Rechteverwaltung unter openCRX

Handbuch Version 0.7

openCRX Software v1.4.0

openCRX

Rechteverwaltung unter openCRX

Version 0.7
openCRX v1.4.0

Dieses Handbuch ist aus einer Version entstanden, die für kommerzielle Zwecke geschrieben wurde. Die verwendeten Screenshots stammen aus der kommerziellen Version und konnten aus Gründen des damit verbundenen Arbeitsaufwandes nicht durch Screenshots aus der openCRX Software Version ersetzt werden. Es gelten die nachfolgenden Bestimmungen einer BSD Lizenz.

Dokumentennummer: 511-004-1

Inhaltsverzeichnis

Teil I.

Einführung

Kapitel 1.

Über dieses Handbuch

Dieses Handbuch behandelt ausschließlich Funktion zur Rechteverwaltung innerhalb des openCRX Systems und ergänzt das *openCRX Handbuch*. Es gibt Ihnen eine Einführung in alle Verfahren und wichtige Hinweise, die für eine effiziente Arbeit mit der Rechteverwaltung erforderlich sind. Mit Hilfe dieses Handbuches werden Sie schnell in der Lage sein, Nutzern des CRM Systems individulle Rechte für den Umgang mit den erfassten Daten zu gewähren.

Diese Handbuch und die im Rahmen dieses Handbuches beschriebene Software werden im Rahmen einer BSD Lizenz bereitgestellt und dürfen nur in Übereinstimmung mit den Bedingungen dieser Lizenz benutzt werden. Diese Lizenzbedingungen, sind im Handbuch auf der zweiten Seite dokumentiert.

Alle in diesem Handbuch als Beispiel genutzten Angaben für Unternehmen oder Personen sind frei erfunden. Eventuelle Ähnlichkeiten mit tatsächlich existierenden Unternehmen oder Personen sind rein zufällig.

Zielgruppen

Dieses Handbuch richtet sich vor allem an Nutzer und Administratoren von openCRX, die an der Vergabe von individuellen Nutzerrechten und sicherheitsrelevanten Themen interessiert sind.

Es wird vorrausgesetzt, das der Leser mit der Bedienung der openCRX Software vertraut ist.

Version und Auflage der Dokumentation

Die Version der Auflage des Handbuches können Sie an Hand der Dokumentennummer auf Seite 2 erkennen. Die ersten drei Ziffern kennzeichnen das Dokument, die nachfolgenden drei Ziffern zeigen die Versionsnummer an. Die Versionsnummer wird bei jeder neuen Release der Software erhöht. Die nachfolgende Nummer indiziert die Auflage innerhalb einer Software Version.

1.1. Der Aufbau des Handbuches

Das Handbuch ist in folgende Hauptteile gegliedert:

- Einführung in die Grundlagen der Rechteverwaltung
- Rechtevergabe bei openCRX
- Beispiele

Es ist keinesfalls notwendig, dass Sie das gesamte Handbuch lesen oder alle Funktionen beherrschen müssen, um mit Rechten zu arbeiten. Mit den Hinweisen aus dem Kapitel 2 sollten Sie zuerst prüfen, ob eine Rechteverwaltung für Sie überhaupt interessant ist. Das Handbuch gibt Ihnen Hinweise, wie Sie beginnen können sich schrittweise in die Bedienung einzuarbeiten und wie Sie Ihre Arbeit effektiv gestalten können.

Während der Arbeit mit dem CRM System werden Sie erfahren wie nützlich die zahlreichen Funktionen zur Rechtevergabe für Sie sind und können bei Problemen jederzeit auf das Handbuch zurückgreifen.

Kapitel 2.

Grundlagen

Die Verwendung der Rechtevergabe hängt im Wesentlichen von der Anzahl der Nutzer und ihrer Unternehmensstruktur ab. Wenige Nutzer in kleinen Unternehmen haben wenige Anforderungen an eine Rechteverwaltung. Mit einer zunehmenden Anzahl von Nutzern steigt die Komplexität der Beziehungen im Unternehmen und es entwickelt sich in der Regel das Bedürfnis, Rechte zu vergeben und zu verwalten.

Die im CRM System vergebenen unterschiedlichen Rechte können einfach beschrieben werden:

- Wem werden bestimmte Daten angezeigt?
- Wer kann bestimmte Daten verändern?
- Wer kann bestimmte Daten löschen?

Rechtevergabe heißt im CRM System in erster Linie der Entzug von Rechten. Der Entzug von Rechten ist in der praktischen Arbeit mitunter hilfreich und notwendig. Hier ein paar Beispiele:

- Ein Vertriebsmitarbeiter, würde es sicher als unangenehm empfinden, wenn jemand anderes die Vertriebsdaten von seinen Kunden ohne sein Wissen ändert.
- Persönliche Informationen bleiben nur dann vertraulich, wenn für andere Mitarbeitern der Zugang gesperrt ist.
- Die Buchhaltung würde scheitern, wenn Vertriebsmitarbeiter Rechnungen im Nachhinein verändern könnten.
- Das Management möchte nicht, das Mitarbeiter die Budgetplanung einsehen können.
- Nur freigegebene Dokumente stehen dem Vertrieb zur Übergabe an den Kunden zur Verfügung.

- Der Produkt- oder Dienstleistungskatalog des Unternehmens wird nur von einer Person verändert.

Es sollten deshalb von vornherein immer nur solche Rechte vergeben werden, die auch wirklich notwendig sind.

Das Handbuch ist so aufgebaut, das es den Umgang mit der Rechteverwaltung an Hand von Beispielen erläutert, die zunehmend komplexer werden.

2.1. Rechteverwaltung nach Nutzerzahl

Alle Berechtigungen im CRM System werden nach dem Prinzip der Eigentümerschaft vergeben. Das heisst, dass jeder Eintrag in dem CRM System einen Eigentümer hat. Generell ist immer der Nutzer Eigentümer eines Eintrages, der einen Eintrag im CRM System erstellt hat.

Auf der Basis dieses Prinzips werden durch den Nutzer die Rechte vergeben. Diese Rechte werden genutzt, um die Fähigkeiten von Nutzern oder Nutzergruppen zu kontrollieren, Daten anzusehen, Daten zu löschen oder Daten zu verändern.

Das kann z.B. so aussehen:

- Nur der Nutzer „Produktmanager“ kann Produkte in der Produktliste Einfügen, Ändern oder Löschen,
- Jeder Nutzer aus der Nutzergruppe „Vertrieb“ kann die Kontaktdaten einsehen,
- Nur das Mangement hat Zugang zum Budget, usw.

In wie weit die Möglichkeiten des CRM Systems zur Rechtevergabe genutzt werden, hängt von den Bedürfnissen Ihres Unternehmens ab. Im Folgenden werden die Grundsätze an Hand der Nutzerzahl erläutert.

2.1.1. Rechteverwaltung für Einzelnutzer

Einzelnutzer brauchen keine Rechte verwalten. Sie haben und brauchen alle Rechte an den im CRM System eingegebenen Daten. Die Standardeinstellung zur Rechtevergabe des CRM Systems ist im Kapitel 7 beschrieben.

Trotzdem ist es zweckmäßig die Möglichkeiten der Rechtevergabe in den Grundzügen zu kennen. Das wird mitunter dann benötigt, wenn später weitere Mitarbeiter mit dem

CRM System arbeiten sollen. Insbesondere wird die Einarbeitung in das Thema Gruppen empfohlen, wie im Kapitel 2.2 beschrieben.

2.1.2. Rechteverwaltung für wenige Nutzer

Eine geringe Anzahl von Nutzern, die das CRM System gemeinsam unter einer Lizenz nutzen, sollten mit den einfachen Lösungen vertraut sein, welche die Rechtevergabe Ihnen bietet. Dazu zählen insbesondere:

- Verhindern, dass andere Mitarbeiter Informationen ansehen können: Damit läßt sich innerhalb des CRM Systems eine Privatsphäre aufbauen, in der ggf. persönliche Kontakte oder andere Informationen abgelegt werden.
- Verhindern, dass andere Mitarbeiter Informaionen löschen oder verändern: Damit wird gewährleistet, dass der Autor von Daten die Daten auch schützen kann.

Diese Art des Entzugs von Rechten kann durch jeden besitzenden Nutzer indivduell bei der Anlage der Daten oder während der Arbeit mit diesen Daten festgelegt werden. Die Standardeinstellung zur Rechtevergabe des CRM Systems ist im Kapitel 7 beschrieben.

In der Regel gibt es zwischen diesen Mitarbeitern keine ausgeprägte Hierachie, so dass eine komplexe Rechteverwaltung nicht aufgebaut werden muss. Sollte es jedoch erforderlich sein, Rechte an Daten feiner zu granulieren, sollte mit der Bildung von Gruppen, wie im Kapitel 2.2 beschrieben, begonnen werden. Jeder Nutzer sollte Mitglied von einer oder mehreren Gruppen werden, die mit bestimmten Rechten ausgestattet worden sind.

