



NACIONALNI LABORATORIJ ZA
ZDRAVJE, OKOLJE IN HRANO

**Specifikacija storitev
operativnega vzdrževanja in varovanja omrežja**

Kazalo vsebine

| | |
|--|---|
| Opis obstoječega sistema | 2 |
| Centralna lokacija | 2 |
| Oddaljene lokacije | 2 |
| Požarne pregrade | 3 |
| Sistem za upravljanje privilegiranih dostopov | 3 |
| Nadzor dostopa do omrežja | 3 |
| Zahtevane storitve | 3 |
| Vzdrževanje komunikacijske opreme naročnika | 4 |
| Vzdrževanje nadzornega sistema računalniškega omrežja | 4 |
| Vzdrževanje požarnih pregrad Stormshield | 5 |
| Vzdrževanje sistema PAM Wallix Bastion | 5 |
| Vzdrževanje sistema NAC Cisco Identity Services Engine | 6 |
| Splošni pogoji | 6 |
| Status in usposobljenost ponudnika | 6 |
| Kadri | 7 |
| Reference | 7 |

Opis obstoječega sistema

Računalniško omrežje naročnika je razvejano po vseh naročnikovih lokacijah v Sloveniji (Maribor, (sedež), Ljubljana, Brežice, Celje, Hrastnik, Koper, Kranj, Murska Sobota, Nova Gorica, Novo mesto, Slovenska Bistrica).

Centralna lokacija

Na centralni lokaciji v Mariboru se nahajajo jedrna stikala Cisco Catalyst serije C9500. Na dostopovnem nivoju so stikala proizvajalcev Cisco, HP in Huawei. Dostopovna stikala so redundantno (dvojno) vpneti na jedrna stikala.

Strežniki podatkovnega centra so povezani preko podatkovnih stikal Cisco Nexus na jedrna stikala.

Z logično razdelitvijo omrežja in uporabo segmentov VLAN je strežniška infrastruktura ločena od uporabnikov. Prav tako je dodatno izvedena segmentacija omrežij za upravljanje, laboratorijsko opremo in omrežje za goste. Vsi prehodi med temi omrežji so natančno definirani z dostopnimi seznamami.

Dostopovna stikala v istih komunikacijskih vozliščih so dodana v sklad, kjer je to mogoče. S tem je povečana prepustnost omrežja, poenoteno upravljanje stikal in odpravljena potreba po uporabi redundantnih protokolov (STP). Zaradi morebitnih redundantnih povezav (namernih ali nenamernih) je STP protokol v omrežju obvezen.

Brezžično omrežje je urejeno na ravni organizacije. V Mariboru je postavljen krmilnik za krmiljenje brezžičnih dostopnih točk. S pomožnimi krmilniki dostopnih točk po posameznih oddaljenih lokacijah je zagotovljeno, da je na vseh lokacijah brezžično omrežje poenoteno, hkrati pa je zagotovljen visok nivo zanesljivosti brezžičnega omrežja. Gesla za uporabnike se črpajo iz centralnega sistema Active Directory ne glede na to, kje se uporabnik nahaja.

Zagotovljena je primarna internetna povezava prepustnosti 10 Gb/s ponudnika Arnes, prav tako pa tudi sekundarna povezava, ki se samodejno aktivira v primeru odpovedi primarne povezave. Na tej lokaciji je v uporabi tudi povezava do omrežja zNET, ki hkrati služi za dostop do aplikacij zNET ostalim oddaljenim lokacijam. Vse navedene zunanje povezave so povezane preko požarnih pregrad proizvajalca Stormshield.

Na lokaciji je urejen nadzor komunikacijske in strežniške opreme, ki se nahaja lokalno, kakor tudi za opremo na vseh oddaljenih lokacijah. Preko vzpostavljenih povezav VPN se spremlja obremenjenost povezav in opreme, stanje strojne opreme, spremljanje samih VPN povezav.

Za glavna vozlišča po posameznih lokacijah, kjer se nahajajo usmerjevalniki, je zagotovljeno brezprekinitveno napajanje.

Oddaljene lokacije

Povezave do interneta so izvedene preko požarnih pregrad proizvajalca Stormshield. Oddaljene lokacije imajo poleg primarne optične povezave zagotovljeno tudi sekundarno povezavo LTE. Požarne pregrade služijo za vzpostavitev povezave VPN do centralne lokacije v Mariboru. Hkrati je na usmerjevalnikih zagotovljena možnost redundantne povezave preko mobilnega omrežja (LTE). V primeru potrebe po uporabi aplikacij, ki potrebujejo povezljivost zNET, se le ta zagotovi preko enotne povezave zNET na centralni lokaciji.

