

TEHNIČKA SPECIFIKACIJA ZA NABAVU SOFTVERSKOG RJEŠENJA ZA
MIKROSEGMENTACIJU MREŽE ZA POTREBE SLUŽBE ZA INFORMATIKU
(MICROSEGMENTATION / ZERO TRUST LATERAL MOVEMENT PREVENTION)

Sadržaj

1. TEHNIČKA SPECIFIKACIJA	3
1.1. PREDMET NABAVE	3
1.2. TEHNIČKA SPECIFIKACIJA I OPSEG USLUGE	3
1.2.1. Opis projekta	3
1.2.2. Upute ponuditeljima.....	3
1.3. TABLICA ZAHTJEVA	3

1. TEHNIČKA SPECIFIKACIJA

1.1. PREDMET NABAVE

Predmet ove dokumentacije su tehničke specifikacije za nabavu rješenja koje povećava sigurnost informacijskog sustava Naručitelja sprječavanjem lateralnog kretanja unutar mreže primjenom kombinirane mrežne i identitetske mikrosegmentacije (u daljnjem tekstu: rješenje).

Cilj nabave je zaštita kritične zdravstvene informacijske infrastrukture ograničavanjem neovlaštenog pristupa i kretanja unutar mreže, smanjenjem površine napada te poboljšanjem ukupne sigurnosne razine. Odabrano rješenje mora se neometano integrirati s postojećom sigurnosnom infrastrukturom Naručitelja te pružati fleksibilne politike za mrežnu segmentaciju, upravljanje identitetima i kontrolu pristupa po načelu najmanje privilegije.

1.2. TEHNIČKA SPECIFIKACIJA I OPSEG USLUGE

1.2.1. Opis projekta

Projekt obuhvaća uspostavu cjelovitog pristupa sprječavanju lateralnog kretanja kroz primjenu strategija mrežne i identitetske segmentacije. Rješenje će na mrežnoj razini provoditi mikrosegmentaciju kako bi ograničilo komunikacijske putove između resursa te integrirati identitetske kontrole radi provođenja korisnički specifičnih ograničenja pristupa.

Kombinacijom obje razine kontrole projekt će povećati sposobnosti prevenciju i otpornost Naručitelja i učinkovito blokirati neovlašteno lateralno kretanje unutar okruženja. Projekt obuhvaća faze tehnološke implementacije, testiranja i usklađivanja s regulatornim zahtjevima primjenjivim na zdravstvene ustanove.

1.2.2. Upute ponuditeljima

Ponuditelj je dužan u stupcu „DA / NE“ za svaki pojedini zahtjev iz tablice u poglavlju 1.3 označiti zadovoljava li ponuđeno rješenje predmetni zahtjev.

„DA“ – ponuđeno rješenje u potpunosti zadovoljava traženi zahtjev.

„NE“ – ponuđeno rješenje ne zadovoljava traženi zahtjev.

U stupcu „Napomena“ ponuditelj je dužan navesti referencu na dokumentaciju proizvođača (naziv dokumenta, broj poglavlja/stranice ili URL) iz koje je vidljivo zadovoljavanje zahtjeva. Za sve obvezne zahtjeve (oznaka „DA“ u stupcu „Obvezno“) odgovor „NE“ ili izostanak odgovora dovodi do isključenja ponude kao neprikladne.

Naručitelj zadržava pravo zatražiti demonstraciju (Proof of Concept) bilo koje navedene funkcionalnosti u okviru postupka pregleda i ocjene ponuda.

1.3. TABLICA ZAHTJEVA

U nastavku je objedinjena tablica svih obveznih i poželjnih zahtjeva koje ponuđeno rješenje mora zadovoljiti. Stupac „Kategorija“ označava skupinu zahtjeva (Funkcionalni, Tehnički, Razlikovni – općeniti / mrežna segmentacija / identitet / RPC / arhitektura, Podrška, Usklađenost). Ponuditelj je dužan za svaki zahtjev popuniti stupac „DA / NE“ te u stupcu „Napomena“ navesti referencu na dokumentaciju proizvođača.