2.1.3. Rechteverwaltung für größere Anzahl von Nutzern

Will man eine größere Anzahl von Nutzern mit unterschiedlichen Nutzerrechten ausstatten, ist eine klare Struktur der Rechtevergabe notwendig. Sinnvoller Weise verbindet man darin Nutzerrechte mit der Stellung oder der Aufgabe im Unternehmen.

Eine Zusammenfassung von individuellen Nutzern in Gruppen mit identischen Rechten erleichtert den Aufbau einer strukturierten Rechtevergabe sowie deren Verwaltung und ist im nachfolgenden Kapitel erläutert. Die Standardeinstellung zur Rechtevergabe des CRM Systems ist im Kapitel 7 beschrieben.

Je nach Komplexität empfiehlt es sich, vor der Einführung von Rechten einen Plan zur Rechtevergabe zu erstellen und diesen mit den Nutzern abzustimmen.

2.2. Gruppen

Gruppen sind ein sehr effektives und wirksames Mittel, um Nutzer mit gleichartigen Rechten auszustatten. Solche Gruppen können im CRM System beliebig zusammengestellt werden.

Praktisch kann jede Art von Bezug als Basis einer Gruppe dienen, wie z.B.

- gemeinsamer Standort (z.B. alle Mitarbeiter einer Niederlassung)
- gemeinsame Aufgabe (z.B. alle Projektmitarbeiter)
- gemeinsame Position im Unternehmen (z.B. alle Vertriebsbeauftragte)
- Zugehörigkeitszeit zum Unternehmen (z.B. Probezeit)

Das Beispiel einer solchen Gruppe von Vertriebsmitarbeitern ist in der Abbildung 2.1 zu sehen. Hier bilden zwei Personen die Gruppe mit dem Namen „Team A“. Die Gruppe

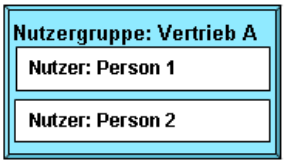

Abbildung 2.1.: Beispiel: Gruppe von Vertriebsmitarbeitern

kann mit bestimmten Rechten ausgestattet werden, die für alle Mitglieder dieser Gruppe gelten. Darüber hinaus kann jeder individuelle Nutzer für die Daten, die er erstellt, Rechte vergeben.

Um u.a. hierarchische Strukturen im Unternehmen abzubilden, können Gruppen wiederum Teil einer anderen Gruppe sein. In der Abbildung 2.2 ist dazu beispielhaft eine Vertriebsorganistion mit einem Vertriebsleiter und zwei Vertriebsteams gebildet worden. Die Gruppen mit dem Namen „Vertrieb A“ und „Vertrieb B“ und der „Vertriebsleiter“ als Person sind Mitglieder der Gruppe „Vertrieb“. Die Gruppe „Vertrieb“ als auch der Vertriebsleiter stehen hierarchisch über den Gruppen „Vertrieb A“ und „Vertrieb B“.

Darüber hinaus können einzelne Nutzer als auch Gruppen, auch Mitglied in verschiedenen Gruppen sein. In der Abbildung 2.3 ist zu sehen, das der Nutzer mit dem Namen „Person 4“ gleichzeitig Mitglied der Gruppen mit dem Namen „Vertrieb A“ und „Vertrieb B“ ist. Das wäre z.B. sinnvoll, wenn die „Person 4“ die Urlaubsvertretung eines Mitarbeiters aus dem Team A übernimmt.

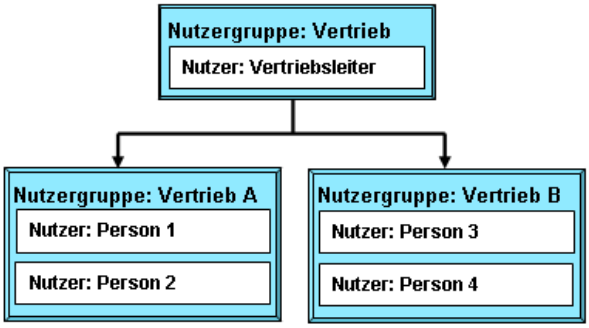

Abbildung 2.2.: Beispiel: Hierarchische Gruppenorganisation

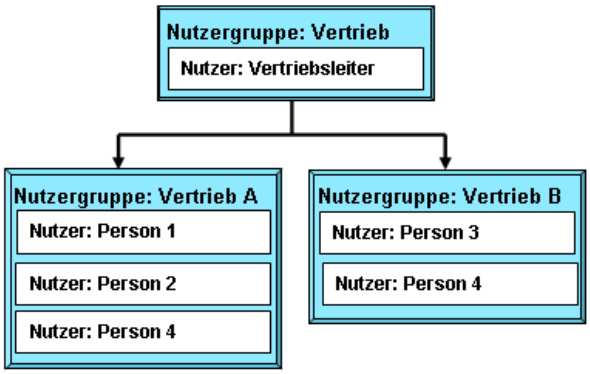

Abbildung 2.3.: Beispiel: Ein Nutzer in mehreren Gruppen

Die Abbildung 2.4 zeigt in einer anderen Darstellungsform ein Beispiel, in der eine Gruppe mit dem Namen „Vertriebsassistenz“ mit 2 Nutzern („Person 5 und 6“) gleichzeitig Mitglied der Gruppen mit dem Namen „Vertrieb A“ und „Vertrieb B“ ist.

In diesem Beispiel sehen Sie vier Gruppen mit 6 Mitgliedern in drei Hierarchiestufen.

Das CRM System erlaubt Ihnen jede Art von Gruppen und Nutzern beliebig miteinander zu kombinieren und praktisch damit jede Art von Strukturen in der Rechtevergabe aufzubauen.

2.3. Rechtevergabe

2.3.1. Berechtigungsarten

Im Detail sind für Berechtigungen die folgenden Angaben relevant:

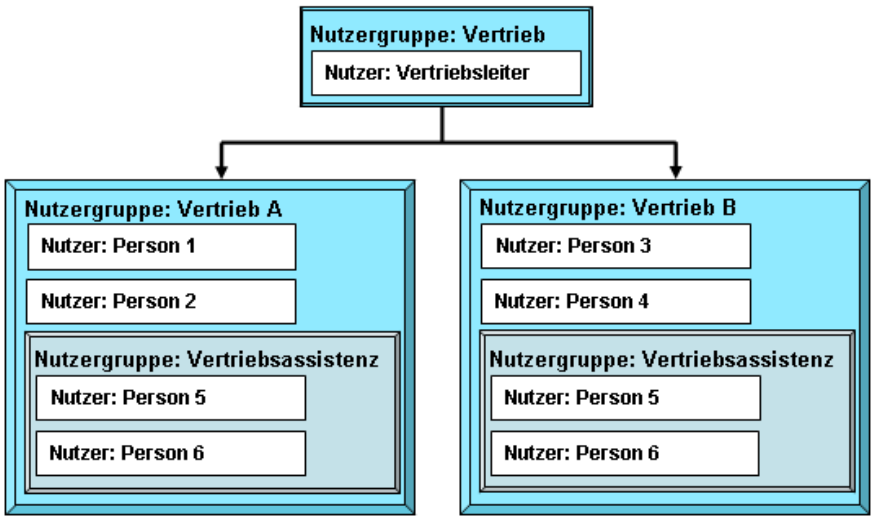

Abbildung 2.4.: Beispiel: Zuordnung einer Gruppe zu mehreren Gruppen

- **Besitzender Nutzer:** Das ist die Festlegung, welcher Nutzer einen Daten Eintrag „besitzt“. Dieser Nutzer kann jederzeit die Daten ansehen, löschen oder verändern. Es ist dem Administrator auch möglich, allen Nutzern den Zugang zu Daten zu sperren.
- **Besitzende Nutzergruppe:** Das ist die Festlegung, welche Nutzergruppen gemeinsam Rechte für einem Zugang zu den Daten besitzt. Darin können z.B. besondere Privilegien eingeschlossen sein.
- **Berechtigung zum Ansehen:** Mit dieser Angabe wird festgelegt, welche Nutzer oder Nutzergruppen sich Daten ansehen können.
- **Berechtigung zum Löschen:** Mit dieser Berechtigung wird festgelegt, welcher Nutzer oder welche Nutzergruppe Daten löschen können.
- **Berechtigung zum Verändern:**Mit dieser Berechtigung wird festgelegt, welchem Nutzer oder Nutzergruppe das Recht eingeräumt wird, Daten zu verändern. Das schließt das Recht ein, zusätzliche Daten zu einem Datensatz hinzuzufügen (wie z.B. Adressen zu einem Kontakt).

