SiTS

Your Trusted
Cyber Security Partner

Top 15: Things to Know about Securing Privileged Accounts

1 What are the current threats and regulations impacting cyber security?

The cyber security landscape is shaped by increasing cyber threats such as ransomware, phishing, and insider attacks. Regulatory requirements like NIS2, GDPR, HIPAA, and DORA enforce strict rules on data protection and Identity security, necessitating robust security measures.

2 How do these threats affect IT security professionals?

These threats put significant pressure on IT security professionals to protect sensitive data and ensure compliance with regulations. They must develop a comprehensive security roadmap that addresses emerging threats while maintaining operational efficiency.

3 What challenges do security leaders face in developing a security roadmap?

Security leaders must balance various security measures, including identity security, network security, endpoint protection, and user education. Managing privileged accounts, which pose a high risk due to their elevated access rights, is a crucial challenge as part of identity security.

4 What are privileged accounts, and why are they important?

Privileged accounts grant extensive access to critical systems and data, including internal admin accounts, vendor access, and machine or application accounts. They are crucial for managing your applications and systems but can lead to severe security breaches if mismanaged.

5 What risks do privileged accounts pose?

Compromised privileged accounts can result in unauthorized data access, system disruptions, and compliance violations. Their high level of access makes them attractive targets for cybercriminals and a critical point of vulnerability.

6 What is PAM and how does it help?

PAM (Privileged Access Management) involves security practices and technologies designed to control and audit privileged access to critical systems and data. It ensures only authorized users can perform privileged actions, mitigating the risk of misuse and breaches.

7 What are the benefits of implementing PAM?

PAM enhances security by enforcing least privilege principles, providing detailed audit trails, reducing the attack surface, and ensuring compliance with regulatory requirements. It also helps manage and monitor privileged account activities.

8 What types of PAM implementations are available?

Do It Yourself On-Premise PAM: Installed within the organization's infrastructure, providing control and security but necessitating ongoing in-house maintenance and customizations.
Do It Yourself Cloud PAM: Hosted in the cloud, offering scalability and reduced in-house management overhead but reliant on the provider's security and skilled resources.
PAM as a Service (PAMaaS): Managed by third-party providers, offering end-to-end PAM solutions ideal for SMEs with limited IT resources.

9 What are the differences between Do It Yourself and managed PAM services?

Do It Yourself: Provides complete control and customization but demands extensive internal expertise and resources.
Managed Services: Offers a turnkey solution with continuous management and support, allowing SMEs to focus on core business activities while ensuring robust security.

10 Why should SMEs consider PAM as a Service?

PAMaaS delivers several advantages for small and medium enterprises, including:
Access to expert management: No need for internal specialists, saving costs on training and certifications.
Lower upfront costs: Reducing the need for significant initial investment.
Scalability: Easily adjustable to the organization's growth and needs.
Fast deployment and short buying cycles: Rapid setup and procurement process.
Short use of resources for buying, contracting, and onboarding services: Minimizes the internal effort required.
Flexibility in services: Short contract termination clauses offer flexibility and reduced risk.

11 What alternative solutions do I have besides a PAM security technology or service?

Alternatives include manual management of privileged accounts, which involves using spreadsheets or basic access control lists, and relying on built-in operating system features. However, these methods can be error-prone and lack the advanced security features provided by dedicated PAM solutions. Take into account that not all security risk can be eliminated.

12 What if I do not use a specialist technology or service managed by a specialist?

Without a specialist PAM solution, your organization may face higher risks of security breaches due to inadequate control and monitoring of privileged accounts. This can lead to unauthorized access, data loss, and non-compliance with regulatory requirements, potentially resulting in severe financial and reputational damage.

13 Am I personally liable in case of security breaches if there is no proper PAM plan and solution?

While personal liability can vary depending on jurisdiction and organizational policies, IT security leaders can face professional repercussions, including job loss or legal action, if found negligent in implementing necessary security measures. Ensuring robust PAM practices can mitigate these risks.

14 Are there any prerequisites that I should complete before starting on a specialist PAM technology service?

Before implementing a PAM solution, conduct a thorough assessment of your current privileged account landscape. Identify and catalog all privileged accounts, assess their usage, and understand associated risks. Additionally, ensure your organization has clear security policies and procedures in place.

15 What costs are associated with PAM solutions, and what elements determine these costs?

The cost of PAM solutions can vary significantly based on several factors:
One-time Costs: Initial setup and implementation expenses, including hardware and software procurement.
Recurring Costs: Ongoing maintenance, subscription fees for cloud-based services, and support contracts.
In-house Resource Costs: Salaries and training for staff required to manage and maintain the solution internally.
Benefits of PAM as a Service: For SMEs, PAMaaS can be more cost-effective, reducing the need for significant upfront investment and providing access to expert management without the need for dedicated in-house resources. Additionally, it offers fast deployment, short buying cycles, minimal internal resource use for contracting and onboarding, and flexibility with short contract termination clauses.

Get Started!

Request your Demo or Webinar!

Sign up for a Demo or Webinar now and discover how to enhance your security measures. Reduce the risk of data breaches and ensure adherence to regulatory standards.

Receive your pricing quotation in 48 hours!

- No set-up charges;
- Only a fixed monthly fee;
- Scalable in Users;
- Transparent & predictable.

✉ info.de@sits.com
info.ch@sits.com
info.dk@sits.com
info.nl@sits.com

www.sits.com

SITS