**Berechtigungsverwaltung**

1. **Berechtigungsverwaltung generell**

Der Sinn einer Berechtigungsverwaltung sollte relativ Nahe liegen bei jeder eigentlich jeder Anwendung. Die Berechtigungsverwaltung ermöglicht es in Anwendungen, die Access Control Berechtigungen auf die verschiedenen Benutzer zu verteilen. Hierbei werden die Benutzer in verschiedene Benutzergruppen eingeteilt und es wird sichergestellt, dass jeder Nutzer nur diejenigen Funktionen der Anwendung nutzen kann, die er zur Ausübung seiner – für ihn vorbestimmten – Tätigkeit in der Anwendung benötigt. Außerdem wird mit der Berechtigungsverwaltung entschieden welche Elemente ein Benutzer überhaupt in der Anwendung sehen kann und welche für ihn zur Benutzung freistehen.

Mithilfe der Berechtigungsverwaltung können wiederverwandbare Richtlinien mit bestimmten Regelsätzen erstellt werden, die den Zugriff auf bestimmte Dateien, Ordner, Datei-Hashes und einige Systemsteuerungskomponenten der Anwendung festlegen und für manche Benutzergruppen erweitern oder einschränken. Eine Berechtigungsverwaltung läuft meistens nach dem Prinzip der geringsten Rechte, also es werden Benutzern nur so viele Reiche eingeräumt, wie sie zur Ausübung ihrer Tätigkeit in der Anwendung benötigen, ohne diesen gleich Administratorrechte vergeben zu müssen. (Quelle: https://help.ivanti.com/iv/help/de\_DE/isec/94/Topics/About%20Privilege%20Management.htm)

1. **Berechtigungsverwaltung im Programm**

Die Berechtigungsverwaltung in unserem Programm verläuft wie im Unterkapitel „Aufbau der Datenbank“ [Pascals Datenbank Doku Unterkapitel 1.2] so, dass in der Datenbank zwei Tabellen erstellt wurden, ein Mal die Tabelle „Berechtigungen“ und die Tabelle „User“. Die Berechtigungen der Benutzergruppen sind festgelegt und es gibt die zwei Gruppen „Administrator“ und „Benutzer“.

Bei der Erstellung eines neuen Users schreibt das Programm in die User-Tabelle den jeweiligen Namen, das Passwort in Form eines Hash und die Referenz auf die Berechtigungs-ID der Person als Fremdschlüssel. Dabei kann jedoch jeder User nur eine einzige Berechtigung besitzen und dadurch auch nur die mit der Berechtigung verbundenen Tätigkeiten im Programm ausführen. Ihm wird also eine der Benutzergruppen zugewiesen und somit entschieden, ob der Nutzer die Rechte eines Administrators nutzen kann oder nur über die Grundfunktionen verfügt. Über welche Berechtigungsgruppe der Benutzer verfügt, entscheidet der Administrator beim Anlegen des Benutzers, da Benutzer erstmal von einem Administrator mit einem vorbestimmten Passwort angelegt werden, das nach der ersten Anmeldung umgeändert werden kann.

Ein normaler Benutzer verfügt hierbei über die Grundfunktionen des Programms, er kann sich also anmelden mit seinen zuvor umgeänderten Anmeldedaten, er kann CI-Typen und dann darauf basierend CI-Records anlegen und diese auch bearbeiten. Er kann sein eigenes Profil anlicken, sich abmelden und generell die Funktionen der Anwendung nutzen. Ein Administrator hingegen verfügt über alle Grundfunktionen, kann aber auch Änderungen an der Seite vornehmen und hat so gesehen die Rechte alles zutun wie z.B. CI-Records, die von anderen Nutzern angelegt wurden, wieder zu löschen. Er kann auch wie vorher angesprochen, neue Benutzer erstellen und ihr vorrübergehendes Passwort festlegen. (Ich bin mir nicht ganz sicher gewesen was genau ein Admin im Vergleich zu einem Nutzer kann, also falls hier was fehlt, ergänzen!)

Unsere Berechtigungsverwaltung ist somit relativ simpel aufgebaut und unterscheidet nur zwischen den Administratoren und den normalen Nutzern, einfach nur um normalen Nutzern nicht die Rechte zu geben, dass sie einfach unser Programm verändern könnten und somit der Software schaden könnten. Es dient also dazu, unser Programm vor Leuten zu schützen, die nicht in der Lage sein sollten etwas daran zu ändern.