
Politika ochrany proti malwaru (Anti-Malware Policy)

Verze: 1.0

Platnost od: 27. 01. 2026

Garant procesu: Fleet Manager / IT Administrátor

Vazba na ISO/IEC 27001:2022:

- A.8.7 – Ochrana proti malwaru (endpointy)
- A.8.32 – Ochrana proti malwaru (servery / infrastruktura)

---

1. Účel

Účelem této politiky je chránit informační aktiva organizace před škodlivým kódem (viry, ransomware, spyware), snížit riziko kompromitace systémů a stanovit jednotná pravidla pro nasazení a provoz ochranných mechanismů (AV/EDR).

2. Rozsah nasazení ochrany

Ochrana proti malwaru je aplikována dle typu aktiva a jeho technických možností:

Typ aktiva	Úroveň ochrany	Odpovědnost
Administrátorské a uživatelské stanice	EDR / AV s behaviorální detekcí	IT Administrátor
Backendové servery	AV + behaviorální ochrana + FIM	IT / Externí dodavatel
Telemetrické jednotky (IoT)	Integrita FW + whitelisting	Vývoj / System Specialist

3. Technická opatření

Organizace uplatňuje následující opatření:

- **Centrální správa:** Ochranné nástroje jsou spravovány centrálně, včetně aktualizací signatur a politik.
- **Rezidentní ochrana:** Skenování v reálném čase je povinné na všech stanicích s přístupem k backendu nebo VPN.

- **Behaviorální detekce:** EDR nástroje sledují podezřelé chování (např. masové šifrování souborů).
- **Externí média:** Použití externích nosičů na administrátorských stanicích je zakázáno bez schválení a kontroly.

4. Ochrana telemetrických jednotek

(Reakce na RISK-FW-01) Vzhledem k omezeným prostředkům IoT zařízení je ochrana realizována nepřímo:

- **Code Signing:** Spuštění je povoleno pouze pro digitálně podepsaný firmware.
- **Whitelisting:** Povolen je pouze definovaný seznam procesů a služeb.
- **Minimalizace útokové plochy:** Nepotřebné služby a porty jsou trvale deaktivovány.

5. Reakce na detekci malwaru

Při zjištění malware se postupuje následovně:

1. **Izolace:** AV/EDR automaticky izoluje soubor nebo zařízení.
2. **Hlášení:** Incident je okamžitě nahlášen IT Administrátorovi.
3. **Analýza a náprava:** Je provedena analýza příčiny a odstranění hrozby. Závažné případy se řeší dle *Směrnice pro řešení bezpečnostních incidentů*.

6. Odpovědnosti

- **IT Administrátor:** Správa, monitoring a aktualizace ochranných nástrojů.
- **Externí dodavatel:** Ochrana serverové infrastruktury dle smluvních závazků.
- **Zaměstnanci:** Povinnost respektovat varování ochranných nástrojů a hlásit incidenty.

7. Auditní důkazy

Pro účely auditu jsou evidovány:

- Reporty z centrální správy AV/EDR.
- Logy detekcí a řešení incidentů.
- Konfigurační standardy ochrany koncových bodů a serverů.