Installation of software on operational systems

ISO 27002 Control 8.19

Control

Procedures and measures should be implemented to securely manage software installation on operational systems

Purpose

To ensure the integrity of operational systems and prevent exploitation of technical vulnerabilities

Why is it important?

- Inappropriate software installation can compromise operational system integrity and introduce vulnerabilities
- Mitigates risks associated with using unsupported or unmaintained software versions
- Follows the principle of least privilege regarding user installation rights

What should be put in place ?

- Perform updates only by trained administrators with management authorization
- Only install approved executable code (no development code/compilers)
- Test software extensively before installation
- Define a rollback strategy before changes
- Maintain an audit log of all updates

Best practices

- Performing updates only by trained administrators upon appropriate management authorization
- Defining a rollback strategy before changes are implemented
- Enforcing strict rules on which types of software users can install (least privilege principle)

Link with other frameworks

- NIST 800-53 rev5 : CM-5, CM-7(4)*, CM-7(5)*, CM-11*
- NIST CSF 2.0 : ID.RA-07, PR.DS-01, PR.PS-01, DE.CM-01, DE.CM-09

Renaud Dardenne
Asphalia Consulting