Република Србија
МИНИСТАРСТВО ПОЉОПРИВРЕДЕ,
ШУМАРСТВА И ВОДОПРИВРЕДЕ
Управа за шуме
Број: 001921497 2024 14844 000 000 405 023
Датум: 13.06.2024. године
Б е о г р а д

**ПОЗИВ ЗА ПОДНОШЕЊЕ ПОНУДЕ**

Управа за шуме, Министарства пољопривреде, шумарства и водопривреде спроводи поступак **набавке софтвера за потребе рада Управе за шуме следећих спецификација**:

Tehničke specifikacije softvera za antivirus zaštitu

Tehnička specifikacija za nabavku rešenja za endpoint security, implementiranog u cloud okruženju, obuhvata precizne i specijalizovane zahteve koje rešenje mora ispunjavati kako bi se osigurala robustna cyber odbrana za organizacionu IT infrastrukturu. Specifikacije su formulisane kroz terminologiju specifičnu za oblast kibernetske bezbednosti.

Opšti Zahtevi

- Cloud-Native Management: Rešenje mora biti cloud-native, omogućavajući secops timovima da implementiraju i upravljaju zaštitnim merama endpointa preko centralizovanog cloud-based kontrolnog panela, bez zahteva za lokalnom infrastrukturom.
- Comprehensive Threat Protection: Integralno rešenje treba da obezbedi zaštitu od širokog spektra vektora napada, uključujući, ali ne ograničavajući se na, malware, ransomware, spear phishing, i APT (Advanced Persistent Threat) kampanje.

Tehnički Zahtevi

- Real-Time Threat Detection & Response: Implementacija tehnologija za detekciju pretnji u realnom vremenu i odgovarajući automatizovani odgovor, koristeći kombinaciju signature-based, heuristic-based, i behavior-based analize.
- Behavioral Analysis & Anomaly Detection: Upotreba behavioral analytics za identifikaciju atipičnih aktivnosti koje mogu ukazivati na kompromitaciju endpointa, uz podršku machine learning algoritama za poboljšanje tačnosti detekcije.
- Ransomware Mitigation: Specijalizovane tehnike za prepoznavanje i neutralizaciju ransomware taktika, uključujući mehanizme za automatsko backupovanje i recovery kritičnih podataka u slučaju enkripcije.
- Phishing Protection: Advanced email filtering tehnologije za detekciju i blokiranje phishing napada, sa sposobnošću analize linkova i priloga u realnom vremenu.
- Web Content Filtering: Implementacija URL filteringa radi kontrole pristupa web sadržaju, sa mogućnošću definisanja politika zasnovanih na kategorijama web lokacija i reputaciji.
- Application Control & Whitelisting: Mogućnost detaljne kontrole aplikacija, omogućavajući whitelisting pouzdanih aplikacija i blokiranje ili ograničavanje izvršenja nepouzdanih ili neproverenih aplikacija.

- Device Control: Upravljanje pristupom eksternim uređajima (npr. USB drives), radi sprečavanja potencijalnih data leakage incidenata i infiltracije malware-a.

Performanse i Kompatibilnost

- Low System Footprint: Rešenje mora demonstrirati minimalni uticaj na sistemsku performansu endpointa, osiguravajući da radne stanice i serveri ostanu performantni tokom operacija.
- Cross-Platform Compatibility: Podrška za širok dijapazon operativnih sistema, uključujući ali ne ograničavajući se na, Windows, macOS, Linux distribucije, kao i mobilne OS-e poput Android i iOS.

Administracija i Izveštavanje

- Centralized Security Dashboard: Potreba za intuitivnim web-based interfejsom koji pruža SOC timovima kompletan uvid u sigurnosno stanje organizacije, aktuelne pretnje, i odgovore na incidente.
- Detailed Reporting: Funkcionalnost za generisanje detaljnih izveštaja o detekcijama pretnji, preduzetim akcijama odgovora, kao i compliance izveštavanju u skladu sa regulativama.
- Incident Response Automation: Kapaciteti za automatizaciju odgovora na incidente, uključujući integraciju sa drugim security alatima i platformama za efikasan incident management.

Ponuđači trebaju da obezbede detaljne tehničke dokumentacije koje potvrđuju kako njihova rešenja ispunjavaju ove specifične zahteve. Osim toga, potrebno je da ponude jasne smernice za integraciju sa postojećim alatima i platformama unutar organizacije, kao i dokaz o sposobnosti svojih rešenja da se skaliraju u skladu sa rastućim potrebama i kompleksnošću IT okruženja.