Hinweis: Die Berechtigung zum Löschen von Daten schließt die hierachisch untergeordneten Daten mit ein. Wenn z.B. ein Kontakt gelöscht wird, werden auch die Adressen, Notizen, Dokumente usw., die für diesen Kontakt spezifisch erfaßt wurden, mit gelöscht. Aus diesem Grund ist es zu empfehlen, die Berechtigung zum Löschen anderen Nutzeren oder Nutzergruppen nur in Ausnahmefällen zu erteilen.

2.3.2. Berechtigungsniveaus

Die folgenden Berechtigungsniveaus sind auswählbar:

- **0 - N/A:** kein Zugang zu den Daten
- **1 - privat:** Zugang zu den Daten hat nur der Eigentümer
- **2 - normal:** der Zugang zu den Daten ist möglich, wenn:
  - a) der Nutzer Eigentümer der Daten ist, **oder**
  - b) der Nutzer Mitglied irgendeiner Nutzergruppe ist, die Eigentümer der Daten ist, **oder**
  - c) irgendeine Nutzergruppe, die Eigentümer der Daten ist, ist eine Untergruppe von irgendeiner Gruppe, zu der der Nutzer gehört
- **3 - erweitert:** der Zugang zu den Daten ist möglich, wenn:
  - a) der Nutzer Eigentüer der Daten ist, **oder**
  - b) der Nutzer Mitglied irgendeiner Nutzergruppe ist, die Eigentümer der Daten ist, **oder**
  - c) irgendeine Nutzergruppe, die Eigentümer der Daten ist, ist eine Untergruppe von irgendeiner Gruppe, zu der der Nutzer gehört, **oder**
  - d) irgendeine Nutzergruppe, die Eigentümer der Daten ist, ist eine Untergruppe von irgendeiner Obergruppe einer Gruppe, zu der der Nutzer gehört
- **4 - global:** Allen Nutzer ist der Zugang möglich.

Untergruppe: Eine Untergruppe von einer Gruppe „A“, die Eigentümer von Daten ist, ist eine Gruppe die Mitlied der Gruppe „A“ ist.

Obergruppe: Eine Obergruppe von einer Gruppe „A“, die Eigentümer von Daten ist, ist eine Gruppe in welcher die Gruppe „A“ Mitglied ist.

Teil II.

Rechtevergabe bei openCRX

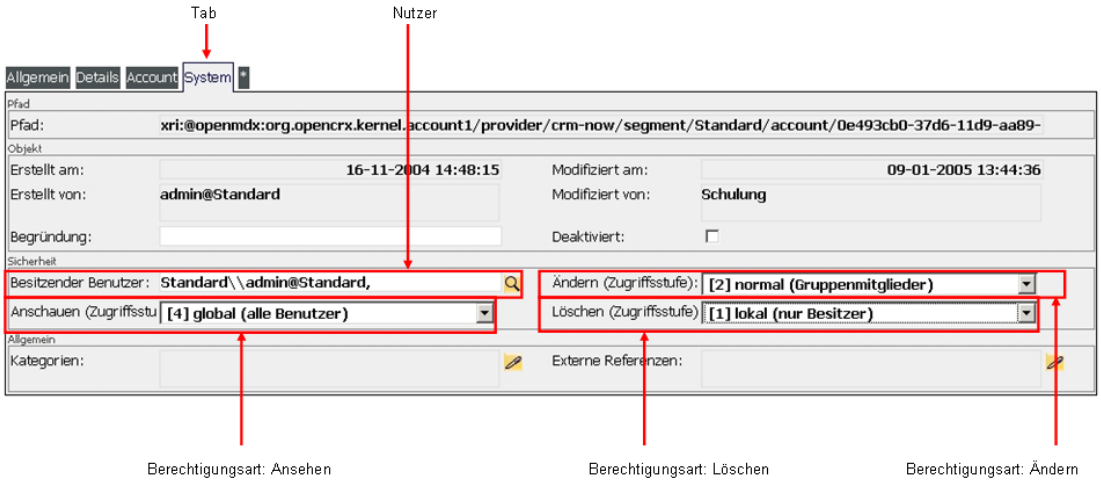

Abbildung 2.5.: Datensatz: System

Jedes mal, wenn Sie Daten im CRM System erfassen, werden diese mit Standardrechten ausgestattet, wie im nachfolgenden Kapitel beschrieben. Veränderungen der Einstellungen zur Rechtevergabe an Daten werden üblicher Weise bei der Erstellung eines Datensatzes vorgenommen, können aber auch später geändert werden.

Für die Einstellung der Nutzerrechte klicken Sie auf *Bearbeiten* und gehen Sie zu dem Tab „System“ in Ihrem Datensatz und Sie sehen ein Eingabefenster wie es in der Abbildung 2.5 ausschnittsweise zu sehen ist.

In der Abbildung sehen Sie die Eingabefelder für zur Einstellung der Rechte. Mit Hilfe der Lupe hinder dem Eingabefeld „Besitzende Benutzer“ können Sie den Besitzer des Datensatzes festlegen. Die anderen Eingabefelder dienen zum Setzen der Berechtigungen, wie im Kapitel 2.3.1 beschrieben.

Kapitel 3.

Datenstrukturen

Die in openCRX gepeicherten Daten sind hierarchisch zusammengestellt um Ihnen ein möglichst schnelle und zweckmässige Bedienung zu ermöglichen. So können z.B. Adressdaten zu einem Kontakt hinzugefügt werden. Die Adressdaten gehören damit zu diesem Kontakt und können nur über diesen Kontakt verändert oder gelöscht werden. Diese hierachische Ordnung wird bei der Rechtevergabe berücksichtigt.

In der Abbildung 3.1 sehen Sie einen Bildschirmausschnitt zu einem Kontakt. Dieser soll hier beispielhaft herangezogen werden, um das Prinzip der Abhängigkeit der Rechtevergabe von den Datenstrukturen und die Konsequenzen daraus zu erläutern.

Die in der Abbildung 3.1 als „Inspektor“ gekennzeichnet Daten, wurden bei der Erstellung dieses Kontaktes generiert. Alle weiteren Daten, wie sie unter Adressen, Partner, Kontakte usw. im unteren Teil der Abbildung eingegeben werden können, sind als „Untergeornete Daten“ bezeichnet, da sie den Daten im Inspektor untergeordnet sind.

Das ist, wie leicht einzusehen ist, sehr sinnvoll, da die untergeordneten Daten nur für diesen Kontakt gültig sind. Diese Abhängigkeit wird bei der Rechtevergabe durch ein rekursives Verfahren berücksichtigt.

Dieses Verfahren sagt aus, dass Rechte an übergeordneten Daten auf untergeornete Daten übertragen werden.

Zur Illustration ist in der Abbildung 3.2 eine Datenstruktur für einen Kontakteintrag mit Telefonnummer bezogen auf die beispielhafte Vertriebsstruktur aus dem Kapitel 10, Abbildung 10.1 dargestellt:

Die Telefonnummer und die E-Mail sind dem Kontakteintrag untergeordnet. Mit dem vergebenen Rechten, ist es in Bezug auf die Abbildung dem Nutzer „Person 1“ nicht möglich den Eintrag der E-Mail direkt zu löschen, da diese von der „Person 2“ vorgenommen wurde, und die Berechtigung auf „1-privat“ gesetzt wurde.