Br.	Kategorija	Zahtjev	Obvezno	DA / NE	Napomena
001	Funkcionalni	Rješenje mora omogućiti detaljnu (fine-grained) segmentaciju do razine pojedinačnog resursa te provoditi načelo najmanje privilegije (least privilege).	DA		
002	Funkcionalni	Rješenje mora spriječiti lateralno kretanje napadača izoliranjem kompromitiranih uređaja i korisničkih računa.	DA		
003	Funkcionalni	Rješenje mora inherentno provoditi Zero Trust sigurnosni model uz eksplicitnu autorizaciju svake komunikacije između mrežnih resursa.	DA		
004	Funkcionalni	Rješenje mora automatski definirati kontekstualna pravila te primjenjivati pristupne politike na temelju ponašanja korisnika i kriterija temeljenih na riziku.	DA		
005	Funkcionalni	Rješenje mora pružati pregled mrežnog prometa i ponašanja resursa u stvarnom vremenu te izvještavanje o provođenju politika segmentacije i kontrolama pristupa.	DA		
006	Funkcionalni	Rješenje mora omogućiti simulaciju predloženih pravila prije njihova provođenja (test/learning mode).	DA		
007	Funkcionalni	Rješenje mora osigurati identitetski temeljenu segmentaciju (kontrolu pristupa na temelju identiteta korisnika).	DA		
008	Funkcionalni	Rješenje mora omogućiti samoposlužno (self-service) odobravanje pristupa ovlaštenim korisnicima radi rasterećenja operativnih timova.	DA		
009	Funkcionalni	Rješenje mora automatski kreirati pristupne politike za servisne račune i ograničavati sustave i metode pristupa kojima se servisne vjerodajnice mogu koristiti.	DA		
010	Funkcionalni	Rješenje mora omogućiti dinamičke mrežne dozvole na temelju verifikacije identiteta korisnika integracijom s višefaktorskom autentikacijom (MFA).	DA		

Br.	Kategorija	Zahtjev	Obvezno	DA / NE	Napomena
011	Funkcionalni	Rješenje mora omogućiti dinamičke pristupne dozvole na razini operativnih sustava integracijom s MFA mehanizmima.	DA		
012	Funkcionalni	Rješenje mora pružati vlastite MFA metode te se integrirati s postojećim MFA pružateljima naručitelja.	DA		
013	Funkcionalni	Rješenje mora osigurati zasebnu zaštitu Active Directory Domain Controllera i sprječavati napade putem RPC protokola pomoću integriranog sustava prevencije s automatskim generiranjem zaštitnih politika.	DA		
014	Tehnički	Rješenje mora omogućiti rad bez instalacije agenata (agentless) na svim podržanim operativnim sustavima, kako on-premises tako i u oblaku, koristeći isključivo native mogućnosti operativnih sustava za prikupljanje informacija i provođenje pravila pristupa.	DA		
015	Tehnički	Rješenje mora podržavati automatska ažuriranja koja ne zahtijevaju ručnu intervenciju.	DA		
016	Tehnički	Rješenje mora podržavati ažuriranja bez prekida rada (zero-downtime updates).	DA		
017	Tehnički	Rješenje mora minimizirati potrebu za specijaliziranim tehničkim znanjima za održavanje i ažuriranje softvera.	DA		
018	Tehnički	Rješenje ne smije uzrokovati značajno dodatno opterećenje procesorskih i memorijskih resursa na klijentskim i poslužiteljskim sustavima, neovisno o količini mrežnog prometa te broju i složenosti primijenjenih sigurnosnih politika.	DA		
019	Tehnički	Rješenje mora biti skalabilno za podršku tisućama sustava bez pada performansi i bez utjecaja na vrijeme potrebno za izradu i distribuciju politika segmentacije.	DA		
020	Tehnički	Rješenje mora osigurati visoku raspoloživost (HA) svih arhitekturnih komponenti (on-premises i u oblaku)	DA		