Dodatni Zahtevi

- Threat Intelligence Integration: Integracija sa globalnim threat intelligence feedovima za pravovremeno ažuriranje o najnovijim pretnjama i kampanjama, uključujući indicator of compromise (IoC) podatke za brzu detekciju.
- Vulnerability Management: Uključivanje funkcionalnosti za upravljanje ranjivostima, omogućavajući identifikaciju i remedijaciju softverskih slabosti na endpointima pre nego što budu iskorišćene od strane napadača.
- Endpoint Detection and Response (EDR): Napredne EDR sposobnosti koje omogućavaju detaljnu forenzičku analizu i dubinsko razumevanje sigurnosnih incidenata, uključujući root cause analizu i timeline aktivnosti napada.
- Security Awareness Training Integration: Mogućnost integracije sa platformama za obuku zaposlenih u oblasti cyber sigurnosti, povećavajući svest o bezbednosnim pretnjama i najboljim praksama za njihovo sprečavanje.

Uslovi Implementacije i Podrške

- Implementation Plan: Detaljan plan implementacije koji uključuje faze pilotiranja, testiranja i potpune implementacije, uz minimalan uticaj na poslovanje.
- Training and Knowledge Transfer: Pružanje obuke za IT i sigurnosni tim, uključujući pristup online resursima, webinari i hands-on trening sesije za efikasno korišćenje i upravljanje rešenjem.
- Technical Support and SLA: Jasno definisani uslovi tehničke podrške, uključujući dostupnost 24/7 podrške za kritične incidente, sa dogovorenim vremenima odziva u skladu sa Service Level Agreement (SLA).

2. Softver za replikaciju i bekap

Tehnička Specifikacija za Nabavku Softvera za Replikaciju i Backup

1. Opis Proizvoda:

- Traženi proizvod je softver za replikaciju i backup, dizajniran za mala i srednja preduzeća, koji pruža sveobuhvatnu zaštitu podataka za virtualizovane, fizičke, cloud i SaaS okruženja.

2. Licenciranje i Edicija:

- Softver će biti licenciran na godišnjem nivou.
- Potrebna edicija treba da podržava osnovne funkcionalnosti backupa i replikacije za enterprise okruženje, fokusirajući se na osnovne potrebe malih i srednjih preduzeća.

3. Funkcionalnosti:

- Softver treba da podržava centralizovano upravljanje backupom i replikacijom virtualnih mašina, fizičkih servera i radnih stanica.
- Moraju biti omogućeni kontinuirani backup i real-time replikacija, kao i instant oporavak aplikacija i podataka.
- Treba da uključuje napredne funkcije deduplikacije podataka, kompresije, i šifriranja kako bi se optimizovala efikasnost pohranjivanja i osigurala bezbednost podataka.
- Podrška za backup na više destinacija, uključujući lokalne, cloud i offsite lokacije.

4. Podrška za Platforme:

- Softver mora biti kompatibilan sa vodećim virtualizacionim platformama kao što su VMware vSphere i Microsoft Hyper-V.
- Treba da omogući backup i replikaciju za fizičke servere i radne stanice sa operativnim sistemima Windows i Linux.

5. Skalabilnost i Performanse:

- Rešenje mora biti skalabilno kako bi podržalo rast preduzeća, sa mogućnošću proširenja za dodatne servere, aplikacije i radne stanice bez značajnog uticaja na performanse.
- Softver treba da garantuje visoke performanse backupa i replikacije kako bi minimizirao vreme van servisa i osigurao brzi oporavak.

6. Integracija i Kompatibilnost:

- Potrebna je integracija sa cloud servisima, uključujući ali ne ograničavajući se na, Amazon AWS, Microsoft Azure, i Google Cloud Platform.
- Softver treba da podržava direktno backupovanje u NAS uređaje, kao i integraciju sa glavnim storage rešenjima.

7. Održavanje i Podrška:

- Ponuda mora uključivati detaljan plan održavanja i podrške, sa jasno definisanim nivoima usluge (SLA) i dostupnošću tehničke podrške.

3. Softver za naprednu zaštitu od pretnji

Tehničke specifikacije softvera za naprednu zaštitu od pretnji:

Arhitektura i Kompatibilnost

- Kompatibilnost sa Uređajem: Rešenje mora biti direktno kompatibilno sa Fortinet FortiGate 40F uređajem, bez potrebe za dodatnim hardverskim modifikacijama.
- Integracija sa FortiOS: Mora se nesmetano integrisati sa operativnim sistemom FortiOS, omogućavajući konzistentno upravljanje i politike sigurnosti preko Fortinet ekosistema.