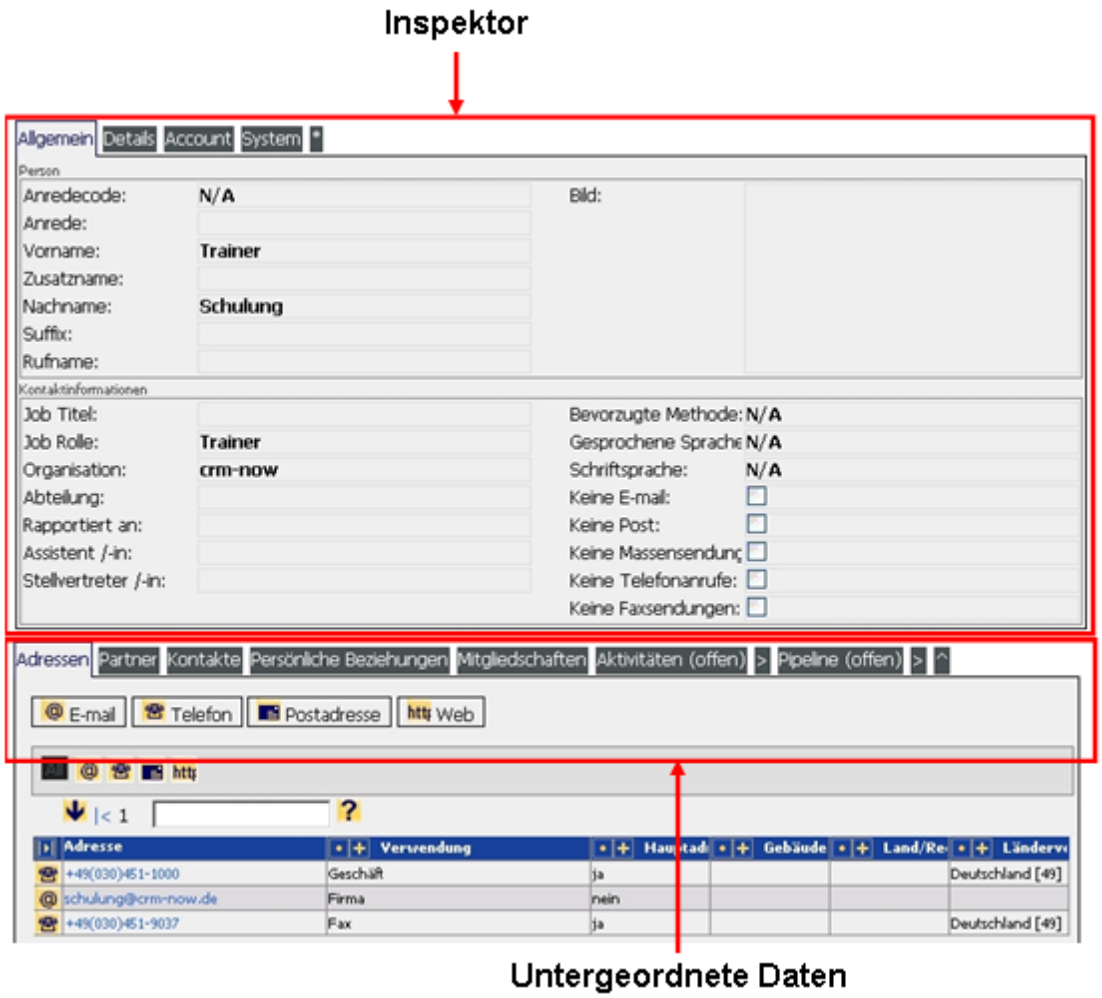

Abbildung 3.1.: Datenstruktur für Kontakt

Es gilt jedoch zu beachten, dass der Nutzer „Person 1“ auf Grund der Rechte an dem gesamten Kontakt die Berechtigung hat, diesen gesamten Kontakt zu löschen. Das schließt die E-Mail Adresse mit ein.

Dieses, als rekursives Verfahren, bezeichnete Prinzip ist für alle Einträge im CRM System gültig und ein praktisches Mittel, die Vergabe von Berechtigungen zu rationalisieren.

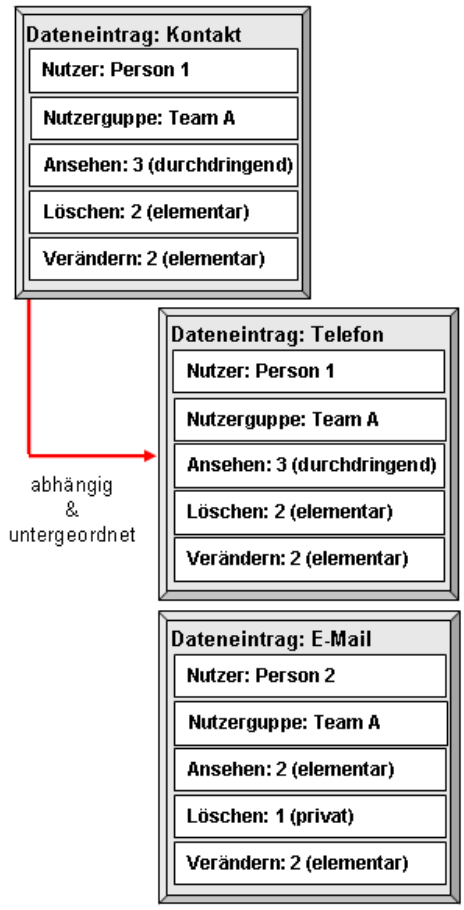

Abbildung 3.2.: Beispiel für Datenstruktur Kontakt

Hinweis: Das für die Nutzung am kritischsten zu betrachtende Benutzerrecht ist das „Löschen“. Jeder Löschvorgang wirkt rekursiv und kann, wenn das nicht beachtet wird, sich auf Daten auswirken, die man eigentlich nicht löschen will. Gelöschte Daten sind durch das CRM System automatisch nicht mehr herstellbar. Um Daten wieder herzustellen, kann u.U. das Backup der Daten genutzt werden.

Sinngemäß kann man das Prinzip der Rechtevergabe in Abhängigkeit von der Datenstruktur für alle abgespeicherten Daten, die hierachisch organisiert sind, übertragen.

Kapitel 4.

Administration

Ausgangspunkt für die Rechtevergabe sind die Nutzerlogins. Jedes Login stellt einen Zugang zum CRM System her, der mit bestimmten Rechten ausgestattet ist. Diese Rechte können durch einen Administrator in Ihrem Unternehmen festgelegt werden. Ihr openCRX Login könnte sich z.B. wie folgt zusammensetzen:

Nutzername-Unternehmensteil
Passwort

Nutzernamen und Unternehmensteil werden von Ihnen individuell ausgesucht. Zusätzlich, zu den von Ihnen ausgewählten Namen, gibt es als Lizenznehmer die Zugangsdaten für einen Nutzer „admin“, in diesem Beispiel mit dem Namen:

admin-Unternehmensteil
Passwort

Mit dem Nutzernamen **admin-Unternehmensteil** und dem dazugehörenden Passwort haben Sie einen besonderen Zugang zu dem CRM System mit dem Sie die Rechte der anderen Logins verwalten können.

In der folgenden Abbildung 4.1 ist das Prinzip graphisch dargestellt. Hier werden die Logins mit dem Ausdruck „Nutzernamen“ beschrieben. Für jeden Login gibt es einen Nutzernamen. Der Administrator mit dem Login Namen „admin-Unternehmensteil“ kann diesem eine Rolle, z.B. die Funktion im Unternehmen zuweisen.

Diese Rolle wird dann mit Berechtigungen versehen. Folglich hat jeder Nutzer eine Rolle (z.B. Vertriebsmitarbeiter), die mit Berechtigungen versehen ist.

Die Rechte des Nutzers „admin-unternehmensteil“ werden beim Einrichten vergeben und können von Nutzern nicht verändert werden.

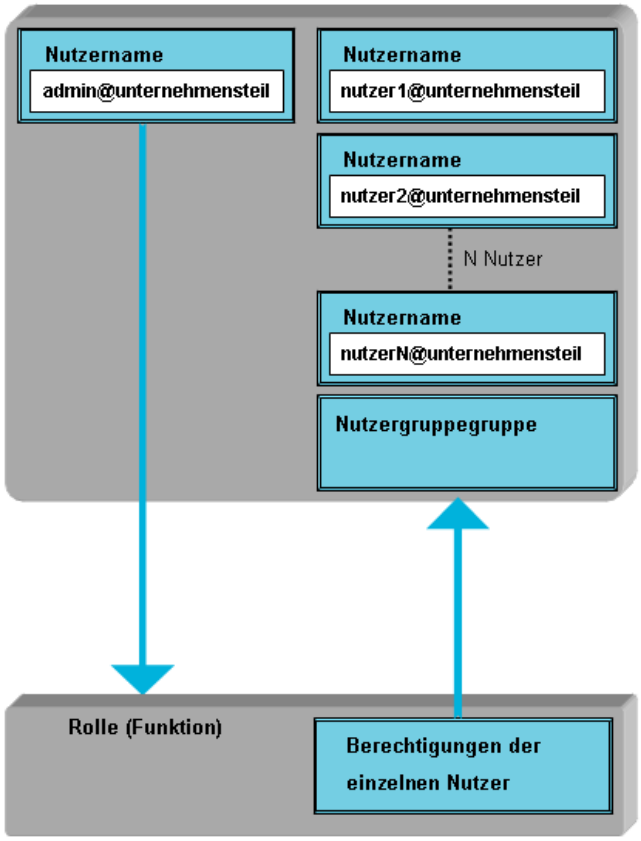

Abbildung 4.1.: Die Rolle von Nutzern

4.1. Nutzer

Als reale Person werden die konkreten Anwender des CRM Systems bezeichnet. Jede reale Person kann mit einem oder mehreren Nutzernamen verbunden sein und unter verschiedenen Nutzernamen Zugang zum CRM System bekommen. Das hat folgenden Hintergrund. Eine reale Person, wie z.B. Herr Meier, kann mehrere Funktionen innerhalb des Unternehmens haben, wie z.B. Leiter Vertrieb und gleichzeitig auch Mitglied des Unternehmensmanagements.