Naslovni prostori (IP omrežja), ki se uporabljajo v segmentu LAN poslovalnice, so usklajeni z enotno naslovno shemo IP organizacije, s čimer so izključeni morebitni konflikti posameznih lokalnih naslovnih prostorov pri vzpostavljanju VPN povezav.

Uporaba jedrnih stikal v poslovalnicah praviloma ni potrebna, saj je segmentacija omrežja urejena na požarnih pregradah ali usmerjevalnikih.

Stikala v istih komunikacijskih vozliščih so postavljena v sklad, s čimer je poenostavljeno upravljanje in zagotovljena ustrezna redundanca.

Požarne pregrade

Seznam požarnih pregrad Stormshield:

| Model | Lokacija |
|--------|--------------------|
| SN210 | Maribor |
| SN210 | Brežice |
| SN310 | Maribor |
| SN310 | Koper |
| SN310 | Slovenska Bistrica |
| SN310 | Hrastnik |
| SN310 | Ljubljana |
| SN310 | Maribor |
| SN3100 | Ljubljana |
| SN3100 | Maribor |
| SN3100 | Maribor |
| SN510 | Novo mesto |
| SN510 | Novo mesto |
| SN510 | Murska Sobota |
| SN510 | Nova Gorica |
| SN710 | Ljubljana |
| SN710 | Koper |
| SN710 | Kranj |
| SN720 | Maribor |
| SN720 | Novo mesto |
| SN720 | Celje |

Sistem za upravljanje privilegiranih dostopov

Naročnik ima implementiran sistem za upravljanje privilegiranih dostopov (Privilege Access Management – PAM) Wallix Bastion. Implementacija ni zaključena za vse skrbnike sistemov.

Nadzor dostopa do omrežja

Naročnik je v fazi implementacije sistema za nadzor dostopa do omrežja (Network Access Control – NAC) Cisco Identity Services Engine (ISE).

Zahtevane storitve

Predmet tega sklopa naročila je izvajanje storitev vzdrževanja in upravljanja:

- komunikacijske opreme naročnika,
- nadzornega sistema računalniškega omrežja,
- požarnih pregrad Stormshield,
- sistema PAM Wallix Bastion,
- sistema NAC Cisco Identity Services Engine.

Vzdrževanje komunikacijske opreme naročnika

Ponudnik nadzoruje in upravlja vse aktivne omrežne naprave.

Tekoče vzdrževanje komunikacijske opreme zajema sledeče storitve izvajalca.

1. V primeru izpada izvajalec posreduje v predpisanem odzivnem času do odprave napake.
2. Izvajalec koordinira ekipe za vzdrževanje ostale opreme, v kolikor je potrebna skladnost s to opremo (internetni ponudniki, ...).
3. Izvajalec dokumentira izvajanje storitev tehničnega vzdrževanja.
4. Izvajalec vsakih 6 mesecev skupaj z naročnikom opravi letni pregled stanja in predlaga izboljšave v omrežju.
5. Izvajalec shranjuje konfiguracije omrežne opreme v primeru sprememb.
6. Izvajalec odpravlja težave in analizira sistemske infrastrukturne težave ter ugotavlja njihov izvor.
7. Izvajalec vzpostavlja elemente informacijske infrastrukture, ki so predmet tega naročila, v delujoče stanje.
8. Izvajalec preventivno vzdržuje omrežno infrastrukturo v obliki rednih pregledov.
9. Izvajalec na zahtevo naročnika izdelava poročila o ustreznosti stanja strojne in programske opreme.
10. Izvajalec vodi dokumentacijo o stanju strojne in programske opreme, ki je predmet tega naročila.
11. Izvajalec namešča popravke in posodobitve programske opreme po priporočilih proizvajalcev.
12. Izvajalec pripravlja predloge izboljšav delovanja strojne in programske opreme.
13. Izvajalec pomaga naročniku pri načrtovanju sprememb informacijskega sistema.
14. Izvajalec vodi dokumentacijo o izvedenih posegih.

Vzdrževanje nadzornega sistema računalniškega omrežja

Izvajalec proaktivno spremlja delovanje sistema s pomočjo implementiranega nadzornega sistema.

V obseg nadzora mora biti vključena vsa oprema iz razpisa.

Za vsa stikala in povezave med njimi je zahtevana aktivna hierarhična vizualna predstavitev, ki bo v realnem času prikazovala obstoječe stanje celotnega omrežja in označevala na katerem segmentu, oziroma napravi se je pojavil dogodek ali napaka. Na najvišjem hierarhičnem nivoju morajo biti prikazane posamezne lokacije s prikazanim hrbteničnim podatkovnim omrežjem. Nižji nivo mora predstavljati dostopovno omrežje na nivoju vozlišča, kamor so priključeni uporabniki. Omogočeno mora biti enostavno prehajanje med posameznimi nivoji.

