REPUBLIKA HRVATSKA
MINISTARSTVO FINANCIJA

KLASA: 406-01/16-01/69
URBROJ: 513-03-04-16-2

Zagreb, 10. svibnja 2016.

DOKUMENTACIJA ZA BAGATELNI POSTUPAK NABAVE

PENETRACIJSKI TEST INTERNE INFORMATIČKE INFRASTRUKTURE MINISTARSTVA FINANCIJA

Bagatelna nabava: 3/16

Naručitelj: REPUBLIKA HRVATSKA
MINISTARSTVO FINANCIJA

Zagreb, svibanj 2016.

1. NAZIV I SJEDIŠTE NARUČITELJA

MINISTARSTVO FINANCIJA
Katančićeva 5
10000 Zagreb

Telefon: 01 459 1315
Telefax: 01 459 1070
Internetska adresa: www.mfin.hr
Adresa elektroničke pošte: ponuda@mfin.hr

2. JEZIK

Naručitelj će voditi postupak nabave i pripremiti Dokumentaciju na hrvatskom jeziku. Ponude moraju biti pripremljene na hrvatskom jeziku i latiničnom pismu. Komunikacija tima Ponuditelja i Naručitelja se odvija na hrvatskom jeziku. Ukoliko zaposlenici Ponuditelja ne vladaju tečnim hrvatskim jezikom, obveza je Ponuditelja na svoj trošak osigurati stalnu prisutnost prevoditelja.

3. PREDMET NABAVE

Predmet nabave je Penetracijski test interne informatičke infrastrukture Ministarstva financija.

CPV 79417000-0 Usluge savjetovanja na području sigurnosti

Procijenjena vrijednost nabave: 198.000,00 kuna

Ponuditelj je dužan ponuditi predmet nabave s tehničkim značajkama opisanima u Tehničkoj specifikaciji koja se nalazi u prilogu i čini sastavni dio Dokumentacije za bagatelni postupak nabave (Prilog 3).

OBVEZE PONUDITELJA

Usluga podrazumijeva Penetracijski test interne informatičke infrastrukture Ministarstva financija na lokacijama Ministarstva u jedinstvenom računalno mrežnom komunikacijskom sustavu.

Lokacije Naručitelja: Katančićeva 5, Zagreb; Vukovarska 72, Zagreb; Frankopanska 1, Zagreb; Veslačka 4, Zagreb; Svilajska 35, Osijek; Fiorella La Guardie 13, Rijeka te Mažuranićevo šetalište 24b, Split.

Sve usluge Ponuditelj dužan je realizirati u roku do 60 dana od dana potpisa Ugovora. Ponuditelj je u ponudi dužan dostaviti podatke o projektnom timu koji će u projektu sudjelovati.

Usluge savjetovanja

Cilj usluga savjetovanja je unapređenje rada IS-a, povećanje njegove funkcionalnosti i efikasnosti te upoznavanje s mogućnostima korištenja novih IT tehnologija. Kroz ove usluge Ponuditelj mora osigurati metodološki ujednačen pristup za sljedeće potrebe Naručitelja:

- Tehnološko savjetovanje o korištenju i unapređivanju sustava
- Uvođenje novih funkcionalnosti u sustav
- Upravljanje promjenama sustava
- Unaprjeđenje performansi sustava

4. IZMJENA DOKUMENTACIJE ZA NADMETANJE

Naručitelj može do krajnjeg roka za dostavu ponuda, prema osobnoj prosudbi ili temeljem Ponuditeljeva zahtjeva za objašnjenje Dokumentacije, izmijeniti Dokumentaciju u obliku dodatka o izmjeni. Dodatak o izmjeni Dokumentacije, Naručitelj će objaviti u elektroničkom obliku na internetskim stranicama Ministarstva financija.

5. CIJENA PONUDE

Cijena ponude mora biti izražena u kunama i pisana brojkama. U cijenu ponude bez PDV-a uračunavaju se svi troškovi i popusti. Cijenu ponude potrebno je prikazati na slijedeći način: cijena (bez PDV-a), iznos PDV-a te cijena ponude s PDV-om.
Cijena ponude izražava se za cjelokupan predmet nabave. Ponuditelj treba ispuniti originalni Troškovnik (Prilog 2), te treba ponuditi sve zatražene stavke iz Troškovnika. Ponude kod kojih nisu popunjene sve stavke Troškovnika smatrat će se neprihvatljivima.
Cijena ponude je nepromjenjiva za vrijeme trajanja ugovora i ne može se mijenjati ni po kojoj osnovi.

