Data Backup, Mitigation M1053 - Enterprise

Archived: 2026-04-05 13:11:18 UTC

Data Backup involves taking and securely storing backups of data from end-user systems and critical servers. It ensures that data remains available in the event of system compromise, ransomware attacks, or other disruptions. Backup processes should include hardening backup systems, implementing secure storage solutions, and keeping backups isolated from the corporate network to prevent compromise during active incidents. This mitigation can be implemented through the following measures:

Regular Backup Scheduling:
- Use Case: Ensure timely and consistent backups of critical data.
- Implementation: Schedule daily incremental backups and weekly full backups for all critical servers and systems.

Immutable Backups:
- Use Case: Protect backups from modification or deletion, even by attackers.
- Implementation: Use write-once-read-many (WORM) storage for backups, preventing ransomware from encrypting or deleting backup files.

Backup Encryption:
- Use Case: Protect data integrity and confidentiality during transit and storage.
- Implementation: Encrypt backups using strong encryption protocols (e.g., AES-256) before storing them in local, cloud, or remote locations.

Offsite Backup Storage:
- Use Case: Ensure data availability during physical disasters or onsite breaches.
- Implementation: Use cloud-based solutions like AWS S3, Azure Backup, or physical offsite storage to maintain a copy of critical data.

Backup Testing:
- Use Case: Validate backup integrity and ensure recoverability.
- Implementation: Regularly test data restoration processes to ensure that backups are not corrupted and can be recovered quickly.

Source: https://attack.mitre.org/mitigations/M1053