Detekcija i Prevencija

- Napredna Analiza Pretnji: Implementacija tehnika mašinskog učenja za detekciju anomalijskih obrazaca u mrežnom saobraćaju, što omogućava identifikaciju sofisticiranih pretnji u ranim fazama.
- Sandboxing u Oblaku: Korišćenje cloud-based sandboxing tehnologije za analizu sumnjivih datoteka i aplikacija u bezbednom okruženju, što minimizira rizik od infekcije unutar korisničke mreže.
- SSL/TLS Inspekcija: Dubinsko inspektiranje šifrovanog saobraćaja, uključujući SSL/TLS, radi otkrivanja skrivenih pretnji bez kompromitovanja privatnosti krajnjeg korisnika.

Performanse i Optimizacija

- CPU i Memorija: Rešenje treba efikasno koristiti CPU i memoriju FortiGate 40F uređaja, osiguravajući visoke performanse bez degradacije usluga mreže.
- Optimizacija Propusnosti: Treba da podržava visoku propusnost mreže uz minimalno kašnjenje, čak i kada su uključene napredne funkcije inspekcije i analize.

Upravljanje i Izveštavanje

- Centralizovano Upravljanje Sigurnošću: Integracija sa Fortinet Security Fabric za centralizovano upravljanje, što omogućava jednostavnu implementaciju politika sigurnosti i sinhronizaciju konfiguracija preko više uređaja.
- Detaljna Izveštavanja: Automatizovano generisanje izveštaja o bezbednosnim događajima, analize trendova pretnji i uspešnosti implementiranih politika zaštite.
- Forenzička Analiza: Mogućnost detaljne forenzičke analize nakon sigurnosnih incidenata, uključujući tragove invazije, putanju infekcije, i preporuke za remedijaciju.

Dodatni Bezbednosni Servisi

- Web Filtering: Automatsko blokiranje pristupa štetnim ili neprimjerenim web lokacijama na osnovu ažuriranih baza podataka i kategorizacije sadržaja.
- Application Control: Kontrola aplikacija omogućava detaljno granulirane politike za upravljanje korišćenjem aplikacija unutar mreže, uključujući blokiranje ili ograničavanje aplikacija koje predstavljaju bezbednosni rizik.
- Intrusion Prevention System (IPS): Visoko prilagodljiv IPS za identifikaciju i blokiranje napada koji ciljaju poznate slabosti u mreži ili aplikacijama.

Sigurnost na Više Nivoa

- Zaštita od Botneta: Detekcija i blokiranje saobraćaja koji je povezan sa botnet mrežama, sprečavajući širenje malvera i DDoS napade.
- Zaštita od Napada Nultog Dana: Upotreba naprednih tehnologija za prepoznavanje i blokiranje pretnji koje još uvek nisu javno poznate, koristeći napredne tehnike predviđanja i analize.
- Adaptivna Sigurnost: Mogućnost rešenja da se prilagodi promenljivom bezbednosnom pejzažu, automatski ažurirajući svoje definicije pretnji i taktike detekcije na osnovu globalnih obaveštajnih podataka o pretnjama.

Interoperabilnost i Ekosistem

- Integracija sa Trećim Stranama: Podrška za integraciju sa alatima i platformama trećih strana, uključujući SIEM sisteme, analitičke alate i druge bezbednosne uređaje, za unapređenje vidljivosti i odziva na incidente.
- API Podrška: Pružanje RESTful API-ja za automatizaciju zadataka upravljanja, konfiguracije i izveštavanja, omogućavajući integraciju sa korporativnim procesima i alatima.

Dodatni Zahtevi

- Tehnička Podrška: Ponuđač mora obezbediti stalnu tehničku podršku za konfiguraciju i optimizaciju ovih servisa i konsultacije.
- Usklađenost sa Regulativama: Rešenje mora biti u skladu sa lokalnim i međunarodnim standardima i regulativama u oblasti zaštite podataka i privatnosti.

4. Softver za izradu identičnih kopija

Opšti Zahtevi

- Portabilnost Softvera: Softver mora biti portabilan i omogućiti tehničarima da ga koriste sa USB uređaja ili drugih prenosivih medija bez potrebe za stalnom instalacijom na svakom računaru.
- Licenciranje: Licenca treba da dozvoljava upotrebu softvera od strane više tehničara unutar organizacije, uz mogućnost kreiranja neograničenog broja backupova i obnavljanja sistema.

