**Obrazac 6.**

**TEHNIČKE SPECIFIKACIJE**

Postupak nabave: **Softversko sigurnosno rješenje**

Evidencijski broj:  **E-JN-39/2017/R3**

Ponuditelj: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(upisati naziv ponuditelja/zajednice gospodarskih subjekata, adresa, OIB)*

*Ako nije drugačije definirano, zahtjevi definirani Tehničkim specifikacijama predstavljaju minimalne tehničke uvjete koje ponuđeno softversko rješenje mora zadovoljavati.*

*Ponuditelj* ***OBAVEZNO POPUNJAVA*** *stupac «UVJETI ISPUNJENI (Da/Ne)» te ukoliko odgovori „DA“ na taj se način obvezuje na nuđenje rješenja koje minimalno ispunjava traženi tehnički uvjet. Ukoliko se prilikom pregleda utvrdi da je neki odgovor „NE“ ili uopće nije odgovoreno, ponuda će biti odbijena.*

*Ukoliko ponuditelj nudi jednakovrijedan proizvod/rješenje ili proizvod/rješenje boljih tehničkih uvjeta od traženih, u stupcu "Ponuđeno" potrebno je upisati točan naziv/karakteristiku/značajku komponente koju ponuditelj nudi, a koja mora biti ista ili bolja od traženih uvjeta.*

*U stupcu «Bilješke, napomene, reference na tehničku dokumentaciju» ponuditelj upisuje bilješke, napomene vezano za ponuđeno proizvod /rješenje odnosno web stranicu proizvođača na kojoj je vidljiva specifikacija nuđenog proizvoda/rješenja tj. navod o mogućnosti provjere tražene specifikacije u obliku testne instalacije i/ili demonstracije kod korisnika navedenoga kao referenca.*

*Stupac «Ocjena DA/NE» ponuditelj* ***NE*** *POPUNJAVA, s obzirom na to da je stupac predviđen za ocjene naručitelja.*

*Kako bi se ponuda smatrala valjanom, ponuđeni predmet nabave mora zadovoljiti sve što je traženo u obrascu Tehničkih specifikacija.*

