Řízení přístupu (Access Control)

Řízení přístupu je klíčovou součástí informační bezpečnosti. Definuje procesy a technologie, které určují, kdo (subjekt) může přistupovat k čemu (objekt) a jaké operace s ním může provádět.

Základní pilíře (IAAA)

Aby bylo řízení přístupu efektivní, musí projít čtyřmi základními fázemi:

```
  Identifikace: Uživatel sdělí systému, kdo je (např. zadání uživatelského jména).
```

```
  Autentizace: Ověření identity uživatele (např. heslo, otisk prstu, certifikát).
```

```
  Autorizace: Prověření, zda má daný uživatel právo provést požadovanou akci.
```

```
  Audit (Accountability): Zaznamenávání aktivit uživatele pro pozdější kontrolu.
```

Modely řízení přístupu

V praxi se setkáváme s několika standardními modely, které určují, jak jsou oprávnění přidělována:

==== 1. DAC (Discretionary Access Control) ==== Libovolné řízení přístupu. Vlastník objektu (např. souboru) má plnou kontrolu nad tím, komu k němu udělí přístup.

```
  Výhoda: Flexibilita.
```

```
  Nevýhoda: Vysoké riziko chyby uživatele a šíření malware.
```

==== 2. MAC (Mandatory Access Control) ==== Povinné řízení přístupu. Oprávnění určuje centrální autorita na základě bezpečnostních úrovní (např. Přísně tajné vs. Veřejné). Často se používá v armádě.

```
  Výhoda: Maximální bezpečnost.
```

```
  Nevýhoda: Náročná správa a nepružnost.
```

==== 3. RBAC (Role-Based Access Control) ==== Řízení přístupu na základě rolí. Přístup není přidělován jednotlivcům, ale skupinám (rolím), jako je „Účetní“, „Administrátor“ nebo „Editor“.

```
  Výhoda: Snadná správa ve velkých organizacích.
```

```
  Příklad: Nový zaměstnanec dostane roli "HR" a automaticky získá přístup ke všem složkám personálního oddělení.
```

==== 4. ABAC (Attribute-Based Access Control) ==== Řízení na základě atributů. Nejpokročilejší model, který rozhoduje na základě kontextu (čas, poloha, zařízení, typ dat).

```
  Příklad: Uživatel má přístup k databázi pouze v pracovní době a pouze pokud se připojuje z firemní sítě.
```

Metody autentizace

Moderní systémy by měly využívat více než jen heslo. Doporučuje se Vícefaktorová autentizace (MFA), která kombinuje:

```
  Něco, co vím: (Heslo, PIN)
```

```
  Něco, co mám: (Token, mobilní telefon, čipová karta)
```

```
  Něco, čím jsem: (Biometrie – otisk prstu, sken sítnice)
```

Doporučené postupy (Best Practices)

```
  Princip minimálních privilegií (Least Privilege): Uživatel by měl mít pouze ta oprávnění, která nezbytně potřebuje pro svou práci, a nic navíc.
```

Pravidlo	**Popis**	Separation of Duties	Rozdělení úkolů mezi více lidí, aby jeden člověk nemohl zneužít systém (např. jeden platbu zadá, druhý schválí).	Pravidelná revize	Kontrola oprávnění alespoň jednou za čtvrt roku.	Zánik přístupu	Okamžité odebrání přístupů při ukončení pracovního poměru.

Související témata:

```
  [[bezpecnost:autentizace|Autentizační metody]]
```

```
  [[it:sitova_bezpecnost|Síťová bezpečnost]]
```

```
  [[normy:iso27001|Norma ISO 27001]]
```