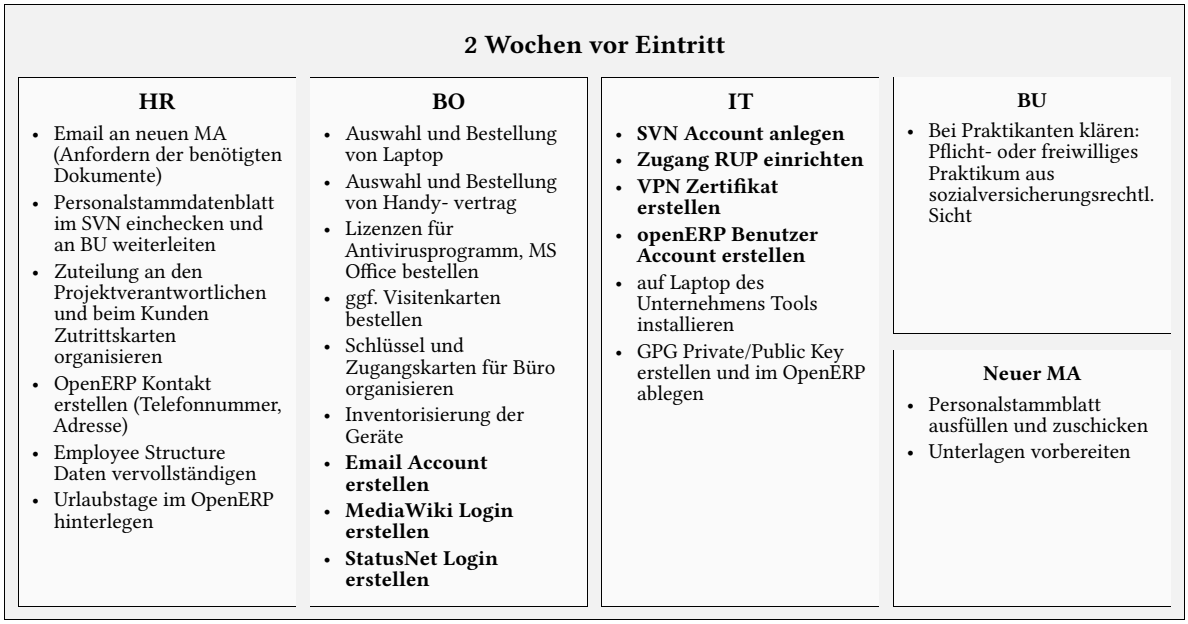

Abbildung 2.2.: Unternehmensprozess: Mitarbeiter tritt in das Unternehmen ein

In Abbildung 2.2 ist ein Ausschnitt des Prozesses für den Mitarbeiter Eintritt dargestellt. Die relevanten Punkte im Bezug auf Veränderungen von Benutzerkonten sind dabei hervorgehoben. Der komplette Prozess ist im Anhang zu sehen.

2.3.2. Mitarbeiter Austritt aus dem Unternehmen

Dieser Prozess befasst sich mit den einzelnen Schritten die erledigt werden müssen, wenn ein Mitarbeiter das Unternehmen verlässt. Hier gilt es vor allem sicherzustellen, dass dem Mitarbeiter an seinem letzten Arbeitstag sämtliche Rechte entzogen werden, sodass keinerlei Zugriffe mehr auf die Systeme des Unternehmens erfolgen können. Hierzu werden vom Backoffice am letzten Arbeitstag des verlassenden Mitarbeiters das MediaWiki und StatusNet Benutzerkonto gelöscht und das E-Mail Konto auf inaktiv gesetzt. Am selben Tag wird von der IT jeglicher SVN, RUP (Samba) und Unix Zugang entfernt. Des Weiteren wird das OpenERP Konto gesperrt und das OpenVPN Zertifikat zurück verlangt.

Abbildung 2.3 zeigt einen Ausschnitt des Prozesses für den Mitarbeiter Austritt, bei welchem die für diese Prozessanalyse relevanten Punkte hervorgehoben werden. Der komplette Prozess ist im Anhang zu sehen.

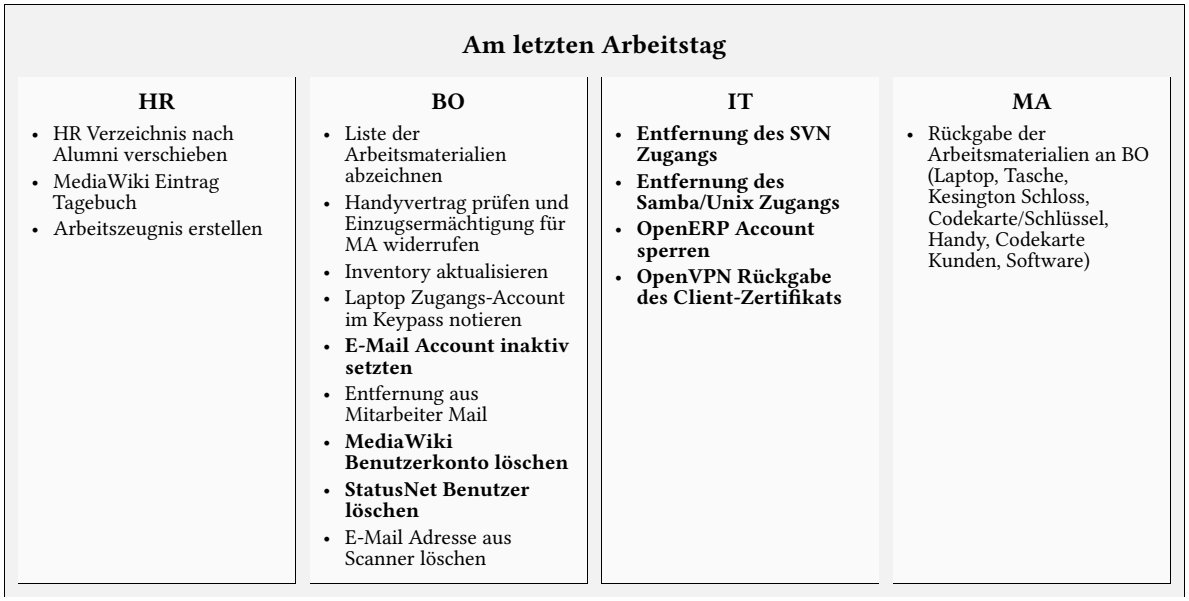

Abbildung 2.3.: Unternehmensprozess: Mitarbeiter verlässt das Unternehmen

2.3.3. Mitarbeiter Eintritt in ein Projekt

In Abbildung 2.4 werden die Schritte dargestellt, die durchgeführt werden müssen, um einen neuen Mitarbeiter zu einem schon existierenden Projekt hinzuzufügen. Dem neuen Projektmitarbeiter müssen zum einen Schreib- und Leserechte für das SVN-Repository gegeben werden und zum anderen muss der neue Projektmitarbeiter im OpenERP dem Projekt zugewiesen werden, damit dieser beispielsweise seine für das Projekt aufgewendete Zeit buchen kann.

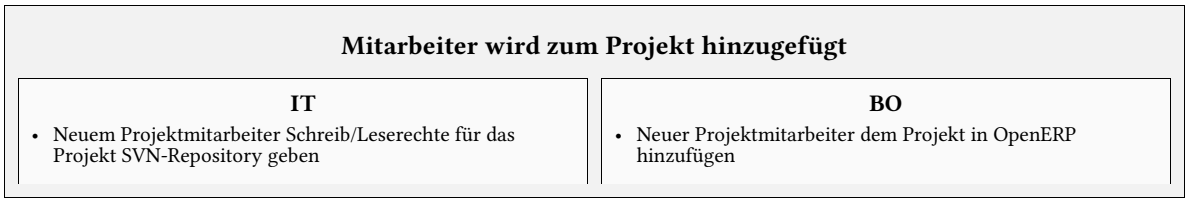

Abbildung 2.4.: Unternehmensprozess: Mitarbeiter wird zu einem Projekt hinzugefügt

2.3.4. Mitarbeiter Ausscheiden aus einem Projekt

Die durchzuführenden Schritte die nach dem Ausscheiden eines Mitarbeiters aus einem Projekt durchgeführt werden müssen, sind in Abbildung 2.5 zu sehen. Zuerst muss dem Mitarbeiter der Schreibzugriff entzogen werden, um weitere Änderungen am Projekt zu verhindern. Der Lesezugriff kann erhalten bleiben, damit ein Mitarbeiter weiterhin auf den Code für eventuell schon gelöste Probleme zugreifen kann. Weiterhin muss der Mitarbeiter aus dem Projekt in OpenERP entfernt werden.

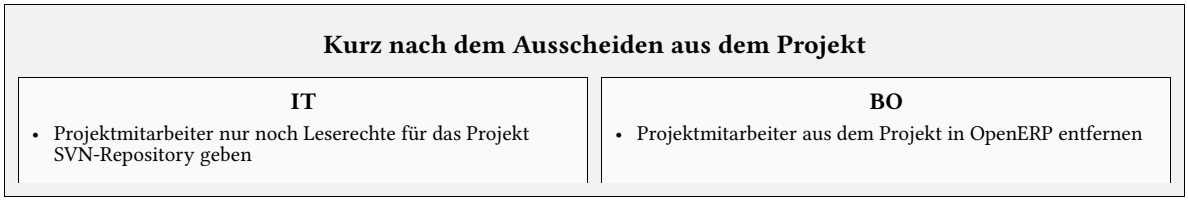

Abbildung 2.5.: Unternehmensprozess: Mitarbeiter scheidet aus einem Projekt aus

2.3.5. Projektbegin

Kurz bevor ein neues Projekt startet, müssen die in Abbildung 2.6 zu sehenden Aktionen ausgeführt werden. Da von der Geschäftsführung die Verwaltung des SVN gehandhabt wird, muss diese ein neues SVN-Repository anlegen und den beteiligten Mitarbeitern entsprechende Schreib- und Leserechte erteilen. Um das neue Projekt verwalten zu können, muss dieses im OpenERP eingetragen werden. Diese kann entweder vom Backoffice (BO) oder auch direkt vom Projektleiter vorgenommen werden. Anschließend müssen die einzelnen Projektmitarbeiter dem neu angelegten OpenERP-Projekt hinzugefügt werden, damit diese zum Beispiel ihre Zeiten buchen können. Zum Schluss sollte das Projekt zugunsten einer guten Dokumentation im Wiki eingetragen werden.

