



Številka: 416-04/26-36/5
Ljubljana, 19. 10. 2026

SPREMEMBA RAZPISNE DOKUMENTACIJE ZA ODDAJO JAVNEGA NAROČILA Z OZNAKO 416-04/26-36

Razpisna dokumentacija za oddajo javnega naročila po odprtem postopku z oznako 416-04/26-36, katerega predmet je »Vzpostavitev in zagotavljanje operativnega delovanja sistemov kibernetских zaščit ter izvajanje storitev varnostno-operativnega centra«, ki je bila objavljena na Portalu javnih naročil dne 24. 9. 2026 pod številko objave JN007533/2026-EUe16/01 se spremeni kot sledi:

– **besedilo v točki 8.1 (2) iz poglavja Razlogi za izključitev in pogoji za sodelovanje se spremeni tako, da se po novem glasi:**

- (2) Če pri preverjanju v skladu s 77., 79. in 80. členom ZJN-3 ugotovi, da gospodarski subjekt ne izpolnjuje obveznih dajatev in drugih denarnih nedavčnih obveznosti v skladu z zakonom, ki ureja finančno upravo, ki jih pobira davčni organ v skladu s predpisi države, v kateri ima sedež, ali predpisi države naročnika. Šteje se, da gospodarski subjekt ne izpolnjuje obveznosti iz prejšnjega stavka, če ima na rok za oddajo ponudb neporavnane neplačane zapadle obveznosti, ki znašajo 50 eurov ali več in nima predloženih vseh obračunov davčnih odtegljajev za dohodke iz delovnega razmerja za obdobje zadnjih petih let do roka za oddajo ponudbe.

– **besedilo v poglavju 9 razpisne dokumentacije (Merilo), točka 3 se spremeni tako, da se po novem glasi:**

Dodatne ustrezne reference ponudnika za SUVID/SIEM (T3) – do največ 5 točk
V skladu z zahtevami iz razpisne dokumentacije mora ponudniku naročniku zagotoviti in izkazati, da je v obdobju zadnjih treh (3) let pred datumom za oddajo ponudbe uspešno in kvalitetno izvedel vsaj en (1) referenčni posel s področja dobave, namestitve in implementacije Sistema za upravljanje varnostnih informacij in dogodkov (SUVID) ali sistema SIEM, z zbiranjem podatkov iz varnostnih sistemov, aktivnega imenika in aplikativnih strežnikov v vrednosti najmanj 25.000 EUR z DDV. V primeru, da ponudnik predloži več referenc kot je zahtevano v točki 8.2.2 (2), prejme točke kot je prikazano v spodnji preglednici:

Tehnična sposobnost – reference ponudnika za SUVID/SIEM	T3
število ustreznih referenčnih projektov = 1 (ponudnik izpolnjuje pogoj za sodelovanje iz točke 8.2.2.(2))	pogoj za sodelovanje
število ustreznih referenčnih projektov = 2 ali več (za vsak ustreznih referenčni projekt od 2 in naprej ponudnik prejme po	do 5 točk

eno točko vendar največ 5 točk)	
---------------------------------	--

- besedilo v poglavju 15 razpisne dokumentacije (Izvajanje storitev varnostno operativnega centra (SOC) se spremeni tako, da se po novem glasi:

15. IZVAJANJE STORITEV VARNOSTNO OPERATIVNEGA CENTRA (SOC)

V sklopu javnega naročila bo izvajalec:

- 1) v varnostno-operativni center vključil naročnikove vire in
- 2) izvajal storitve varnostno operativnega centra (SOC).

Varnostno operativni center (SOC) mora biti vzpostavljen na lokaciji v Republiki Sloveniji.

- besedilo v obrazcu 16.4 razpisne dokumentacije (Izjava o vzpostavljenem centru SOC) se spremeni tako, da se po novem glasi:

16.4. IZJAVA O VZPOSTAVLJENEM CENTRU SOC

Izjavljamo, da imamo vzpostavljen center za izvajanje storitev SOC 24 ur na dan 7 dni v tednu, vzpostavljen na lokaciji v Republiki Sloveniji in ima za ta center vpeljan sistem upravljanja neprekinjenega poslovanja in sistem varovanja informacij.

