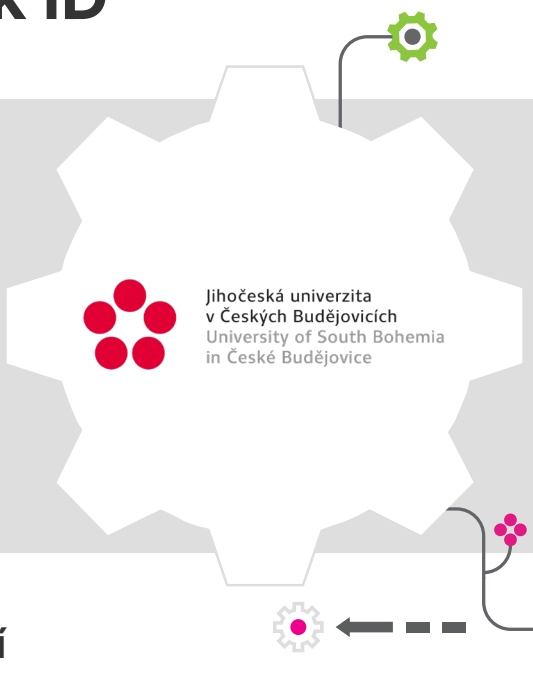
Případová studie

Jihočeská univerzita: Reset hesla s ověřením přes NIA / Bank iD

Jihočeská univerzita v Českých Budějovicích celkově spravuje více než 15 000 aktivních digitálních identit. Pro jejich správu využívá IDM řešení od společnosti Orchitech postavené na open-source platformě Wren:IDM. V rámci tohoto systému bylo potřeba najít způsob, jak zefektivnit a zároveň lépe zabezpečit proces nastavení a resetu hesla. Řešením se stalo napojení IDM na NIA a Bank iD.



Výchozí situace

Specifikem univerzitního prostředí je každoroční přírůstek velkého množství nových identit. To klade vysoké nároky na správu uživatelských účtů a hesel. Jedním ze základních problémů je, jak novým studentům bezpečně doručit iniciální hesla.

V původním procesu správy hesel bylo několik oblastí, které vyžadovaly pozornost:

- **Slabá iniciální hesla** - z důvodu obtížného doručení byla generována z osobních údajů a při prvním přihlášení si musel student iniciální heslo změnit.
- **Časová náročnost** - při zapomenutí hesla musel uživatel kontaktovat administrátora (osobně, telefonicky nebo přes Service Desk), který následně heslo ručně resetoval do iniciálního tvaru.
- **Omezená možnost ověření totožnosti** - pokud se uživatel nedostavil osobně, nebylo možné jeho identitu spolehlivě ověřit.

Řešení

Po zvážení různých možností jsme se ve spolupráci s Jihočeskou univerzitou rozhodli využít ověření totožnosti pomocí **NIA a Bank iD**. Cílem bylo umožnit uživatelům bezpečný a plně automatizovaný proces nastavení a resetu hesla.

Výsledkem bylo zavedení **self-service resetu hesla** s ověřením přes NIA nebo Bank iD, které vytvářejí federativní prostředí propojující poskytovatele služeb (SP/RP) a poskytovatele identit (IdP).

Do IDM byla začleněna autentizační brána:

- **Integrace s NIA** probíhá přes protokol SAML 2.0, univerzitní IDM vystupuje v roli Service Provider (SP).
- **Integrace s Bank iD** probíhá přes OpenID Connect, IDM v tomto případě funguje jako Relying Party (RP).

Po úspěšné autentizaci jsou do IDM předány vyžádané údaje a dochází ke ztotožnění uživatele, tedy dohledání jeho identity v systému.

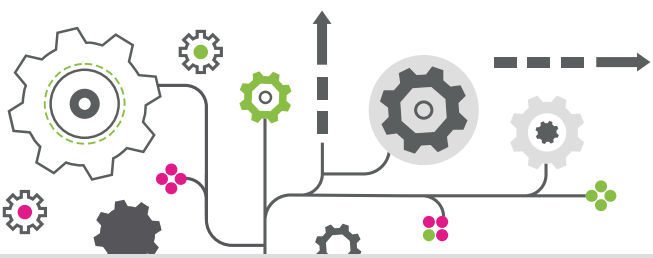
Výsledky a přínosy

- **Zásadní snížení požadavků na administrátorský reset hesla**
  Nyní jsou řešeny jen výjimečné situace, kdy uživatel nevlastní žádný prostředek pro identifikace prostřednictvím NIA / Bank iD.
- **Zrychlení procesu resetu hesla a komfort pro uživatele**
  Reset hesla probíhá okamžitě, bez čekání na zpracování, odkudkoli a přes pro uživatele známé a bezpečné služby.
- **Zrušení generování iniciálního hesla odvozeného z osobních údajů uživatele**
  Pro nový účet je generováno náhodné heslo, které si uživatel při první příležitosti vyresetuje.
- **Zvýšení bezpečnosti v oblasti práce s hesly**
  Odstranění teoreticky odhadnutelného iniciálního hesla odvozeného z osobních údajů uživatele.

Díky zavedení self-service resetu hesla s ověřením přes NIA / Bank iD univerzita dosáhla vyšší bezpečnosti, efektivnější IT podpory a lepšího uživatelského komfortu.

Průběh resetu hesla z pohledu uživatele

1. Uživatel na přihlašovací stránce zvolí „Zapomenuté heslo / Nastavení nového hesla“.
2. Vybere způsob ověření (NIA nebo Bank iD).
3. Po úspěšné autentizaci je přesměrován zpět do IDM a nastaví si nové heslo.



O klientovi

Jihočeská univerzita v Českých Budějovicích patří mezi deset největších univerzit v ČR. Navštěvuje ji přes deset tisíc studentů, jejichž výuka zaměstnává stovky pracovníků.

Řízení přístupů k IS/IT je na JU náročné nejen kvůli počtu identit, ale i díky pravidelnému nárazovému příchodu a odchodu studentů v jednotlivých studijních obdobích.

S Orchitechem spolupracuje již od roku 2014.

O Orchitechu

Pomáháme IT oddělením:

- efektivně řídit identity a přístupy
- automatizovat rutinní činnosti
- zvyšovat bezpečnost
- šetřit čas a náklady

Naše řešení zajišťují soulad s legislativními požadavky, včetně GDPR, NIS2, nového kybernetického zákona a dalších. Působíme na trhu více než 18 let a realizovali jsme již více než 100 projektů pro 50 klientů z veřejného i soukromého sektoru.

https://orchi.tech/ +420 216 216 850 info@orchitech.cz