Employee lifecycle with Identity Management

Evgen Jamnikar, Simon Feldin

Complex information systems consist of a variety of applications and services, therefor organizations require a lot of effort and time in managing user accounts and determining the access rights of the user. The dynamism of business processes and user mobility consequently means continuous changes in determining access for users. IT departments are usually overloaded with many other operational tasks and are unable to provide up to date state in the area of access to information systems.

When employees leave an organization, transferred to another department or progress and gain a new role in the company, they rarely remember that it is reasonable to revoke unnecessary access rights or at least re-check if the person in question still needs current access rights. Many user accounts after the departure of the employees from the organization remains active, which means security risk - potential for a variety of data theft, abuse or other actions in the information system, causing commercial harm.

Through presentation we will highlight:

- The most common challenges in managing user accounts and rights,
- How to solve challenges of the topic,
- Examples of dynamic allocation of rights to users and
- Some good practice in the management of user identities and their rights.