6. UVJETI I ZAHTJEVI KOJE PONUDITELJI MORAJU ISPUNITI

6.1. Ponuditelj je obvezan dostaviti Izjavu o nekažnjavanju iz Priloga 3. Dokumentacije.
Izjavu daje osoba po zakonu ovlaštena za zastupanje gospodarskog subjekta. Izjava ne smije biti starija od tri mjeseca računajući od dana početka postupka bagatelne nabave, a mora biti potpisana od strane odgovorne osobe i ovjerena pečatom/štambiljem.

6.2. Ponuditelj je obvezan dostaviti Potvrdu porezne uprave o nepostojanju duga, odnosno da je ispunio obvezu plaćanja dospjelih poreznih obveza i obveza za mirovinsko i zdravstveno osiguranje, osim ako mu prema posebnom zakonu plaćanje tih obveza nije dopušteno ili je odobrena odgoda plaćanja (primjerice u postupku predstečajne nagodbe).
Kako bi dokazao uvjete i zahtjeve koje mora ispuniti Ponuditelj je obvezan dostaviti Potvrda porezne uprave o stanju duga ili važeći jednakovrijedni dokument nadležnog tijela države sjedišta gospodarskog subjekta ako se ne izdaje gore navedena potvrda, ili izjava pod prisegom ili odgovarajuća izjava osobe koja je po zakonu ovlaštena za zastupanje gospodarskog subjekta ispred nadležne sudske ili upravne vlasti ili bilježnika ili nadležnog strukovnog ili trgovinskog tijela u državi sjedišta gospodarskog subjekta ili izjavu s ovjerenim potpisom kod bilježnika, ako se u državi sjedišta gospodarskog subjekta ne izdaje gore navedena potvrda ili jednakovrijedni dokument.

Potvrda ne smije biti starija od 30 dana računajući od dana početka postupka bagatelne nabave.

6.3. Ponuditelj mora dokazati svoj upis u sudski, obrtni, strukovni ili drugi odgovarajući registar države sjedišta. Ponuditelj mora biti registriran za djelatnost u vezi s predmetom nabave.
Za dokazivanje sposobnosti potrebno je dostaviti odgovarajući izvod, a ako se on ne izdaje u državi sjedišta gospodarskog subjekta, može se dostaviti izjava s ovjerom potpisa kod nadležnog tijela (javnobilježnička ovjera ili ovjera mjerodavnog tijela države sjedišta ponuditelja).
Izvod ili izjava ne smiju biti stariji od tri mjeseca računajući od dana objave poziva za dostavu ponuda
Izjavu potpisuje osoba ovlaštena za zastupanje ponuditelja

6.4. Popis ugovora o izvršenim uslugama
Popis ugovora o izvršenim uslugama u godini u kojoj je započeo postupak javne nabave i tijekom tri godine koje prethode toj godini. Ako je druga ugovorna strana naručitelj u smislu Zakona o javnoj nabavi, popis kao dokaz o uredno pruženoj usluzi sadrži ili mu se prilaže potvrda potpisana ili izdana od naručitelja. Ako je druga ugovorna strana privatni subjekt, popis kao dokaz o uredno pruženoj usluzi sadrži ili mu se prilaže njegova potvrda, a u nedostatku iste vrijedi izjava gospodarskog subjekta uz dokaz da je potvrda zatražena. Ako je potrebno, javni naručitelj može izravno od druge ugovorne strane zatražiti provjeru istinitosti potvrde.

Za dokazivanje sposobnosti potrebno je dostaviti popis, potvrdu/potvrde ili izjavu, potpisane od strane odgovorne osobe i ovjerene pečatom/štambiljem. Potvrda obvezno mora sadržavati sljedeće elemente: predmet nabave (predmet ugovora), iznos, datum pružene usluge, te naziv druge ugovorne strane, naručitelja u smislu Zakona o javnoj nabavi ili privatnog subjekta.

