
Proces bezpečné CI/CD pipeline (Secure CI/CD Process)

Verze: 1.1

Platnost od: 27. 01. 2026

Garant procesu: Vedoucí IT / Lead Developer

Vazba na ISO/IEC 27001:2022:

- A.8.25 – Zabezpečení životního cyklu vývoje
 - A.8.29 – Bezpečnost v testování a provozu
 - A.8.31 – Správa změn
-

1. Účel

Účelem tohoto procesu je zajistit, aby veškerý software a konfigurace (firmware, backendové služby, infrastruktura jako kód) byly před nasazením do produkce automaticky testovány, bezpečnostně ověřeny, schváleny a auditně dohledatelné. Proces minimalizuje riziko zavlečení zranitelností, neautorizovaných změn a kompromitace dodavatelského řetězce.

2. Architektura CI/CD pipeline

CI/CD pipeline je navržena jako posloupnost povinných **Quality Gates**, které musí být úspěšně splněny pro pokračování do další fáze.

Fáze	Aktivita	Povinná bezpečnostní kontrola
1. Commit	Commit kódu do Git repozitáře	Secret Scanning
2. Build	Kompilace / sestavení artefaktu	SCA (závislosti)
3. Test	Unit & integrační testy	SAST
4. Staging	Nasazení do testovacího prostředí	DAST
5. Release	Schválení vydání	Code Signing
6. Deploy	Nasazení do produkce	Auditní záznam

Poznámka: Neúspěch v kterékoliv fázi automaticky zastavuje pipeline.

3. Bezpečnostní kontroly v pipeline

- **Secret Scanning:** Automatická detekce úniku hesel, API klíčů, certifikátů nebo tokenů. Commit obsahující tajemství je zablokován.
- **Software Composition Analysis (SCA):** Kontrola všech závislostí na známé zranitelnosti (CVE). Kritické zranitelnosti (CVSS \geq 9.0) blokuji build.
- **Statická analýza (SAST):** Automatizovaná analýza zdrojového kódu zaměřená na bezpečnostní chyby (např. injekce, špatná práce s pamětí, autentizace).
- **Code Review (pravidlo čtyř očí):** Každá změna musí být schválena minimálně jedním dalším vývojářem před sloučením do hlavní větve.
- **Dynamická analýza (DAST):** Testování běžící aplikace nebo API ve staging prostředí s cílem detekce runtime chyb a slabin autentizace/autorizace.

4. Správa artefaktů a digitální podpisy

(Vazba na RISK-FW-01)

- Všechny produkční artefakty (zejména firmware) musí být digitálně podepsány v rámci CI/CD pipeline.
- Podpis probíhá pomocí klíčů uložených v zabezpečeném Key Vaultu dle *Procesu správy kryptografických klíčů*.
- Nasazení artefaktu, který nepochází z oficiální CI/CD pipeline nebo není podepsán, je zakázáno.

5. Prostředí a řízení přístupu

- **Oddělení prostředí:** Vývojové, testovací (staging) a produkční prostředí jsou striktně oddělena.
- **Produkční přístup:** CI/CD pipeline používá dedikované servisní účty s minimálními oprávněními.
- **Zákaz přímého přístupu:** Vývojáři nemají přímý zápisový přístup do produkčních systémů, databází ani infrastruktury.

6. Vazba na řízení změn

Každé produkční nasazení je považováno za změnu:

- Nasazení musí být dohledatelné k RFC / ticketu.
- Změny podléhají *Politice řízení změn*.

- Rollback postup je povinnou součástí release.

7. Odpovědnosti

- **Lead Developer:** Odpovídá za návrh pipeline a nastavení Quality Gates, schvaluje technické změny v pipeline.
- **Security Officer:** Provádí revize bezpečnostních nástrojů, schvaluje výjimky při falešných pozitivních nálezech.
- **IT Administrátor / DevOps:** Spravuje infrastrukturu CI/CD, zajišťuje aktualizace nástrojů a runnerů.

8. Auditní důkazy

Organizace uchovává:

- Build a pipeline logy včetně výsledků bezpečnostních kontrol.
- Záznamy o schválení merge requestů.
- Historii nasazení verzí do produkce.
- Vazbu release → ticket / změna.