Innovative tools and services optimize role and authorization management

Organizing Workflows

The definition and assignment of roles and authorizations is crucial for ERP systems, as they allow companies to define and implement user access rights in processes and workflows.

By Philipp Latini, Sivis

For company and employees alike, the definition and allocation of roles and authorizations in ERP systems offers a high level of security and transparency – at least in theory. In reality, authorization management is often in disarray, its handling unstructured, leading to serious security concerns. As dangerous as neglected role management and authorization can be, the effort and time a thorough manual evaluation of all roles and authorizations takes is almost impossible to spare. However, new intelligent software tools promise to tackle this challenge, offering companies a realistic opportunity to sustainably optimize their authorization management without Herculean effort.

Old and new roles

In SAP systems alone, there are roughly 150,000 transactions that can be assigned to individual users, user groups, roles, or composite roles. Experience shows that new users, roles, and authorizations are added fairly regularly, but the existing ones are rarely reviewed. More often than not, their number only gets reduced if an employee decides to leave the company.

This doesn't come as a surprise. Systems that have been organically growing over years, even decades, accumulate quite a lot of data to sift through. Reviewing each and every authorization the traditional (manual) way would be nearly impossible, not least because many companies do not even leverage so-called tracing yet to see which user utilizes which authorizations.

At the same time, the security risks that arise from inadequate authorization concept are not to be underestimated. One example would be if an employee in procurement switches to accounting, registers themselves as a supplier and pays their own invoices for goods that were never ordered or delivered – and this is only the beginning.

Security concerns are exacerbated by the Covid-19 pandemic and the (forced) trend towards remote work. Opening up internal systems for external access carries an inherent risk either way, but at least all authorizations should be consistent to avoid becoming an easy target for cybercriminals.

Only then can unauthorized access to critical information be prevented and mistakes due to lack of transparency and an inadequate authorization concept be avoided.

Furthermore, if your authorization management is in disarray, you could be paying more for your licenses than you realize. A common example: Paying for licenses for users that neither need nor use the programs. Authorization management is therefore also important when it comes to audits.

High time, then, to start reviewing and declutter one's own authorization management. The good news is that there are new intelligent solutions available that help companies entangle their unmanageable authorization concepts.

The foundation is tracing

A good starting point is to implement access tracing, as it is used to evaluate which user uses which authorizations and roles the most. Every access and action is documented for six to twelve months to provide a solid data base for reviewing which authorizations, roles, and licenses are actually needed.

Based on the tracing data, intelligent new software solutions such as the Sivis Reduction Manager review every recorded action automatically. All roles or authorizations that have not been used during the tracing period are sent to the responsible employee to review. The same goes for role constellations that seem inconsistent, like parallel authorizations for procurement and accounting. The biggest benefit of intelligent software solutions in this case is that not all existing authorizations have to be reviewed, but only the ones that can be assumed to be out of date. At the same time, the manual review and decision-making process ensure that authorizations are not erroneously taken away. After all, there are some legitimate reasons why authorizations might not have been used for a longer period of time.

Automated suggestions

For security and cost efficiency reasons, quality, transparency and consistency of the authorization management are indispensable. Up to now, redesigning existing systems was hardly feasible due to the high amount of work involved.

Innovative software solutions now offer companies the opportunity to automatedly scan, evaluate, and contrast all authorizations. Striking constellations that seem out of date or inconsistent are sent to the responsible employee to review to avoid erroneously deleting legitimate roles or authorizations. Consequently, the required effort can be reduced significantly. Some providers like Sivis offer a combination of software solutions and service, again reducing the involved effort for companies.

Philipp Latini, CEO Sivis

Please also have a look at our Community Info entry

SIVIS
smart · simple · safe