Mit der Zuordnung von realen Personen zu verschiedenen Nutzernamen kann das CRM System berücksichtigen, dass diese unterschiedlichen Funktionen mit unterschiedlichen Rechten versehen sind. In Abhängigkeit von seiner Aufgabe, kann Herr Meier damit seine unterschiedlichen Rechte wahrnehmen. Wenn Herr Meier das Budget kontrollieren möchte, loggt Herr Meier sich als Mitglied der Unternehmensleitung ein. Wenn er mit seinem Vertrieb arbeiten möchte, benutzt er seinen Login als Vertriebsleiter.

Hinweis: Für jedem Nutzer sind im CRM System die Zugangsdaten so abgelegt, dass es möglich ist, auch für verschieden Nutzernamen das gleiche Passwort zu benutzen.

4.1.1. Homepage

Jeder Login, d.h. jeder Nutzername führt automatisch auf eine individuelle Homepage. Ob andere Nutzer diese Seite auch sehen können, hängt von der Rechtevergabe ab. Verschiedene Logins führen zu einer eigenen Homepages.

Das ist inbesonders dann zweckmässig, wenn ein Nutzer das CRM System entsprechend der individuellen Funktion im Unternehmen zu verschiedenen Zwecken nutzt. Über die History kann bei jedem Login sofort gesehen werden, was zuvor mit dem CRM System gemacht wurde und schnell an vorrangegangenen Arbeiten angeknüpft werden. Hat ein Nutzer zwei Funktionen im Unternehmen, kann er eine Historie nutzen um z.B. seine Aktivitäten als Mitglied der Unternehmensleitung nachzuverfolgen, eine andere Historie als Vertriebsleiter nutzen.

Hinweis: Bitte denken Sie daran, dass die Historie eines vorrangegangen Logins nur dann richtig dargestellt wird, wenn man zuvor einen korrekten Logout (mit dem Button an der obern rechten Ecke des Bildschirms) durchgeführt hat. Mit dem Logout wird die Historie gespeichert und steht bei einem neuen Login wieder zur Verfügung.

Teil III.

Hinweise für Nutzer

Kapitel 5.

Wichtige Empfehlungen

Das CRM System unterscheidet zwischen Nutzern und dem Administrator. Zwischen beiden sollten Sie eine klare Aufgabentrennung festlegen.

In der Praxis hat es sich bewährt, dass Sie als Nutzer sich bei der Vergabe von Zugangsrechten ausschließlich darauf beschränken, die von Ihnen angelegten oder verwalteten Daten zu betreuen.

Einzelnutzer oder wenige Nutzer, denen nicht hierarchisch im CRM System Rechte zugewiesen werden sollen, benötigen keinen Administrator.

Bei einer größeren Nutzerzahl sollte es ausschließlich der Administrator übernehmen, gemeinsame Nutzer mit gleichwertigen Zugangsrechten in Gruppen zusammenzufassen und eine hierarchische Struktur aufzubauen.

Kapitel 6.

Fehleranzeige

Der Besitzer eines Datensatzes kann den anderen Nutzern Zugangsrechte entziehen. Besitzen Sie z.B. nicht das Recht Kontaktinformationen zu verändern, so können Sie das auch nicht tun. Versuchen Sie ein Zugangsrecht in Anspruch zunehmen, welches Ihnen durch den Besitzer der Daten nicht erteilt wurde, meldet das CRM System einen Fehler, wie in der Abbildung 6.1 zu sehen.

Abbildung 6.1.: Fehlermeldung

Die Ursache des Fehlers, wird am unterem Bildschrimrand angezeigt, wie in der Abbildung 6.2 zu sehen.

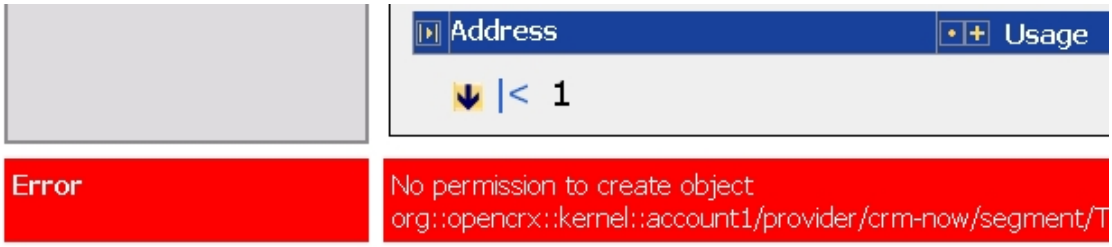

Abbildung 6.2.: Fehlermeldung

„No Permission“ heißt, das Sie nicht das Recht hatten, die Handlung (z.B. einen Datensatz verändern) auszuführen. Sie können zu dem Datensatz unter dem Tab *System* die zu diesem gehörenden Rechte und Besitzer einsehen, um die Ursache des Verbots zu ermitteln.

Kapitel 7.

Voreinstellungen bei openCRX

openCRX setzt für Sie immer bereits automatisch Standardberechtigungen, wenn Sie einen neuen Satz Daten anlegen.

Diese Berechtigungen sind wie folgt festgelegt:

- Besitzender Nutzer: der Nutzer, der die Daten anlegt
- Besitzende Gruppe: die primäre Nutzergruppe („Primary user group“), die dem Nutzer zugeordnet wurde, als dieser durch den Systemadminstrator angelegt wurde
- Berechtigung zum Ansehen: 3 (erweitert)
- Berechtigung zum Löschen: 2 (normal)
- Berechtigung zum Verändern: 2 (normal)

In der Praxis brauchen Einzelnutzer oder eine kleine Anzahl von Nutzern ohne hierarchischer Struktur diese Einstellungen in der Regel nie verändern. Automatisch wird als besitzender Nutzer, der Nutzer erfasst, der die Daten anlegt. Da keine verschiedenen Gruppen existieren, braucht die Gruppenzugehörigkeit nicht betrachtet werden und die gesetzten Standardberechtigungen zum Ansehen, Löschen oder Verändern geben allen gemeinsamen Nutzern die gleichen Rechte.

Wollen Sie die Rechte der anderen gemeinsamen Nutzer beschränken, setzen Sie die Rechte für Ansehen, Löschen oder Verändern auf 1 (privat).

Auch nach der Einführung von Nutzergruppen für größere Organisationen, wird es selten notwendig sein, von den Standardrechten abzuweichen. Der Administrator kann durch eine sorgfältige Zusammenstellung von Nutzergruppen darauf hinwirken. Dem entsprechende Hinweise finden Sie im Kapitel IV.

Teil IV.

Hinweise für den Administrator

Administrative Aufgaben entstehen in der Regel nur dann, wenn die Rechte der einzelnen Nutzer beschränkt werden sollen. Das geschieht vor allem durch eine Zuordnung einzelner Nutzer zu verschiedenen Gruppen, wie im Kapitel 2.2 erläutert wurde.

Hinweis: Um admininstrative Aufgaben wahrnehmen zu können, müssen Sie sich als Administrator einloggen.

Im Folgenden wird beschrieben, wie ein Admininstrator mit openCRX Gruppen bilden kann. Es sein nochmals darauf hingewiesen, dass eine Gruppenbildung nur dann sinnvoll sein kann, wenn hierarchische Strukturen in openCRX aufgebaut werden sollen.

Kapitel 8.

Gruppen organisieren

Die Organisation einer gruppenbasierten Rechtevergabe, erfordert im wesentlichen drei Arbeitsschritte:

- Gruppen bilden: Die sich aus Hierarchie ergebende erforderlich Anzahl von Gruppen muss definiert werden.
- Gruppen ordnen: Die Gruppen müssen entsprechend ihrer heirarchischen Ordnung sortiert werden.
- Gruppenmitglieder zuordnen: Den einzelnen Gruppen müssen Nutzer zugeordnet werden.

In Abhängigkeit von der Anzahl der Gruppen und Nutzer des CRM Systems, können damit zahlreiche Eingaben verbunden sein. Um die Arbeit organisieren zu helfen, sind im Kapitel 9 entsprechende Hinweise zu finden.

8.1. Neue Gruppen bilden

Um neue Gruppen zu bilden, müssen Sie als Administrator angemeldet sein. Klicken Sie auf den Menüpunkt „Security User / Gruppen“ auf der linken Seite des Bildschirms auf Ihrer Startseite. Es öffnet sich das in der Abbildung 8.1 zu sehende Fenster.

In der Abbildung sehen Sie, dass bereits der Administrator (admin-Tseg) und die Nutzer „User1 Testuser“ bis „User4 Testuser“ angelegt worden sind.

Hinweis: Der Administrator hat keine Rechte, neue Nutzer anzulegen.

Um eine neue Gruppe zu bilden klicken Sie auf den Button *Lokale Benutzergruppe*. Es öffnet sich das in der Abbildung 8.2 zu sehende Fenster.