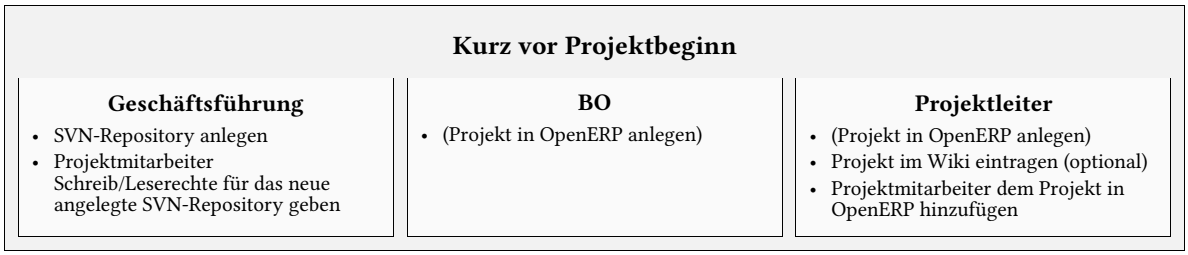

Abbildung 2.6.: Unternehmensprozess: Projekt beginnt

2.3.6. Projektende

Kurz nach dem das Projekt offiziell abgeschlossen wurde, müssen die in Abbildung 2.7 zu sehenden Aktionen durchgeführt werden. Die Geschäftsführung sollte den einzelnen Projektmitarbeitern nur noch lesenden Zugriff auf das SVN-Repository geben. Hierdurch können die Mitarbeiten weiterhin den Quellcode anschauen, um zum Beispiel auf zuvor gelöste Probleme zugreifen zu können, können allerdings nicht durch ein Versehen Änderungen an dem Projekt durchführen. Das Backoffice (BO) muss das Projekt im OpenERP schließen, um auch hier ungewollte Änderungen zu verhindern und um das Projekt als vollendet zu markieren. Zu guter Letzt muss die IT alle für Kunden angelegte Benutzerkonten (wie zum Beispiel für FTP) deaktivieren, beziehungsweise entfernen.

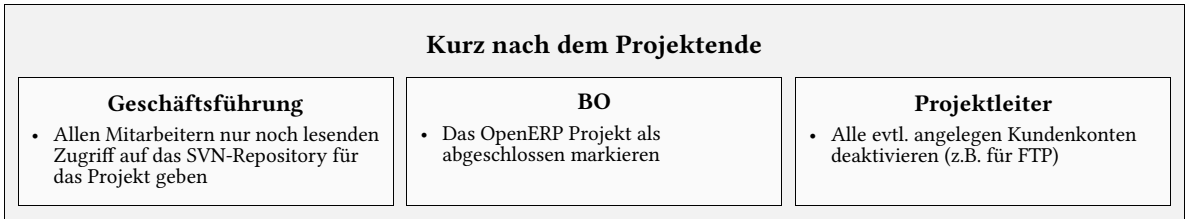

Abbildung 2.7.: Unternehmensprozess: Projekt endet

2.4. Informationssicherheit

Bei der Analyse der Systeme und der verschiedenen Prozesse wurden Probleme im Bezug auf die Informationssicherheit festgestellt. Die Beschreibung dieser Probleme werden im Folgenden Abschnitt aufgeführt. Die entsprechende Lösungsvorschläge folgen dann im Rahmen der Realisierung in Kapitel 4. Besonders bei den Daten innerhalb des OpenERP Systems bedarf es großer Aufmerksamkeit. Das Systeme beinhalten personenbezogene Daten der Mitarbeiter und unter Umständen sensible Projektdaten der Kunden.

2.4.1. Externer Zugriff auf die Systeme

Neben den Systemen, die sich im internen Netz befinden, gibt es eine Reihe von Systemen die sich auf einem externen Server befinden. Im Gegensatz zu den intern gehosteten Systemen, die nur über das Firmennetz oder durch eine gesicherte VPN Verbindung zu erreichen sind, kann man die Systeme bei Strato über das Internet von jedem beliebigen Rechner aus erreichen. Durch Aufrufen der entsprechenden URL im Browser, gelangt man beispielsweise zu der Seite, die als Anmeldemaske des OpenERP Systems dient. Da sich im ERP-System meist sensible Firmeninformationen wie Kundendaten oder ähnliches befinden, stellt dies eine reizvolle Angriffsmöglichkeit für Hacker oder andere an den Daten interessierten Personen dar. Hacker haben so die Möglichkeit, sich völlig ungestört auf ihre Arbeit zu konzentrieren um sich Zugang zu den sensiblen Daten zu beschaffen. Denkbar ist auch, dass durch den unvorsichtigen Umgang der Mitarbeiter mit Passwörtern, die Anmeldeinformationen des OpenERP Systems in die Hände dritter Fallen, die sich damit unbemerkt im OpenERP System von jedem beliebigen Ort aus anmelden können.

2.4.2. OpenVPN Zertifikat

Um den Zugriff von Außen auf das Firmennetzwerk zu ermöglichen, wird OpenVPN in Verbindung mit einem Sicherheitszertifikat verwendet. Jeder Mitarbeiter bekommt bei Eintritt in das Unternehmen ein persönliches Zertifikat bereitgestellt, welches es ermöglicht, über den OpenVPN Client die Verbindung mit dem Firmennetzwerk herzustellen. Verlässt ein Mitarbeiter das Unternehmen, so hat er am letzten Arbeitstag die Aufgabe, dieses Sicherheitszertifikat zurückzugeben. Damit soll verhindert werden, dass sich der Mitarbeiter weiterhin in das Firmennetz einloggen kann. Durch diesen Prozessablauf kann jedoch nie sicher festgestellt werden, ob der Mitarbeiter das Zertifikat nicht in irgendeiner Form vervielfältigt hat und damit weiterhin Zugriff auf das interne Firmennetzwerk erlangen kann.

2.4.3. Passwörter

Gerät ein Passwort für eines der Systems in die Hände dritter, können diese sich unbemerkt und auf unbestimmte Zeit in die Systeme einloggen. Dieses Risiko besteht primär für die externen Systeme. Bei dem Unternehmen ist kein automatisches System vorhanden, das dafür sorgt, dass Passwörter nach einer bestimmten Zeit geändert werden müssen. Dies bedeutet, dass Passwörter nie ablaufen und nur bei Bedarf manuell geändert werden. Das hängt unter anderem mit der Vielzahl an vorhandenen Systemen und deren unabhängige Administration zusammen.

3. Lösungsansätze

Zur Vereinheitlichung und Zusammenführung der Rechtegruppen der verschiedene Systeme wird eine Plattform gesucht, die die Bedürfnisse des Unternehmens abdeckt. Das Ziel soll sein, den Verwaltungsaufwand der Benutzer und Rechte zu reduzieren und eine einheitliche und übersichtliche Struktur zu gestalten. In folgendem Abschnitt werden dazu drei Lösungsansätze vorgestellt, die eine Realisierung dieses Zieles ermöglichen. Dabei werden als Lösungsansätze Active Directory, die Anbindung an OpenERP und die Verwendung von LDAP untersucht. Für jeden dieser Lösungsansätze werden einige Vorteile und Nachteile dargestellt. Das Kapitel schließt mit einem direkten Vergleich der Lösungsansätze und einem Fazit ab.

3.1. Active Directory

Der erste Lösungsansatz stellt das Active Directory (AD) von Microsoft dar, welches für Windowsumgebungen geschaffen ist (Domain) und daher in vielen dieser Umgebungen zum Einsatz kommt. Es handelt sich dabei um ein Verzeichnisdienst, mit dem Unternehmensstrukturen abgebildet werden um diese zu organisieren und zu verwalten.

Aufgebaut ist das Active Directory aus vier Hauptkomponenten. Die erste Komponente stellt das LDAP-Verzeichnis dar. Es enthält Informationen über Benutzer und Gruppenzugehörigkeit, welche über das LDAP-Protokoll selbst abgefragt werden können. Zur Authentifizierung der Benutzer nutzt das Active Directory ein Protokoll mit der Bezeichnung Kerberos. Die dritte Komponente ist das sogenannte Common Internet File System (CIFS)-Protokoll, welches die Ablage der Dateien im Netzwerk verwaltet. Zum Auffinden der einzelnen Computer und Dienste wird die vierte Komponente, das Domain Name System (DNS) gebraucht. Es sorgt für die Namensauflösung im Netzwerk. [Wik14]

Zur Organisation und Verwaltung stehen Objekte zur Verfügung, die miteinander verknüpft werden können. Dabei handelt es sich beispielsweise um Benutzer, Gruppen, Computer oder auch Server. Mit Hilfe dieser Objekte lassen sich die reellen Unternehmensstrukturen abbilden.[Wik14] Es ist damit möglich mit wenig Aufwand Gruppen zu erstellen, diesen Benutzern zuzuordnen und letztendlich Berechtigungsgruppen für Dateizugriffe oder ähnliches festzulegen. Somit hat man die Möglichkeit nur bestimmten Benutzern, oder bei Bedarf ganzen Gruppen, Zugriff auf Dateien oder Ordner im Netzwerk zu gewähren. Viele Systeme bieten außerdem die Möglichkeit das Active Directory anzubinden. Dies bedeutet, dass die Gruppen und Benutzer für die Rechtevergabe innerhalb des Systemes verwendet werden können. Die verschiedenen Gruppen und Benutzer können in einer grafischen Oberfläche, in einer übersichtlichen Baumstruktur verwaltet werden.

Diese Lösung eignet sich hervorragend für reine Windowsumgebungen, die lediglich aus Windows Clients bestehen. Windows Clients sind dafür ausgelegt in den Domains zu interagieren und lassen sich ohne weiteres in diese integrieren. Die Kommunikation mit Domain Controller und Active Directory, die in der Regel auf einem Windows Server implementiert sind, stellt keine große Herausforderung dar. Will man Linux Clients einbinden, oder das Active Directory auf nicht Windowsumgebungen implementieren, ist dies nicht mehr ohne weiteres möglich. Seit Version 4 des frei erhältlichen SMB/CIFS-Servers Samba gibt es jedoch Fortschritte in diesem Bereich. [sam12] Durch Veröffentlichung der offiziellen Dokumentation des Protokolls seitens Microsoft, ist es den Entwicklern gelungen, eine beinahe vollständig mit dem Protokoll kompatible Implementierung zu realisieren. Ganz ausgereift ist diese Implementierung jedoch noch nicht.

3.1.1. Vorteile und Nachteile

Das Active Directory stellt eine sehr komfortable Lösung für eine übersichtliche und vereinheitlichte Verwaltung der Benutzer und Gruppen dar. Da es ein Microsoft Produkt ist und in vielen Umgebungen zum Einsatz kommt, ist der Support bei Problemen hervorragend. Der Support seitens Microsoft stellt jedoch gleichzeitig ein Nachteil dar, da er sehr kostspielig ist und in gewisser Weise eine Abhängigkeit von Microsoft generiert, da Supportverträge für alte Versionen auslaufen.

