Protection against malware

ISO 27002 Control 8.7

Control

Protection against malware should be implemented and supported by appropriate user awareness.

Purpose

To ensure information and other associated assets are protected against malware

Why is it important?

- Malware detection software alone is usually inadequate (requires integrated controls like awareness and allow listing)
- Ensures protection at different points (defence in depth), such as network gateways and user endpoint devices
- Ensures appropriate business continuity plans are in place for recovering from malware attacks (8.13)

What are good properties ?

- Presence, coverage and update of antimalware and antivirus
- Whitelist of applications used
- Network filtering of software downloads
- Regular scans
- Scans of incoming files + zips + attachements
- Proxy filtering
- Incident management for viruses/malware
- Virus/malware awareness

What are the best practices ?

- Using defence in depth principles (detection at gateway and endpoints)
- Implementing rules and controls to prevent or detect the use of unauthorized software (e.g., application allow listing)
- Providing user awareness or training on how to identify and potentially mitigate malware receipt

Link with other frameworks

- NIST 800-53 rev5 : AT-2, SI-3
- NIST CSF 2.0 : DE.CM-01, DE.CM-09

Renaud Dardenne
Asphalia Consulting