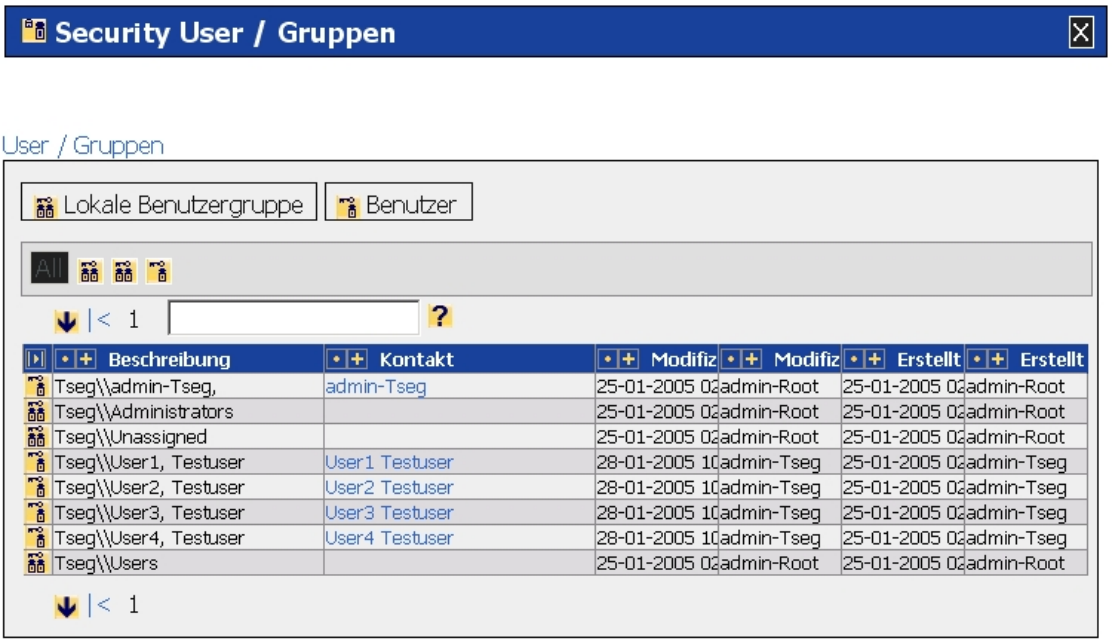

Abbildung 8.1.: Security User / Gruppen

Wie in der Abbildung beispielhaft zu sehen, geben Sie der Gruppe einen Namen und fügen ggf. weitere Informationen hinzu. Klicken Sie auf *Speichern*, um die Angaben zu sichern.

Hinweis: Wiederholen Sie diesen Vorgang für jede Gruppe, die Sie anlegen wollen.

Als Ergebnis erhalten Sie eine Liste von neuen Gruppennamen, die für die weitere Verwendung im CRM System zur Verfügung stehen,

Abbildung 8.2.: Lokale Benutzergruppe

8.2. Gruppen hierarchisch ordnen

In der Abbildung 8.3 ist zu sehen, dass bezogen auf die Abbildung 8.1 vier neue Gruppen („Vertrieb“, „Vertrieb A“, „Vertrieb B“ und „Vertriebsassistenz“) entsprechend der Anweisungen aus dem Kapitel 8.1 gebildet worden sind.

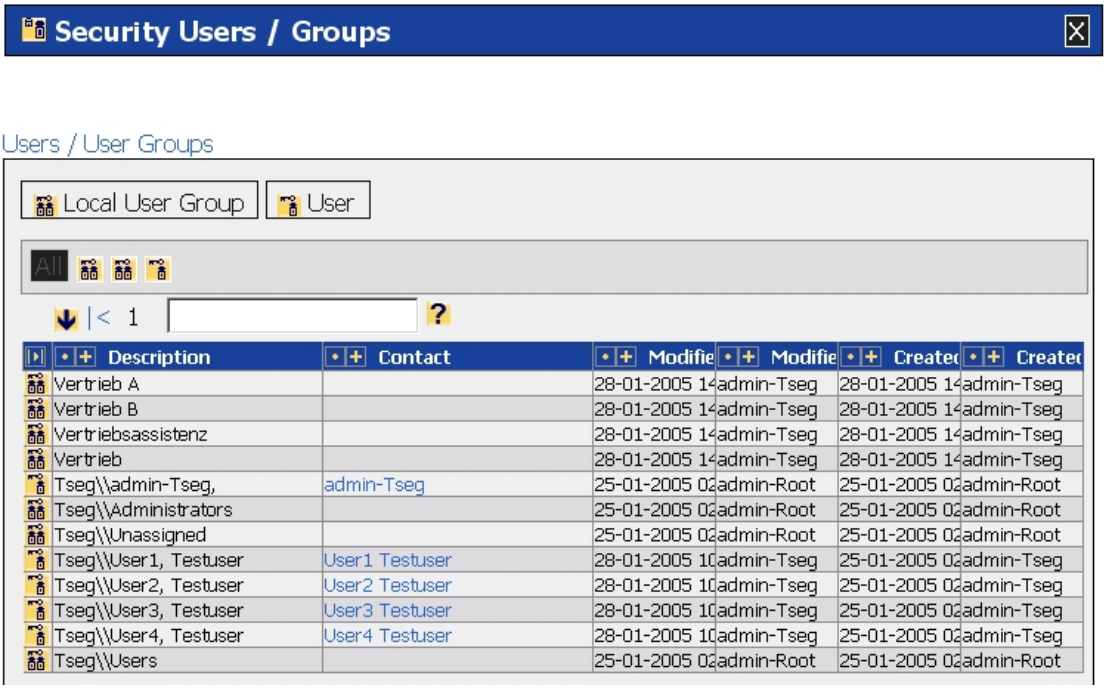

Abbildung 8.3.: Übersicht der existierenden Gruppen

Um die Gruppen hierarchisch zu ordnen, klicken Sie auf das Icon am Anfang der Zeile mit der gelisteten Gruppe, um diese zu öffnen. Für die Beispielgruppe „Vertrieb“, öffnet sich das in der Abbildung 8.4 gezeigte Fenster.

Im unteren Teil können Sie mit der Hilfe der Lupe weiter Gruppen auswählen, in den die Gruppe „Vertrieb“ Mitglied ist. In dem Beispiel wurde das bereits für die Gruppen „Vertrieb A“ und „Vertrieb B“ gemacht.

Hinweis: Wiederholen Sie diesen Vorgang für jede Gruppe, denen Sie eine Mitgliedschaft in anderen Gruppen einräumen wollen.

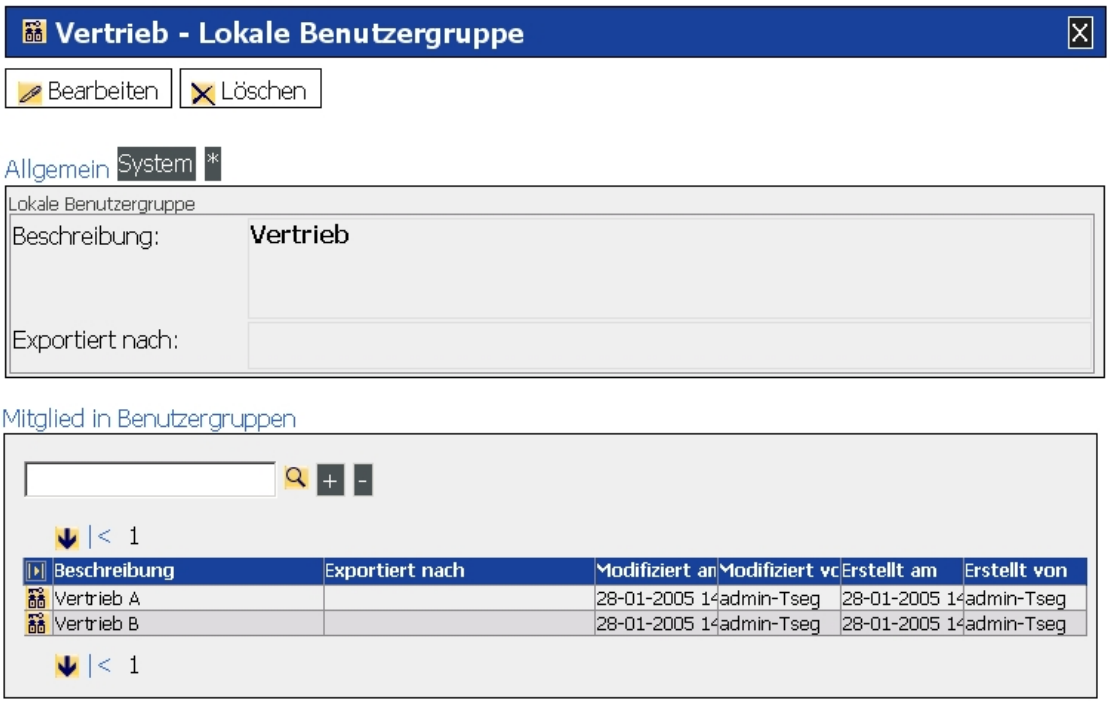

Abbildung 8.4.: Lokale Gruppe Vertrieb

8.3. Gruppenmitglieder zuordnen

Jeder Nutzer kann einer Gruppe zugeordnet werden. Bitte beachten Sie, das jeder Nutzer bereits Mitglied einer Gruppe mit dem Namen „...Users“ ist, und das in der Regel auch bleiben muss. Die Gruppe beinhaltet alle Nutzer und wurde beim Einrichten des CRM Systems angelegt.

