



Číslo objednávky uveďte laskavě na dodacím listu a **faktuře**

Vyřizuje: Ing. Stanislav Bogdanov

Telefon: [REDACTED]

Zadavatel: MMR ČR

IČO: 660 02 222

Bankovní spojení: ČNB Praha 1, Účet č.: [REDACTED]

485 000Kč bez DPH (586 850 Kč s DPH)

Č. úkolu: 366100/6111/38/32

Dodavatel: I3 Consultants s.r.o.

IČO: 27921344

K Trninám 945/34, 163 00 Praha 6, Česká republika

Zástupce: Ing. Igor Prosecký, [REDACTED]

Předmět

Předmětem objednávky jsou následující činnosti:

1. Externí penetrační test

Cílem je prověřit bezpečnost a funkčnost prvků NEN dostupných z veřejné sítě Internet. Cílem testů je tedy prověření bezpečnosti veřejně dostupných systémů.

Externí penetrační testy se budou skládat z:

- testů k získání informací, identifikace funkčních systémů,
- všeobecných testů zranitelnosti,
- testů týkajících se charakteristiky infrastruktury systému,
- testů spolehlivosti konfigurace,
- testů existence backdoors,
- testů autentizace a schémat pro kontrolu přístupu,
- testů firewallů,
- testů routerů,
- kontroly operačních systémů,
- testů aplikačních chyb a vad v systému,
- testů nedostatečného provozního zabezpečení.

Externí penetrační testy budou probíhat vzhledem ke kooperativnímu charakteru ve dvou fázích:

- Jako neautorizovaný uživatel.
- S testovacím účtem.

2. Interní penetrační test

Bude proveden řízený útok na infrastrukturu NEN, tj. bude simulováno počínání potencionálního útočníka pokoušejícího se o průnik z vnitřní sítě.

Bude proveden řízený útok ze sítě LAN NEN.



Interní penetrační testy budou prováděny z prostředí interní LAN sítě NEN. Jejich cílem je prověření bezpečnosti systému v rámci jeho provozního prostředí a provozu interní sítě. Interní penetrační testy budou částečně kopírovat externí testy pro interní datovou síť a dále budou zaměřeny na: odposlech komunikace se systémem,

- odchyčení a přesměrování této komunikace,
- zneužití odchyčených informací a komunikace směrem k aplikačním službám (serverům),
- útoky na uživatele systému prostřednictvím tohoto systému.

3. Testování zátěže

Cílem testování benchmarkových a nárokových testů je celá infrastruktura aplikace NEN (základem bude přístup k databázovým datům, tak, aby byly měřitelné údaje napříč infrastrukturou). Primárním cílem bude stanovení a ověření mezních hodnot současně přistupujících uživatelů.

Použité aplikace a benchmarky:

- Apache Benchmark (několik rozlišných instancí (lokálně i externě)),
- JMeter,
- Wikto,
- Vmstat,
- Gnuplot,
- Specifické dávky v PERLu.

Všechny tyto nástroje budou nasazeny opakovaně se stejnými (i odlišnými vstupy) v odlišných dobách (měřeno konkrétním využitím serveru v čase) a budou zaznamenány a logovány výkonnostní výkyvy i na samotném serveru, tak, aby se předešlo možným aberacím.

Pro testy zátěže budou definovány testovací scénáře, pokrývající:

- Testy trvající 30 minut.
- Testy trvající definovaný počet transakcí,
- Testy trvající určitý počet požadavků.

Definované metriky pro sledování na straně klienta:

- Simultánní kliknutí myši klienta (tj. zaslání požadavku serveru) a odpověď serveru klientu (resp. poskytnutí nutných přesměrování/framů a obrázků).
- Požadavky klienta v rámci jakékoli vrácené odpovědi.
- Kompletně uskutečněné http požadavky (tj. i odpověď serveru musí být kompletní).
- DNS – čas nutný k resolvingu URL klientem (používán DNS systém klienta).
- Čas nutný k ustanovení spojení klienta a serveru.
- TFB (Time to first byte) – čas mezi zahájením požadavku a získáním prvního byte dat od serveru.
- Čas, po který musel uživatel čekat, než byl jeho „klik“ skončen (včetně nutných přesměrování/framů a obrázků, viz výše).
- Uživatelské pásmo (tj. jeho šíře, kterou byl uživatel schopen dosáhnout).
- Celkové počty odeslaných požadavků a přijatých odpovědí, včetně statistik (chyb, ztrát, apod.).

4. Retest po odstranění zjištění z externích a interních penetračních testů

Externí a interní bezpečnostní testy se zaměřením na zjištěné nedostatky vyplývající z nálezů v bodech 1 a 2.

Výstupy z testování

Předmětem objednávky je jak samotná příprava testovacích scénářů, tak provedení testů. Výstupem každého z realizovaných testů bude hodnotící zpráva, v které budou uvedeny informace o:

- Předmětu testování (co bylo testováno)
- Způsobu testování (tj. např. jaké testovací scénáře byly pro testování využity)
- Výsledek testování (popis výsledků a finální závěr, jestli NEN test úspěšně absolvoval či nikoliv)



Po provedení všech požadovaných testů a retestů bude v požadovaném termínu (viz níže) předložena finální hodnotící zpráva, jež bude obsahovat:

- souhrn informací o všech provedených testech (viz průběžné hodnotící zprávy),
- finální výsledky provedených testů,
- případný seznam opatření vzešlých z výsledků testování, které dodavatel doporučuje realizovat

Cena a platební podmínky

Cena za dodání plnění je stanovena ve výši maximálně 485 000Kč bez DPH (586 850 Kč s DPH).

Cena za poskytnutí plnění bude hrazena v návaznosti na akceptaci celého plnění. Akceptační protokol je ze strany objednatele schvalován: Ing. Stanislav Bogdanov (MMR ČR).

Termín realizace díla

Plnění bude provedeno v průběhu měsíců září - říjen 2016 s termínem předání závěrečné hodnotící zprávy k akceptaci (po realizaci všech výše uvedených činností) maximálně do 11. 11. 2016.



Ing. Stanislav Bogdanov

Ředitel odboru elektronizace veřejných zakázek a koncesí



Ing. Igor Prosecký

I3 Consultants s.r.o.

V Praze dne

15/09/2016