Iz prikazanih povezav med stikali mora biti razvidna poraba pasovne širine na tej povezavi. Za vsako stikalo morajo biti iz vizualne predstavitve razvidni tudi osnovni parametri, kot so vrsta stikala, dosegljivost, CPU in RAM stanje ter, če naprava omogoča, prikaz temperature in stanje ventilatorjev. S klikom na posamezni parameter naprave nadzorni sistem prikaže grafični prikaz zgodovine le-tega.

Grafični prikaz mora vsebovati ločen prikaz IP uporabnikov v omrežju, ki jih je moč prikazati glede na njihovo lokacijo ali pripadajoč VLAN.

Iz grafičnega vmesnika nadzornega sistema morajo biti dosegljive vse funkcionalnosti nadzornega sistema.

Grafični vmesnik nadzornega sistema mora biti pregleden, enostaven za uporabo, postavljen na spletnem strežniku in dosegljiv iz lokalnega podatkovnega omrežja NLZOH.

Nadzorni sistem mora vsebovati grafične prikaze posameznih spremljanih parametrov opreme za obdobje vsaj enega leta.

Nadzorni sistem mora za vsa stikala omogočati spremljanje naslednjih parametrov:

- dosegljivost (uspešen/neuspešen ping in zakasnitev ali SNMP),
- status (aktiven - »up«/neaktiven – »down«/ugasnjen »adm down«) posameznih vhodov/izhodov (port-ov) in porabo pasovne širine v odstotkih,
- parameter CPU v odstotkih,
- parameter RAM v odstotkih,
- omrežne parametre na stikalo priključenih naprav (naslov IP, naslov MAC),
- lociranje določenega odjemalca IP (na katerem portu in na katerem stikalu je odjemalec priključen),
- zasedenost naslovnih prostorov IP,
- temperatura in stanje ventilatorjev opreme, ki to omogoča.

Nadzorni sistem mora omogočati vključitev drugih omrežnih naprav, ki podpirajo standardizirane protokole: SNMP, Syslog in WMI.

Posebna funkcionalnost nadzornega sistema mora biti tudi arhiviranje konfiguracij omrežne opreme, vključene v nadzorni sistem. Nadzorni sistem mora arhivirati konfiguracije na izbran časovni interval, pri čemer se zapis izvede le v primeru sprememb. Pri tem se zabeleži čas spremembe ter ime administratorja (uporabniško ime), ki je povzročil spremembo.

Nadzorni sistem za podatkovno omrežje javlja alarme preko e-pošte. Različni dogodki se obravnavajo različno (nekateri javimo na e-pošto, o nekaterih dogodkih pa ne želimo biti posebej obveščeni). Sistem mora omogočati nastavitve alarma za vse lastnosti omrežnih naprav, ki jih spremljamo.

Strežnik za nadzorni sistem mora biti nameščen v lokalno virtualno okolje VMware, kjer naročnik zagotovi potrebne vire na zahtevo ponudnika.

Ponudnik zagotovi usposabljanje naročnikovih administratorjev nadzornega sistema, s pomočjo katerega bodo sposobni sami upravljati z nadzornim sistemom in izkoriščati osnovne funkcionalnosti.

Vzdrževanje požarnih pregrad Stormshield

Ponudnik upravlja vse naročnikove požarne pregrade. Upravljanje požarnih pregrad zajema:

- upravljanje povezav z naročnikovim omrežjem,
- usmerjanje prometa,
- konfiguracijo usmerjevalnih protokolov, pravil,
- statistike, poročila, opozorila,
- filtriranje naslovov URL,
- upravljanje povezav VPN.

Vzdrževanje sistema PAM Wallix Bastion

Ponudnik upravlja naročnikov sistem Privilege Access Management Wallix Bastion. Implementacijo v času trajanja pogodbe razširi na vse skrbnike sistemov (dodatnih 20) in na 100 zaposlenih, ki občasno opravljajo delo od doma. Upravljanje sistema zajema:

- zunanje upravljanje sistema PAM,
- dopolnjevanju politik,
- posodabljanje konfiguracij in programske opreme,
- izvedbo rednih tedenskih preverjanj stanja sistema in sistemskih sporočil,
- pomoč pri obravnavi incidentov.

Platforma, na katero je nameščena programska oprema, ni predmet vzdrževanja.

Vzdrževanje sistema NAC Cisco Identity Services Engine

Ponudnik v času trajanja naročila zaključi implementacijo sistema za nadzor dostopov do omrežja Cisco ISE in prevzame upravljanje sistema. Upravljanje zajema:

- implementiranje politik,
- dodajanje naprav/uporabnikov,
- nastavitve pravil, parametrov za različne tipe dostopov,
- politike overjanja in pooblaščenja različnih tipov naprav in uporabnikov,
- razvrščanje tipov naprav in uporabnikov,
- beleženje različnih tipov dogodkov.

