Sicherheit in OPDE

× **Bitte beachten Sie:** Dieser Artikel ist noch nicht fertig.

In diesem Abschnitt schildere ich Ihnen das Sicherheitskonzept in OPDE. Zum einen bezieht sich das auf Zugriffbeschränkungen innerhalb der Software, zum anderen behandele ich den Schutz gegen unbefugten Zugriff außerhalb des Programms.

Damit Sie sich auch der Restrisiken bewusst sind, beschreibe ich die mir bekannten Szenarien, wie man die Sicherheit in OPDE dennoch aushebeln könnte, wenn die entsprechenden Situationen eintreten.

Authentifikation

Benutzer

Gruppen

Autorisierung

ACL

Das ACL System in OPDE gewährt bis zu 13 verschiedene Rechte auf die jeweiligen Programm-Module. Allerdings werden nirgendwo alle Rechte benötigt. Welche Rechte ein Programm-Modul beachtet, lege ich während der Programmierung fest. Sie können später den einzelnen Benutzergruppen allerdings die jeweiligen Rechte zuweisen.

In der Regel sollten die Standard-Einstellungen ausreichend sein.

- SELECT
- INSERT
- DELETE
- CANCEL
- UPDATE
- GRANT
- EXECUTE
- PRINT
- USER1
- USER2
- USER3
- USER4
- ARCHIVE
- MANAGER

Die Bezeichnung habe ich weitestgehend aus den SQL Berechitungen übernommen. Wie OPDE z.B. ein SELECT interpretiert ist von Modul zu Modul unterschiedlich.

Modul	ACL	Auswirkung
Pflegeberichte	**PRINT**	Berichte ausdrucken
Pflegeberichte	**UPDATE**	Neue Berichte eingeben, bestehende änder bzw. löschen. Dateien und/oder Vorgänge anhöngen.
BHP	**PRINT**	Tagesplan ausdrucken
BHP	**UPDATE**	dieses Recht ist grundsätzlich nötig, wenn der betreffende User die BHPs abklicken möchte. Dieses Recht sollte der Examensgruppe vorbehalten sein.

Schutz gegen externen Zugriff

Grenzen der Sicherheit

Datenbank

FTP Server

OPDE kontaktiert den FTP Server über eine unverschlüsselte Verbindung. Da dieser Server sowieso nur intern verfügbar ist, erscheint mir das ausreichend. Es ist wohl nicht zu erwarten, dass jemand sich in der Pflegeeinrichtung mit einer Netzwerk-Spionage Ausrüstung auf die Lauer legt.

Es muss aber auch klar sein, dass die Anmeldung zwischen OPDE und dem FTP Server auch das Passwort unverschlüsselt überträgt. Diese Verbindung wird jedes mal aufgebaut, wenn Sie eine Datei in das OPDE System hochladen.

Die Anmeldedaten für den FTP Server werden in der Datenbank in der Tabelle `sysprops` abgespeichert. Auch dort steht das Passwort unverschlüsselt. Das ist dann eine Gefahr, wenn sich ein Angreifer die Datenbank kopiert und mitnimmt.

Daher muss der Zugang zum Datenbankserver gesichert sein. Also sollte nicht jeder diesen Datenbank Rechner physisch erreichen können. Auch müssen die Datensicherungsdateien an einem sicheren Ort aufbewahrt werden (Tresor).

lokales Verzeichnis

Katastrophen

Vandalismus