Privileged Access Management (PAM)

Professional management of privileged access

Privileged users and systems are particularly worth protecting in companies and their IT environments. However, privileged accounts lead to massive compliance and security risks and are therefore the preferred target of hackers. For this reason, it is essential for companies to manage privileged access effectively and securely.

PAM content and requirements

Privileged Access Management, or PAM for short, is the management of privileged user accounts. These are administrative accounts that are used to manage and control systems and networks (e.g. email accounts, Microsoft Exchange Server). As these administrative accounts allow access to critical information, they are referred to as privileged. They are therefore the target of most hacker attacks that gain access to these accounts and their sensitive company data. Larger companies in particular usually have a large number of administrative accounts, which are often accessed by multiple users. In addition, administrative accounts and therefore also so-called service accounts are an easy target for attacks in most companies, as passwords are never or very rarely changed. PAM protects your company from deliberate or unintentional misuse of privileged access. It covers two main areas: password management and session management for privileged accounts. In this way, both privileged access and administrative activities (sessions) are secured, recorded and managed.

The most important ToDos at a glance

The following tasks are recommended for the secure management of privileged accounts:

- Conduct an inventory of your privileged accounts, including the users and systems that use them.
- Ensure that your privileged passwords are stored securely.
-

Enforce strict administrative processes for changing privileged account passwords.

- Where possible, ensure clear responsibilities and grant only the minimum level of authorization required.
- Review the use of privileged access regularly.

A central element in the PAM system is the vault. It is where the “secrets” are kept. It is therefore the most critical part. Secrets such as passwords are managed by the PAM solution, e.g. by enforcing regular password rotation.

The advantages of PAM at a glance

Fulfillment of compliance requirements

Privileged users with high risk, risky behavior and unusual events are clearly identified. Hacker attacks via administrative accounts are warded off.

Efficient creation of monitoring reports

System access by external service providers and internal users is monitored. These can be called up as reports at any time to document the maintenance of integrity.

Simplify the management of privileged accounts and sessions

The automated password change of administrative accounts and service accounts as well as the central

password management for network, server, applications and service accounts simplify administration.

Mitigating the potential damage of security breaches

Passing on passwords is not possible and single sign-on simplifies operation for administrators.

Improved protection for sensitive data and company information

Recording the admin session ensures quality optimization and proof of quality. Data breakdowns and downtimes are reduced due to uncontrolled access. Full access transparency is guaranteed.

ASCONSIT: We focus on holistic PAG solutions!

The implementation of PAM is an important part of IT security strategies to increase the security of IT systems and data by reducing the attack surface for cyber criminals. Together with clear account access and standardized lifecycle management in IAM and GRC, privileged account governance (PAG) is implemented. This ensures the most comprehensive protection of identities and privileged accounts.

With IAM, GRC and PAM, you can rely on ASCONSIT's holistic PAG solutions and the expertise of our process specialists!