1) Penetrační testování

Zadavatel požaduje reálnou simulaci hackerských útoků:

a) externí ověření systémů, zařízení a infrastruktury zadavatele, přístupných z veřejné sítě internet na dodaném IP rozsahu DMZ zóny zadavatele (celkem 40 veřejných IP adres)
b) interní ověření celé infrastruktury zadavatele složené z aktivních prvků Cisco, (switche, Wifi routery apod.), fyzických a virtuálních serverů s OS Windows Server nebo Linux. Testování prostupů mezi jednotlivými WLANy.
c) ověření průchodnosti a bezpečnosti VPN - odolnost vůči MITM útokům, nebo šifrovacím algoritmům

2) Provedení testů

Zadavatel požaduje provedení penetračních testů dle standardního schématu:

• **skenování prostředí** – zjišťování otevřených portů, OS běžících na detekovaných zařízeních, identifikace služeb a aplikací běžících na jednotlivých IP adresách zadavatele,

• **automatizované testy** – testy zranitelností, automatizované útoky apod.,

• **manuální testování** – testy, ověření a využití znalostních postupů v částech, kde byla zjištěna zranitelnost,

• **zpracování závěrečné zprávy** – včetně osobní prezentace výsledků zadavateli.

Dodavatel musí provést skenování:

• externích IP adres zadavatele,

• všech dostupných vnitřních IP adres infrastruktury zadavatele,

• systémů na kterých se nacházejí služby a prostředí zadavatele. Dodavatel musí provést skenování otevřených TCP a UDP portů, současně dodavatel musí provést identifikaci použitého protokolu a rovněž použitého SW pro zajištění služby na detekovaném portu. Seznam takto zjištěných portů včetně použitého protokolu a SW bude součástí závěrečné zprávy.

a) Automatizované testy

Jednotlivé služby identifikované na detekovaných portech dodavatel otestuje pomocí nástrojů pro automatizované testování zranitelností, aby byla zajištěna komplexnost testování zranitelností. Dodavatel musí do závěrečné zprávy uvést, jaké nástroje a pro jaký typ testování použil. Seznam identifikovaných zranitelností bude součástí závěrečné zprávy včetně detailního popisu zranitelnosti, její závažnosti a doporučení pro její odstranění či eliminaci hrozby s ní spojené.

b) Manuální testování

V případě zjištění zranitelnosti, která umožňuje hlubší průnik do systému zadavatele, dodavatel musí provést manuální testování s využitím uvedené zranitelnosti s cílem dosáhnout částečného nebo úplného převzetí systému, případně oprávnění, která mu nenáleží. Hlavní důvod manuálního ověření nebo jiné verifikace u nálezů je vyřazení „False positive“ nálezů a prověření případů, u kterých dle expertního odhadu existuje vysoké riziko zneužití útočníkem. Součástí závěrečné zprávy musí být zjištění získaná v průběhu testování včetně negativních zjištění (zranitelnost nebylo možné využít). Manuální ověření nebo jiná verifikace musí být provedena u všech zjištěných zranitelností skenováním nebo automatizovanými testy označené za kritické a vysoké zranitelnosti nebo opakující se u více systémů/služeb se střední zranitelností obdobného typu. V případě pozitivních zjištění dodavatel podrobně popíše dosažený výsledek a současně i okolnosti, které mu tento výsledek umožnily dosáhnout (slabá hesla, nesprávné verze protokolu atd.).

Testy budou realizovány bez přihlášení, bez znalosti architektury nebo infrastruktury aplikace.

c) Závěrečná zpráva

Do závěrečné zprávy musí dodavatel uvést minimálně:

• popis metod, metodik, norem, doporučení a vlastních postupů, které byly použity,

• seznam a charakteristiku nástrojů, které byly použity,

• popis prostředí, které bylo předmětem testů včetně, o seznamu IP adres, které byly předmětem testu, o seznam identifikovaných portů a na nich běžících služeb a protokolů použitých pro komunikaci s těmito porty a rovněž identifikovaného SW použitého pro realizaci služeb na portech, o seznam aplikací, které byly předmětem testu,

• seznam a charakteristiku testů, které byly provedeny,

• detailní seznam zjištění, minimálně v rozsahu: o identifikace zjištění zranitelnosti, o popis kde a jakým způsobem byla zranitelnost identifikována, o označení/název zranitelnosti (pokud lze přiřadit), o charakteristika zranitelnosti včetně potenciálního dopadu, o klasifikace zranitelnosti podle použité metodiky, kde bude obsaženo:

- kategorii/typ zranitelnosti,
- úroveň zranitelnosti,
- dle pravděpodobnosti zneužití,
- náročnosti odstranění/nápravy.
- popis zranitelného místa/nálezu,
- navržené opatření nebo doporučení k eliminaci nebo minimalizaci zranitelnosti, případně odkazy na doporučení výrobce/distributora nebo jiné best practice,
- další využití zranitelnosti, pokud bylo v rámci manuálních testů,
- další podstatné skutečnosti,
- stručné shrnutí včetně přehledových charakteristik a celkového hodnocení zabezpečení prostředí, ZT a systémů zadavatele,
- závěrečné zhodnocení provedeného testu a hodnocení aktuálně dosažené úrovně bezpečnosti infrastruktury, testovaných aplikací a ZT zadavatele,
- celková doporučení nebo navržení dalších kroků,
- součástí zprávy bude i excelovský soubor, který bude obsahovat celkový přehled identifikovaných zranitelností (včetně nízkých zranitelností) a ručně validované minimálně ve struktuře výše uvedené, kdy každá zranitelnost bude na jednom řádku. Excelovský soubor bude na samostatném listu obsahovat výčet nálezů manuálně validovaných a vyhodnocených za „False positive“, lze použít ve struktuře výstupu z automatizovaného nástroje.
- přílohy (výstupy z použitých nástrojů, důkazy apod.).

Závěrečná zpráva musí být předána v elektronické podobě.