
Proces správy technických zranitelností (Vulnerability Management)

Verze: 1.0

Platnost od: 20. 01. 2026

Garant procesu: Fleet Manager / Vedoucí IT

Vazba na ISO 27001:2022: A.8.8 (Správa technických zranitelností), A.5.7 (Threat Intelligence)

---

1. Účel procesu

Cílem procesu je minimalizovat riziko zneužití slabin v telemetrickém ekosystému (jednotky, API, backend) prostřednictvím systematické detekce, vyhodnocení a odstranění zranitelností.

Tento proces vychází z **Registru rizik (RISK-VULN-01)** a přímo realizuje doporučené opatření: zavedení systematického skenování a řízení oprav.

---

2. Cyklus správy zranitelností

Fáze 1: Vyhledávání (Skenování)

Organizace provádí pravidelné skenování aktiv podle typu:

Aktivum	**Nástroj / metoda**	**Interval**
API a Web App	OWASP ZAP / Burp Suite	Minimálně 1× měsíčně a po každé významné změně kódu
Backend infrastruktura	Nessus / OpenVAS	1× kvartálně
Firmware jednotek	Statická analýza kódu	Před každým vydáním nové verze

Fáze 2: Vyhodnocení a prioritizace

Každá nalezená zranitelnost se hodnotí podle CVSS (*Common Vulnerability Scoring System*):

Kritičnost	CVSS skóre	Dopad
Kritická	9.0 – 10.0	Přímé ohrožení dat zákazníků (např. SQL Injection v API)
Vysoká	7.0 – 8.9	Možnost kompromitace systému (např. chybějící MFA u VPN)
Střední / Nízká	0.1 – 6.9	Informační zranitelnosti nebo obtížně zneužitelné chyby

Fáze 3: Lhůty pro nápravu (SLA)

Na základě prioritizace se stanovují závazné lhůty pro opravy (patching):

Priorita	Lhůta pro opravu	Odpovědnost
Kritická	**Do 48 hodin**	Vývojový tým / Správce backendu
Vysoká	**Do 14 dnů**	Vývojový tým / Správce backendu
Střední	Do 60 dnů	Plánovaná údržba
Nízká	Dle uvážení	Plánovaná údržba

---

3. Výjimky (Reakce na RISK-VULN-09)

Pokud nelze zranitelnost opravit v dané lhůtě (např. nekompatibilita starší telemetrické jednotky), musí být:

- Zapsána do Registru výjimek.
- Schválena Fleet Managerem (vlastník rizika).
- Zajištěna **kompenzačním opatřením** (např. přísnější monitoring v SIEM, izolace v síti).

---

4. Threat Intelligence (Sledování nových hrozeb)

IT oddělení pravidelně sbírá a analyzuje relevantní informace o hrozbách z externích zdrojů:

- **Konektivita:** Bulletiny mobilních operátorů a výrobců SIM modulů.
- **Backend:** Oznámení používaných databází a OS (např. Linux security advisories).
- **API / Web:** Novinky a doporučení od komunity OWASP.

Na základě těchto informací organizace provádí risk-based aktualizace procesu patchování a prioritizuje mitigaci hrozeb, které se aktuálně objevují v železničním nebo telemetrickém sektoru.

---

5. Auditní důkazy a reporting

Pro potřeby ISO 27001 auditu (články 9.1 a 10.2) se eviduje:

1. **Reporty ze skenerů:** Doklad, že skenování proběhlo podle plánu.
2. **Tickets / úkoly (Jira):** Důkaz, že nalezené zranitelnosti byly opraveny v termínu SLA.
3. **Seznam schválených výjimek:** Evidence výjimek a kompenzačních opatření.
4. **Reportování pro vedení:** Vedoucí IT předkládá Fleet Managerovi kvartální souhrnný report (*Vulnerability Dashboard*), který obsahuje:
    - Počet detekovaných zranitelností dle kritičnosti.
    - Procento zranitelností opravených v rámci SLA.
    - Přehled schválených výjimek.
5. **Dokumentace SLA / RTO / RPO:** Pokud zranitelnost souvisí s dostupností či obnovou dat.