*U slučaju postojanja sumnje u istinitost podataka navedenih u ponuđenim tehničkim specifikacijama, naručitelj zadržava pravo provjere navedenih podataka bilo kojim prikladnim sredstvom / načinom (npr. provjerom podataka kod korisnika navedenoga kao reference).*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | | | | |
| **Red.Br.** | **Minimalni tehnički uvjeti** | **UVJETI ISPUNJENI DA/NE** | **PONUĐENO** | **Bilješke, napomene, reference na tehničku dokumentaciju** | **OCJENA NARUČITELJA DA/NE** |
| 1 | Rješenje mora podržavati sljedeće server operativne sustave: Windows Server 2012, 2012 R2, 2012 R2 Update 1: Basic,Standard,DataCentar MC Exchange 2013, 2016  Windows Server 2008, 2008 R2, Standard, DataCentar, Enterprise,Web Linux Server Ubuntu, Suse |  |  |  |  |
| 2 | Rješenje mora podržavati sljedeće klijentske operativne sustave 32bit, 64 bit: Windows 10, 8.1, 8, 7, Vista Windows Standard, Pro, Enterprise MAC i LInux |  |  |  |  |
| 3 | Objedinjeno upravljanje i administriranje rješenja putem jedinstvene web središnje konzole koji mora podržavati instalaciju na Vmwareu, bez dodatnih troškova ( dodatnih licenci za pokretanje antivirusnog rješenja ) |  |  |  |  |
| 4 | Upravljanje sa drugim dijelovima rješenja iz istog upravljačkog sustava. |  |  |  |  |
| 5 | Mogućnost upravljanja rješenjem iz oblaka ili lokalno. |  |  |  |  |
| 6 | Podržani preglednici za korištenje web upravljačke konzole: -Microsoft Internet Explorer; Verzije 8,9,10,11 -Mozilla Firefox; od verzije 3.0 -Google Chrom; od verzije 4.0 |  |  |  |  |
| 7 | Uvid u status antivirusnog rješenja na svim računalima u mreži |  |  |  |  |
| 8 | Udaljena instalacija/reinstalacija antivirusnog softvera na sva računala neovisno o domenskom sustavu i administratorskim ovlastima na klijentskom računalu i po potrebi reinstalacija softvera (nove verzije) |  |  |  |  |
| 9 | Čišćenje zaraženih računala uključujući i ona kod kojih je onemogućeno ažuriranje |  |  |  |  |
| 10 | Centralizirano upravljanje ažuriranjem antivirusnih i ostalih definicija, upravljanje nadogradnjom softvera i upravljanje klijentskim vatrozidom pomoću središnje konzole |  |  |  |  |
| 11 | Redovno preuzimanje i distribucija nadogradnji softvera i definicija za vrijeme valjanosti licencija kako bi sva računala imala najnoviju verziju zaštite. |  |  |  |  |
| 12 | Izvješćivanje i javljanje o prijetnjama putem poruka e-pošte i putem poruka na računalu |  |  |  |  |
| 13 | Izvješćivanje i javljanje o prijetnjam putem središnje konzole (kreiranje sumarnih izvješća i grafičko izvješćivanje o radu softvera koji pruža precizan uvid u prijetnje i druge događaje) s mogućnošću filtriranja pregleda klijentskih računala prema željenoj kategoriji |  |  |  |  |
| 14 | Centralizirano skladištenje, čuvanje i pretraživanje informacija o klijentskom dijelu antivirusnog rješenja i njihove konfiguracije (obavljenom skeniranju, otkrivanju i uklanjanju virusa, kao i o rasporedu ažuriranja antivirusne baze) putem središnje konzole. |  |  |  |  |
| 15 | Mogućnost automatskog i ručnog skeniranja na zahtjev (on‐demand), po pristupu (on‐access) i u prethodno zakazano vrijeme ( raspored) iz centralne kozole i iz sučelja klijenta |  |  |  |  |
| 16 | Podesiv interval nadogradnje |  |  |  |  |
| 17 | Centralizirano direktno uklanjanje otkrivenih prijetnji bez potrebe za lokalnim pokretanjem skeniranja zaštićenog računala. Uklanjanje prijetnji podrazumijeva otkrivanje, blokadu, uklanjanje svih vrsta zlonamjernog softvera u realnom vremenu, uključujući viruse, crve, trojanske konje, spyware, adware, rootkit-ove kao i ukljanjanje drugih zlonamjernih programa |  |  |  |  |
| 18 | Zaštita korištenjem potpisa i uzoraka za poznate prijetnje i ranjivosti |  |  |  |  |
| 19 | Podržan heuristički pristup za otkrivanje nepoznatih virusa |  |  |  |  |
| 20 | Upozoravanje na potencijalno zlonamjerne aplikacije |  |  |  |  |
| 21 | Identifikacija poznatih i nepoznatih prijetnji |  |  |  |  |
| 22 | Proaktivno sprječavanje sumnjivog ponašanja procesa (ZeroDay zaštita) i zaštita od crypto virusa, zaštitu od ransomware virusa |  |  |  |  |
