RBAC – Role-Based Access Control

RBAC je metoda správy přístupových práv, kde jsou oprávnění seskupena do logických celků nazývaných **role**. Uživatelé k těmto právům nepřistupují přímo, ale skrze přiřazené role (např. „Editor“, „Administrátor“, „Účetní“).

1. Základní principy RBAC

RBAC stojí na třech hlavních pravidlech:

- **Přiřazení role (Role assignment):** Uživatel může vykonávat operaci pouze tehdy, pokud mu byla přiřazena role.
- **Autorizace role (Role authorization):** Uživatel může aktivovat pouze tu roli, ke které má oprávnění.
- **Oprávnění role (Permission authorization):** Role definuje konkrétní akce, které lze v systému provádět (např. číst soubor, smazat databázi).

---

2. Klíčové výhody oproti ACL

Zatímco ACL (Access Control Lists) jsou vhodné pro malé systémy, RBAC dominuje v podnikovém prostředí (Enterprise):

Vlastnost	ACL	RBAC
Správa	Náročná (každý uživatel se nastavuje zvlášť)	Snadná (změna v roli ovlivní všechny uživatele)
Škálovatelnost	Nízká	Vysoká (vhodné pro tisíce uživatelů)
Přehlednost	Často nepřehledné (kdo má kam přístup?)	Jasná (kdo má jakou roli?)
Nábor nových lidí	Nutnost kopírovat práva	Stačí přiřadit roli „Nový zaměstnanec“

---

3. Hierarchické RBAC (HRBAC)

V pokročilých systémech se používá hierarchie, kde vyšší role dědí práva rolí nižších.

- **Příklad:** Role „Vedoucí projektu“ automaticky obsahuje všechna práva role „Vývojář“, plus přidává práva pro schvalování rozpočtu.

—

4. Princip minimálních privilegií (PoLP)

RBAC je ideálním nástrojem pro implementaci **Principle of Least Privilege**. To znamená, že uživatel má k dispozici pouze ty role a práva, které nezbytně potřebuje pro výkon své práce. Tím se dramaticky snižuje riziko v případě kompromitace uživatelského účtu útočníkem.

---

5. Praktické nasazení

RBAC se dnes používá téměř všude:

- **Cloudové platformy:** AWS IAM, Azure RBAC (správa přístupu k serverům a databázím).
- **CMS systémy:** WordPress (Administrátor vs. Redaktor vs. Návštěvník).
- **Operační systémy:** Správa skupin v Active Directory (Windows Server).
- **Kubernetes:** Řízení toho, kdo může nasazovat kontejnery do clusteru.

---

6. Výzvy a rizika

- **Role Explosion (Exploze rolí):** Situace, kdy v systému vznikne příliš mnoho specifických rolí, až se správa stane opět nepřehlednou.
- **Statická povaha:** RBAC hůře reaguje na dynamické faktory (např. „povolit přístup jen v pracovní době z kanceláře“). Pro tyto účely se používá pokročilejší **ABAC** (Attribute-Based Access Control).

Související články:

- ACL – Access Control List
- IAM – Identity and Access Management
- Bezpečnostní standardy a princip minimálních práv

Tagy: security rbac iam access-control administration enterprise