Identity Management (IDM) Deployment Case Study

Affordable IDM solutions – security for everyone

Employees come, employees go, and everyone needs to be taken care of. Not only to have their jobs, but also to have the right access to all the necessary information systems (IS) and also to lose this right when they leave the company. That's why Identity Management is here, not only for large companies, but also for small and medium-sized enterprises.

CASE STUDY

IDM Features

IDM is a fast, flexible and affordable solution that eliminates many problems in businesses of all sizes. So why shouldn't smaller companies take advantage of technological advances that until now only large corporations could afford?

SERVICES PROVIDED

It's here. A new employee just walked into the building. What about him? In order to work properly, the local IT department has to provide him with all the necessary access to the information systems. These tasks are usually handled by internal regulation, typically a time-consuming system of requests and approval processes, at the end there is an information system administrator who ensures the necessary settings.

Similar problems, but of an opposite nature, are also faced by companies when employees leave them. Moreover, there is a significant security risk associated with their leaving. Often, the competent persons who should revoke or, better still, cancel the relevant authorizations are not aware of the fact that they have left. There is also a risk of changing the position of an employee, where there is often a cumulative access, because the employee is assigned new rights, but the originally assigned rights remain.

Security audits, which companies should regularly undergo, are an essential safeguard against such problems. In fact, part of the audit should be devoted to the management of information system users. A typical question asked by an auditor is: „Who is allowed access to which information systems and who has authorised it?". However, preparing and defending the relevant reports is often a „nightmare" for the responsible IT managers, not to mention that the company may not learn from the audit findings.

Magic of IDM

Identity Management (IDM) is an information system that takes care of the identity lifecycle of each user, ensuring effective management of their access permissions. IDM is linked to the HR system, from which it receives information on all changes in employee data (change of position, surname, employee joining, resignation...). On the other hand, the IDM is integrated with individual information systems and automatically manages IS users based on rules defined in the IDM.

GEM System | Štětkova 1638/18, 140 00 Praha 4 – Nusle, Czech Republic | sales@gemsystem.cz | www.gemsystem.cz

Who offers IDM

There are currently a number of IDM solutions on the market, based on commercial products from software companies such as Oracle, Microsoft, IBM, Novell or CA, as well as on the basis of opensource solutions such as OpenIDM, Apache Syncope, midPoint or OpenIAM.

Identity Management

Every change in the employee requires changes in user settings data in information systems of the company. Specialised software guarantees efficient management of the IDM agenda, which includes:

- automatic promotion of changes to user accounts in IS,
- ensuring consistency in user accounts across the IS,
- evidence of all changes and changes made to the actions (audit),
- formalization and automation of IDM processes,
- central record of all user accounts in the IS,
- self-service system for basic IDM tasks (password change, request/ approval of access permissions).

In addition to automatic actions, IDM offers the ability to assign access based on approved requests. The approval process activates the creation of a request and individual approvers are derived from the organisational structure of the enterprise.

IDM is a central unified record of all access permissions across all enterprise information systems. To ensure information consistency in the IDM and in the integrated IS, it is necessary to synchronise user permissions. The process is called „reconciliation“ and makes it possible to detect unauthorised modifications of user permissions that have taken place outside the IDM solution.

Thanks to the “reconciliation” process, all application accounts are linked to specific users, so all their activities are quickly and clearly identifiable with personal responsibility.

Of course, the IDM also includes an audit function, which ensures the recording and subsequent traceability of changes in user records.

IDM allows to use appropriate corporate roles (e.g. HR officer, accountant, sales representative) and thus abstract from specific application roles of information systems (e.g. write_erp_saldo, write_history_bank). Using of individual application roles is not intuitive for professional (non-IT) departments and thus unnecessarily complicates their work performance. On the other hand, the using of clear named enterprise roles – as is done in IDM – achieves significant simplification in all necessary tasks. In addition, enterprise roles are an effective tool that minimizes the accumulation of permissions during the transition employee to another position.

By far the best part of all this is that it is not a technology whose robustness or price is affordable only to large enterprises. In fact, it can be quickly and inexpensively built on any platform for small and medium-sized businesses as well. Many customers, especially in the smaller business segment, are concerned about the financial complexity of IDM solutions. Then they are surprised to find out that the investment is not in the order of millions but hundreds of thousands. After all, every company must manage employee rights and entitlements, regardless of whether it employs one hundred, one thousand or ten thousand workers.