Gospodarski subjekt mora dokazati da je pružao usluge koje su predmet ovog postupka javne nabave temeljem izvršenja najmanje tri ista ili slična ugovora u posljednje tri godine čija je pojedinačna vrijednost bila najmanje 100.000,00 kn (bez PDV-a).Pod sličnim ugovorom Naručitelj smatra ugovor čija vrijednost iznosi minimalno 100.000,00 kn (bez PDV-a), te da su u isti uključene usluge iz najmanje 2 od sljedeća 3 područja:
- penetracijsko testiranje infrastrukturnih informacijskih sustava kao što su npr.vatrozid, web

poslužitelj, poslužitelj elektroničke pošte i sl.
- penetracijsko testiranje web aplikacija, web servisa, mobilnih aplikacija ili client-server aplikacija,
- forenzička analiza računalnih sustava i8 mobilnih telefonskih uređaja nakon sigurnosnog incidenta.

Pod sličnim ugovorom ne smatraju se općenito usluge i savjetovanja iz područja sigurnosti, savjetovanje u području uvođenja sustava upravljanja informacijskom sigurnošću, analize sigurnosnih produkata, analize i savjetovanja o otkrivenim sigurnosnim ranjivostima i sl.

Ovim dokazom gospodarski subjekt dokazuje tehničku i stručnu sposobnost za uredno izvršavanje usluga koje su predmet ovog nadmetanja.

6.5. Certifikati zaposlenika

Ponuditelj je obvezan u svojoj ponudi kao njen sastavni dio priložiti stručne certifikate tehničkih stručnjaka kojima dokazuje da raspolaže stručnim znanjima za izvršenje usluga iz predmeta nabave, i to najmanje slijedeće certifikate:

- ECC C/EH (Certified Ethical Hacker)
- (ISC)2 CISSP (Certified Information Systems Security Professional)
- GIAC GPEN (GIAC Penetration Tester)
- GIAC GCFE (GIAC Certified Forensic Examiner)
- GIAC GXPN (GIAC Exploit Researcher and advanced penetration tester)
- Offensive Security OSWP (Offensive Security Wireless Professional)
- Offensive Security OSCP (Offensive Security Certified Professional)
- Offensive Security OSCE (Offensive Security Certified Expert)

6.6. Popis tehničkih stručnjaka

Ponuditelj je obvezan u svojoj ponudi kao njen sastavni dio priložiti Popis tehničkih stručnjaka kojim dokazuje da će za cijelo vrijeme trajanja ugovora imati na raspolaganju najmanje 4 (četiri) stručnjaka iz predmetnog područja. Tražena sposobnost dokazuje se Popisom tehničkih stručnjaka koje ponuditelj ima na raspolaganju a koji posjeduju naprijed navedene važeće certifikate i preslikama certifikata.

Ponuditelji mogu u Popisu tehničkih stručnjaka navesti i certifikate koji su jednakovrijedni traženima, koje moraju priložiti svojim ponudama, ali u tom slučaju Ponuditelji moraju dostaviti dokaz jednakovrijednosti certifikata (npr. Potvrda izdavatelja traženog certifikata ili neovisnog ovlaštenog stručnog tijela da je dostavljeni certifikat jednakovrijedan traženom i slično). Pojam važeći certifikat znači da certifikat nije vremenski istekao, ukoliko je izdan na ograničeni rok važenja. Svaki certifikat mora sadržavati ime i prezime osobe na koju glasi, te mora biti izdan od strane davatelja certifikata. Certifikati priloženi u ponudi moraju biti na hrvatskom jeziku, a ukoliko su na nekom drugom jeziku, u ponudi se mora priložiti i prijevod certifikata na hrvatski jezik izrađen po ovlaštenom sudskom tumaču. Naručitelju je prihvatljivo da ponuditelj u ponudi priloži dva ili više certifikata za jednu te istu osobu. Sve navedene osobe nositelji certifikata moraju poznavati hrvatski jezik u govoru i pismu.

