# Podrobná specifikace předmětu smlouvy – Nákup služeb – bezpečnostní audit a penetrační testy

## Úvod:

Předmětem této zakázky je provedení penetračních testů k dílu, které je budováno v rámci veřejné zakázky „Pořízení HW a SW vybavení – Zvýšení kybernetické bezpečnosti významných ISKÚ pro PO zavedením nových technologií (nástrojů)". Smlouva k veřejné zakázce je zveřejněna v registru smluv pod tímto odkazem: https://smlouvy.gov.cz/smlouva/29032096

Penetrační testy budou zaměřeny na ověření bezpečnosti technologické a aplikační infrastruktury, která zajišťuje komplexní bezpečnost sdílených služeb poskytovaných z Technologického centra kraje (dále jen „TCK") pro příspěvkové organizace Středočeského kraje (dále jen „PO SčK").

Testy zahrnují také kontrolu bezpečnosti centrálního systému řízení identit (IDM), který umožňuje centrální správu identit a oprávnění PO SčK, včetně přístupů do agendových a informačních systémů poskytovaných objednatelem. Cílem je ověřit zabezpečení těchto systémů a jejich napojení na bezpečnostní infrastrukturu využívanou TCK a Krajským úřadem Středočeského kraje, v souladu se zákonem o kybernetické bezpečnosti a bezpečnostními standardy.

Prostředí, které bude předmětem testování, zahrnuje technologie implementované v rámci Krajského úřadu a příspěvkových organizací, včetně jejich integrace do centrální bezpečnostní infrastruktury. Penetrační testy mají identifikovat potenciální zranitelnosti, hodnotit úroveň zabezpečení a poskytnout doporučení k posílení kybernetické odolnosti těchto systémů.

Provedení penetračních testů předpokládáme na přelomu dubna a května 2025.

# Přehled testovaných technologií

V rámci projektu byly nasazeny následující klíčové prvky technologického řešení:

1) **NGFW (Next Generation Firewall)**

- Použití firewallů FortiGate (modely 600E v TCK, 100F, 80F a 40F (na PO SčK) pro ochranu perimetru organizace.
- Zajištění vysoké dostupnosti (HA) pro klíčové systémy.
- Správa bezpečnostních pravidel, vytváření zabezpečených spojení – VPN tunel.
- Zavedení centralizovaného systému pro zaznamenávání a analýzu síťové aktivity.

2) **IDM systém (Identity Management)**

- Centralizovaná správa uživatelských identit a přístupových práv k informačním systémům (IS).
- Propojení s Active Directory (AD) a synchronizace uživatelských údajů.

3) **SAIW (Systém pro Automatizaci Incidenčních Workflow)**
- Automatizace procesů souvisejících s řešením bezpečnostních incidentů.
- Sjednocení výstrah z bezpečnostních systémů (NGFW, IDM) a dalších komponent.

# Cíl testování

### Testování má za hlavní úkol:

- Ověřit správnou implementaci výše uvedených technologií.
- Odhalit případné zranitelnosti jak v interním, tak externím prostředí.
- Zkontrolovat, zda konfigurace odpovídají doporučeným bezpečnostním postupům.
- Prověřit funkčnost klíčových bezpečnostních mechanismů, jako jsou přihlášení, VPN nebo síťová segmentace.
- Navrhnout opatření pro odstranění zjištěných nedostatků a posílení celkového zabezpečení.
- V rámci penetračního testování je cílem prověřit celkovou kvalitu a odolnost nasazeného systému. Testování se primárně zaměří na základní sadu penetračních testů, včetně síťového skenování a vyhodnocení konfigurace všech relevantních systémů. Eskalace privilegií není součástí požadovaného rozsahu testů.

## Testování se soustředí na následující oblasti:

- Ochranu perimetru organizace prostřednictvím firewallů FortiGate.
- Bezpečnost komunikace mezi jednotlivými částmi IT infrastruktury.
- Správu identit a přístupových práv v rámci IDM systému.
- Automatizaci reakce na bezpečnostní incidenty pomocí systému SAIW.
- Výsledky testování poskytnou ucelený přehled o současné úrovni zabezpečení infrastruktury a přispějí k jejímu lepšímu odolání kybernetickým hrozbám.

