Clock synchronization

ISO 27002 Control 8.17

Control

The clocks of information processing systems used by the organization should be synchronized to approved time sources

Purpose

To enable the correlation and analysis of security-related events and other recorded data, and to support investigations into information security incidents

Why is it important?

- Consistent time is essential for correlating logs between systems for effective analysis and incident investigation
- Inaccurate audit logs can hinder investigations and damage the credibility of evidence in legal/disciplinary cases
- Time requirements may be imposed by legal, statutory, regulatory, or contractual mandates

How can it be implemented ?

- Document external and internal requirements for time reliability and accuracy
- Define and implement a standard reference time source (e.g., GPS or atomic clock)
- Use synchronization protocols (e.g., NTP, PTP) to ensure all networked systems are in sync
- Monitor and record clock differences when using multiple cloud or hybrid services

Common misconceptions

- Minor clock discrepancies are acceptable (even small variances hinder log correlation)
- Synchronization is only needed for servers (it should apply to all systems used to aid investigations)

Link with other frameworks

- NIST 800-53 rev5 : AU-8
- NIST CSF 2.0 : PR.DS-01, PR.DS-02, PR.DS-10, PR.PS-04

Renaud Dardenne
Asphalia Consulting