Management of technical vulnerabilities

ISO 27002 Control 8.8

Control

Information about technical vulnerabilities of information systems in use should be obtained, the organization's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken

Purpose

To prevent exploitation of technical vulnerabilities

Why is it important?

- An accurate asset inventory is a prerequisite for effective management
- Failure to update systems promptly is a primary cause of breaches
- Ensures compliance with supplier requirements regarding vulnerability reporting

How can it be implemented ?

- Obtain information about vulnerabilities from internal/external resources and suppliers
- Evaluate identified vulnerabilities to determine associated risks and actions
- Implement a software update management process to ensure patches are installed
- If no update is available, consider compensatory controls (e.g., adjusting access controls, increasing monitoring, virtual patching)

Attention should be given to

- The timeline to react to notifications of relevant technical vulnerabilities should be defined
- The organization should develop procedures and capabilities to receive vulnerability reports from internal or external sources
- If adequate testing of updates is not possible, a delay in updating can be considered to evaluate the associated risks based on other users' experience

Link with other frameworks

- NIST 800-53 rev5 : RA-3, RA-5, SI-2, SI-5
- NIST CSF 2.0 : ID.AM-08, ID.RA-01, PR.DS-01, PR.PS-02, PR.PS-03

Renaud Dardenne
Asphalia Consulting