Br.	Kategorija	Zahtjev	Obvezno	DA / NE	Napomena
		bez jedinstvene točke kvara (no single point of failure).			
021	Tehnički	Rješenje mora moći automatski generirati politike segmentacije temeljem promatranog mrežnog prometa, čime se smanjuje vrijeme potrebno za definiranje pravila.	DA		
022	Razlikovni – općeniti	Rješenje mora omogućiti segmentaciju Windows i Linux sustava, Kubernetes okruženja te OT (Operational Technology) sustava putem jedinstvene upravljačke konzole.	DA		
023	Razlikovni – općeniti	Rješenje mora podržavati on-premises, IaaS i hibridna okruženja.	DA		
024	Razlikovni – općeniti	Rješenje mora podržavati fizička, virtualna i kontejnerizirana okruženja.	DA		
025	Razlikovni – općeniti	Rješenje mora omogućiti segmentaciju kroz neintruzivni agent i bez agenta (agentless deployment).	DA		
026	Razlikovni – općeniti	Rješenje mora provoditi politike povezivosti koristeći nativni firewall Windows i Linux operativnih sustava.	DA		
027	Razlikovni – općeniti	Rješenje ne smije biti u liniji (inline) s mrežnim prometom, ne smije imati utjecaj na performanse mreže te smije imati zanemariv utjecaj na CPU i memoriju.	DA		
028	Razlikovni – mrežna segmentacija	Rješenje mora generirati sigurnosna pravila u potpunosti automatski, bez potrebe za ručnim pregledom svakog pravila.	DA		
029	Razlikovni – mrežna segmentacija	Rješenje mora omogućiti provjeru ponašanja predloženih politika u odnosu na promet zabilježen u proteklih najmanje 90 dana.	DA		
030	Razlikovni – mrežna segmentacija	Rješenje mora omogućiti otvaranje portova na zahtjev i vremenski ograničeno (just-in-time port opening), uz prethodno odobrenje putem MFA ili OTP-a.	DA		
031	Razlikovni – mrežna segmentacija	Rješenje mora moći identificirati izvorni i/ili odredišni proces pojedine konekcije.	DA		

Br.	Kategorija	Zahtjev	Obvezno	DA / NE	Napomena
032	Razlikovni – mrežna segmentacija	Rješenje mora omogućiti filtriranje konekcija po sljedećim atributima: izvorni host, odredišni host, izvorna oznaka (tag), odredišna oznaka, odredišni port i odredišni proces.	DA		
033	Razlikovni – mrežna segmentacija	Rješenje mora omogućiti razdoblje učenja mrežnih komunikacija u trajanju od najmanje 30 dana, na temelju kojeg se automatski grupiraju i označavaju resursi te generiraju preporučene segmentacijske politike.	DA		
034	Razlikovni – mrežna segmentacija	Rješenje mora podržati segmentaciju neupravljanih (unmanaged) OT/IoT uređaja putem integracije s mrežnim preklopnici i usmjerivačima, prikupljanjem metapodataka veza i automatskim generiranjem mrežnih ACL pravila ograničenih isključivo na operativno potrebne komunikacije.	DA		
035	Razlikovni – identitet	Rješenje mora omogućiti kontrolu logon dozvola (prijava) za Windows resurse.	DA		
036	Razlikovni – identitet	Rješenje mora automatski razlikovati i kategorizirati ljudske od servisnih računa.	DA		
037	Razlikovni – identitet	Rješenje mora prepoznati i klasificirati servisne račune te identificirati na kojim poslužiteljima i u kojim procesima se koriste.	DA		
038	Razlikovni – identitet	Rješenje mora omogućiti označavanje privilegiranih korisnika i predefinirano (deny by default) blokirati njihov pristup svakom sustavu, uz mogućnost ručnog kreiranja pravila s ili bez MFA izazova.	DA		
039	Razlikovni – identitet	Rješenje mora uključivati funkcionalnosti najmanje privilegije (least privilege) unutar iste konzole/rješenja.	DA		
040	Razlikovni – identitet	Rješenje mora omogućiti primjenu just-in-time pristupnih dozvola nakon uspješnog MFA izazova ili korištenja OTP-a.	DA		
041	Razlikovni – identitet	Rješenje mora omogućiti otkrivanje i prikaz aktivnosti korištenja servisnih	DA		

