Předmětem plnění veřejné zakázky je zajištění externího penetračního testu vnějšího perimetru, jehož cílem bude detekce bezpečnostních mezer (ať už daných používanými technologiemi, či vzniklých chybnou konfigurací), které by mohly posloužit potencionálnímu útočníkovi k průniku do vnitřního perimetru organizace. Testovat se budou bezpečnostní prvky, tak i webové aplikace z hlediska bezpečnosti. Dále se bude jednat o interní penetrační test, který prověří bezpečnost vnitřní sítě. Toto testování musí být v souladu s metodikou OSSTMM a standardy NIST 800–115 a OWASP Top 10.
Součástí prověřování jsou technická opatření (dle vyhlášky o kybernetické bezpečnosti):

- §18 Bezpečnost komunikačních sítí
- §20 Řízení přístupových oprávnění
- §24 Sběr a vyhodnocování kybernetických bezpečnostních událostí (bude provedeno zprávou s výsledky penetračního testu)
- § 26 Kryptografické prostředky (šifrování zpráv)
- §27 Zajišťování úrovně dostupnosti informací

Zhotovitel připraví a navrhne testovací plán, který bude obsahovat rozsah testu, jeho typ a související rizika, naplánovaný čas a datum provedení testu a určení cílových komponent nebo systémů.
Objednatel poskytne potřebnou součinnost.

Zhotovitel předloží na prvním kontrolním dni testovací plán objednateli ke schválení. V rámci schválení testovacího plánu se objednatel seznámí s rozsahem testu, cílovými komponentami nebo systémy, které jsou předmětem testu, a souvisejícími riziky. Objednatel může k posouzení žádosti vyžadovat další informace od zhotovitele. Objednatel může omezit rozsah testu, stanovit a implementovat další opatření před provedením penetračního testu.

Zjištění kritického nálezu případně zjištění, která vyžadují okamžitou nápravu, bude hlášeno objednateli okamžitě po zjištění.

Testovat se bude 8 veřejných IP adres, které budou zhotoviteli poskytnuty po podpisu smlouvy.

Testování bude probíhat ve dvou fázích – sken zranitelností a manuální penetrační test, který bude obsahovat minimálně níže uvedené testy:

- Detailní detekce TCP a UDP portů
- Detekce aktivních IP adres a zjištění topologie sítě
- Test získání informací a identifikací systémů, webových aplikací a služeb
- Test DNS serverů, průzkum DNS zón, podvržení DNS serverů
- Odchycení odchozí a příchozí komunikace a následné získání informací, přesměrování této komunikace
- Test přihlašovacích údajů detekovaných systémů, webových aplikací a služeb
- Test detekovaných systémů, webových aplikací a služeb na známé bezpečnostní problémy z databáze zranitelností
- Test narušení dostupnosti služeb
- Test bezpečnosti, odolnosti a spolehlivosti bezpečnostních prvků
- Testy autentizace a autorizace systémů, webových aplikací a služeb

Provádění veškerých testů nesmí žádným způsobem ohrozit a ani omezit funkčnost produkčního prostředí Objednatele (zachování plné funkčnosti, neprodloužení odezvy aplikací atd.). Případné výjimky z tohoto ustanovení musí být před provedením konkrétního testu výslovně odsouhlaseny Objednatelem.

Zhotovitel vyhotoví Závěrečnou zprávu o nálezech zranitelností, která popisuje zjištění na základě provedeného penetračního testu. Zpráva u každé zranitelnosti klasifikuje její závažnost, místo výskytu, postup ověření zranitelnosti a jednoznačný odkaz testu v metodice, resp. ve standartu, který je součástí metodiky. Součástí zprávy je také doporučená strategie nápravy, tj. jak zranitelnosti odstranit a v jakém pořadí.

Výstupem testů bude podrobná závěrečná zpráva v elektronické podobě, která bude obsahovat:

- manažerské shrnutí,
- harmonogram testu,
- přesné zadání testu,
- omezení testu,
- použitou metodologii,
- nalezené problémy,
- detailní popis zranitelností,
- doporučení k odstranění nálezů, nebo zmírnění rizik, případně odkazy na doporučení výrobce/distributora nebo jiné best practice
- přehledové excelovské tabulky (tabulka nálezů, tabulka systémů apod.).

Získaný výsledek penetračního testu bude poskytnut jako podklad pro úpravu nastavených technických opatření.