Data leakage prevention

ISO 27002 Control 8.12

Control

Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information

Purpose

To detect and prevent the unauthorized disclosure and extraction of information by individuals or systems

Why is it important?

- DLP protects sensitive organizational information (e.g., IP, trade secrets)
- It addresses the legal concerns (privacy, data protection) inherently raised by monitoring personnel communications
- Actions can be oriented to confuse an adversary's decisions (e.g., replacing authentic information with false information)

What are good examples ?

- Email content filtering and scanning
- USB/removable media controls
- Cloud storage monitoring and restrictions
- Screen capture and print blocking
- Data classification and labeling
- Endpoint DLP agents
- Network traffic inspection for sensitive data

What are the risks if badly implemented ?

- Unauthorized disclosure and extraction of sensitive information by individuals or systems
- Legal concerns related to privacy, data protection, and interception of data if monitoring is improperly deployed
- Adversary obtaining confidential or secret information through intelligence actions
- Disclosure of sensitive information via unprotected backups

Link with other frameworks

- NIST 800-53 rev5 : AU-13, PE-3(2)*, PE-19, SC-7(10)*, SI-20
- NIST CSF 2.0 : NA

Renaud Dardenne
Asphalia Consulting