6.7. Izjava o alatima, uređajima ili tehničkoj opremi

Ponuditelj mora dostaviti izjavu da posjeduje alate, uređaje i tehničku opremu za izvršenje usluga skeniranja ranjivosti računalnih sustava, komunikacijskih sustava i web aplikacija, te priložiti popis. Izjava mora biti potpisana i ovjerena pečatom/štambiljom.

6.8. Izjava ponuditelja da su usluge u cijelosti sukladna zahtjevima iz tehničke specifikacije

Ponuditelj mora dati izjavu da je ponuđena usluga u cijelosti sukladna naručiteljevim zahtjevima iz tehničke specifikacije. Izjava mora biti potpisana i ovjerena pečatom/štambiljom.

6.9. Ukoliko gospodarski subjekt pri dostavi dokumenata priloži lažne podatke kojima kao natjecatelj ili ponuditelj dokazuje da ne postoje razlozi isključenja, odnosno da ispunjava uvjete sposobnosti, ponuda mu neće biti odabrana.

7. JAMSTVA

Jamstvo za uredno ispunjenje ugovora za slučaj povrede ugovornih obveza Ponuditelj je obvezan uz ponudu priložiti pisanu izjavu da će u roku od 10 (deset) dana od dana potpisa ugovora s Naručiteljem

dostaviti garanciju banke ili zadužnicu ili bjanko zadužnicu kao jamstvo za uredno ispunjenje ugovora (Prilog 5).
Ukoliko jamstvo za uredno ispunjenje ugovora bude naplaćeno, a ugovor se ne raskine, Ponuditelj je obvezan dostaviti novo jamstvo u roku od 10 (deset) dana od dana poziva na dostavu, u protivnom će Naručitelj raskinuti ugovor. Svi dokumenti mogu se dostaviti u neovjerenoj preslici. Neovjerenom preslikom smatra se i neovjereni ispis elektroničke isprave.

8. SADRŽAJ PONUDE

Ponuda mora sadržavati:
1. Obrazac ponude, Prilog 1;
2. Ponudbeni troškovnik, Prilog 2;
3. Izjava o nekažnjavanju, Prilog 4;
4. Izjava o dostavi jamstva za uredno ispunjenje ugovora, Prilog 5;
5. Potvrdu Porezne uprave o stanju duga;
6. Dokaz o upisu u sudski, obrtni, strukovni ili drugi odgovarajući registar;
7. Popis ugovora o izvršenim uslugama;
8. Izjavu da je ponuđena usluga u cijelosti sukladna zahtjevima iz tehničke specifikacije;
9. Izjava o posjedovanju alata, uređaja i tehničke opreme za uslugu Penetracijskog testa interne informatičke infrastrukture Ministarstva financija: skeniranja ranjivosti računalnih sustava, komunikacijskih sustava i web aplikacija, te priložiti popis.
10. Stručni certifikati tehničkih stručnjaka kojima dokazuje da raspolaže stručnim znanjima za izvršenje usluga iz predmeta nabave:
    - ECC C/EH (Certified Ethical Hacker)
    - (ISC)2 CISSP (Certified Information Systems Security Professional)
    - GIAC GPEN (GIAC Penetration Tester)
    - GIAC GCFE (GIAC Certified Forensic Examiner)
    - GIAC GXPN (GIAC Exploit Researcher and advanced penetration tester)
    - Offensive Security OSWP (Offensive Security Wireless Professional)
    - Offensive Security OSCP (Offensive Security Certified Professional)
    - Offensive Security OSCE (Offensive Security Certified Expert
11. Popis tehničkih stručnjaka projektnog tima koji će u projektu sudjelovati kojim dokazuje da će za cijelo vrijeme trajanja ugovora imati na raspolaganju najmanje četiri stručnjaka iz predmetnog područja.

9. PREUZIMANJE DOKUMENTACIJE

Ponuditelji Dokumentaciju za nadmetanje u bagatelnom postupku nabave preuzimaju u elektroničkom obliku na internetskim stranicama Ministarstva financija.

10. OZNAČAVANJE PONUDE

Ponuditelj predaje ponudu napisanu neizbrisivom tintom u papirnatom obliku. Ponuda mora biti uvezana u cjelinu.

