Identity management na UK

Hned úvodem si položme jednoduchou otázku. Potřebuji jako uživatel službu takového systému? Odpověď je lehce protichůdná. Navenek není nic nového vidět, ale pro přechod do digitálního světa identit je to základní stavební kámen. A právě uživatelské digitální identity jsou elektronickou reprezentací každé osoby nebo objektu v informačním systému.

Po Helpdesku prezentujeme další nezbytnou část fungování IT na univerzitě. Pojem Identity management (IDM) se týká způsobu, jakým jsou řízeny a spravovány zdroje související s uživateli a poskytováním služeb. Do oblasti IDM spadá vše, co nějakým způsobem souvisí s životním cyklem digitální identity. Příkladem je přiřazení oprávnění spojeného s příchodem nového zaměstnance či studenta, jejich změnou napříč UK až případným odchodem.

Příklady konkrétních činností:

- vytváření účtů a e-mailových schránek,
- přiřazení do skupin a týmů,
- přidělení oprávnění,
- nastavení a změna hesel,
- následný úklid, anonymizace či smazání dat tak, aby nedošlo k potenciálnímu zneužití.

Správa životního cyklu uživatelů, management přístupu k informačním systémům, zvýšení bezpečnosti a zefektivnění typicky schvalovacích procesů

Díky možnosti vytvářet a vynucovat centralizovaná pravidla a nastavovat oprávnění je snazší zajištění přístupu uživatelů k?souborům, datům, týmům a zařízením, která potřebují. Opačně oprávnění zamezují přístup k citlivým informacím, které uživatelé nepotřebují. To je základ řízení podle role. Role se dají přiřazovat na základě příslušnosti do skupin nebo individuálně.

IDM funguje jako centrální bod informačních systémů (IS), mezi kterými je třeba sdílet a synchronizovat informace o uživatelích, jejich rolích a oprávněních. Odpadá tak chybovost spojená se "síti" nezávislých synchronizačních mechanismů, které se obtížně provozují, udržují, koordinují a vyvíjí.

Správa uživatelských identit a rolí v?IS UK je dlouhodobým problémem. Historicky existuje na UK několik funkčně oddělených informačních systémů, které jsou mezi sebou navzájem přímo propojené. Při nárustů počtu těchto systémů se stává situace výměny dat o identitách a rolích jen obtížně udržitelná.

Koncem roku 2022 ÚVT začal pracovat na Koncepci správy uživatelských identit na UK. Tím byl položen základ pro zahájení implementace centrálního IDM. UK již desítky let úspěšně používá pro implementaci Centrální autentizační služby (CAS) opensource řešení Apereo. I tento dobrý příklad užití open source umožnil vybrat midPoint.

Poprvé je systém midPoint uplatněn v rámci celouniverzitního helpdeskového systému. IDM už do budoucna využijí všechny nově vyvíjené IT systémy. Postupně bude v?závislosti na finančních možnostech implementován i do stávajících částí IS. Komplexní standardizace (jak procesní, tak technická) prostředí správy identit na UK je však projektem na několik dalších let.