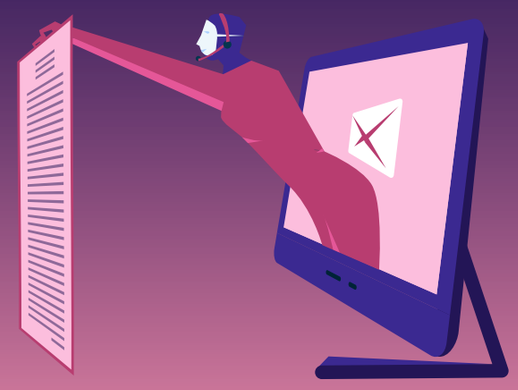
Top 15 Mistakes Companies Make
in Privileged Access Management (PAM)



Privileged Access Management (PAM) is critical for securing sensitive accounts and reducing cyber risks. However, many companies make mistakes that leave them vulnerable to security breaches. Below are the top 15 most common mistakes organizations make when implementing PAM.

01

Lack of a Comprehensive PAM Strategy

Many organizations fail to create a well-defined PAM strategy, leading to gaps in security controls and inconsistent implementation.

02

Not Identifying All Privileged Accounts

Companies often overlook service accounts, application credentials, and non-human identities, leaving them unmanaged and exposed.

03

Overprovisioning Privileged Access

Excessive access rights increase the risk of insider threats and cyberattacks. Least privilege access should be enforced to limit exposure.

04

Weak or Reused Passwords for Privileged Accounts

Storing or reusing weak passwords makes it easier for attackers to compromise accounts. Implementing password vaults and rotating credentials is essential.

05

Not Implementing Multi-Factor Authentication (MFA)

Failing to enforce MFA on privileged accounts makes them more susceptible to unauthorized access and credential theft.

06

Inadequate Session Monitoring and Auditing

Without continuous monitoring and logging of privileged sessions, companies lack visibility into suspicious activities.

07

Failure to Regularly Rotate Privileged Credentials

Static credentials increase the likelihood of credential theft. Automated credential rotation should be enforced to reduce risks.

08

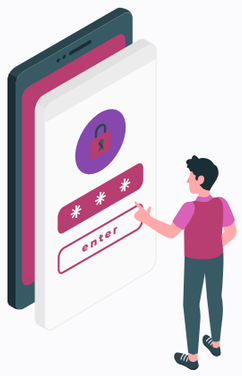
Ignoring Just-in-Time (JIT) Access

Providing persistent access instead of Just-in-Time access increases the attack surface. Temporary access should be granted only when needed.

For more content like and follow me:

@bertblevins

09



Not Enforcing Role-Based Access Controls (RBAC)

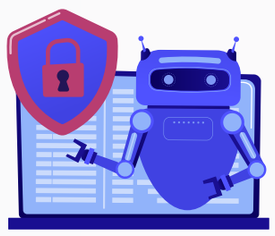
Assigning privileged access without considering user roles leads to excessive permissions and weak security controls.

10

Neglecting Third-Party and Vendor Access Management

External vendors often require privileged access but are not monitored or secured properly, creating a major security risk.

11



Lack of Automated PAM Processes

Relying on manual processes increases errors and security gaps. Automation improves efficiency and reduces human mistakes.

12

Poor Integration with Other Security Systems

PAM solutions must integrate with IAM, SIEM, and endpoint security tools for a holistic security approach.

13

Failure to Conduct Regular Privileged Access Reviews

Without regular audits, orphaned accounts and excessive privileges remain undetected, leading to compliance and security risks.

14

Underestimating Insider Threats

Employees and administrators can misuse privileged accounts if proper controls and monitoring are not in place.

15

Not Preparing for PAM Implementation Challenges

Deploying a PAM solution without proper planning can lead to resistance from users, technical issues, and poor adoption.

Conclusion

Avoiding these common PAM mistakes is crucial for strengthening security, reducing risks, and ensuring compliance. Organizations should continuously refine their PAM strategy, enforce best practices, and leverage automation to enhance privileged access security.

For more content like and follow me:  **@bertblevins**