Bei dem Unternehmen werden Windows und Linux Clients eingesetzt. Außerdem wird bereits ein interner Linux Server betrieben. Um vollständig auf eine Windowsumgebung zu setzten wären umfangreiche Anschaffungen und Umstellungen vorhandener Systeme notwendig.

3.2. OpenERP

Ein weiterer Lösungsansatz ist es, alle vorhandenen Systeme an OpenERP anzubinden. OpenERP selbst wird schon seit längerer Zeit bei dem Unternehmen eingesetzt. Es wird unter anderem dazu verwendet die Zeiterfassung für die einzelne Projekte und jegliche buchhalterische Aufgaben durchzuführen. Aus diesem Grund bekommt jeder neue Mitarbeiter beim Eintritt in die Firma ein OpenERP-Benutzerkonto. Dies bedeutet wiederum, dass kein zusätzlicher Aufwand bei der Administration der Benutzer notwendig ist.

Momentan wird OpenERP auf einem virtuellen Server des Internetdienstanbieters Strato gehostet und ist frei über das Internet erreichbar. Dadurch ist es für Angreifer leichter in das System einzudringen als wenn dieses im internen Netzwerk gehostet werden würde und nur über eine VPN-Verbindung erreichbar wäre. Da innerhalb des OpenERP sensible Daten bezüglich der Mitarbeiter, der Kunden und den einzelnen Projekten gespeichert sind, sollte das System nicht über eine unverschlüsselte Internetverbindung erreichbar sein. Aus diesem Grund sollte OpenERP innerhalb des Unternehmensnetzwerks betrieben werden und nach außen nur über eine VPN-Verbindung erreichbar sein.

Um auf die OpenERP-Daten zuzugreifen gibt es zwei verschiedene Methoden. Zum einen ist es möglich direkt auf die verwendete PostgreSQL-Datenbank zuzugreifen und des Weiteren besteht die Möglichkeit über einen Webservice mit OpenERP zu kommunizieren. Beide Vorgehensweisen

würden es erfordern, dass für jedes anzubindende System ein Adapter geschrieben werden muss. Hervorzuheben ist, dass diese Adapter selbst geschrieben werden müssen, da keines der im Unternehmen eingesetzten Systeme einen schon bekannten Adapter besitzt.

Folgend werden die Vor- und Nachteile der zwei verschiedenen Arten von Adapter genauer betrachtet.

3.2.1. Datenbankadapter

Beim Datenbankadapter wird direkt auf die PostgreSQL-Datenbank der OpenERP Installation zugegriffen. In der OpenERP Dokumentation wird aber vor dieser Vorgehensweise gewarnt [Ope14a]. Es wird empfohlen vor dem Zugriff auf die Datenbank den OpenERP-Server herunterzufahren, um Caching- und Nebenläufigkeitsprobleme zu vermeiden. Des Weiteren wird empfohlen diese Methode nur durchzuführen, wenn man sich genau über die Auswirkungen bewusst ist.

Aufgrund von eventuell auftretenden und unvorhersehbaren Nebeneffekten ist diese Art des Zugriffes nicht zu empfehlen. Aus diesem Grund wird der Datenbankadapter hier nicht weiter betrachtet.

3.2.2. Geschäftslogikadapter

Beim Geschäftslogikadapter wird über den von OpenERP angebotenen Webservice kommuniziert. Hierbei muss man sich nicht wie bei dem Datenbankadapter um Nebeneffekte beim Zugriff auf die Daten Sorgen machen, da alle Datenbankzugriffe direkt von OpenERP übernommen werden.

Um mit dem Webservice zu kommunizieren ist es mögich entweder *net-RPC* oder *XML-RPC* zu verwenden. Bei net-RPC werden Objekte der Programmiersprache Python in ein binäres Format serialisiert und über einen Socket gesendet. Folglich funktioniert diese Methode nur, wenn Python als Programmiersprache eingesetzt wird. Diese Methode hat den Vorteil, dass sie performanter als XML-RPC ist. Dies liegt daran, dass OpenERP intern mit Python Klassen und Objekten arbeitet [Ope14b] und die gesendeten Objekte somit nur noch deserialisiert und nicht auf aufwändige Weise umgewandelt werden müssen. Bei XML-RPC wird XML zur Kommunikation verwendet. Dies hat den Vorteil, dass diese Methode unabhängig von einer Programmiersprache oder Plattform ist. Durch den Einsatz von XML entsteht allerdings ein größerer Overhead im Vergleich zu den serialisierten Python-Objekten, weswegen diese Methode auch langsamer ist.

Über den Webservice können mit Hilfe der *ORM Methoden* von OpenERP einzelne Objekte gelesen und manipuliert werden. ORM steht für *Object-Relational Mapping* und ist ein zentraler Part von OpenERP. Es dient als Datenmodell um auf einfache Weise die bei OpenERP eingesetzten Python Objekte und Klassen mit der darunter liegenden relationalen Datenbank (PostgreSQL) kommunizieren zu lassen. Über diese Objekte lassen sich auch die für die Authentifikation nötigen Daten auslesen.

3.2.3. Vorteile und Nachteile

Es ist möglich die Authentifizierungsvorgänge anderer System mit Hilfe der OpenERP-Benutzerdaten abzuwickeln. Von den zwei grundsätzlichen Vorgehensweise ist der direkte Datenbankzugriff über einen Datenbankadapter nicht zu empfehlen, da es zu unvorhersehbaren Komplikationen kommen kann. Die Alternative ist der Zugriff über den von OpenERP angebotenen Webservice mittels eines Geschäftslogikadapters. Das große Problem beider Vorgehensweisen ist, dass für jedes anzubindende System wiederum ein eigener Adapter zur Kommunikation mit OpenERP geschrieben werden muss. Dies bringt abermals andere Probleme mit sich. Es kann zu Problemen kommen, wenn eines der Systeme aktualisiert wird. Durch eine Aktualisierung ändert sich teilweise der innere Aufbau eines Systems, was erneut dazu führt, dass der jeweilige Adapter angepasst werden muss. Auch die Kosten der Eigenentwicklung von Adaptern sollte beachtet werden, da Mitarbeiter die sich um Adapter kümmern in dieser Zeit an keinen anderen Projekten arbeiten können. Das eigene Adapter geschrieben werden müssen kann aber auch als Vorteil gesehen werden. Dadurch, dass man den Code selber schreibt hat man die volle Kontrolle über ihn und kann die Lösung perfekt an die eigenen Bedürfnisse anpassen.

3.3. LDAP

Im Zusammenhang mit einer zentralen Benutzerverwaltung wird häufig der Lightweight Directory Access Protocol (LDAP) Standard diskutiert, welcher auch bereits als Teil des Microsoft Active Directory (siehe Kapitel 3.1) erwähnt wurde.

Der LDAP Standard selbst ist ein offenes und anbieterunabhängiges Applikations-Protokoll welches ein Verzeichnisdienst über das Netzwerk zur Verfügung stellt. Ein Verzeichnisdienst ermöglicht es so Daten zentral zu speichern und über das Netzwerk für jeden abrufbar zu machen. Die Form der Daten ist dabei nicht auf Benutzerdaten beschränkt. Eine flexible und hierarchische Struktur ermöglicht es so z.B. auch Adressdaten oder andere Formen von hierarchischen Daten zu verwalten. Häufig ist im Zusammenhang mit einem LDAP-Server jedoch eine zentrale Benutzerverwaltung gemeint. [?]

Aufgrund der großen Beliebtheit von LDAP unterstützen viele Applikationen und Softwaresysteme eine Anbindungen eines LDAP-Servers direkt oder über Erweiterungen. Von jedem der im Kapitel 2.1 dargestellten Systeme wird die Anbindung eines LDAP-Servers unterstützt. Dadurch ist die Integration eines LDAP-Server mit wenig Aufwand umzusetzen.

3.3.1. Vorteile und Nachteile

Der größte Vorteil bei der Verwendung von LDAP ergibt sich durch die vollständige Unterstützung für LDAP durch alle vorhandenen Systeme. Dies hat eine einfache Integration zur Folge. Wenn das System durch das Unternehmen selbst betrieben und administriert wird, fallen auch keine weiteren Kosten für den Betrieb an. Der bereits intern betriebene Linux Server könnte um die Funktion eines LDAP Servers leicht erweitert werden. Eine Authentifizierung gegen einen LDAP-Server ist auch betriebssystemübergreifend durch entsprechende Software sichergestellt, wodurch es möglich ist den Computer-Login zu authentifizieren.

3.4. Evaluation

In diesem Kapitel werden die drei zuvor beschriebenen Lösungsansätze genauer gegeneinander verglichen. Daher werden zunächst in Tabelle 3.1 nochmals stichpunktartig die einzelnen Vorteile und Nachteile der Lösungsansätze aufgelistet.

Lösungsansatz	Vorteile	Nachteile
Active Directory	• Einfache Verwaltung • Guter Support seitens Microsoft	• Die Systemumgebung sollte sinnvollerweise aus Windowsgeräten bestehen • Kosten • Abhängigkeit von Microsoft
OpenERP	• OpenERP ist schon jahrelang im Einsatz • Zentralisierung der Verwaltung um OpenERP	• Keine vorhandenen Adapter zur Anbindung der anderen Systeme • Eigenaufwand für Integration sehr hoch • Abhängigkeit von OpenERP
LDAP	• Weit verbreiteter Standard für die Verwaltung von Benutzern und Gruppen • Jedes der eingesetzten Systeme bietet eine Anbindung an LDAP an • Geringer Integrationsaufwand • Keine Lizenzkosten	• Zusätzliches System, das gewartet und administriert werden muss

Tabelle 3.1.: Übersicht von Vorteilen und Nachteilen der Lösungsansätze

Zum weiteren Vergleich der drei Lösungsansätze werden verschiedene Kategorien definiert, welche die wichtigsten Kriterien zur Auswahl das passenden Systems darstellen. Da die verschiedenen Kategorien nicht von gleicher Wichtigkeit sind, gibt es zusätzlich eine Gewichtung, die besonders wichtigen Kategorien einen entsprechenden Bonus in der direkten Gegenüberstellung liefern. Die direkte Gegenüberstellung wird in Form einer Tabelle realisiert, bei dem jeder Lösungsansatz pro Kategorie 0 bis 10 Punkte erzielen kann. 0 Punkte stellt dabei die niedrigste zu erreichende Punktzahl, 10 Punkte die am höchsten zu erreichende Punktzahl dar. Bei der Punktevergabe wird besonders der geschätzte Aufwand, der sich aus Manntagen und den Kosten zusammensetzt, berücksichtigt. Es folgt die Definition der verschiedenen Kategorien.