Tehnički Zahtevi

- Kreiranje Slike Diska: Softver mora omogućiti kreiranje potpune slike diska, uključujući operativni sistem, aplikacije, i korisničke podatke, koje se mogu koristiti za potpuno obnavljanje sistema u slučaju kvara ili gubitka podataka.
- Podrška za Više Platformi: Softver mora podržavati različite operativne sisteme, uključujući, ali ne ograničavajući se na, sve trenutno podržane verzije Windows i macOS operativnih sistema.

- Incremental i Differential Backup: Podrška za incremental i differential backup, omogućavajući korisnicima da minimiziraju vreme potrebno za backup i optimizuju skladištenje.
- Bootable Rescue Media: Mogućnost kreiranja bootable rescue medija koji omogućava oporavak sistema čak i kada operativni sistem nije u stanju da se pokrene.
- Enkripcija i Zaštita Lozinkom: Softver treba da pruža opcije za enkripciju backup fajlova i zaštitu lozinkom, kako bi se osigurala bezbednost i privatnost podataka.
- Planiranje Backupova: Softver mora omogućiti automatsko planiranje backup operacija, omogućavajući korisnicima da podešavaju redovne backupove bez potrebe za ručnom intervencijom.

Uslovi za Podršku i Usavršavanje

- Tehnička Podrška: Ponuđač mora obezbediti tehničku podršku koja je dostupna putem emaila, telefona, ili live chata, sa odgovarajućim vremenom odziva za rešavanje problema.
- Ažuriranja i Nadogradnje: Softver treba redovno da prima ažuriranja i nadogradnje koje uključuju nove funkcionalnosti, poboljšanja performansi, i ispravke bezbednosnih propusta.

5. Softver za udaljeni pristup

Funkcionalnosti

- Bezbedsni pristup bez nadzora: aplikacija treba da omogućava uspostavljanje brze i bezbedne везе sa udaljenim računarima i serverima za koje nije potreban lokalni korisnik.
- Transfer datoteka: aplikacija treba da omogućava sigurni i pouzdani transfer datoteka i foldera između lokalnog i udaljenog računara tokom sesije daljinskog pristupa.
- Adresar online kontakta: aplikacija treba da prikazuje status online/offline kontakata bez potrebe za uspostavljanjem veze sa njihovim uređajem.
- Prilagođavanje interfejsa: aplikacija treba da omogući konfiguraciju korisničkog.
- Automatsko ažuriranje: aplikacija treba da omogući automatsko ažuriranje klijentskog softvera na udaljenim uređajima i najnovije funkcije.
- Chat komunikacija: aplikacija treba da omogući komuniciju sa korisnicima tokom sesije daljinskog pristupa pomoću integrisanog chata.
- Štampanje na lokalnoj štampaču:
- Red za podršku aplikacija treba da omogući red za podršku kako bi korisnici mogli da zahtevaju asistenciju.
- Automatsko i masovno instaliranje:
- Monitoring konekcija: aplikacija treba da omogući praćenje svih dolaznih i odlaznih konekcija uređaja povezanih na nalog.
- Napredna podešavanja: aplikacija treba da omogući kreiranje jednog ili više klijenata sa prilagođenim funkcijama i željenim podešavanjima.

| Врста софтвера | Количина |
|---|---|
| Antivirus zastita | 74 |
| Softver za replikaciju i bekap | 1 |
| Fortinet FortiGate-40F | 1 |
| Softver za izradu identičnih kopija | 2 |
| Softver za udaljeni pistup | 1 |
| Укупно | 79 |

Наручилац набавља **79 комада** софтвера.

Чланом 27, став 1, тачка 1 Закона о јавним набавкама („Службени гласник РС“ број 91/19 и 92/23), прописано је да се одредбе овог закона не примењују се на набавку добара,

услуга и спровођење конкурса за дизајн, чија је процењена вредност мања од 1.000.000 динара и набавку радова чија је процењена вредност мања од 3.000.000 динара. Процењена вредност набавке је : 734.000,00 динара без ПДВ-а.

Средства за реализацију набавке обезбеђена су Законом о буџету Републике Србије за 2024. годину ("Службени гласник РС" број 92/2023) раздео 24, глава 24.4, функција 420, економска класификација 515111, а наведена јавна набавка се налази у интерном плану набавки Наручиоца за 2024. годину, под редним бројем: 2.

**Рок за подношење понуде је 18.06.2024 године до 11:00 сати.**

Критеријум за избор најповољнијег понуђача јесте **најнижа понуђена цена**.

