ŽUPANIJSKA BOLNICA ČAKOVEC

Broj: 01-1122/6/2026
Čakovec, 17.04.2026. godine

ZAINTERESIRANIM GOSPODARSKIM SUBJEKTIMA

PREDMET: „GAP ANALIZA KIBERNETIČKE SIGURNOSTI (EU NIS 2)“

-dostavlja se-

Poštovani,
objavljuje se odgovor na upit zainteresiranog gospodarskog subjekta kako slijedi:

Upit:

Poštovani,

u vezi s otvorenim pozivom **„GAP ANALIZA KIBERNETIČKE SIGURNOSTI (EU NIS 2)”, EVIDENCIJSKI BROJ NABAVE: JN-67/2026**, dostavljamo dodatna pitanja.

Pitanja su organizirana prema redni brojevima stavaka iz **Troškovnika i Specifikacijama za uslugu provođenja gap analize kibernetičke sigurnosti**, na koje se pojedinačno referiramo radi jasnog definiranja očekivanog opsega i metodologije.

Redni broj 1.

Traži se "Popis i procjenu kritičnosti svih IT resursa". Da li bolnica ima postojeći popis IT imovine (asset inventory) koji ponuditelj treba pregledati i dopuniti ili se očekuje izrada potpunog popisa od nule?

Ako se radi o izradi od nule, da li možete okvirno navesti veličinu IT okruženja — broj servera, radnih stanica, mrežnih uređaja i medicinskih uređaja spojenih na mrežu?

Redni broj 2.

Traži "Reviziju sigurnosnih ugovora i razgraničenje odgovornosti s vanjskim partnerima". Da li se očekuje pravna revizija postojećih ugovora s konkretnim prijedlozima izmjena ili je u opsegu procjena trenutnog stanja upravljanja sigurnošću dobavljača kroz intervjue i pregled dokumentacije s identifikacijom GAP ova?

Redni broj 3.

Navodi penetracijsko testiranje terminal servera i provjeru mrežne segmentacije. Možete li pojasniti očekivani opseg testiranja — koliko terminal servera je u pitanju, koliko mrežnih segmenata postoji i koliko je medicinskih uređaja bez AV zaštite koji zahtijevaju poseban pristup pri testiranju?

Da li se očekuje ručno penetracijsko testiranje s aktivnom eksploatacijom ranjivosti ili je prihvatljiv kombinirani pristup — automatizirani scan i automatizirano penetracijsko testiranje korištenjem dedicirane platforme za tu svrhu? Automatizirano pen testiranje se izvodi on site i svi rezultati i podaci se ne iznose van vaše ustanove.

Da li je OSPC ili jednakovrijedan certifikat nešto što je zaista potrebno, pogotovo ukoliko se prihvaća i automatizirano penetracijsko testiranje?

Postoje li vremenski prozori u kojima je dozvoljeno provoditi testiranje (npr. noćne smjene, vikendi) s obzirom na to da sustavi podržavaju medicinske procese koji ne smiju biti prekinuti?

Redni broj 4.

Stavka 4 traži vulnerability scan uz „poštivanje specifičnosti medicinske opreme". Da li postoji popis medicinske opreme koja je spojena na mrežu i za koju se skeniranje ne smije provoditi ili se mora provoditi pod posebnim uvjetima?

Tko preuzima odgovornost u slučaju da skeniranje utječe na rad medicinskog uređaja?

Redni broj 10.1.

Navodi da su "detaljno penetracijsko testiranje ili dubinska analiza ranjivosti sustava dio opsega ove GAP analize". Možete li pojasniti odnos između stavki Rednog broja: 3, 4 i 10.1 — radi li se o jednoj ili više zasebnih aktivnosti testiranja? Penetracijsko testiranje i vulnerability scan nisu dio klasične GAP analize.

Redni broj 12.

Navodi kao očekivani ishod "Potpuna zakonska usklađenost". GAP analiza po svojoj prirodi identificira nedostatke i daje preporuke, ali sama po sebi ne donosi usklađenost — za to su potrebne dodatne aktivnosti poput procjene rizika, izrade dokumentacije (politike, procedure, planovi), implementacije tehničkih mjera, edukacije zaposlenika i službene samoprocjene prema ZSIS metodologiji.

Možete li pojasniti da li se pod "potpunom zakonskom usklađenošću" podrazumijeva da GAP analiza treba rezultirati planom za postizanje usklađenosti ili se očekuje da ponuditelj u okviru ovog ugovora provede i sve korektivne aktivnosti?

Uredba NN 135/2024 zahtijeva formalnu procjenu kibernetičkih rizika s registrom rizika, procjenom vjerojatnosti i utjecaja te planom obrade rizika. Ova aktivnost nije eksplicitno navedena u troškovniku. Da li naručitelj očekuje da procjena rizika bude dio ovog ugovora ili je to planirana kao zasebna nabava?