Installation: Aufwand zur Installation und Konfiguration des Lösungsansatzes im Netzwerk des Unternehmens.

Realisierung: Aufwand um die existierenden Systeme für einen Betrieb mit dem entsprechenden Lösungsansatz anzupassen und kommunikationsfähig zu machen.

Support: Möglichkeit bei Problemen Hilfe zu bekommen. Dies beinhaltete nicht nur den direkten Kontakt zu Experten, sondern auch die öffentliche Hilfestellungen durch beispielsweise FAQ's oder Communities im Internet.

Bedienbarkeit: Möglichkeit auf einfache Art und Weise die Aufgaben die während des laufenden Betriebes durch das System erledigt werden sollen zu erfüllen. Hierzu zählen hauptsächlich Benutzer/Gruppen anlegen, ändern und löschen.

Erweiterbarkeit: Möglichkeit weitere Systeme an das umgesetzte System und Umgebung anzubinden.

	Gewichtung	**Active Directory**	**OpenERP**	**OpenLDAP**
Installation	2x	4	9	7
Realisierung	3x	3	1	8
Support	1x	7	2	7
Bedienbarkeit	2x	9	7	8
Erweiterbarkeit	2x	8	1	8
Gesamtsumme (Gewichtet)		**58**	**39**	**77**

Tabelle 3.2.: Vergleich der Lösungsansätze anhand der Wichtigkeit verschiedener Kriterien

Die Installation und Konfiguration gestaltet sich bei OpenERP am einfachsten. Das System existiert bereits und ist daher schon für die Bedürfnisse des Unternehmens angepasst. Da sich das System jedoch noch bei dem externen Anbieter Strato befindet, muss ein Umzug und eine Migration auf einen Server im internen Firmennetz realisiert werden. Dies stellt den größten Teil der Installation des OpenERP Systems dar. OpenLDAP dagegen muss komplett neu aufgesetzt werden. Damit ist der Aufwand ziemlich groß. Der Vorteil Gegenüber des Active Directory's liegt darin, dass OpenLDAP in der existierenden Umgebung installiert werden kann. Für das Active Directory muss ein zusätzlicher Windows Server angeschafft und konfiguriert werden.

Bei der Realisierung kann OpenLDAP die meisten Punkte erzielen. Da es keine Vorgaben an die Mitarbeiter gibt, welches Betriebssystem diese einsetzen müssen, gibt es einige Clients die Windows und andere die Linux nutzen. Da sich sowohl Windows als auch Linux Clients ohne größeren Aufwand an OpenLDAP anbinden lassen, stellt das OpenLDAP eine gute Lösung für die einheitliche Benutzer- und Rechteverwaltung dar. Für die Anbindung der vorhandenen Systeme an den LDAP Server ist nur geringer Aufwand notwendig, da alle eingesetzten Systeme diese Möglichkeit bieten. Das Active Directory erzielt in dieser Kategorie nur wenig Punkte, da es zwar die Möglichkeit gibt, Linux Clients anzubinden, dies aber oft nicht so einfach umzusetzen ist und immer wieder Probleme auftreten. Für das Active Directory wäre es daher notwendig auf eine Windowsumgebung umzustellen, da ein zuverlässiger Betrieb mit dem Active Directory nur in einer homogenen Windowsumgebung garantiert werden kann. Dieser Umstellungsschritt der Clients stellt einen hohen Realisierungsaufwand dar. Am schlechtesten schneidet in dieser Kategorie das OpenERP System ab. Keines der im Einsatz

befindlichen System bietet die Möglichkeit, die Benutzer und Gruppen des OpenERP Systems zu verwenden. Es ist daher notwendig, für jedes System einen Adapter zu implementieren, um die Verwendung zu ermöglichen. Dies stellt einen sehr großen Aufwand dar. Außerdem kann es durch Update eines Systems sein, dass der entsprechende Adapter nicht mehr funktioniert und angepasst werden muss.

Das Active Directory und OpenLDAP erreichen in der Kategorie Support die meisten Punkte. Microsoft bietet einen guten direkt Support, lässt ihn sich jedoch auch gut bezahlen. Die Möglichkeit des Supports ist abhängig von den entsprechenden Lizenzverträgen, die in der Regel sehr teuer sind und zu hohen laufenden Kosten führt. Da es sich um ein Microsoft Produkt handelt und in vielen Unternehmen und Organisationen zum Einsatz kommt, gibt es auch eine große Community und Informationen im Internet, um Hilfe zu erhalten. Dies ist auch bei OpenLDAP der Fall. Die Software kommt häufig zum Einsatz und es existieren deshalb viele hilfreiche Informationen im Internet. Da es sich um ein Open Source Produkt handelt, gibt es keinen direkten Hersteller, bei dem man Support bekommt. Es gibt jedoch einige Firmen die sich darauf spezialisiert haben im Unternehmensumfeld LDAP einzurichten und zu administrieren. Bei der Verwendung von OpenERP als zentrale Benutzer- und Rechteverwaltung strebt man eine ungewöhnliche Lösung an. Es ist eine individuelle Implementierung von Adaptern für alle vorhandenen Systeme notwendig. Es ist daher nicht einfach Informationen darüber im Internet zu finden. Auch professionelle Hilfe zu bekommen, wird bei dieser Art der zentralen Benutzer- und Rechteverwaltung sehr schwierig. Es müsste dort entsprechende teure maßgeschneiderte Software entwickelt werden. OpenERP schneidet deshalb in dieser Kategorie mit den wenigstens Punkten ab.

In Sachen Bedienbarkeit erzielt das Active Directory die meisten Punkte. Es bietet eine grafische Oberfläche in Form einer Baumstruktur, die man von Windows, zum Beispiel vom Dateiexplorer, gewohnt ist. Über diese Oberfläche ist es dann möglich Benutzer und Gruppen per Maus oder Tastatur anzulegen. Es ist daher mit wenig Schulungsaufwand möglich, einen User in dieses Tool ein zu lernen. Auch OpenLDAP bietet eine grafische Benutzeroberfläche zum Verwalten der Gruppen und Benutzer. Die Struktur ist jedoch nicht so übersichtlich wie bei Active Directory und gestaltet sich nicht so intuitiv. Daher schneidet OpenLDAP weniger gut wie Active Directory ab. OpenERP erzielt auch hier die wenigstens Punkte, da es bei dem Unternehmen zwar Gang und Gebe ist, aber in Betracht auf Neueinstellungen das Bedienkonzept weniger vertraut ist wie bei Active Directory oder OpenLDAP, die besonders Systemadministratoren bekannt sind.

Bei der letzten Kategorie, die Erweiterbarkeit, sind Active Directory und OpenLDAP gleich auf. Kommen neue Systeme hinzu, die auf die Benutzer und Gruppen zugreifen sollen, lassen sich diese meist ohne großen Aufwand anbinden. So wie die Momentan eingesetzten System die Möglichkeit von Haus aus die Möglichkeit bieten, die beiden Systeme anzubinden, wird dies auch in den meisten neu dazu kommenden Systemen der Fall sein. Sollte dies nicht zutreffen, so gibt es mit Sicherheit andere Unternehmen und Erfahrungswerte die das gleiche umgesetzt haben, auf die man sich berufen kann. OpenERP schneidet auch hier schlecht ab, da für jedes neu dazu kommende System, ein weitere Schnittstelle oder Adapter implementiert werden muss.

In dieser Evaluation schneidet das OpenLDAP System mit 77 Punkten vor dem Active Directory mit 58 Punkten am Besten ab. Schlusslicht bildet das OpenERP System mit 39 Punkten. OpenLDAP stellt daher für das Unternehmen das am besten geeignete System für eine zentrale Benutzer- und Rechteverwaltung dar.

4. Realisierung

In diesem Kapitel wird beschrieben, wie eine zentrale Benutzer- und Rechteverwaltung mit Hilfe von LDAP umgesetzt werden kann. Dafür wird zunächst die Gruppen- und Rechtestruktur betrachtet und wie eine zentrale Struktur aus den vorhandenen Systemen in einem LDAP-Verzeichnis abgebildet werden kann. Anschließend werden die einzelnen Systeme und deren technische Umsetzung zur Anbindung an einen zentralen LDAP-Server genauer untersucht. Schließlich werden die aus der zentralen Benutzer- und Rechteverwaltung resultierenden Prozessabläufe angepasst und Lösungen für die vorhandenen Sicherheitsprobleme vorgeschlagen.

4.1. Rechtestruktur

Um eine einfachere Verwaltung der Benutzer der verschiedenen Rechtegruppen und den dazugehörigen Rechten zu realisieren, wurde eine einfache Gruppenstruktur erstellt. Innerhalb dieser Struktur kann die Benutzerverwaltung aller untersuchten Systeme realisiert werden.

Jeder Benutzer ist in der Gruppe *user* und bekommt somit Zugriff auf die allgemeinen Systeme MediaWiki und StatusNet. Unterhalb der Gruppe *user* sind folgende Gruppen angeordnet:

- **division**: Dieser Gruppe werden Untergruppen zugeteilt, entsprechend der Abteilungsstruktur innerhalb des Unternehmens. Somit können jeder Abteilung die für ihr Aufgabengebiet nötige Rechte für die einzelnen System zugeordnet werden. Um die einzelnen Abteilungen zu repräsentieren wurden folgende Gruppen als benötigt identifiziert:
  - **students**: Enthält alle studentischen Mitarbeiter
  - **backoffice**: Enthält alle Mitarbeiter, die in der Verwaltung und/oder dem Sekretariat arbeiten
  - **sales**: Enthält alle Mitarbeiter, die für das Verkaufen zuständig sind
  - **marketing**: Enthält alle Mitarbeiter, die für das Marketing verantwortlich sind
  - **hr**: Enthält alle Mitarbeiter, die in der Personalabteilung tätig sind
  - **accounting**: Enthält alle Mitarbeiter, die buchhalterische Aufgaben durchführen
  - **research**: Enthält alle Mitarbeiter die an der Entwicklung neuer Dienstleistungen oder Produkte beteiligt sind
  - **develop**: Enthält alle Mitarbeiter, die an aktuellen Projekten arbeiten

- **admin**: Innerhalb dieser Gruppe werden die Administratoren der verschiedenen Systeme verwaltet. Für jedes der zu verwaltenden System wird eine eigene Untergruppe erstellt um eine feinere Kontrolle über diese zu bekommen.
- **management**: Innerhalb dieser Gruppe befindet sich die Geschäftsführung
- **businessUnitLead**: In dieser Gruppe befinden sich die Benutzer, die für eine bestimmte Business Unit zuständig sind
- **topicLead**: Benutzer dieser Gruppe sind für ein Themengebiet innerhalb des Unternehmens verantwortlich
- **headOfBrach**: Die Benutzer dieser Gruppe besitzen die Leitung über eine der verschiedenen Geschäftszweige
- **privacyOfficer**: Wird ein Benutzer dieser Gruppe zugeordnet, so befindet sich dieser in der Rolle des Datenschutzbeauftragten
- **functionOwners**: Benutzer die querschnittliche Funktionalitäten haben, werden dieser Gruppe zugeordnet
- **outOfRole**: Diese Gruppe nimmt innerhalb der gesamten Rechtestruktur eine besondere Rolle ein. Die Untergruppen dieser Gruppe sollen für ein sehr spezielles Zugriffsrecht eines beliebigen Systems stehen. Benötigt ein Benutzer nun Rechte die standardmäßig nicht innerhalb seiner Funktion oder Abteilung gewährt werden, so können diese hier definiert werden. Somit besteht die einfache Möglichkeit einem einzelnen Benutzer spezielle Rechte zu gewähren.