Br.	Kategorija	Zahtjev	Obvezno	DA / NE	Napomena
		računa te identifikaciju neaktivnih ili neiskorištenih servisnih računa radi uklanjanja iz okruženja.			
042	Razlikovni – identitet	Rješenje mora aktivno spriječiti napade na vjerodajnice u Active Directory okruženju, uključujući Pass-the-Ticket, Golden Ticket i Kerberoasting napade, kroz automatsko ograničavanje logon prava servisnih i administrativnih računa.	DA		
043	Razlikovni – identitet	Rješenje mora omogućiti automatsko učenje svih mrežnih logon događaja u razdoblju od najmanje 30 dana te na temelju toga automatski generirati politike koje ograničavaju servisne račune isključivo na potrebne resurse i odbijaju logon prava na sve ostale resurse.	DA		
044	Razlikovni – RPC zaštita	Rješenje mora omogućiti uvođenje zaštitnog sloja iznad RPC servisa s automatskom segmentacijom kojom se odobravaju samo autorizirane operacije, čime se osigurava zaštita od širokog raspona napada (uključujući zero-day eksploite i napade lateralnog kretanja) bez prekida normalne mrežne aktivnosti.	DA		
045	Razlikovni – arhitektura	Središnja upravljačka komponenta rješenja mora biti realizirana kao virtualni „stateless“ appliance, instalabilan iz jednog (1) virtualnog stroja, uz mogućnost dodavanja drugog (2) za potrebe redundancije/visoke raspoloživosti. Centralna komponenta ne smije pohranjivati stanje koje bi bilo izgubljeno u slučaju ispada.	DA		
046	Razlikovni – arhitektura	Inicijalna instalacija i osnovno puštanje u rad središnje upravljačke komponente ne smije trajati dulje od osam (8) radnih sati.	DA		
047	Razlikovni – arhitektura	Postizanje pune mrežne pokrivenosti (segmentacijske politike na svim definiranim resursima Naručitelja) mora biti moguće u roku od najviše trideset (30) kalendarskih dana od početka učenja prometa.	DA		

Br.	Kategorija	Zahtjev	Obvezno	DA / NE	Napomena
048	Razlikovni – arhitektura	Rješenje mora automatski otkrivati nove uređaje i aplikacije koji se pojave u mreži te im automatski pridijeliti odgovarajuće politike najmanje privilegije, bez ručne intervencije („Day-2 ready“).	DA		
049	Razlikovni – arhitektura	Provođenje politika mora se ostvarivati isključivo kroz native komponente operativnih sustava (npr. Windows Filtering Platform / WFP, IPTables, NFTables, ACL), bez instalacije dodatnih kernel ili in-line modula koji presreću mrežni promet.	DA		
050	Razlikovni – arhitektura	Memorijski otisak bilo koje komponente koja se izvršava na zaštićenom poslužitelju ili klijentu ne smije prelaziti pedeset (50) MB pri normalnom radu, neovisno o opterećenju i složenosti politika.	DA		
051	Razlikovni – arhitektura	Ažuriranja središnje upravljačke komponente moraju biti potpuno automatizirana i ne smiju zahtijevati zakazane „maintenance window“ prozore (server stateless, automatic updates without downtime).	DA		
052	Razlikovni – arhitektura	Rješenje mora omogućiti zatvaranje administrativnih portova RDP, RPC, SSH, WMI i SMB prema načelu „default deny“, uz njihovo otvaranje isključivo na temelju pojedinačnog vremenski ograničenog zahtjeva administratora i uspješnog MFA izazova, čime se osigurava „clean pen-test“ rezultat za navedene portove.	DA		
053	Razlikovni – arhitektura	Rješenje mora osigurati da se najmanje 90% kritičnih resursa Naručitelja segmentira pravilima u roku od 90 dana od početka učenja prometa.	DA		
054	Razlikovni – AI / LLM zaštita	Rješenje mora omogućiti otkrivanje, popis i kontrolu aktivnih AI agenata (autonomnih softverskih komponenti koje koriste velike jezične modele) u okruženju Naručitelja, uz prikaz s kojim resursima komuniciraju i kojim protokolima.	DA		
055	Razlikovni – AI / LLM zaštita	Rješenje mora omogućiti primjenu istih politika identitetski temeljene	DA		