Um in Bezug auf die Abbildung 8.3 einer Gruppe einen Nutzer zuzuordnen, klicken Sie auf das Icon in der ersten Spalte der Zeile, in welcher der Nutzer gelistet ist. Es öffnet sich das in der Abbildung 8.5 gezeigte Fenster.

Mit Hilfe der Lupe können Sie dem Nutzer weitere Gruppenmigliedschaften zuweisen, wie es in der Abbildung bereits für die Gruppe „Vertrieb“ gemacht wurde. D.h. auch, dass ein Nutzer Mitglied von mehreren Gruppen sien kann, wie bereit im Kapitel 2.2 erläutert.

Hinweis: Wiederholen Sie diesen Vorgang für jeden Nutzer, dem Sie eine Mitgliedschaft in einer Gruppe einräumen wollen.

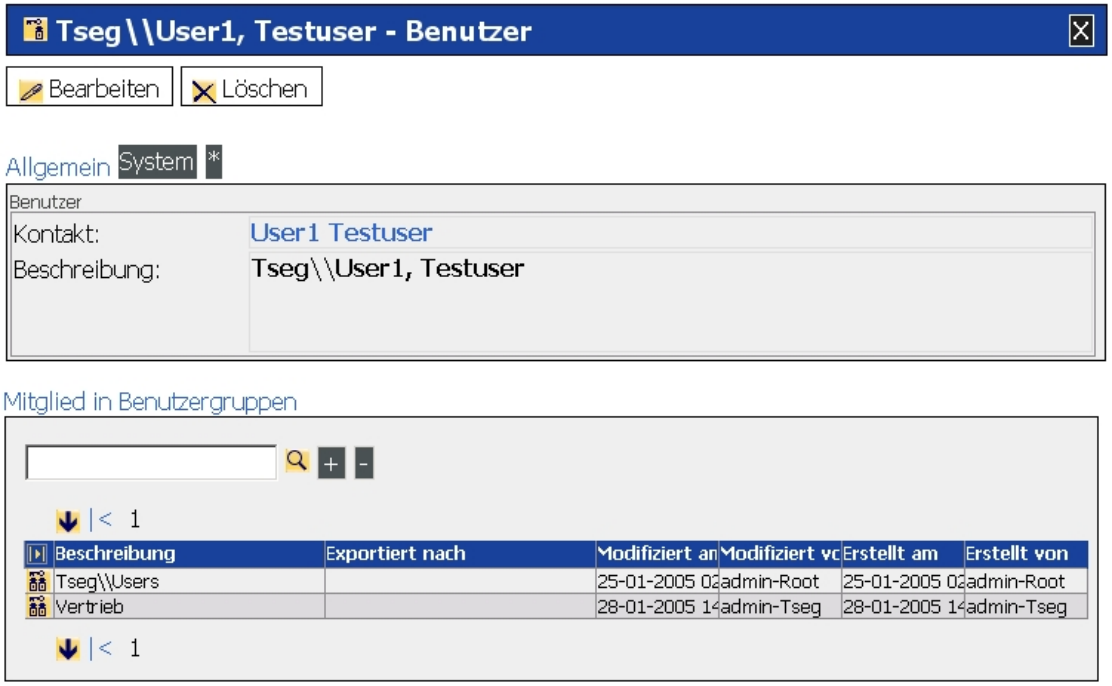

Abbildung 8.5.: Gruppenmitgliedschaft eines Nutzers

Kapitel 9.

Praktische Tips

Bevor der Administrator Gruppen einrichtet, sollte er sich Hilfsmittel schaffen, um die Übersicht zu behalten und Fehler zu vermeiden.

Es ist zu empfehlen, sich eine Skizze des hierarchischen Aufbaus der Rechtevergabe an die einzelnen Nutzer zu machen. Das soll hier am Beispiel der schon im Kapitel 2.3 erläuterten Abbildung 9.1 gemacht werden.

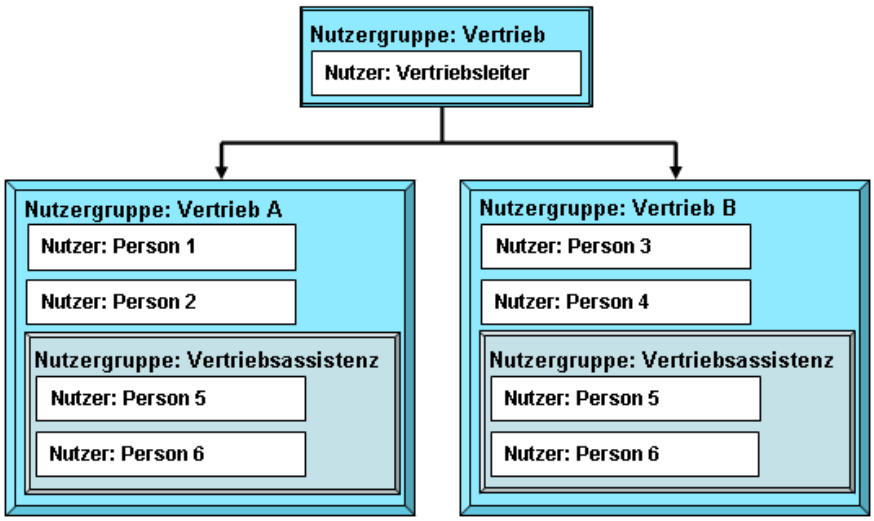

Abbildung 9.1.: Beispielhafte Gruppenzuordnung

Diese Abbildung spiegelt eine hierarchische Struktur wieder, in der die Personen aus der Vertriebsassistenz beiden Vertriebsgruppen gleichermaßen zur Verfügung stehen und innerhalb der Gruppen mit gleichen Rechten ausgestattet werden sollen.

Um diese Struktur in openCRX umzusetzen, haben sich folgende Arbeitsschritte bewährt:

1. Ermittlung der Anzahl der benötigten administrativen Gruppen
2. Eindeutige Namensvergabe an diese Gruppen
3. Ermittlung der Beziehungen zwischen den Gruppen
4. Zuordnung der Nutzer zu diesen Gruppen

Bezogen auf die Abbildung fig:EineGruppeTeilVonMehrerenGruppen ergibt sich die Zusammenstellung, wie in Abbildung 9.2 zur sehen.

Gruppenname	Hierarchiestufe	Nutzer
Vertrieb	1	Vertriebsleiter
Vertrieb A	2	Person 1
		Person 2
Vertrieb B	2	Person 3
		Person 4
Vertriebsassistenz	3	Person 5
		Person 6

Abbildung 9.2.: Tabelle Vertriebsgruppen

Mit Hilfe der Hierarchiezuordnung bestimmen Sie welche Gruppe Teil einer anderen Gruppe sein wird. In Bezug auf die Abbildung ergibt sich die folgende Zuordnung:

- Die Gruppe „Vertrieb A“ ist Mitglied in der Gruppe „Vertriebsassistenz“
- Die Gruppe „Vertrieb B“ist Mitglied in der Gruppe „Vertriebsassistenz“
- Die Guppe „Vertrieb“ ist Mitglied in den Gruppen „Vertrieb A“ und „Vertrieb B“
- Weder die Gruppen „Vertrieb A“, „Vertrieb B“ noch die Gruppe „Vertriebsassistenz“ sind Mitglied der Gruppe „Vertrieb“

Wie in openCRX die Gruppen angelegt und wie die Gruppenmitglieder zugeordnet werden, ist im Kapitel 8.1 gezeigt. Weitere Beispiele finden Sie im Kapitel V

Teil V.

Beispiele

Kapitel 10.

Beispiel Vertriebsgruppe mit individuellen Nutzern

Für das Setzen von Nutzerrechten ist es in den meisten Fällen zweckmäßig, die Struktur eines Unternehmens heranzuziehen. Die Abbildung 10.1 zeigt dafür ein Beispiel für eine Vertriebsorganisation. Um diese Organisation mit dem CRM System bedienen zu können, benötigen Sie 5 Nutzerzugänge.

