**Příloha č. 4 – Technická specifikace**

**Minimální specifikace penetračních testů**

1. Poskytovanou službou je **provedení penetračních testů aplikačního a infrastrukturního prostředí ČRo.** Testovány budou tyto tři platformy:
   1. Platforma redakčního systému Diego
      1. PHP 8+
      2. Symfony 6/7+
         * Doctrine ORM
         * Symfony Mailer
         * API Platform
         * OAuth2
         * AssetMapper
         * Redis (cache)
         * RabbitMQ (message broker
      3. Stimulus (Symfony UX)
      4. Vue (3)
      5. React (17+)
      6. Tailwind
      7. Bootstrap (5.3+)
      8. MySQL
      9. AWS S3
      10. Docker
      11. Kubernetes
   2. Webové aplikace iROZHLAS 2.0 včetně souvisejících API
      1. HTML5 a SASS s použitím metodik BEM/ITCSS
      2. Tailwind CSS
      3. Twig/Nunjucks
      4. React, Vue
      5. Vanilla JS (ES2015+) a TypeScript
      6. Shaka Player
      7. npm, Gulp, Babel
   3. Integrační a datové platformy rAPI
      1. PHP 8.1+
      2. Symfony 6.4+
         * Doctrine
      3. PHPCS
      4. SQL (MariaDB)
   4. další ad-hoc aplikace a projekty:

Testování serverových aplikací a software, jejich infrastruktura, webové rozhraní a API.

Bude realizováno jen v tom případě, že rozpočet rámcové dohody nebude kompletně vyčerpán na přechozí tři penetrační testy.

1. Služby jsou poptávané za účelem identifikace zranitelností, architektonicky či technicky slabých míst a potenciálních rizik souvisejících s informační bezpečností. Testování bude provedeno za účelem posílené bezpečnosti systému, ochrany citlivých dat, zlepšení architektury či technických vlastností testovaných systémů a aplikací. Testování a jeho jednotlivé kroky budou prováděny v úzké koordinaci s objednatelem a dodavatelem serverové infrastruktury.
2. Cílem penetračních testů je ověřit úroveň zabezpečení, zejména pak zda:

* lze získat neoprávněný přístup k službám/datům/systémům,
* lze neoprávněně modifikovat/zničit data,
* lze narušit dostupnost služeb/systémů,
* lze získat autentizační údaje,
* lze zneužít infrastrukturu k útokům na sítě a služby třetích stran a existují zranitelnosti, které mohou vést k předchozím bodům
* lze zneužít aplikační prostředí nebo UI.

1. Testování (včetně retestování) bude provedeno na základě metodiky **OWASP (Open Web Application Security Project)** nebo jejích ekvivalentů.
2. Prezentace výstupů bude realizována osobně nebo formou videokonference.
3. Na základě výsledů testů zadavatel případně implementuje následná opatření na straně aplikace nebo infrastruktury.
4. Po implementaci opatření výše Poskytovatel retestuje relevantní zranitelnosti s cílem ověřit účinnost přijatých opatření

**Specifikace výstupů**

1. Ohlášené grey-box penetrační testy, tzn. testy probíhají z hlediska jejich uživatelů nebo potenciálních útočníků. Dodavateli bude rozkryta základní logika aplikace/infrastruktury a dodána základní dokumentace a popis jejich fungování.
2. Předmětem testování jsou serverové aplikace a software, jejich infrastruktura, webové rozhraní a API.
3. Penetrační testování bude spočívat zejména v:

(demonstrativní výčet)

* 1. automatizovaném skenování zranitelností
  2. ruční exploitaci
  3. ruční post-exploitaci
  4. dodání závěrečné zprávy obsahující zejména:
     1. Popis prováděných testů
     2. Kompletní seznam nálezů, tj. nalezených bezpečnostních zranitelností, jejich klasifikace dle závažnosti a navrhovaný způsob nápravy včetně časového harmonogramu
     3. Závěrečné zhodnocení provedeného testu
     4. prezentaci Závěrečné zprávy fyzicky či online
  5. re-testu po vyřešení zjištěných problémů ze strany objednatele po přiměřeném čase
  6. dodání závěrečné zprávy z retestu

**Předpokládaný harmonogram plnění**

* únor 2025
  + integrační a datová platforma rAPI
* duben 2025
  + redakční systém Diego
* červen 2025
  + webová aplikace iROZHLAS 2.0 včetně souvisejících API
* září 2025 – Bude realizováno jen v tom případě, že rozpočet rámcové dohody nebude kompletně vyčerpán na přechozí tři penetrační testy.
  + ad-hoc projekty