Ein Visualisierung dieser Struktur ist in Abbildung 4.1 zu sehen.

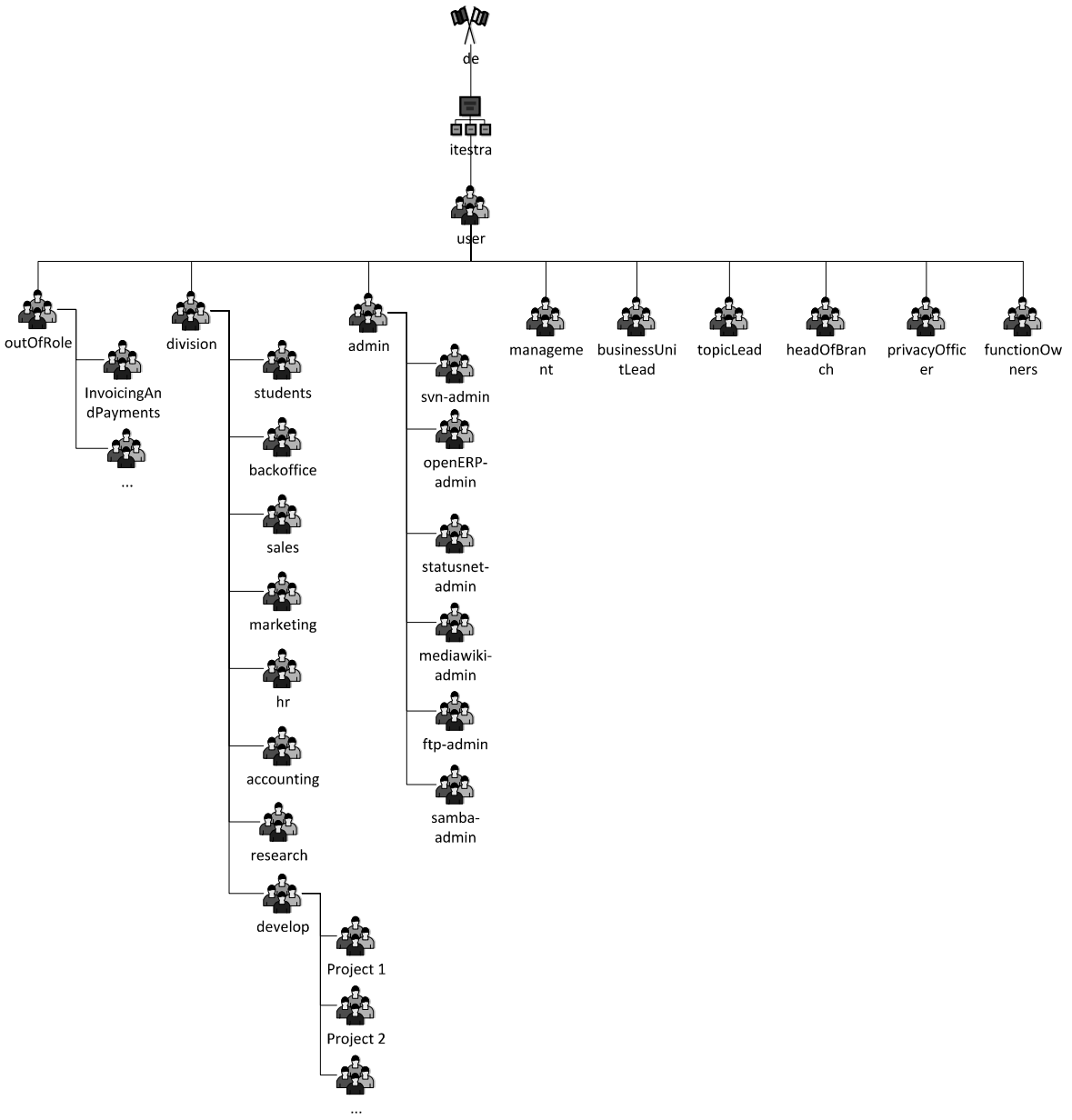

Abbildung 4.1.: Kombinierte Rechtestruktur

4.2. Anpassung der Systeme

Folgend wird beschrieben, auf welche Weise die einzelnen Benutzergruppen mit den verschiedenen Systemen in Verbindung gebracht werden können.

E-Mail

Da es nicht möglich ist das E-Mail System an eine zentrale Benutzerverwaltung anzuschließen, gibt es auch keine Möglichkeit dieses automatisiert zu verwalten. Aus diesem Grund muss wie schon praktiziert eine Verwaltung der Benutzer über das von Strato angebotene Webinterface vorgenommen werden.

FTP

Jeder Benutzer der sich innerhalb einer der Projektgruppen befindet bekommt Zugriff auf den FTP-Server. Hierbei wird für jedes Projekt ein eigener Ordner angelegt und der Benutzer bekommt nur Zugriff auf den Projektordner.

Samba

Der Zugriff auf den Samba-Server wird ähnlich wie der Zugriff auf den FTP-Server verwaltet. Auch hier sollen projektspezifische Ordner angelegt werden und Benutzer des entsprechenden Projekts Zugriff auf diesen erteilt werden. Des Weiteren sollen alle Benutzer (Benutzer der Gruppe *user*) Zugriff auf einen öffentlichen Teil des Servers bekommen.

OpenERP

Benutzer verschiedener Abteilungen haben verschiedene Ansichten innerhalb des OpenERP Systems. Somit definieren in erster Linie die Gruppen unterhalb der Obergruppe *division*, welche Bereiche für den Benutzer zugänglich sind. Ist der Benutzer innerhalb des Unternehmens in einer besonderen Position, so kann er über diese weitere Rechte erteilt bekommen. Sollten die über die Abteilung und Funktion erteilten Rechte nicht genügen, können über eine Untergruppe von *outOfRole* weitere Rechte erteilt werden.

Subversion

Ähnlich wie bei OpenERP bekommen auch hier die Benutzer anhand der Abteilung und Funktion Zugriff auf bestimmt Verzeichnisse. Um erweiterten Zugriff, welcher nicht über die Abteilung oder die Funktion definiert ist, zu bekommen, können wiederum die Untergruppen der Gruppe *outOfRole* verwendet werden.

MediaWiki

Jeder Nutzer der innerhalb des LDAP-Verzeichnisses registriert ist, bekommt Zugriff auf das Wiki. Somit sind alle Mitglieder der Gruppe *user* Nutzer des Wikis.

StatusNet

Die Verwaltung von StatusNet verhält sich genau wie die des MediaWikis. Auch hier bekommen alle Benutzer die der Gruppe *user* angehören Zugriff.

OpenVPN

OpenVPN bietet zwar eine Anbindung an einen LDAP-Server an, allerdings wird hier empfohlen wie seither mit Zertifikaten zu arbeiten. Somit ist dieses System nicht an den LDAP-Server angebunden.

4.3. Prozessänderungen

Im Folgenden wird gezeigt, in wie fern die in Kapitel 2.3 vorgestellten Prozesse an die neue Benutzerverwaltung angepasst werden müssen. Punkte die sich im Vergleich zum vorherigen Prozess geändert haben, sind hervorgehoben.

4.3.1. Mitarbeiter Eintritt in das Unternehmen

Im Vergleich zum dem in Kapitel 2.3.1 vorgestellten Prozess, ist das Anlegen eines neuen Benutzers, wie in dem Prozessausschnitt in Abbildung 4.2 zu sehen, für alle Systeme stark vereinfacht. Die Mitarbeiter des Backoffice (BO) müssen nur noch den E-Mail Account erstellen. In der IT muss nur noch ein Benutzer im LDAP-Verzeichnis angelegt und dieser den entsprechenden Gruppen zugeordnet werden, damit der neue Mitarbeiter Zugriff auf alle von dem Unternehmen verwendeten Systeme bekommt.

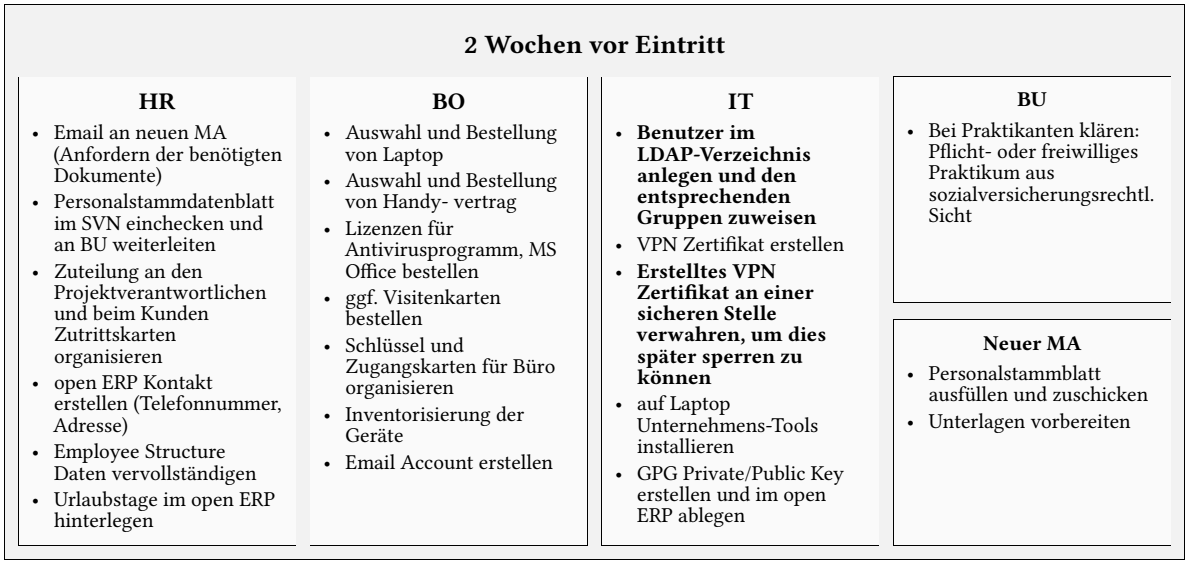

Abbildung 4.2.: Angepasster Unternehmensprozess: Mitarbeiter tritt in das Unternehmen ein

4.3.2. Mitarbeiter Austritt aus dem Unternehmen

Wie in dem Prozessausschnitt in Abbildung 4.3 zu sehen ist, ist das Entfernen eines Benutzers im Vergleich zu dem in Kapitel 2.3.2 beschriebenen Prozess stark vereinfacht. Das Backoffice (BO) muss nun nur noch den E-Mail Account deaktivieren. Die IT muss den Benutzer aus dem LDAP-Verzeichnis entfernen und das OpenVPN-Zertifikat sperren, damit der ausscheidende Mitarbeiter keinen Zugriff mehr auf das Unternehmensnetzwerk hat.