11. DOSTAVA PONUDA

Ponude se dostavljaju u jednom primjerku. Elektronička dostava ponuda nije dopuštena.

Ponuda se dostavlja u zatvorenoj omotnici s naznakom:
NE OTVARAJ
"Bagatelna nabava 3/16"
te adresom Ponuditelja.

Ako omotnica nije obilježena kako je to navedeno u Dokumentaciji, Naručitelj se ne smatra odgovornim ako se omotnica zagubi ili prerano otvori.

Krajnji rok za dostavu ponuda je 25. svibnja 2016. godine do 12:00 sati.

12. OTVARANJE PONUDA

Ponude se otvaraju 25. svibnja 2016. godine s početkom u 12:00 sati na adresi Naručitelja.

Otvaranje ponuda nije javno. Ponude otvaraju najmanje dva ovlaštena predstavnika Naručitelja. Prilikom otvaranja ponuda, Naručitelj će voditi zapisnik. Nakon što se ponude javno otvore i pročitaju, ostaju kod Naručitelja i ne vraćaju se Ponuditelju.

13. POJAŠNJENJE PONUDE

Naručitelj može tijekom postupka pregleda, ocjene i usporedbe ponuda tražiti od Ponuditelja potrebna tumačenja radi pojašnjenja ponude ili otklanjanja sumnji u valjanost ponude.

Nikakve promjene u ponudi, promjene cijene, osim ispravka računske pogreške ili promjene koje bi neprihvatljivu ponudu činile prihvatljivom, Naručitelj neće zahtijevati, nuditi niti dopustiti od strane Ponuditelja.

Naručitelj će u zahtjevu za pojašnjenje ponude odrediti primjeren rok u kojem Ponuditelj treba dostaviti zatraženo objašnjenje.

Naručitelj će isključiti ponudu Ponuditelja koji unutar postavljenog roka nije dao zatraženo objašnjenje ili njegovo objašnjenje nije za Naručitelja prihvatljivo.

14. ODABIR

Naručitelj će između prihvatljivih ponuda odabrati ponudu s najnižom cijenom. Prihvatljiva ponuda je ponuda sposobnog Ponuditelja, dostavljena cjelovito za usluge iz predmeta nabave i koja potpuno zadovoljava sve tražene uvjete i zahtjeve Dokumentacije za nadmetanje. Neprikladna je ona ponuda čija cijena prelazi planirana sredstva Naručitelja. Nepravilna ponuda je ponuda koja ne ispunjava uvjete vezane za svojstvo predmeta nabave, te time ne ispunjava u cijelosti zahtjeve Naručitelja određene u Dokumentaciji za nadmetanje.

15. SKLAPANJE UGOVORA

U ovom će se bagatelnom postupku nabave sklopiti Ugovor o nabavi usluga Penetracijskog testa interne informatičke infrastrukture Ministarstva financija s rokom isporuke 60 dana.

16. ROKOVI I MJESTO ISPORUKE

Rok isporuke je 60 (sezdeset) dana, a počinje teći odmah po sklapanju Ugovora.

Mjesto isporuke na lokacijama Naručitelja: Katančićeva 5, Zagreb; Vukovarska 72, Zagreb; Frankopanska 1, Zagreb; Veslačka 4, Zagreb; Svilajska 35, Osijek; Fiorella La Guardie 13, Rijeka te Mažuranićevo šetalište 24b, Split.

Naručitelj nabavu usluga Penetracijskog testa interne informatičke infrastrukture Ministarstva financija smatra projektom i Ponuditelj je dužan osigurati vođenje projekta.

Ponuditelj treba dodijeliti voditelja projekta te izraditi terminski plan isporuke najkasnije sedam dana nakon sklapanja ugovora:

- početak projekta,
- faze projekta s popisom i opisom planiranih aktivnosti,
- kontrolne točke projekta i
- završetak projekta.

Ponuditelj je u ponudi dužan dostaviti podatke o projektnom timu koji će u projektu sudjelovati.

17. UVJETI, ROKOVI I NAČIN PLAĆANJA

Naručitelj se obvezuje plaćati temeljem ispostavljenih računa, sukladno terminskom planu aktivnosti i prethodno ovjerenom Zapisniku o primopredaji uplatom ugovorenog iznosa u korist računa Ponuditelja. Rok plaćanja je 30 (trideset) dana od dana zaprimanja računa.