Isto se odnosi na planove kontinuiteta poslovanja (BCP) i oporavka od katastrofa (DRP) te upravljanje incidentima — da li se očekuje njihova izrada u okviru ovog ugovora ili samo identifikacija GAP ova u tom području?

Da li je ŽBČ već kategoriziran od strane nadležnog tijela kao ključni ili važni subjekt prema ZKS u i koja razina mjera (osnovna, srednja, napredna) se primjenjuje na bolnicu? Ovo je ključno za određivanje ciljne razine usklađenosti u GAP analizi.

Da li se u sklopu ovog opsega posla očekuje generiranje dokumentacije koja će zadovoljiti zahtjeve ZKS a i Uredbe?

Odgovor Naručitelja:

Redni broj 1.
Stručne osobe navode:

- „Imamo postojeći Asset inventory, 520 PC radnih stanica 11 terminal servera u load balansingu u CDU, jedan domenski VM server lokalno i dva na CDU, 5-6 aktivnih servera lokalno + claster s 6 virtualki. WS2016“

Redni broj 2.
Stručne osobe navode:

- „U opsegu je procjena trenutnog stanja upravljanja sigurnošću dobavljača kroz intervjue i pregled dokumentacije s identifikacijom GAP ova.“

Redni broj 3.
Stručne osobe navode:

- „Radi se o 10-tak radnih stanica, dvije telemetrijske stanice bez AV sa po 10 dojavnih jedinica, testiranje na nivou osiguranja potrebne razine sigurnosti za prijetnje s lokacija radnih stanica.“
- „Prihvatljiv je kombinirani pristup — automatizirani scan i automatizirano penetracijsko testiranje.“
  „Automatizirano pen testiranje se izvodi on site i svi rezultati i podaci se ne iznose van naše ustanove u skladu s normom NIS2.“
- „Da li je OSPC ili jednakovrijedan certifikat nešto što je zaista potrebno, pogotovo ukoliko se prihvaća i automatizirano penetracijsko testiranje? DA - u skladu s kategorizacijom NCSC-a za IT sustave srednje razine kibernetičke sigurnosti i prema 27001.“
- „Postoje li vremenski prozori u kojima je dozvoljeno provoditi testiranje (npr. noćne smjene, vikendi) s obzirom na to da sustavi podržavaju medicinske procese koji ne smiju biti prekinuti? Postoje takvi procesi ali testiranje ih nebi trebalo moći zaustaviti, no opreza radi konstatiramo da postoje.“

Redni broj 4.
Stručne osobe navode:

- „Mogućnost preuzimanja rizika od radiološke opreme tipa MR, CT i uređaj za kateterizaciju (Shimadzu), sve je moguće koordinirati s dobavljačima.“

Redni broj 10.1..
Stručne osobe navode:

- „Radi se o opsežnoj GAP analizi.“

Redni broj 12.
Stručne osobe navode:

- „Možete li pojasniti da li se pod “potpunom zakonskom usklađenošću” podrazumijeva da GAP analiza treba rezultirati planom za postizanje usklađenosti ili se očekuje da ponuditelj u okviru ovog ugovora provede i sve korektivne aktivnosti?
  Podrazumijeva se da GAP analiza treba rezultirati planom za postizanje usklađenosti.“
- „Uredba NN 135/2024 zahtijeva formalnu procjenu kibernetičkih rizika s registrom rizika, procjenom vjerojatnosti i utjecaja te planom obrade rizika. Ova aktivnost nije eksplicitno navedena u troškovniku. Da li naručitelj očekuje da procjena rizika bude dio ovog ugovora ili je to planirana kao zasebna nabava?
  Podrazumijeva se procjena u skladu s uredbom.“

- „Isto se odnosi na planove kontinuiteta poslovanja (BCP) i oporavka od katastrofa (DRP) te upravljanje incidentima — da li se očekuje njihova izrada u okviru ovog ugovora ili samo identifikacija GAP ova u tom području?
  Očekuje se njihova izrada u okviru ovog ugovora .“
- „Da li je ŽBČ već kategoriziran od strane nadležnog tijela kao ključni ili važni subjekt prema ZKS u i koja razina mjera (osnovna, **srednja**, napredna) se primjenjuje na bolnicu? Ovo je ključno za određivanje ciljne razine usklađenosti u GAP analizi.
  Srednja razina mjera.“
- „Da li se u sklopu ovog opsega posla očekuje generiranje dokumentacije koja će zadovoljiti zahtjeve ZKS a i Uredbe?
  Da, očekuje se generiranje dokumentacije koja će zadovoljiti zahtjeve ZKS a i Uredbe.“

S poštovanjem,

Odsjek za javnu nabavu, nabavu i EU fondove