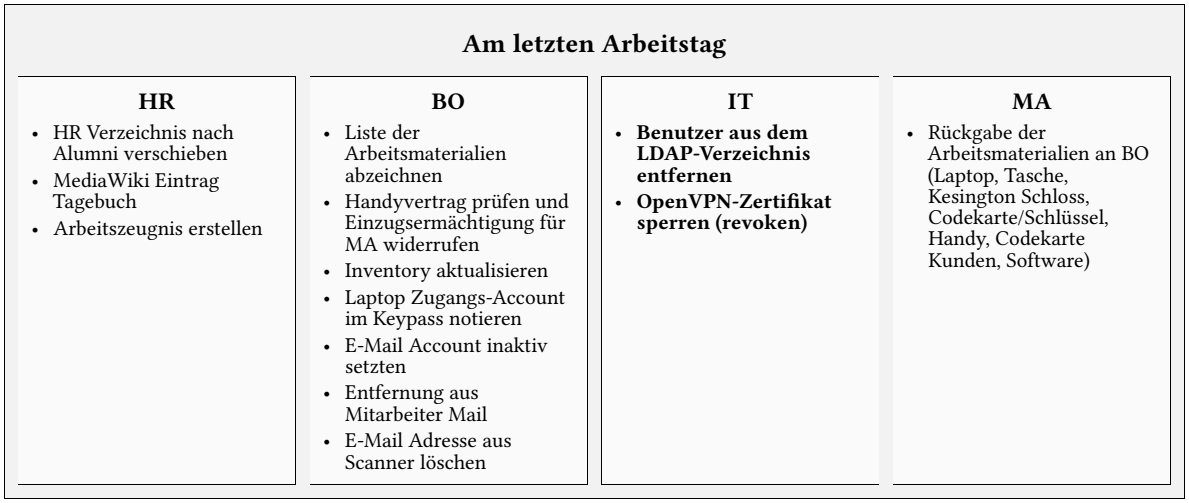

Abbildung 4.3.: Angepasster Unternehmensprozess: Mitarbeiter verlässt das Unternehmen

4.3.3. Mitarbeiter Eintritt in ein Projekt

Abbildung 4.4 zeigt den einzigen Schritt der noch durchgeführt werden muss, um einen neuen Mitarbeiter einem vorhanden Projekt zuzuweisen. Der neue Projektmitarbeiter muss nur noch dem entsprechenden Projekt innerhalb des LDAP-Verzeichnisses hinzugefügt werden, um alle benötigten Rechte zu erhalten.

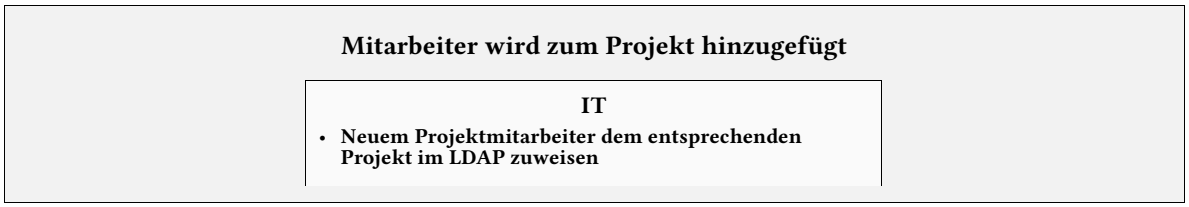

Abbildung 4.4.: Angepasster Unternehmensprozess: Mitarbeiter wird zu einem Projekt hinzugefügt

4.3.4. Mitarbeiter Ausscheiden aus einem Projekt

Mussten im vorherigen Prozess noch jedem Mitarbeiter einzeln die Rechte entzogen werden, so muss dies nur noch für die Projektgruppe durchgeführt werden. Hiermit werden auch alle dieser

Gruppe angehörigen Mitarbeiter die entsprechenden Rechte entzogen. Der angepasste Prozess ist in Abbildung 4.5 zu sehen.

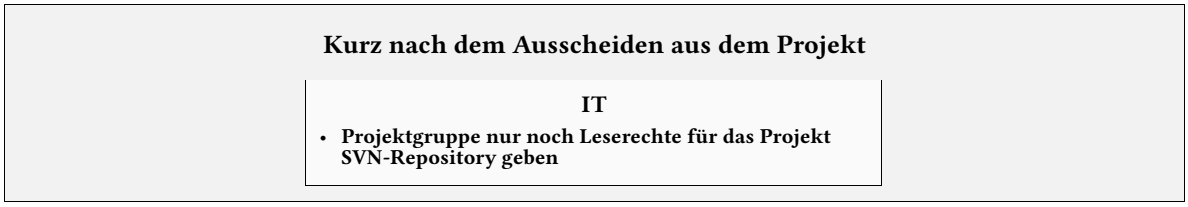

Abbildung 4.5.: Angepasster Unternehmensprozess: Mitarbeiter scheidet aus einem Projekt aus

4.3.5. Projektbegin

Abbildung 4.6 zeigt die durchzuführende Schritte bei einem Projektbeginn. Die IT muss zuerst ein neues SVN-Repository für das neue Projekt anlegen. Anschließend muss eine neue Gruppe für das Projekt im LDAP-Verzeichnis angelegt werden und die Projektmitarbeiter müssen dieser zugeordnet werden. Des Weiteren müssen der neuen Gruppe Schreib- und Leserechte für das SVN-Repository gegeben werden. Zum Schluss muss sowohl das SVN-Repository als auch das vom Backoffice (BO) oder dem Projektleiter angelegte OpenERP-Projekt mit der LDAP Projektgruppe verknüpft werden.

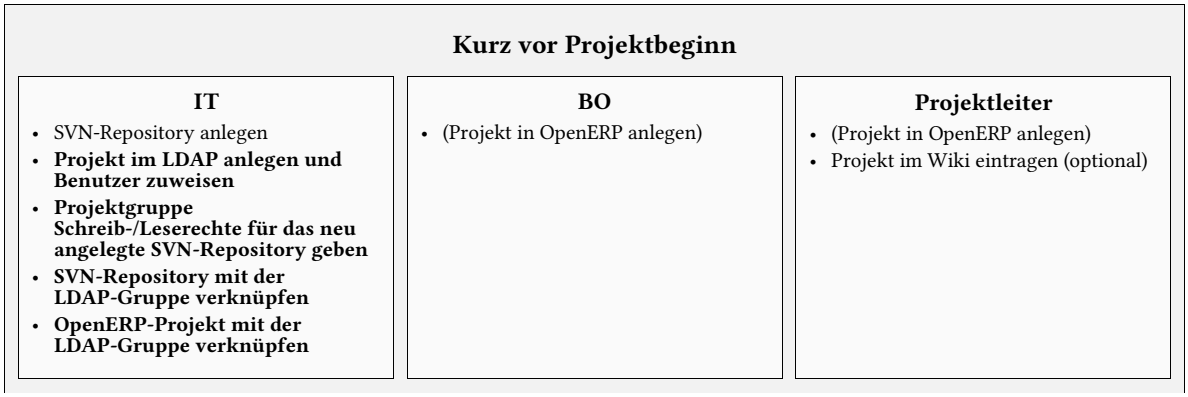

Abbildung 4.6.: Angepasster Unternehmensprozess: Projekt beginnt

4.3.6. Projektende

An diesem Prozess müssen keine Anpassungen vorgenommen werden, da der in Kapitel 2.3.6 beschriebene Prozess direkt übernommen werden kann.

4.4. Informationssicherheit

Bei der Analyse der Systeme und Prozesse sind einige Sicherheitslücken zum Vorschein gekommen. Diese werden in Abschnitt 2.4 näher erläutert. Zum Schließen der Sicherheitslücken sind Änderungen an den Prozessen und das Anwenden von bestimmten Techniken notwendig. In folgendem Kapitel wird beschrieben, wie es möglich ist, diese Sicherheitslücken zu schließen.

4.4.1. Externer Zugriff auf die Systeme

Wie in Abschnitt 2.4.1 beschrieben, ist der Zugriff auf die Systeme, die bei Strato gehostet sind, von jedem beliebigen Rechner über das Internet möglich. Geschützt sind die Systeme momentan über die jeweils integrierte Zugangskontrolle, welche aus einer Benutzername und Passwort Kombination besteht. Eine Möglichkeit diese Sicherheitslücke zu schließen, stellt die Migration der extern gehosteten Systeme in das interne Netz dar. Durch das bereits vorhandene VPN, ist ein Zugriff über einen gesicherten Tunnel von einem Gerät eines Mitarbeiters möglich. Somit bleibt die Möglichkeit bestehen von Unterwegs auf die Systeme zuzugreifen, ohne das System für jedermann erreichbar zu machen.

Für das Unternehmen ist dies keine akzeptable Lösung. Es gibt einige Mitarbeiter, die über einen längeren Zeitraum ein Projekt bei einem Kunden arbeiten und auch die Systeme der Kunden benutzen. Dies hat zur Folge, dass ein Zugriff auf das interne Firmennetz durch den VPN Tunnel aufgrund von fehlendem VPN Zertifikat oder Restriktionen des Netzwerkes des Kunden in bestimmten Fällen nicht möglich ist. Somit kann durch Umzug der Systeme in das Firmennetz auch das OpenERP System nicht von überall erreicht werden. Da die Mitarbeiter jedoch Zugriff auf das System benötigen um beispielsweise ihre Projektstunden einzutragen, muss es jedoch von jedem beliebigen Ort aus erreichbar sein. Die Strategie, das System extern zu betreiben und über das Internet erreichbar zu machen, ist daher bewusst gewählt. Die komplette Integration des OpenERP Systems ist aufgrund dieses Prozesses und des dazu benötigten OpenERP Modul zum Eintragen und Einsehen der Arbeitsstunden nicht möglich. Weitere Module die über das Internet erreichbar sein müssen sind die Adressdaten und die Aufgaben der einzelnen Projekte innerhalb des OpenERP Systems. Es muss daher eine Lösung gefunden werden, die das OpenERP System in das geschützte Firmennetzwerk integriert, aber gleichzeitig einige Module und deren Funktionen zur Verfügung stellt, die über das Internet erreichbar sind.