18. ŽALBA

Ponuditelji nemaju pravo žalbe u postupcima bagatelne vrijednosti

Prilog 1

REPUBLIKA HRVATSKA
MINISTARSTVO FINANCIJA

OBRAZAC PONUDE

Naručitelj: REPUBLIKA HRVATSKA
MINISTARSTVO FINANCIJA
Katančićeva 5, 10000 Zagreb
OIB: 18683136487 i MB 03205991

Tvrtka ili naziv Ponuditelja: _____

Adresa Ponuditelja……: _____

OIB Ponuditelja……..: _____

Broj računa (IBAN) i naziv banke: _____

Adresa elektroničke pošte: _____

Predmet nabave: Penetracijski test interne informatičke infrastrukture Ministarstva financija

Način nabave: Bagatelni postupak nabave 3/16

Uvjeti i način plaćanja u kunama:

Cijena ponude bez PDV-a: _____
(brojkama)

Iznos PDV-a: _____
(brojkama)

UKUPNA cijena ponude s PDV-om: _____
(brojkama)

Rok valjanosti ponude: 60 dana

Rok isporuke: 60 dana od sklapanja Ugovora

_____ M.P. _____
(čitko ime i prezime ovlaštene osobe Ponuditelja) (potpis ovlaštene osobe Ponuditelja)

_____
Mjesto i datum

Prilog 2

REPUBLIKA HRVATSKA
MINISTARSTVO FINANCIJA

Naziv ponuditelja: _____

PONUDBENI TROŠKOVNIK Bagatelna nabava 3/16			
Redni broj	Opis usluga	Količina	Cijena
1.	Penetracijski test interne informatičke infrastrukture Ministarstva financija	1 komplet	
		Ukupno bez PDV-a:	
		PDV:	
		Ukupno s PDV-om:	

Cijena ponude mora biti iskazana u kunama kao nepromjenjiva. Ponuditelj mora popuniti ponudbeni troškovnik, ovjeriti ga pečatom i potpisom odgovorne osobe i priložiti ponudi.

_____ M.P. _____
(čitko ime i prezime ovlaštene osobe Ponuditelja) (potpis ovlaštene osobe Ponuditelja)

_____
Mjesto i datum

TEHNIČKA SPECIFIKACIJA

U nastavku je detaljan popis zahtjeva predmeta nabave. Ponuditelj je dužan priložiti ponudi Izjavu da je ponuđena usluga u cijelosti sukladna zahtjevima iz tehničke specifikacije.

Ponuditelj mora testirati ranjivosti i penetracijska testiranja interne informatičke infrastrukture Ministarstva financija za 500 klijentskih računala, 107 poslužitelja (Windows i Linux) i 127 aktivnih mrežnih uređaja.

Aktivnosti

Tražene aktivnosti moraju minimalno uključivati slijedeće:

- Pasivna enumeracija
  - Preslušavanje dostupnog mrežnog prometa na danoj utičnici
  - Analiza prometa i dostupnih računala i servisa
- Aktivna enumeracija
  - Analiza mrežne topologije
  - Port skeniranje (otvoreni, zatvoreni i filtrirani portovi, aktivna računala koja odgovaraju na zahtjeve...)
  - Analiza sustava (operativni sustav, te dostupne informacije koje pruža i ako je moguće)
  - Analiza dostupnih servisa (ime servisa, te inačica ako je dostupno/a)
  - Testiranje sigurnosti dostupnih servisa automatskim postupkom
  - Testiranje sigurnosti dostupnih servisa ručnim postupkom
- Iskorištavanje (Exploitation)
  - Iskorištavanje nađenih ranjivosti na osnovu prethodne faze
  - Eskalacija privilegija (ukoliko postoji ranjivost koja se može iskoristiti)
  - Probijanje zaporki (ukoliko se dođe do zaporki prethodnim metodama)
- Izvješće: Sigurnosna provjera unutrašnje IT infrastrukture

Sva testiranja je potrebno izvršavati na lokaciji Naručitelja. Sve invazivne aktivnosti je potrebno provoditi isključivo u koordinaciji s ovlaštenim predstavnikom Naručitelja. Testiranja ne smiju biti izvršena samo automatskim specijaliziranim alatima za pronalaženje ranjivosti.