- besedilo v Prilogi 2 – Storitve varnostno-operativnega centra (SOC) se spremeni tako, da se po novem glasi:

Odkrivanje, razvrščanje in obravnava varnostnih dogodkov/incidentov

Izvajalec mora vse varnostne dogodke oziroma incidente trižirati¹ glede na vpliv, ki bi ga lahko imeli v informacijskem sistemu naročnika. Naročnik predvideva razvrščanje in obravnavo varnostnih dogodkov/incidentov na sledeč način:

Nivo	Klasifikacija	Opis	Aktivnosti SOC	Podroben opis, primer
4	VARNOST NI DOGODEK	Zaznane kibernetske aktivnosti, ki nimajo vpliva na omrežja in informacijske sisteme ali storitve naročnika. Varnostni dogodek se zaradi zaščit na sistemih ni zgodil.	brez	Manjši enkratni varnostni dogodek, ki ne predstavljajo neposredne grožnje za poslovanje, kot npr.: preprečen klik uporabnika na nedovoljeno povezavo, zaznava in zaustavitev prenosa potencialno okuženega dokumenta iz spleta ali medija, napaka pri prijavi uporabnika, ki se samodejno odpravi ...

¹ Triaža je proces določanja prioritete obravnave dogodkov glede na resnost njihovega stanja.

3	LAŽJI INCIDENT	Enkraten incident, ki ima majhen negativni vpliv na informacijski sistem zaupnost, celovitost in razpoložljivost omrežja, oziroma informacijskih storitev zavezanca. Nima večjega vpliva na nemoteno delovanje zavezanca in mu ni povzročil večje škode. Incident nima negativnega vpliva na druge sisteme.	diagnostika, pregled statusa zaščit na končnem odjemalcu, pregled povezanih sistemov za korelacijo dogodkov	Enkratni incidenti, ki predstavljajo posredno grožnjo za poslovanje, škodljiva aktivnost je bila zaznana, vendar ne preprečena , kot npr.: klik uporabnika na nedovoljeno povezavo, zaznava prenosa potencialno okuženega dokumenta iz spleta ali medija, skeniranje omrežja, poskus prijave uporabnika na sistem, kjer ta uporabnik ni predviden ...
	odzivni čas: 4 ure rešitev: 3 delovne dni			
2	TEŽJI INCIDENT	Enkraten incident ali zaporedje večjega števila različnih incidentov v kratkem obdobju, ki imajo lahko velik negativni vpliv na zaupnost, celovitost in razpoložljivost omrežja ali storitev. Incident ima pomemben vpliv in mu lahko povzroči škodo tudi na drugih sistemi, vendar na te sestave nima kritičnega vpliva.	takojšnja diagnostika, deaktiviranje odjemalca ali sistema, aktiviranje vseh skupin za diagnostiko	Zaznana je bila škodljiva aktivnost odjemalca ali naprave, kot npr. ciklično skeniranje omrežja, DDos napadi, pošiljanje/prejemanje več potencialno okuženih dokumentov, prijava neznanega uporabnika na sistem, delovanje kripto virusov v omejenem obsegu ...
	odzivni čas: 2 uri rešitev: 1 delovni dan			
1	KRITIČNI INCIDENT	Incident ali zaporedje incidentov, ki ima zelo velik negativni vpliv na zaupnost, celovitost in razpoložljivost omrežja, informacijskega sistema oziroma informacijskih storitev. Incident povzroči oteženo delovanje informacijskega sistema ali ga celo onemogoči.	takojšnje deaktiviranje odjemalca, ali delov omrežja AKTIVACIJA NAČRTA IZREDNIH RAZMER	Incidenti, ki povzročijo katastrofalen vpliv na organizacijo, kot so popolni izpadi sistemov ali velika varnostna kršitev, kot npr. obsežni DDoS napadi znotraj omrežij, delovanje kripto virusov, izpad strežnikov, povezav, varnostna kršitev z dostopom do občutljivih podatkov,...
	odzivni čas: 1 dan rešitev: 1 delovni dan			

Naročnik je v sklopu sprememb razpisne dokumentacije spremenil tudi obrazec 16.4. Izjava o vzpostavljenem centru SOC. Obrazec je v prilogi.

Ostala določila razpisne dokumentacije ostanejo nespremenjena.

Spremembe razpisne dokumentacije so sestavni del razpisne dokumentacije predmetnega javnega naročila.

Matjaž Zadravec
vodja Oddelka za razvoj
informacijskega sistema

Bojan Verbič
vodja Informacijskega sektorja

Špela Ocvirk
generalna sekretarka