LU06a - Autorisierung Grundlagen

Autorierung bedeutet das Recht eine bestimmte Aktion durchzuführen. Jeder Service muss prüfen, ob der Client die nötigen Berechtigungen hat.

Autorisierung in einer Applikation bezieht sich darauf, wie die Berechtigungen und Zugriffsrechte für Benutzer oder Systeme innerhalb dieser Applikation verwaltet werden. Autorisierung ist ein wichtiger Bestandteil der Sicherheit und Datenschutzsteuerung in Softwareanwendungen.

Die effektive Implementierung von Autorisierung in einer Applikation erfordert eine sorgfältige Planung und Konfiguration, um sicherzustellen, dass Benutzer angemessenen Zugriff auf Ressourcen haben, während gleichzeitig die Sicherheit und Integrität der Daten gewährleistet werden.

Rollen und Rechte

Um einen Service zu nutzen werden bestimmte Rechte vorausgesetzt. Den verschiedenen Benutzern (Menschen, andere Applikationen) werden die entsprechenden Rechte zugewiesen. Häufig werden diese Rechte in Rollen zusammengefasst. Dadurch kann eine bestimmte Rolle zugewiesen werden und wir müssen nicht jedes Recht einzeln jedem Benutzer zuweisen.

Zugriffkontrolle

Die Autorisierung umfasst die Verwaltung des Zugriffs auf verschiedene Funktionen, Daten oder Dienste innerhalb der Applikation. Dies kann bedeuten, dass bestimmte Benutzer oder Rollen nur auf bestimmte Teile der Anwendung zugreifen dürfen, während anderen Bereiche oder Funktionen verwehrt bleiben. Bevor eine Aktion oder Anfrage eines Benutzers ausgeführt wird, muss die Applikation überprüfen, ob der Benutzer die erforderlichen Berechtigungen für diese Aktion besitzt. Dies geschieht durch einen Prozess der Berechtigungsprüfung, bei dem die aktuellen Berechtigungen des Benutzers mit den erforderlichen Berechtigungen verglichen werden.

Attributbasierte Zugriffssteuerung (ABAC)

Eine erweiterte Form der Autorisierung, bei der zusätzlich zu Benutzerrollen und Rechten auch andere Attribute wie Zeit, Standort, Gerätetyp usw. berücksichtigt werden, um Zugriffsentscheidungen zu treffen. Zum Beispiel können bestimmte Services nur aus dem internen Netzwerk aufgerufen werden.

Auditierung und Protokollierung

Eine wichtige Komponente der Autorisierung ist die Fähigkeit, Zugriffsversuche und -aktionen zu protokollieren und zu überwachen. Dies ermöglicht es, verdächtige Aktivitäten zu erkennen, Compliance-Anforderungen zu erfüllen und im Falle von Sicherheitsvorfällen eine forensische Analyse

durchzuführen.

Autorisation in verteilten Systemen

In der Learning Unit zur Authentifikation hast du gelernt, dass der Client im Erfolgsfall ein Token erhält. Dieses Token enthält alle relevanten Information zur Identifikation des Benutzers. Je nach Umsetzung können auch die Rollen und Rechte des Benutzers in diesem Token gespeichert werden.

Bei jedem Zugriff auf einen Service muss der Client dieses Token mit senden. Die Art wie diese Daten gesendet werden hängt vom Service und den verwendeten Protokollen ab. Im Unterricht werden wir uns eine Umsetzung mit RESTful Flask und JSON Web Token anschauen.

M321-LU06