Isporuke

Nakon provođenja testiranja Ponuditelj mora predati Naručitelju detaljno izvješće koje sadrži minimalno slijedeće cjeline:

- sažetak o provedenom ispitivanju za rukovoditelje
- opseg i metodologija ispitivanja
- sažeti pregled otkrivenih ranjivosti s pripadajućom klasifikacijom
- općenite informacije o ispitanom informacijskom sustavu
- opis svih identificiranih ranjivosti prema razini sigurnosnog rizika
- tehničke preporuke za uklanjanje identificiranih propusta
- ukupna ocjena sigurnosti ispitanog dijela informacijskog sustava

Ukoliko Naručitelj zahtjeva pojašnjenja izvješća Ponuditelj ih mora prezentirati.

Ponovljeno testiranje

Na zahtjev Naručitelja, nakon što Naručitelj otkloni uočene nedostatke Ponuditelj mora ponoviti parcijalno testiranje.

Obveze Naručitelja

Naručitelj će Ponuditelju osigurati korisničke račune za testiranje, te radna mjesta i mrežnu infrastrukturu.

Metodologija testiranja

Testiranje je potrebno provesti prema smjernicama PTES-a (engl. Penetration Testing Execution Standard) koji je prikazan na poveznici http://www.pentest-standard.org/, a sastoji se iz slijedećih faza:

Interakcija prije testiranja

Interakcija prije testiranja omogućuje definirati dva važna područja radi kvalitetne priprema za test: opseg (engl. scope) i uvjete testiranja (engl. rules of engagement): period testiranja, lokaciju, upravljanje osjetljivim podacima, vrijeme u kojem se obavlja testiranje (tijekom radnog vremena, po noći...), postupanje u slučaju problema na infrastrukturi ili u slučaju blokiranja prometa, dobivanje potrebnih dozvola za testiranje.

Skupljanje informacija

Prilikom obavljanja internog penetracijskog testa, skupljanje informacija ima znatno manji opseg od skupljanja informacija prilikom vanjskog penetracijskog testa. U slučaju internog testa, skupljanje informacija se najviše odnosi na prikupljanje korisničkih računa te na skupljanje ostalih informacija koje mogu pomoći prilikom analize ranjivosti i socijalnog inženjeringa.

Modeliranje prijetnji

Modeliranje prijetnji ne spada u proces penetracijskog testiranja, već se radi komplementarno penetracijskom testu u sklopu procedure za upravljanjem rizicima. Penetracijski test na temelju dobivene analize mogućih prijetnji pokušava vjerno emulirati potencijalnu prijetnju kako bi mogao evaluirati rizike vezane uz računalnu infrastrukturu.

Analiza ranjivosti

Prilikom testiranja interne infrastrukture ranjivosti se analiziraju na dva načina:

- Pasivna analiza ranjivosti sastoji se od promatranja mrežnog prometa te nalaženja ranjivosti u njemu.
- Aktivna analiza ranjivosti sastoji se od tri faze:
    - automatsko testiranje
    - ručno testiranje
    - verifikacija rezultata

Automatsko testiranje provodi se pomoću softvera za mrežno testiranje. Također se prilikom internog testiranja koristi i skener za testiranje web aplikacija bez korisničkih računa za autentikaciju. Ručnim testiranjem se pokriva sve ono što nije obuhvaćeno automatskim testiranjem. Verifikacija rezultata se radi pomoću korelacije među rezultatima skenera te ručnom provjerom.

Iskorištavanje ranjivosti

Iskorištavanje ranjivosti je najosjetljivija faza testiranja te zahtijeva planiranje i pravilno postavljanje uvjeta testiranja prije samog početka. Iskorištavanje ranjivosti je ključan dio testiranja koji pokazuje koliki je uistinu rizik koji prijetnja može učiniti pronalaskom ranjivosti. U ovisnosti o veličini projekta i zadanim ciljevima, iskorištavanje može uključivati zaobilaženje antivirusne zaštite, IDS-a, kriptiranje i pakiranje exploita, te otkrivanje 0-day ranjivosti.