Br.	Kategorija	Zahtjev	Obvezno	DA / NE	Napomena
		najmanje privilegije na AI agente kao i na korisnike i uređaje, s eksplicitno definiranim granicama dozvoljenih komunikacija.			
056	Razlikovni – AI / LLM zaštita	Rješenje mora omogućiti zaštitu infrastrukture velikih jezičnih modela (LLM) na mrežnoj razini tako da im pristupaju isključivo autorizirani sustavi, čime se sprječava neovlaštena manipulacija modelima i unos otrovanih podataka.	DA		
057	Razlikovni – AI / LLM zaštita	Rješenje mora spriječiti lateralno kretanje izazvano kompromitiranim AI agentima ili AI-vođenim napadima eliminacijom nepotrebne mrežne povezivosti između resursa.	DA		
058	Razlikovni – AI / LLM zaštita	Rješenje mora omogućiti kontrolu pristupa SaaS AI servisima na mrežnoj razini (npr. ChatGPT, Microsoft Copilot, Gemini) i automatsko blokiranje neautoriziranih (shadow AI) servisa.	DA		
059	Razlikovni – AI / LLM zaštita	Rješenje mora pružiti alat za upite mrežnoj aktivnosti prirodnim jezikom i mapiranje rezultata na regulatorne okvire (npr. NIS2, CIS Benchmarks) s dinamičkim ocjenjivanjem rizika.	NE		
060	Razlikovni – kompetentnost proizvođača	Proizvođač rješenja mora u zadnje tri (3) godine biti pozicioniran kao „Leader” ili ekvivalentna kategorija u barem jednom neovisnom analitičkom izvještaju za područje Microsegmentation / Network Microsegmentation (npr. GigaOm Radar, Forrester Wave, IDC MarketScape).	DA		
061	Razlikovni – kompetentnost proizvođača	Proizvođač rješenja mora biti pozitivno ocijenjen u Gartner Peer Insights kategoriji „Microsegmentation / Network Security Microsegmentation” s prosječnom ocjenom korisnika ne nižom od 4,5/5,0.	DA		
062	Razlikovni – kompetentnost proizvođača	Proizvođač mora dokazati postojanje izravnog tehničkog kanala podrške s lokalnim ili regionalnim partnerom za područje EU/EEA u zadnjih najmanje pet (5) godina.	DA		

Br.	Kategorija	Zahtjev	Obvezno	DA / NE	Napomena
063	Podrška i implementacija	Ponuditelj mora osigurati tehničku podršku 24x7 (24 sata dnevno, 7 dana u tjednu) na hrvatskom i/ili engleskom jeziku.	DA		
064	Podrška i implementacija	Ponuditelj mora osigurati SLA s definiranim vremenima odziva i razrješavanja prema kategorijama prioriteta (Kritično / Visoko / Srednje / Nisko) za cijelo razdoblje trajanja ugovora.	DA		
065	Podrška i implementacija	Ponuditelj mora osigurati pristup proizvođačevoj bazi znanja, dokumentaciji i sigurnosnim obavijestima.	DA		
066	Podrška i implementacija	Ponuditelj mora osigurati edukaciju administratora naručitelja za rad s rješenjem (najmanje dvije osobe).	DA		
067	Podrška i implementacija	Ponuditelj mora osigurati implementaciju i puštanje u rad rješenja u testnom i produkcijskom okruženju naručitelja.	DA		
068	Regulatorna usklađenost	Rješenje mora biti usklađeno s industrijskim najboljim praksama i regulatornim okvirima primjenjivim na zdravstvene ustanove, uključujući Opću uredbu o zaštiti podataka (GDPR / EU 2016/679).	DA		
069	Regulatorna usklađenost	Rješenje mora podržavati zahtjeve Direktive (EU) 2022/2555 (NIS2) i Zakona o kibernetičkoj sigurnosti (NN 14/24) primjenjive na operatore ključnih usluga u zdravstvenom sektoru.	DA		
070	Regulatorna usklađenost	Rješenje mora omogućiti generiranje izvještaja i evidencija (audit log) potrebnih za usklađenost s ISO/IEC 27001, SOC 2 i PCI DSS standardima.	DA		
071	Regulatorna usklađenost	Sva obrada podataka mora biti u skladu s lokacijskim zahtjevima EU/EEA prostora (data residency).	DA		