| 23 | Zaštita od mijenjanja postavki, rekonfiguracije i/ili deaktivacije i deinstalacije antivirusnog softvera na klijentskim računalima pomoću zaporki i drugih sredstava na svim modulima klijentske zaštite. |  |  |  |  |
| 24 | Ugrađena tehnologija sprječavanja onemogućavanja antivirusnog rješenja od strane zlonamjernog softvera |  |  |  |  |
| 25 | Nakon čišćenja zlonamjernog softvera - mogućnost povrata na stanje prije njegovog pokretanja |  |  |  |  |
| 26 | Podržano skeniranje unutar komprimiranih datoteka (.zip, .rar, .tar.bz, ...) |  |  |  |  |
| 27 | Nadogradnja softvera i definicija na računalima u lokalnoj mreži uključujući i ona koja nemaju pristup Internetu tj. kojima je takav pristup ograničen ili blokiran |  |  |  |  |
| 28 | Centralizirana skladištenje, čuvanje i pretraživanje datoteka u karanteni putem središnje konzole sa mogučnošću brisanja i vraćanja datoteka |  |  |  |  |
| 29 | Podržana antivirusna i antispam zaštita za MS Exchange 2013, 2016 server uključujući filtriranje po sadržaju, tekstu, veličini i tipu datoteke te administracija putem središnje konzole |  |  |  |  |
| 30 | Podržana integracija sa Active directory-em i dodjeljivanje pravila za korisnike i grupe iz AD-a |  |  |  |  |
| 31 | Rješenje mora podržavati (opcionalnu) centralnu karantenu svih Exchange servera sa instaliranom zaštitom, na kojoj primatelji e-mail poruka sami mogu definirati vlastite black i white liste. |  |  |  |  |
| 32 | Rješenje mora imati antivirusnu zaštitu e-mail pretinaca i javnih direktorija na Microsoft Exchange |  |  |  |  |
| 33 | Podržana opcija skeniranja SSL-a |  |  |  |  |
| 34 | Podržana opcija kontrole aplikacija (App control) |  |  |  |  |
| 35 | Podržana opcija zaštite podataka (Data protection) |  |  |  |  |
| 36 | Podržana opcija zabrane/dozvole pristupa interneskim stranicama |  |  |  |  |
| 37 | Rješenje mora imati zaštitne mehanizme protiv izvršavanja zlonamjernih skripti IE, JavaScript ili VBScript i ActiveX kontrola |  |  |  |  |
| 38 | Rješenje mora imati mogućnost dinamičke kontrole izvršnih datoteka temeljenih na online i offline reputaciji datoteka. |  |  |  |  |
| 39 | Rješenje mora imati mogućnost obavještavanja ( reporting) o prijetnji na klijentu i pregled događaja iz centralne konzole |  |  |  |  |
| 40 | Rješenje mora imati mogućnost omogućavanja / blokiranja mrežnog prometa po protokolima. |  |  |  |  |
| 41 | Rješenje mora imati mogućnost omogućavanja / onemogućavanja upozorenja pokušaja upada kroz firewall kroz centralnu upravljačku konzolu. |  |  |  |  |
| 42 | Rješenje mora imati mogućnost blokiranja cijelih DNS domena. |  |  |  |  |
| 43 | Rješenje mora imati mogućnost primjenjivanja svako pravila odvojeno na dolazni promet ili odlazni promet prema klijentu. |  |  |  |  |
| 44 | Rješenje mora imati mogućnost proširenja prometnih pravila na osnovi specifikacije putanje do egzekutabilne datoteke koja prima ili otvara konekciju |  |  |  |  |
| 45 | Modul treba imati mogućnost uključivanja pravila bazirana na temelju opće korištenih protokola u svijetu. |  |  |  |  |
| 46 | Rješenje mora imati mehanizme globalnog znanja o prijetnji koja omogućuje konfiguriranje blokiranje veze s visokim rizikom na temelju ugleda IP adrese u online bazi proizvođača. |  |  |  |  |
| 47 | Rješenje mora imati u mogućnost da se automatski blokira web stranice s visokim rizikom koje mogu utjecati na opremu i/ili mreže na klijentu. |  |  |  |  |
| 48 | Rješenje mora imati mogućnost definiranja URL pravila filtriranja po kategorijama. |  |  |  |  |
| 49 | Rješenje mora imati mogućnosti blokiranja pristupa malwareu te proaktivnu zaštitu. |  |  |  |  |
| 50 | Rješenje mora imati mogućnost sinkroniziranja kategorije s bazom podataka ugleda globalnih prijetnji. |  |  |  |  |
| 51 | Rješenje mora imati mogućnost izrade izvještaja o kršenju web politika. |  |  |  |  |
| 52 | Ponuđeno rješenje mora uključivati licence s uključenim originalnim proizvođačkim jamstvom, pravom na nove sadržaje, verzije i sigurnosna ažuriranja te podršku proizvođača. |  |  |  |  |

U \_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_\_\_2017 . godine

**ZA PONUDITELJA:**

(ime i prezime te potpis ovlaštene osobe)

M.P. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_