Post-eksploatacijske aktivnosti

Post-eksploatacijske aktivnosti strogo su definirane uvjetima testa. Kroz uvjete testa, moguće je kao cilj definirati sljedeće aktivnosti: eskalacija privilegija, širenje na računala koja su dostupna s osvojenog računala te pribavljanje osjetljivih informacija s poslužitelja koji su inicijalno označene kao cilj testiranja.

Prilog 4

IZJAVA O NEKAŽNJAVANJU

Ja, _____ iz _____, osobna iskaznica broj _____
(ime i prezime) (mjesto)

i ja, _____ iz _____, osobna iskaznica broj _____
(ime i prezime) (mjesto)

kao osoba ovlaštena po zakonu za zastupanje gospodarskog subjekta

_____
(naziv gospodarskog subjekta)

pod materijalnom i kaznenom odgovornošću izjavljujem da ja osobno niti gore navedeni gospodarski subjekt nismo pravomoćno osuđeni za bilo koje od slijedećih kaznenih dijela, odnosno za odgovarajuća kaznena djela prema propisima države sjedišta gospodarskog subjekta, odnosno države čiji je državljanin:

a) prijevara (članak 236.), prijevara u gospodarskom poslovanju (članak 247.), primanje mita u gospodarskom poslovanju (članak 252.), davanje mita u gospodarskom poslovanju (članak 253.), zlouporaba u postupku javne nabave (članak 254.), utaja poreza ili carine (članak 256.), subvencijska prijevara (članak 258.), pranje novca (članak 265.), zlouporaba položaja i ovlasti (članak 291.), nezakonito pogodovanje (članak 292.), primanje mita (članak 293.), davanje mita (članak 294.), trgovanje utjecajem (članak 295.), davanje mita za trgovanje utjecajem (članak 296.), zločinačko udruženje (članak 328.) i počinjenje kaznenog djela u sastavu zločinačkog udruženja (članak 329.) iz Kaznenog zakona („Narodne novine" br. 125/11, 144/12, 56/15, 61/15).

Za gospodarski subjekt[1]

_____	_____
(ime i prezime ovlaštene osobe gosp. subjekta)	(ime i prezime ovlaštene osobe gosp. subjekta)
M.P.	
_____	_____
(potpis)	(potpis)

U _____, ___.___. 201__.

[1] *Ako gospodarski subjekt zastupa zakonski zastupnik sa najmanje još jednom osobom (drugim zakonskim zastupnikom, prokuristom i sl.) izjavu daju obje ovlaštene osobe.*

Prilog 5

IZJAVA O DOSTAVI JAMSTVA ZA UREDNO ISPUNJENJE UGOVORA

Ja, _____ iz _____
(ime i prezime) (adresa stanovanja)

broj osobne iskaznice _____ izdane od _____

kao odgovorna osoba _____
(naziv i adresa ponuditelja)

ponuditelja izjavljujem da ćemo u roku od 10 (deset) dana od dana potpisa ugovora s Ministarstvom financija, kao naručiteljem, za nabavu

_____

_____
(upisati predmet nabave)

dostaviti garanciju banke ili zadužnicu ili bjanko zadužnicu, kao jamstvo za uredno ispunjenje ugovora. Jamstvo za uredno ispunjenje ugovora mora biti na iznos od 10 % (deset posto) od ukupne vrijednosti ugovora s pripadajućim PDV-om .

Bankarska garancija će biti neopoziva, bezuvjetna, na „prvi poziv" i „bez prigovora".

Jamstvo za uredno ispunjenje ugovora predat ćemo u roku od 10 (deset) dana od dana potpisa ugovora s rokom valjanosti najmanje 60 (šezdeset) dana od dana proteka ugovornog razdoblja.

Jamstvo za uredno ispunjenje ugovora će se aktivirati u slučaju povrede ugovornih obveza.

U _____, ___.___. 201__.

ZA PONUDITELJA

_____
(ime i prezime ovlaštene osobe)

M.P.

_____
(potpis ovlaštene osobe)