

# Access Control

Access Control (v češtině řízení přístupu nebo kontrola přístupu) je základní bezpečnostní mechanismus v informačních technologiích, který určuje, kdo nebo co má právo přistupovat k určitým zdrojům systému, jako jsou soubory, složky, databáze, aplikace, síťová zařízení či fyzické prostory.

Cílem Access Control je:

zajistit důvěrnost, integritu a dostupnost dat a služeb,  
minimalizovat riziko neoprávněného přístupu,  
implementovat princip minimálních oprávnění (principle of least privilege).

## Teoretický popis

Z hlediska teorie se Access Control řeší v rámci bezpečnostních modelů a politik řízení přístupu. Nejčastější modely zahrnují:

DAC (Discretionary Access Control) – vlastník zdroje rozhoduje, kdo má přístup.

MAC (Mandatory Access Control) – přístup je určen centrální bezpečnostní politikou (např. na základě klasifikace důvěrnosti).

RBAC (Role-Based Access Control) – přístup je udělován na základě rolí uživatelů ve vnitřní struktuře organizace.

ABAC (Attribute-Based Access Control) – přístup závisí na dynamických attributech (např. čas, lokace, typ zařízení, uživatelské vlastnosti).

Každý model má své výhody a nevýhody a volba závisí na požadavcích organizace, typu systému a požadované úrovni zabezpečení.

## Praktické uplatnění

V praxi se Access Control implementuje různými technologiemi a mechanismy, například:

Autentizace a autorizace – nejprve se ověří totožnost uživatele (authentication), pak se rozhodne o jeho oprávněních (authorization).

ACL (Access Control Lists) – seznamy, které definují, jaké identity mají jaká oprávnění k jednotlivým objektům (např. u souborových systémů nebo síťových firewallů).

IAM systémy (Identity and Access Management) – centrální nástroje pro správu identit a přístupových práv napříč organizací (např. Microsoft Entra ID, Okta, Keycloak).

Síťová řízení přístupu – jako 802.1X, NAC (Network Access Control), VLAN segmentace apod.

Přístupové řízení na aplikacích – např. v webových aplikacích pomocí OAuth 2.0, OpenID Connect nebo vlastních autorizačních middleware.

## Příklady

Uživatel „Jan“ má roli „Editor“ v redakčním systému → může upravovat články, ale nemůže je publikovat (to může jen role „Administrátor“).

ACL na souboru tajne\_dokumenty.pdf povoluje přístup jen skupině „Vedení“.

Firewall blokuje všechny příchozí požadavky, kromě portu 443 z důvěryhodných IP rozsahů.

## Související pojmy

[[Autentizace]]

[[Autorizace]]

[[Identity and Access Management (IAM)]]

[[Zero Trust]]

[[Principle of Least Privilege]]

## Reference

NIST Special Publication 800-53 – Security and Privacy Controls

ISO/IEC 27001 – Informační bezpečnost

RFC 7235 – HTTP Authentication

From:

<https://serviceit.cz/> - IT ENCYKLOPEDIE

Permanent link:

[https://serviceit.cz/doku.php?id=access\\_control](https://serviceit.cz/doku.php?id=access_control)

Last update: **2025/12/31 18:29**

