Věcné zadání pro penetrační testy systémů AIS SE

1. Úvod

Tento dokument definuje požadavky na penetrační testy systémů „**Agendové informační systémy správních evidencí“ (AIS SE),** které se skládá ze tří agendových systémů: **Evidence obyvatel (AIS EO)**, **Evidence občanských systémů (AIS EOP)** a **Evidence cestovních dokladů (AIS ECD**).

Cílem testů je odhalit zranitelnosti a identifikovat bezpečnostní slabiny v těchto klíčových systémech.

2. Technologie:

Domain	Product	Supplier
Operating system clients	Windows	Microsoft
Operation system servers	Solaris	Oracle
Database server	Informix	IBM
	MS SQL	Microsoft
	Oracle	Oracle
Application server	GlassFish	Opensource
	Sun ONE Application Server	Opensource
WEB server	Apache	Opensource
Development framework	Java	Oracle
	Angular	Opensource
Backup server	Veritas	Veritas

3. Cíle testů

Penetrační testy mají následující cíle:

- Ověřit bezpečnostní opatření v každém ze tří systémů.
- Identifikovat a analyzovat zranitelnosti, které by mohly ohrozit integritu, důvěrnost a dostupnost dat.
- Prověřit přístupová práva a ochranu citlivých informací (osobní údaje, dokumenty).
- Navrhnout doporučení pro zvýšení bezpečnosti aplikací.

4. Rozsah testů

Penetrační testy budou zahrnovat tři hlavní části aplikací AISSE:

- **Evidence obyvatel**: Ověření bezpečnosti osobních údajů, autentizace a autorizace uživatelů systému, ochrana proti úniku dat.

- **Evidence občanských průkazů**: Ověření přístupových práv a bezpečnosti správy dokumentů.

- **Evidence cestovních dokladů**: Ochrana před neoprávněnými úpravami dat a zabezpečení citlivých informací o cestovních dokladech.

Další komponenty:

- **Webová aplikace a API**: Testy zranitelností rozhraní, ochrana dat v přenosu, autentizace.

5. Metodologie

Testování bude zahrnovat:

- **OWASP Top 10**: Identifikace a testování zranitelností podle tohoto standardu.
- **PTES a NIST SP 800-115**: Sledování doporučených fází a technik pro penetrační testování.
- **Testování na zneužití práv a privilegovaného přístupu**

6. Testovací scénáře

- **Autentizace a autorizace**: Testování bezpečnosti přihlašovacích systémů, role uživatelů a ochrany uživatelských účtů.

- **Ochrana dat a osobních údajů**: Ověření, zda jsou data dostatečně chráněna proti úniku a zneužití.

- **API a integrace**: Testování zranitelností v přístupu přes API mezi jednotlivými systémy aplikace.

- **Manipulace s doklady a daty**: Ověření odolnosti proti neoprávněným úpravám údajů v evidencích.

7. Výstupy

Report z penetračního testu by měl být komplexní a obsahovat následující části:

1. Úvod: Tato část by měla obsahovat popis cíle a rozsahu testování, vysvětlení, co bylo testováno a jakým způsobem bylo testováno.
2. Metodologie: Tato část by měla podrobně popisovat, jakým způsobem byl test proveden, včetně použitých nástrojů a technik.
3. Výsledky: Tato část by měla obsahovat výsledky získané během testování, včetně nalezených zranitelností a slabých míst v systému.
4. Analýza: Tato část by měla poskytnout podrobnou analýzu nalezených zranitelností a slabých míst, včetně důvodů, proč byly zjištěny a jak by mohly být využity útočníky.
5. Doporučení: Tato část by měla obsahovat doporučení pro nápravu nalezených zranitelností a slabých míst, včetně prioritizace a způsobu oprav.
6. Závěr: Tato část by měla shrnout hlavní závěry z testování a poskytnout obecný pohled na bezpečnost systému.
7. Přílohy: Tato část by měla obsahovat podrobné technické informace o testování, včetně vstupních dat, výstupních dat, screenshotů a dalších důležitých informací.

   Je důležité, aby report byl srozumitelný, přehledný a detailní, aby poskytoval potřebné informace pro nápravu nalezených zranitelností a ochranu systému proti budoucím útokům.

- Zpráva se zjištěnými zranitelnostmi.

- Posouzení rizik na základě závažnosti.

- Doporučení k opravám a zlepšení bezpečnosti.

8. Časový harmonogram

Penetrační testy budou probíhat ve druhém čtvrtletí roku 2026. Termín zahájení testů stanoví zadavatel, délka trvání testů bude maximálně 14 kalendářních dnů a vlastním testům bude předcházet jejich příprava v délce maximálně 21 kalendářních dnů.

9. Omezení a podmínky

- Testy nebudou zahrnovat DoS/DDoS útoky bez výslovného povolení.
- Bude podepsána NDA neboli "Non-Disclosure Agreement," smlouva o mlčenlivosti, která se uzavírá mezi dvěma nebo více stranami za účelem ochrany důvěrných informací. V rámci NDA se strany zavazují, že nebudou sdělovat ani používat důvěrné informace bez souhlasu druhé strany. Tato smlouva je běžně využívána v obchodních vztazích, například při jednáních o spolupráci, sdílení technických informací nebo provádění penetračních testů, aby se zabránilo úniku citlivých dat.

10. Zodpovědné osoby

Kontaktní osoba: 

Elektronický podpis: 29.5.2026
Certifikát autora podpisu:
Jméno: Mgr. Denisa Škantová PhD., MBA
Vydal: NCA SubCA1/RSA 10/2023
Platnost do: 15.4.2029 14:18 +02:00