Splošni pogoji

Vse storitve se opravljajo v režimu 8×5: vsak delovni dan od 7:00 do 15:00.

Odzivni čas izvajalca:

- največ dve uri za kritično opremo med delovnim časom,
- največ dvanajst ur za drugo, nekritično opremo med delovnim časom.

Med kritično opremo štejemo tisto, od katere je odvisno delovanje hrbteničnega omrežja in strežnikov.

Druge zahteve:

- v primeru izpada izvajalec posreduje do odprave napake,
- koordinacija ekipe uporabnika za vzdrževanje ostale opreme, v kolikor je skladnost z njo potrebna (internetni ponudniki, ...),
- dokumentiranje izvajanja storitev tehničnega vzdrževanja,
- obdobji (kvartalni) pregled stanja skupaj z naročnikom in predlog izboljšav v omrežju,
- shranjevanje konfiguracij opreme v primeru sprememb in njihovo shranjevanje,
- odpravljanje težav in analiza sistemskih infrastrukturnih težav ter ugotavljanje njihovega izvora
- vzpostavitev elementov informacijske infrastrukture, ki so predmet tega naročila, v delujoče stanje,
- preventivno vzdrževanje v obliki rednih pregledov,
- izdelava poročila o ustreznosti stanja strojne in programske opreme (po dogovoru),
- vodenje dokumentacije o stanju strojne in programske opreme, ki je predmet tega naročila,
- izvajanje popravkov in posodobitev novih verzij programske opreme po priporočilih,
- priprava predlogov za izboljšanje delovanja strojne in programske opreme,
- pomoč pri načrtovanju širitve informacijskega sistema,
- vodenje dokumentacije o izvedenih posegih,
- proaktivno spremljanje delovanja sistema s pomočjo implementirane rešitve.

Status in usposobljenost ponudnika

Zahtevani partnerski statusi ponudnika:

- Cisco Premier Integrator,
- Usposobljen Stormshield partner,
- Usposobljen Wallix Partner.

Ponudnik mora izpolnjevati standarde

- ISO 9001,
- ISO 27001,

- ISO 14001,

kar dokaže z verodostojnimi dokumenti, ki izkazujejo lastništva certifikatov za zahtevane standarde.

Ponudnik mora razpolagati z zahtevanimi tehničnimi zmogljivostmi, ki jih bo uporabljal pri izvedbi javnega naročila. Gre za sredstva, ki so potrebna, da lahko ponudnik uspešno izvede celotno javno naročilo.

Kadri

Ponudnik mora zagotavljati svoje lastno tehnično osebje, z vsaj naslednjimi veljavnimi certifikati:

- 2 × Cisco Certified Network Professional Enterprise
- 2 × Cisco Certified Specialist - Enterprise Core
- 2 × Cisco Certified Specialist – Enterprise Advanced Infrastructure
- 1 × Cisco Certified Specialist - Security Identity Management Implementation
- 1 × Certified Stormshield Network Administrator

Ponudnik mora priložiti veljavna potrdila in certifikate iz katerih je razvidno izpolnjevanje zgoraj navedenih usposobljenosti za tehnično osebje, ki bo sodelovalo pri izvajanju storitev tehnične podpore in svetovanju za opremo. Vsa potrdila in statusi usposobljenosti, s katerimi ponudnik dokazuje svojo usposobljenost morajo biti pridobljena pred objavo tega razpisa.

Reference

Ponudnik mora predložiti ustrezno dokazilo (referenčno potrdilo), da je od 01.01.2021 naprej uspešno kot dejanski izvajalec izvedel enakovredne storitve v višini 100.000 € brez DDV.

Pod pojmom »dejanski izvajalec« se razume izvajalca, ki bo po pogodbi sam izvedel storitve (brez posrednikov, podizvajalcev ipd.), in ki je tudi pri referenčnem poslu neposredno sam izvedel storitve.

Naročnik si pridržuje pravico, da preveri obstoj in vsebino navedb v ponudbi, v kolikor se bo pojavil dvom o resničnosti ponudnikovih izjav. Če jih naročnik ne bo mogel preveriti (npr. tudi z ogledom), referenc ne bo upošteval. Referenčna potrdila se lahko seštevajo.

Dokazila:

Ponudnik (partnerji pri skupni ponudbi) mora v informacijskem sistemu e-JN v razdelek druge priloge naložiti potrdila, certifikate in drugo dokumentacijo s katero dokazuje ustreznost ponudbe.