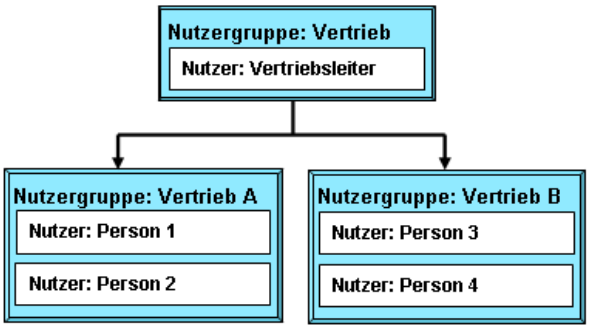

Abbildung 10.1.: Beispiel: Vertriebsgruppe

In unserem Beispiel gibt es 2 Vertriebsteams (Vertrieb A und Vertrieb B) mit je 2 Mitarbeitern (Person 1, Person 2, Person 3, Person 4). Vertrieb A und Vertrieb B sind zwei Nutzergruppen, die hierarchisch auf gleicher Stufe stehen. Den Teams übergeordnet gibt es einen Nutzer Vertriebsleiter, der zur Gruppe Vertrieb gehört.

Wie zuvor schon festgestellt, werden Nutzerrechte auf der Basis von Eigentumsrechten gesetzt. Folglich ist es für das Setzen von Nutzerrechten an bestimmten Daten entscheidend, wie der Nutzer in der Hierarchie des Unternehmens plaziert ist.

An Hand eines Eintrages durch die Person 1 in „Accounts“, werden nachfolgend verschiedene Szenarien erläutert.

1. Szenario
Die Daten sollen von allen Mitgliedern von „Vertrieb A“ und vom Vertriebsleiter angesehen werden können. Nur der Mitarbeiter (Person 1), der die Daten erstellt hat, darf sie auch löschen, kann sie ansehen und verändern.

Setzen der Berechtigungen für den Account Eintrag:

- Besitzender Nutzer: Person 1
- Besitzende Gruppe: Vertrieb A
- Berechtigung zum Ansehen: 3 (erweitert)
- Berechtigung zum Löschen: 1 (lokal)
- Berechtigung zum Verändern: 1 (lokal)

2. Szenario
Die Daten sollen von allen Mitgliedern von Vertrieb A angesehen und verändert werden können. Nur der Mitarbeiter (Person 1), der die Daten erstellt hat, darf sie auch löschen, kann sie ansehen und verändern. Der Vertriebsleiter darf alle Daten sehen, aber nicht verändern oder löschen.

Setzen der Berechtigungen für den Account Eintrag:

- Besitzender Nutzer: Person 1
- Besitzende Gruppe: Vertrieb A
- Berechtigung zum Ansehen: 2 (elementar)
- Berechtigung zum Löschen: 1 (lokal)
- Berechtigung zum Verändern: 3 (erweitert)

3. Szenario
Nur der Mitarbeiter (Person 1), der die Daten erstellt hat, darf sie auch löschen, kann sie ansehen und verändern. Es handelt sich um einen lokalen Kontakt

Setzen der Berechtigungen für den Account Eintrag:

- Besitzender Nutzer: Person 1
- Besitzende Gruppe: Vertrieb A
- Berechtigung zum Ansehen: 1 (lokal)
- Berechtigung zum Löschen: 1 (lokal)
- Berechtigung zum Verändern: 1 (lokal)

4. Szenario
Alle Nutzer des CRM Systems aus dem Unternehmen (über die Vertriebsgruppe hinaus), dürfen die Daten ansehen. Nur der Mitarbeiter, der sie erstellt hat (Person 1) darf sie auch löschen oder verändern.

Setzen der Berechtigungen für den Account Eintrag:

- Besitzender Nutzer: Person 1
- Besitzende Gruppe: Vertrieb A
- Berechtigung zum Ansehen: 4 (global)
- Berechtigung zum Löschen: 1 (lokal)
- Berechtigung zum Verändern: 1 (lokal)

5. Szenario
Alle Nutzer des CRM Systems aus dem Unternehmen (über die Vertriebsgruppe hinaus), dürfen die Daten ansehen. Nur die Mitarbeiter des Vertriebs A, dürfen sie auch löschen oder verändern.

Setzen der Berechtigungen für den Account Eintrag:

- Besitzender Nutzer: Person 1
- Besitzende Gruppe: Vertrieb A
- Berechtigung zum Ansehen: 4 (global)
- Berechtigung zum Löschen: 2 (elementar)
- Berechtigung zum Verändern: 2 (elementar)

6. Szenario
Alle Nutzer des CRM Systems aus dem Unternehmen (über die Vertriebsgruppe hinaus), dürfen die Daten ansehen. Nur die Mitarbeiter des Vertriebs A, dürfen sie verändern. Nur der Mitarbeiter, der den Eintrag erstellt hat, darf ihn auch löschen.

Setzen der Berechtigungen für den Account Eintrag:

- Besitzender Nutzer: Person 1
- Besitzende Gruppe: Vertrieb A
- Berechtigung zum Ansehen: 4 (global)
- Berechtigung zum Löschen: 1 (lokal)
- Berechtigung zum Verändern: 2 (elementar)

7. Szenario
Mitglieder des Vertriebs A und B und der Verteibsleiter, dürfen die Daten ansehen. Nur die Mitarbeiter des Vertriebs A, dürfen sie verändern. Nur der Mitarbeiter, der den Eintrag erstellt hat, darf ihn auch löschen.

Setzen der Berechtigungen für den Account Eintrag:

- Besitzender Nutzer: Person 1
- Besitzende Gruppe: Vertrieb A
- Berechtigung zum Ansehen: 3 (erweitert)
- Berechtigung zum Löschen: 1 (lokal)
- Berechtigung zum Verändern: 2 (normal)

Kapitel 11.

Beispiel Vertriebsgruppe mit gemeinsamen Nutzern

Nutzer können auch Mitglieder mehrerer Gruppen sein. Damit bekommen Sie eine höhere Flexiblilität bei der Vergabe von Rechten. Wie später noch sehen ist, ist es äusserst einfach, Nutzern verschiedenen Gruppen zuzuordnen, so das sich diese Verfahren auch dazu eignet, Nutzern nur eine bestimmte Zeit Zugang zu bestimmten Daten zu gewähren (z.B. Urlaubsvertretung), ohne das die Rechte an den Daten selbst verändert werden müssen.

In der in der Abbildung 11.1 gezeigten Struktur, wurde der Nutzer „Person 4“ aus dem „Vertrieb B“ noch zusätzlich als Nutzer in die Gruppe des „Vertrieb A“ übernommen.

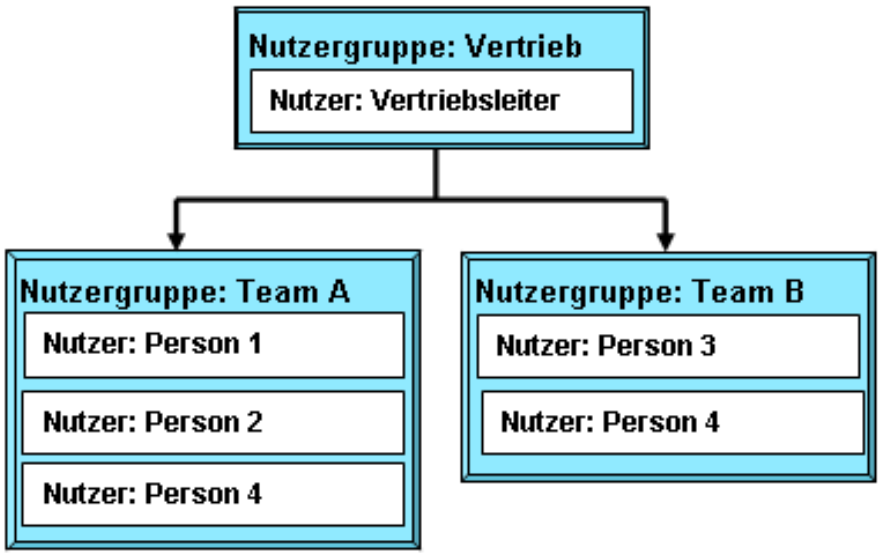

Abbildung 11.1.: Beispiel Vertriebsgruppe umstrukturiert

Dadurch wird z.B. jetzt folgendes Szenario möglich:

Person 3 darf die Daten nicht sehen, aber Personen 1, 2 und 4 und der Vertriebsleiter dürfen es. Nur der Eigentümer Person 1 darf Veränderungen durchführen.

So setzen Sie dafür die Berechtigungen für den Account Eintrag:

- Besitzender Nutzer: Person 1
- Besitzende Gruppe: Vertrieb A
- Berechtigung zum Ansehen: 3 (erweitert)
- Berechtigung zum Löschen: 1 (lokal)
- Berechtigung zum Verändern: 1 (lokal)

Index