Authorization (Autorizace)

Authorization je proces přidělování a ověřování přístupových práv. Zatímco autentizace zjišťuje, **kdo** uživatel je, autorizace určuje, **co** tento uživatel smí v rámci systému dělat (např. číst soubory, mazat data nebo měnit nastavení).

Základní modely autorizace

V IT se používá několik standardizovaných přístupů k tomu, jak definovat a spravovat oprávnění:

1. RBAC (Role-Based Access Control)

Oprávnění nejsou přidělována přímo jednotlivcům, ale **rolím** (např. Administrátor, Redaktor, Host). Uživatelé jsou následně přiřazeni k jedné nebo více rolím.

- **Výhoda:** Snadná správa ve velkých organizacích. Pokud zaměstnanec změní pozici, pouze se mu změní role.

2. ABAC (Attribute-Based Access Control)

Pokročilejší model, který rozhoduje na základě **atributů**. Ty mohou zahrnovat:

- **Atributy uživatele:** (Např. oddělení, věk, prověření).
- **Atributy zdroje:** (Např. typ souboru, citlivost dat).
- **Environmentální atributy:** (Např. čas přístupu, IP adresa, lokalita).
- **Příklad:** „Umožni přístup k finančním výkazům pouze manažerům z účtárny, pokud se připojují z vnitřní sítě v pracovní době.“

3. DAC (Discretionary Access Control)

Vlastník zdroje (např. souboru) má plnou moc nad tím, komu přidělí práva. Je to standardní model používaný v operačních systémech jako Windows nebo Linux pro běžné soubory.

4. MAC (Mandatory Access Control)

Pevně daná pravidla vynucená systémem, která uživatel nemůže změnit. Často se používá ve vojenských nebo vysoce zabezpečených systémech (např. SELinux). Každý objekt má úroveň utajení a každý uživatel úroveň prověření.

Mechanismy a implementace

ACL (Access Control List)

Seznam připojený k objektu (souboru, složce, síťovému rozhraní), který specifikuje, kteří uživatelé nebo procesy mají k objektu přístup a jaké operace s ním mohou provádět (Read, Write, Execute).

OAuth 2.0 a "Scopes"

V moderních webových aplikacích se pro autorizaci používá protokol **OAuth 2.0**. Místo sdílení hesla získá aplikace tzv. **Access Token** s omezeným rozsahem oprávnění (tzv. **Scopes**).

- **Příklad:** Aplikace pro plánování příspěvků na sociální sítě dostane oprávnění pouze k „zápisu příspěvků“, ale nikoliv k „čtení soukromých zpráv“.

Principy bezpečné autorizace

- **Principle of Least Privilege (Princíp nejnižších privilegií):** Uživatel by měl mít k dispozici pouze ta oprávnění, která nezbytně potřebuje pro svou práci. Nic víc.
- **Separation of Duties (Oddělení rolí):** Kritické operace by měly vyžadovat autorizaci od dvou různých lidí (např. jeden platbu vytvoří, druhý ji schválí).
- **Implicit Deny (Implicitní zákaz):** Pokud není přístup výslovně povolen, je považován za zakázaný.

Rozdíly v kostce

Vlastnost	Autentizace	Autorizace
Otázka	Kdo jsi?	Co smíš dělat?
Pořadí	První krok	Druhý krok (po autentizaci)
Metody	Hesla, Biometrie, Tokeny	Role, Atributy, ACL
Příklad	Přihlášení do e-mailu	Možnost smazat e-mail

Související pojmy: Authentication, RBAC, ABAC, ACL, OAuth 2.0, Principle of Least Privilege.