Denkbar ist hier, die benötigten Module und Funktionen nach außen durch eine eigene Webapplikation zur Verfügung zu stellen. Der Datenaustausch und die Kommunikation der Applikation mit dem OpenERP System findet über Webservices statt. Es wird dabei eine *XML-RPC Web Service* Schnittstelle verwendet, die in Abschnitt 3.2.2 beschrieben ist. Somit ist es möglich, Schnittstellen zur Verfügung zu stellen, die über das Internet erreichbar sind. Durch diese Architektur kann erreicht werden, dass das OpenERP System in das geschützte Firmennetz integriert werden kann, jedoch gleichzeitig die benötigten Module und Funktionen durch die Applikation von außen über das Internet erreichbar sind. In der Anwendung müssen die Funktionen eintragen und einsehen von Arbeitsstunden, einsehen der Adressen der einzelnen Projekte und einsehen und bearbeiten der Projekt-Tasks implementiert sein.

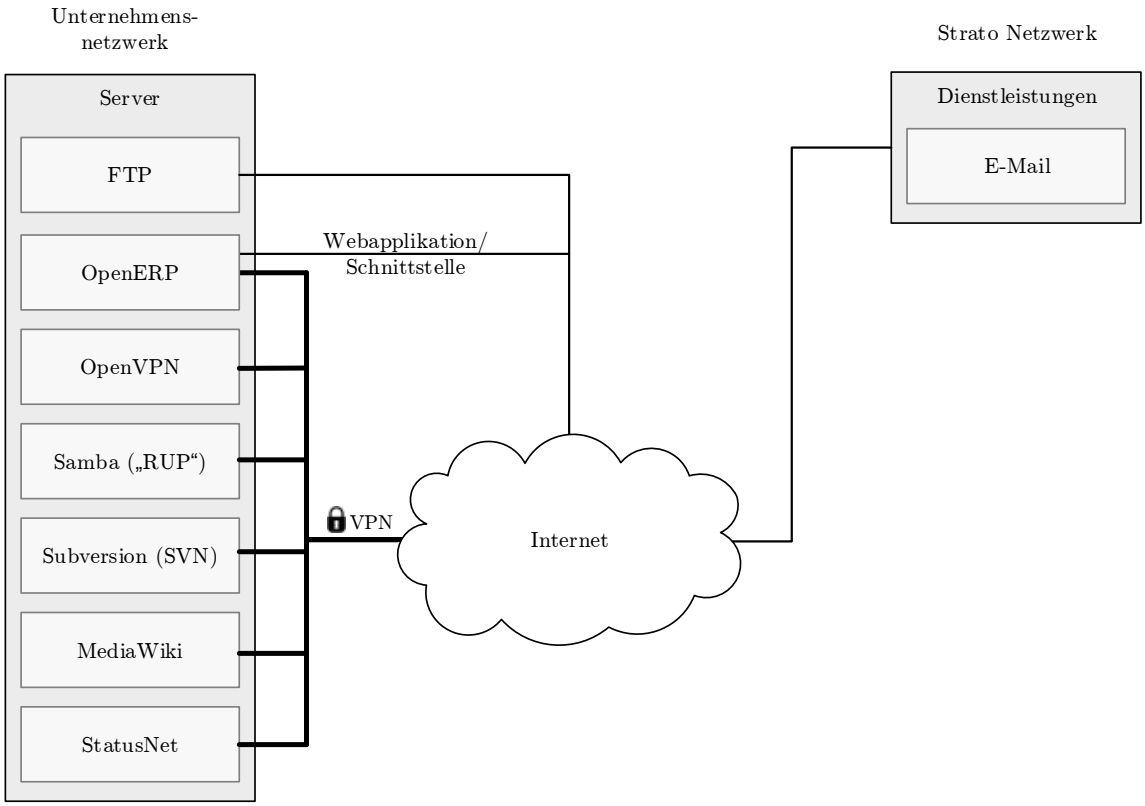

Abbildung 4.7.: Neue Systemübersicht

Neben dem OpenERP System sind noch weitere Systeme bei Strato gehostet und über das Internet erreichbar. Dabei handelt es sich um einen E-Mail-Server, einen StatusNet-Server und einen MediaWiki-Server. Da es sich bei dem E-Mail-Server um einen Server von Strato handelt, der von dem Unternehmen als Dienstleistung für E-Mails verwendet wird, kann dieser nicht in das interne Netz integriert werden. Die beiden andere Server können in das Firmennetz integriert werden. Dabei sind auch keine Schnittstelle nach außen notwendig, da die Informationen die darin enthalten sind nicht zwingend sofort beim Kunden eingesehen werden müssen. Somit genügt es, wenn diese Systeme rein über das VPN erreichbar sind.

Auf Abbildung 4.7 ist die Systemübersicht nach Umzug der extern gehosteten Systeme in das interne Firmennetzwerk zu sehen.

4.4.2. OpenVPN Zertifikat

OpenVPN bietet als Standardfunktion die Möglichkeit ein Zertifikat, welches an einen Mitarbeiter übergeben wurde, zu „revoken“. Dies bedeutet, dass das Zertifikat für ungültig erklärt wird und dadurch nicht mehr für den Authentifizierungsprozess verwendet werden kann. Realisiert wird dies durch eine sogenannte *Certificate Revocation List (CRL)*. Dabei handelt es sich um eine Datei in der die Client Zertifikate die revoked werden sollen eingetragen sind. Ist die CRL Verifikation in den Einstellungen des OpenVPN Servers aktiviert, so wird bei jedem Verbinden eines Clients das Zertifikat gegen die CRL verifiziert. Gibt es einen Eintrag, der zu dem entsprechenden Client passt, so wird die Verbindung verhindert. Die CRL-Datei muss an einen Platz abgelegt werden, auf den der OpenVPN Server Deamon zugreifen kann.

Durch diese Konfiguration, die OpenVPN mit sich bringt, ist es möglich die Sicherheitslücke in diesem Prozess zu schließen.

4.4.3. Kennwörter

Aufgrund der fehlenden Richtlinie, dass Kennwörter ablaufen, werden viele Kennwörter sehr selten beziehungsweise nie geändert. Dies liegt unter anderem an der dezentralen Nutzerverwaltung im Unternehmen. Jedes System hat seine eigene Benutzerverwaltung, was dazu führen würde, dass bei Ablauf Passwörter in allen Systemen geändert werden müssen. Außerdem verwaltet jeder Mitarbeiter seinen Laptop selbst und somit existiert auch keine Anmeldung gegen einen zentralen Authentifizierungsserver wie es beispielsweise in einer Windows Domain der Fall ist. Ist eine zentrale Benutzerverwaltung und Authentifizierung mit Hilfe von LDAP implementiert, so kann eine solche Richtlinie aktiviert werden. LDAP bietet die Möglichkeit einen Parameter zu konfigurieren, der dafür sorgt, dass Kennwörter nur bis zu einem bestimmten Datum gültig sind. Authentifiziert sich ein User gegen die LDAP Datenbank, so ist ein einloggen nicht mehr möglich und das Kennwort muss geändert werden.

5. Zusammenfassung und Ausblick

In dieser Prozessanalyse wurde ein Konzept zu einer einheitlichen Benutzerverwaltung der von einem Beratungsunternehmens genutzten Systeme erarbeitet.

Um dies zu erreichen wurden in einem ersten Schritt die acht zu betrachtenden Systeme (FTP, Samba, OpenVPN, Subversion, E-Mail, OpenERP, StatusNet und MediaWiki) analysiert. Vier dieser Systeme (FTP, Samba, OpenVPN und Subversion) werden innerhalb des Unternehmensnetzwerkes betrieben und die anderen vier (E-Mail, OpenERP, StatusNet und MediaWiki) bei dem externen Internetdienstanbieter Strato AG. Ein Teil der Systeme wird extern betrieben, da diese zu jeder Zeit und jedem Ort für die Mitarbeiter erreichbar sein sollen. Außerdem wurden Unternehmensprozesse betrachtet, in welchen Benutzer zu einem System hinzugefügt oder entfernt werden oder bei welchen eine Änderung der Zugriffsrechte erfolgt. Als wichtige Prozesse wurden der Eintritt und Austritt eines Mitarbeiters in das Unternehmen, der Projektstart, das Projektende, das Hinzufügen eines neuen Mitarbeiters zu einem Projekt und das Entfernen eines Mitarbeiters aus einem Projekt als wichtig identifiziert.

Des Weiteren wurden innerhalb des ersten Schrittes Sicherheitsmängel bezüglich der verwendeten Systeme und der Benutzerverwaltung untersucht. Das schwerwiegendste Problem, welches erkannt wurde, ist, dass die externen Systeme frei über das Internet erreichbar sind und diese nur über den jeweiligen Schutzmechanismus des jeweiligen Systems abgesichert sind. Eine mögliche Lösung dieses Problems wurde in Schritt drei erarbeitet.

Im zweiten Schritt wurden drei verschiedene Möglichkeiten zu einer einheitlichen Benutzerverwaltung miteinander verglichen. Anhand verschiedener und gewichteter Kriterien wurde ein zentraler LDAP-Server, an welchen alle Systeme angeschlossen werden, als beste Lösung identifiziert. Ausgenommen wird hierbei der E-Maildienst, da dieser von Strato betrieben wird und es keine Möglichkeit gibt diesen an den LDAP-Server anzubinden.

Beim dritten und letzten Schritt wurde der gewählte Lösungsansatz genauer ausgearbeitet und eine mögliche Lösung der Sicherheitsprobleme präsentiert. Das zuvor angesprochene Problem der externen Systeme wurde dadurch gelöst, dass diese in das interne Unternehmensnetzwerk verschoben wurden. Hierdurch sind die meisten verschiedenen Systeme von außen nur noch über das VPN erreichbar. Um den Fall zu berücksichtigen, dass es Mitarbeitern manchmal nicht möglich ist eine Verbindung über das VPN herzustellen wurde eine ergänzende Lösung erarbeitet. Wichtige Funktionen der einzelnen Systeme, die zu jedem Zeitpunkt und auch ohne VPN-Verbindung erreichbar sein müssen, können durch gesonderte Schnittstellen angesprochen werden. Die Schnittstellen wiederum werden im Unternehmensnetzwerk betrieben und kommunizieren über eine API mit dem jeweiligen System. Hierdurch ist eine sehr feine Kontrolle der nach außen hin verfügbaren Daten möglich.