С обзиром да Наручилац не користи електронски систем за спровођење изузетих набавки, а који закључава понуде у тренутку подношења тако да се могу откључати тек непосредно по истеку рока за подношење истих, понуда не може бити достављена коришћењем електронске поште.

**Понуђач понуду доставља препорученом поштом или личном предајом на писарници Управе за заједничке послове републичких органа, тако да буде запримљена до времена одређеног за отварање понуда, у затвореној коверти:**

**Управа за шуме**
**Омладинских бригада бр. 1**
**Нови Београд**
**Напомена: НЕ ОТВАРАТИ за набавку софтвера бр. 001921497 2024 14844 000 000 405 023**

**Јавно отварање понуда биће извршено дана 18.06.2024. године са почетком у 11:30 сати, на адреси: Омладинских бригада бр.1, Нови Београд, IV/434.**

Оцена и рангирање понуда врши се на основу утврђеног критеријума, а у складу са Директивом о ближем уређивању поступка јавне набавке број : 404-02-13/23-10 од дана 29.11.2023. године, сачињава се извештај који садржи све основне податке о понуђачима, понуђеним ценама и другим траженим елементима понуде (цене, рокови, услови и начин плаћања, и сл.) и предлогом за закључење предметног уговора са најповољнијим понуђачем.

Наручилац може уместо закључења уговора најповољнијем понуђачу издати наруџбеницу. У овом поступку не доноси се посебна одлука о додели уговора, већ се уговор/наруџбеница закључује на основу извештаја.

**Управа за шуме**
**Министарства пољопривреде,**
**шумарства и водопривреде**

**ПОДАЦИ О ПОНУЂАЧУ**
**001921497 2024 14844 000 000 405 023**

| | |
|---|---|
| ПУН НАЗИВ ПОНУЂАЧА: | |
| АДРЕСА: | |
| МАТИЧНИ БРОЈ: | |
| ПИБ: | |
| ШИФРА ДЕЛАТНОСТИ: | |
| БРОЈ РАЧУНА И НАЗИВ БАНКЕ: | |
| ЛИЦЕ ЗА КОНТАКТ: | |
| ЕЛЕКТРОНСКА АДРЕСА ЛИЦА ЗА КОНТАКТ: | |
| ТЕЛЕФОН ЛИЦА ЗА КОНТАКТ: | |
| ЛИЦЕ ОДГОВОРНО ЗА ПОТПИСИВАЊЕ УГОВОРА: | |

Место и датум: Овлашћено лице Понуђача:

_____ _____

**ОБРАЗАЦ ФИНАНСИЈСКЕ ПОНУДЕ**
**001921497 2024 14844 000 000 405 023**

Број понуде и датум: _____

На основу позива за подношење понуда у поступку набавке софтвера:

**1. ЦЕНА:** Навести цену без ПДВ-а и са обрачунатим ПДВ-ом, искључиво у динарима:

| ПРЕДМЕТ НАБАВКЕ | НАЗИВ ПОНУЂЕНОГ СОФТВЕРА | КОЛИЧИНА (ком) | ЈЕДИНИЧНА ЦЕНА без ПДВ-а | УКУПНА ЦЕНА без ПДВ-а |
|---|---|---|---|---|
| Antivirus zastita | | 74 | | |
| Softver za replikaciju i bekap | | 1 | | |
| Fortinet FortiGate-40F | / | 1 | | |
| Softver za izradu identičnih kopija | | 2 | | |
| Softver za udaljeni pistup | | 1 | | |
| | | | **УКУПНО** | |

**Критеријум за избор најповољнијег понуђача јесте најнижа понуђена цена без ПДВ-а.**

**Уколико два понуђача понуде исту цену, уговор ће се доделити понуђачу који понуди краћи рок испоруке.**

**2. Рок испоруке:**.....дана од дана пријема наруџбенице (најдуже 10 дана)

Фактура доспева за плаћање у законском року од 10 дана од дана прихватања е-фактуре, регистроване у СЕФ-у, од стране Наручиоца. Пружалац услуге је обавезан да у рачуну назначи број уговора. Плаћање се врши на основу ваљано достављене фактуре и Извештаја о раду за претходни месец.

**Напомене:**

- Уколико понуђач није у систему ПДВ-а, уз понуду доставља потврду потписану од стране овлашћеног лица.
- Наручилац није предвидео могућност повећања цене те је понуђена цена коначна.
- **Приликом сачињавања понуде употреба печата није обавезна.**

Место и датум: Овлашћено лице Понуђача:

_____ _____