# Rozsah a požadované aktivity

1) **Penetrační testování vybraných webových aplikací**
    - Penetrační testování bude provedeno na vybraných webových aplikacích využívaných příspěvkovými organizacemi Středočeského kraje – celkový počet 5 aplikací (včetně portálu IDM). Aplikace jsou přístupné přes Firewally Fortinet. Aplikace běží v privátní LAN. Tyto aplikace zahrnují:

- Portál pro správu přístupů – aplikace IDM, určená ke správě oprávnění a přístupů uživatelů. Je kritická z hlediska identity managementu.
- Aplikace IDM využívá následujících pět služeb:
  - IdmUser/Me
  - IdmUser/ListUsersOnOrgUnit
  - IdmUser/Name
  - IdmWorkflow/CreateWorkflow
  - IdmRole/ListRolesOnOrgUnit
- Testování bude realizováno formou gray-box, což znamená, že dodavatel obdrží omezené informace o aplikacích, jako jsou uživatelské účty s různými oprávněními a omezené schéma aplikace.
- Zaměření testů bude podle standardů OWASP, zejména OWASP Top 10. To zahrnuje identifikaci:
  - Injekčních zranitelností (např. SQL, NoSQL, OS command injekce).
  - Špatně implementované autentizace a správy relací.
  - Chybné konfigurace zabezpečení.
  - Cross-site scriptingu (XSS).
  - Citlivých dat vystavených přes nezabezpečené kanály.
- Požadujeme tedy otestovat v roli běžného uživatele aplikace IDM, přístup k získávání jednotlivých aplikačních rolí (e-SPIS Lite, Anonymizér, GINIS PO a iTOP (HelpDesk)), uvažujeme maximálně 3-5 typů uživatelů.
- Očekávaný rozsah cílů je maximálně x.x.x.x/24.

2) **Penetrační testování firewallů Fortinet**

- Dodavatel provede komplexní test perimetru informačních systémů zadavatele, což zahrnuje veškeré služby vystavené na veřejný internet.
- Testy budou zahrnovat:

- Analýzu firewallů a pravidel přístupu na zařízeních Fortinet malé, střední i velké kategorie (modely 100F, 80F a 40F), a to vždy v počtu 1ks od každého typu
- Firewally Fortinet budou zapůjčeny dodavateli v počtu 3ks, vždy jeden od každého modelu a plně nakonfigurovány.
- Testy VPN bran z hlediska bezpečnosti přístupu a konfigurace. Bude dodavateli zapůjčen VPN.
- Simulace útoků typu DoS/DDoS v omezeném rozsahu, aby nedošlo k ohrožení provozu.
- Využití OSINT (Open Source Intelligence) k identifikaci citlivých informací z veřejně dostupných zdrojů.

- Testování bude probíhat formou black-box, kdy budou poskytnuty informace o topologii sítě, rozsahu IP adres a relevantních konfigurací.
- Součástí testu bude ověření aktualizovanosti softwaru a bezpečnostních záplat na perimetru.
- Součástí testování Firewalů budou automatizované skeny zranitelností a skeny známých zranitelností, útoky hrubou silou a hledání konfiguračních chyb manuálním hledáním.

Dodavatel zajistí podrobnou zprávu obsahující:

# Závěrečná zpráva

## Závěrečná zpráva projektu musí obsahovat následující body:

- Popis metod a postupů:
- Přehled použitých metod, rámců, standardů a vlastních přístupů, které byly aplikovány.

## Použité nástroje:

- Seznam a stručná charakteristika všech nástrojů využitých během testování.

## Testované prostředí:

Detailní popis prostředí, které bylo předmětem analýzy, zahrnující:

- Seznam IP adres zahrnutých do testování.
- Identifikované porty včetně přehledu služeb, protokolů a softwaru využívaného na jednotlivých portech.
- Přehled aplikací, které byly součástí testů.

## Prováděné testy:

- Přehled a charakteristika jednotlivých provedených testů.

## Zjištění:

- Detailní popis výsledků, který zahrnuje:
- Identifikaci zranitelností.
- Popis umístění a způsobu odhalení zranitelností.
- Označení nebo název zranitelnosti (pokud je dostupný).
- Charakteristiku a potenciální dopad zranitelnosti.

## Klasifikaci zranitelnosti podle:

- Typu a kategorie.
- Úrovně závažnosti.
- Pravděpodobnosti zneužití.
- Obtížnosti odstranění či mitigace.
- Návrh opatření nebo doporučení k eliminaci zranitelností, včetně odkazů na doporučení od výrobců nebo ověřených best practices.
- Analýzu potenciálního zneužití zranitelnosti a další důležité poznatky.

## Manažerské shrnutí:

- Stručný přehled klíčových zjištění a celkové hodnocení bezpečnostního stavu prostředí a systémů.

## Závěrečné zhodnocení:

- Shrnutí výsledků testování včetně hodnocení aktuální úrovně zabezpečení infrastruktury, aplikací a systémů.
- Doporučení pro další kroky nebo aktivity vedoucí ke zlepšení bezpečnostního stavu.

## Přiložené dokumenty:

## Elektronická podoba přehledu zranitelností ve formě tabulky (například Excel), která bude obsahovat:

- Kompletní seznam identifikovaných zranitelností včetně těch s nízkou závažností.
- Oddělený přehled výsledků validovaných jako „False positive“.
- Přílohy obsahující výstupy z automatizovaných i manuálních testů, včetně důkazů.

## Prezentace výsledků:

Dodavatel je povinen prezentovat výsledky penetračních testů vybraným zástupcům zadavatele osobně.