Des Weiteren wurden im letzten Schritt die zuvor betrachteten Prozesse so angepasst, so dass diese mit der einheitlichen Benutzerverwaltung verwendet werden können.

Ausblick

In dieser Arbeit wurde nur die Konzeption einer einheitlichen Benutzerverwaltung vorgestellt. Im nächsten Schritt muss dieses Konzept in die Praxis umgesetzt werden.

Nachdem eine einheitliche Benutzerverwaltung umgesetzt wurde, könnte auch eine Single-Sign-On Lösung erarbeitet werden, um für die Benutzer die Handhabung der Systeme zu vereinfachen. Mit einem Single-Sign-On müssten sich die Nutzer nur noch an einer zentralen Stelle authentifizieren, um anschließend all Systemen ohne weitere Authentifizierung zu verwenden.

A. Prozesse

A.1. Mitarbeiter Austritt

4 Wochen vor Austritt

HR

- E-Mail mit Informationen über den Austritt an BO, IT, BU
- E-Mail mit Vorlage für das Arbeitszeugnis an Vorgesetzten des auszutestenden Mitarbeiters

BO

- E-Mail an MA mit den Arbeitsmaterialien des auszutretenden Mitarbeiters, welche zurückgegeben werden müssen

Am letzten Arbeitstag

HR

- HR Verzeichnis nach Alumni verschieben
- MediaWiki Eintrag Tagebuch
- Arbeitszeugnis erstellen

BO

- Liste der Arbeitsmaterialien abzeichnen
- Handyvertrag prüfen und Einzugsermächtigung für MA widerrufen
- Inventory aktualisieren
- Laptop Zugangs-Account im Keypass notieren
- E-Mail Account inaktiv setzten
- Entfernung aus Mitarbeiter Mail
- MediaWiki Benutzerkonto löschen
- StatusNet Benutzer löschen
- E-Mail Adresse aus Scanner löschen

IT

- Entfernung des SVN Zugangs
- Entfernung des Samba/Unix Zugangs
- OpenERP Account sperren
- OpenVPN Rückgabe des Client-Zertifikats

MA

- Rückgabe der Arbeitsmaterialien an BO (Laptop, Tasche, Kesington Schloss, Codekarte/Schlüssel, Handy, Codekarte Kunden, Software)

A.2. Mitarbeiter Eintritt

Vertragserstellung

HR
- Vertrag erstellen und vorab zur Prüfung an BU
- Nach Prüfung an MA schicken (in zweifacher Ausführung)

BU
- Prüfung des Vertrags

Neuer MA
- Vertrag unterschreiben
- Ein Exemplar zurücksenden

Unmittelbar nach Vertragsunterzeichnung

HR
- Info über Eintritt an BU, BO und IT
- Profil für MA im SVN unter HR/MA/DE_Nachname_Vorname (für andere Länder entsprechende Länderbezeichnungen) anlegen
- Vertrag einscannen und in MA Ordner unter HR/MA/DE_Nachname_Vorname ablegen
- Original an BU schicken

BU
- Personalnummer erstellen

2 Wochen vor Eintritt

HR
- Email an neuen MA (Anfordern der benötigten Dokumente)
- Personalstammdatenblatt im SVN einchecken und an BU weiterleiten
- Zuteilung an den Projektverantwortlichen und beim Kunden Zutrittskarten organisieren
- OpenERP Kontakt erstellen (Telefonnummer, Adresse)
- Employee Structure Daten vervollständigen
- Urlaubstage im OpenERP hinterlegen

BO
- Auswahl und Bestellung von Laptop
- Auswahl und Bestellung von Handy- vertrag
- Lizenzen für Antivirusprogramm, MS Office bestellen
- ggf. Visitenkarten bestellen
- Schlüssel und Zugangskarten für Büro organisieren
- Inventorisierung der Geräte
- Email Account erstellen
- MediaWiki Login erstellen
- StatusNet Login erstellen

IT
- SVN Account anlegen
- Zugang RUP einrichten
- VPN Zertifikat erstellen
- openERP Benutzer Account erstellen
- auf Laptop Unternehmens-Tools installieren
- GPG Private/Public Key erstellen und im OpenERP ablegen

BU
- Bei Praktikanten klären: Pflicht- oder freiwilliges Praktikum aus sozialversicherungsrechtl. Sicht

Neuer MA
- Personalstammblatt ausfüllen und zuschicken
- Unterlagen vorbereiten

1 Tag vor Eintritt

HR
- Dokumente 2x drucken (Vertraulichkeitserklärung, Datenschutzverpflichtung, Veröffentlichung), Checklist for new employees drucken

BO
- Werbematerial vorbereiten (T- Shirts, Tasse, Kugelschreiber)
- Überlassungsliste drucken

Erster Arbeitstag

HR

- Unterschriebenes Personalstammdatenblatt an BU schicken
- Begrüßung : Kollegen in Empfang nehmen und vorstellen
- Ankündigung des neuen Kollegen und der Projekte in denen er eingesetzt wird, in StatusNet und per Email
- in MediaWiki Tagebuch eintragen
- Checklist for new employees aushändigen und erläutern

BO

- Geschenk überreichen
- Handyvertrag übergeben
- Überlassungsliste unterschreiben lassen
- Termine weiterleiten/Einladungen

Buddy

- Büro und Verpflegungs-möglichkeiten erläutern
- Pausenregelungen und Sicherheitsrichtlinien erläutern
- Drucker erklären
- Ablageort der Vorlagen zeigen
- Unterstützung beim Ausfüllen der HR-Checkliste
- Arbeitszeiterfassung erklären
- Verwendung von Wiki, SVN, OpenERP und StatusNet erklären
- SVN Struktur erklären

BU

- Erfassen der MA-Stammdaten

Neuer MA

- Personalstammblatt unterschreiben
- Benötigte Dokumente Unterschreiben

1 - 6 Monate nach Arbeitsantritt

HR

- Einführungsgespräch (in Woche 1): Leitbild, Werte, Richtlinien, Eigenverantwortung, Projekt ab ersten Tag
- Zielvereinbarung zur Einarbeitung nach zwei Wochen
- Feedbackgespräch nach 2, 4 und 6 Monaten mit HR und PL
- Workshop for new employees (HR, openERP, Datenschutz, Geschäftsführer)
- Lean- Schulung

Buddy

- Verweis auf relevante Literatur (Wiki, Literaturverzeichnis im SVN)

IT

- Gespräch mit Datenschutzbeauftragtem

Neuer MA

- HR Checkliste vervollständigen

A.3. Projekt Beginn

Kurz vor Projektbeginn

Geschäftsführung
- SVN-Repository anlegen
- Projektmitarbeiter Schreib/Leserechte für das neue angelegte SVN-Repository geben

BO
- (Projekt in OpenERP anlegen)

Projektleiter
- (Projekt in OpenERP anlegen)
- Projekt im Wiki eintragen (optional)
- Projektmitarbeiter dem Projekt in OpenERP hinzufügen

A.4. Projekt Ende

Kurz nach dem Projektende

Geschäftsführung
- Allen Mitarbeitern nur noch lesenden Zugriff auf das SVN-Repository für das Projekt geben

BO
- Das OpenERP Projekt als abgeschlossen markieren

Projektleiter
- Alle evtl. angelegen Kundenkonten deaktivieren (z.B. für FTP)

A.5. Projekt Mitarbeiter Entfernen

Kurz nach dem Ausscheiden aus dem Projekt

IT
- Projektmitarbeiter nur noch Leserechte für das Projekt SVN-Repository geben

BO
- Projektmitarbeiter aus dem Projekt in OpenERP entfernen

A.6. Projekt Mitarbeiter Hinzufügen

Mitarbeiter wird zum Projekt hinzugefügt

IT
- Neuem Projektmitarbeiter Schreib/Leserechte für das Projekt SVN-Repository geben

BO
- Neuer Projektmitarbeiter dem Projekt in OpenERP hinzufügen

Literaturverzeichnis

[hei13] heisse.de. Erstes-freies-Active-Directory-Samba-4-ist-da, 2013. URL http://www.heise.de/newsticker/meldung/Erstes-freies-Active-Directory-Samba-4-ist-da-1766883.html.

[Med14] MediaWiki.org. MediaWiki, 2014. URL http://www.mediawiki.org/wiki/MediaWiki.

[Odo14] Odoo. OpenERP becomes Odoo, 2014. URL https://www.odoo.com/blog/Odoo-News-5/post/Odoo-The-New-OpenERP-156. (Zitiert auf Seite 13)

[Ope14a] OpenERP Dokumentation. API, 2014. URL https://doc.openerp.com/6.1/developer/12_api/. (Zitiert auf Seite 25)

[Ope14b] OpenERP Dokumentation. The ORM - Object-relational mapping, 2014. URL https://doc.openerp.com/v6.0/developer/2_5_Objects_Fields_Methods/orm/. (Zitiert auf Seite 25)

[Ope14c] OpenERP Dokumentation. Security in OpenERP: User, Groups, 26.07.2014. URL https://doc.odoo.com/trunk/server/04_security/.

[OT14] I. OpenVPN Technologies. OpenVPN - Open Source VPN, 2014. URL http://openvpn.net/. (Zitiert auf Seite 13)

[sam12] samba.org. Samba Team Releases Samba 4.0, 2012. URL https://www.samba.org/samba/news/releases/4.0.0.html. (Zitiert auf Seite 24)

[Str14] Strato. Mail - Professionelle Kommunikation und Terminplanung, 2014. URL https://www.strato.de/mail/. (Zitiert auf Seite 12)

[Wik14] Wikipedia. Active Directory, 2014. URL http://de.wikipedia.org/wiki/Active_Directory#Aufbau. (Zitiert auf Seite 23)

Alle URLs wurden zuletzt am 11. 10. 2014 geprüft.

Erklärung

Wir versicheren, diese Arbeit selbstständig verfasst zu haben. Wir haben keine anderen als die angegebenen Quellen benutzt und alle wörtlich oder sinngemäß aus anderen Werken übernommene Aussagen als solche gekennzeichnet. Weder diese Arbeit noch wesentliche Teile daraus waren bisher Gegenstand eines anderen Prüfungsverfahrens. Wir haben diese Arbeit bisher weder teilweise noch vollständig veröffentlicht. Das elektronische Exemplar stimmt mit allen eingereichten Exemplaren überein.

Ort, Datum, Unterschrift

Ort, Datum, Unterschrift

Ort, Datum, Unterschrift