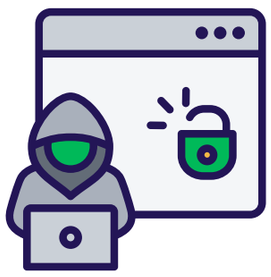
11 Facts You Didn't Know About Privileged Access Management (PAM) !

Delinea

80% of Breaches Involve Privileged Credentials



The Point:

Privileged credentials are a top target for cybercriminals because they provide high-level access.

Business Value:

- Prevents credential-based attacks, reducing financial losses.
- Protects brand reputation by preventing publicized security incidents.
- Avoids costly regulatory fines related to data breaches.

How to Implement:

- Deploy a Privileged Access Management (PAM) solution to secure all privileged credentials.
- Enforce multi-factor authentication (MFA) for all privileged users.
- Continuously monitor and rotate privileged credentials to prevent compromise.

PAM is More Than Just Password Vaulting

The Point:

PAM includes session monitoring, just-in-time (JIT) access, and behavioral analytics—not just password management.

Business Value:

- Enhances security with access control and session monitoring.
- Improves operational efficiency with automated credential rotation.
- Reduces manual security processes, saving time and resources.

How to Implement:

- Implement session recording and monitoring to track privileged activities.
- Use just-in-time (JIT) access to grant temporary privileges instead of persistent access.
- Deploy behavioral analytics to detect unusual privileged activity.

Privileged Accounts Exist in Every IT Layer

The Point:

Privileged accounts are found in OS, cloud, applications, databases, and IoT devices—not just IT admin accounts.

Business Value:

- Identifies and secures hidden privileged accounts to reduce attack surfaces.
- Improves compliance by ensuring all privileged access is properly managed.
- Strengthens overall cybersecurity posture by minimizing unmanaged credentials.

How to Implement:

- Conduct a privileged account discovery to identify all privileged accounts.
- Apply least privilege principles to restrict unnecessary access.
- Implement automated account lifecycle management to onboard and offboard privileged accounts securely.

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

11 Facts You Didn't Know About Privileged Access Management (PAM) !

Delinea

Service Accounts Are a Major Security Risk

The Point:

Service accounts often have static credentials and excessive privileges, making them easy targets for attackers.

Business Value:

- Prevents service account exploitation, reducing risk of lateral movement attacks.
- Automates password rotation, reducing IT overhead.
- Ensures continuous business operations by securing critical automated processes.

How to Implement:

- Replace hardcoded service account credentials with a secure vault.
- Rotate service account passwords automatically to prevent credential compromise.
- Restrict service account privileges to only what is necessary for operations.

Zero Trust Relies on PAM

The Point:

Zero Trust security requires strict access verification, which PAM enforces through least privilege access and MFA.

Business Value:

- Strengthens Zero Trust by enforcing strict access control.
- Reduces insider threats and external attacks by limiting unnecessary access.
- Improves regulatory compliance by ensuring all privileged access is verified.

How to Implement:

- Enforce least privilege access and role-based access control (RBAC).
- Implement continuous authentication and identity verification.
- Ensure real-time privileged access monitoring with adaptive risk scoring.

Humans Aren't the Only Users

The Point:

Machine identities (APIs, bots, scripts) also have privileged access and need to be secured like human users.

Business Value:

- Reduces risk of machine identity abuse by securing non-human accounts.
- Prevents downtime and security breaches caused by compromised API keys and scripts.
- Ensures secure automation and cloud service integration.

How to Implement:

- Use secrets management solutions to store and rotate API keys and credentials securely.
- Implement automated authentication for machine identities.
- Enforce privileged access monitoring for all non-human accounts.

PAM Can Prevent Ransomware Spread

The Point:

Attackers use privileged accounts to move laterally across networks—PAM restricts their ability to spread.

Business Value:

- Limits ransomware damage by restricting lateral movement.
- Reduces financial impact by preventing data encryption and ransom demands.
- Enhances business continuity by ensuring rapid recovery from security incidents.

How to Implement:

- Enforce application whitelisting to prevent unauthorized execution.
- Use endpoint privilege management to restrict local admin rights.
- Implement real-time threat detection for privileged account misuse.

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

11 Facts You Didn't Know About Privileged Access Management (PAM) !

Delinea

Session Recording is a Double-Edged Sword

The Point:

Session recording enhances security but must be managed properly to avoid privacy risks.

Business Value:

- Provides strong security oversight while balancing privacy concerns.
- Enhances compliance by maintaining an auditable trail of privileged activity.
- Reduces risk of insider threats through detailed monitoring of privileged actions.

How to Implement:

- Ensure encrypted and secure storage of recorded sessions.
- Limit access to recordings based on roles and compliance requirements.
- Implement automated anomaly detection in session recordings.

Privileged Access Extends to Cloud and DevOps

The Point:

Traditional PAM focused on on-premise environments, but modern IT includes cloud, DevOps, and CI/CD pipelines.

Business Value:

- Secures cloud and DevOps environments, preventing unauthorized access.
- Reduces security vulnerabilities in dynamic cloud and containerized workloads.
- Improves IT agility by automating access management in fast-moving DevOps workflows.

How to Implement:

- Use cloud-native PAM solutions that integrate with AWS, Azure, and GCP.
- Implement secrets management for DevOps pipelines.
- Automate privileged access provisioning and deprovisioning.

PAM Helps with Compliance (and Saves You from Fines)

The Point:

Regulations like GDPR, HIPAA, PCI DSS, and NIST require strict privileged access controls.

Business Value:

- Helps organizations avoid hefty fines by meeting compliance requirements.
- Reduces legal risks associated with non-compliance.
- Strengthens trust with customers and stakeholders by demonstrating security best practices.

How to Implement:

- Conduct regular compliance audits of privileged access.
- Automate compliance reporting with PAM tools.
- Implement role-based access controls to meet regulatory standards.

Privileged Credential Abuse is Hard to Detect Without PAM

The Point:

Malicious privileged activity often appears normal, making it difficult to detect without PAM monitoring.

Business Value:

- Prevents costly security incidents by identifying and stopping credential abuse.
- Reduces the burden on security teams by automating privileged access monitoring.
- Enhances threat detection capabilities with real-time visibility into privileged activity.

How to Implement:

- Deploy real-time privileged activity monitoring.
- Use AI-driven anomaly detection to identify suspicious behavior.
- Implement privileged session recording and alerts.

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