Technická špecifikácia – Opis predmetu zákazky

Východisková situácia

Úrad pre územné plánovanie a výstavbu Slovenskej republiky (Úrad) vznikol 1. júna 2022 na základe rozhodnutia parlamentu. Odo dňa svojho zriadenia vykonáva všetky činnosti potrebné k zabezpečeniu riadneho chodu úradu a k prechodu práv a povinností v oblasti územného plánovania, výstavby a vyvlastnenia podľa doterajších všeobecne záväzných právnych predpisov z Ministerstva dopravy a výstavby Slovenskej republiky na úrad od 1. januára 2023.

Úrad od 1. júna 2022 vznikol formálne, menovaním predsedu úradu a generálneho tajomníka služobného úradu. Postupne sa úrad rozrastá o realizačný tím, ktorý bude mať za úlohu utvoriť procesy, ktoré budú potrebné zaviesť do praxe k 1. januáru 2023. Následne sa úrad rozrastie, a to delimitáciou niektorých zamestnancov Ministerstva dopravy a výstavby SR a Ministerstva vnútra SR. Nakoľko od 1. januára 2023 prejdú na úrad kompetencie Ministerstva dopravy a výstavby SR na úseku územného plánovania, výstavby a vyvlastnenia.

Pod Úrad pre územné plánovanie a výstavbu Slovenskej republiky budú spadať regionálne úrady, ktoré budú mať určený územný obvod pôsobnosti. Regionálnych úradov bude celkovo 8, a to regionálny úrad so sídlom v Bratislave, Banskej Bystrici, Košiciach, Nitre, Prešove, Trenčíne, Trnave a v Žiline.

Z pohľadu výkonu kompetencií Úradu bude tieto služby v úvodnej fáze zabezpečovať približne 200 pracovníkov na centrálnom úrade a po 80 pracovníkov na regionálnych úradoch.

Úrad bude poskytovať svoje služby tak verejným inštitúciám, ako aj privátnemu sektoru a širokej verejnosti. Z tohto dôvodu musí byť funkčnosť a komunikačná potreba Úradu nastavená na prijatú legislatívu a zároveň musí byť Úrad pripravený a pružne reagovať na všetky súvisiace legislatívne zmeny, ktoré majú jednak dopad aj na rast požiadaviek na rozšírenie, resp. navyšovanie kapacít využívaných elektronických komunikačných služieb, ako aj na aktiváciu nových funkčností poskytovaných elektronickými komunikačnými sieťami v rámci eGoverment.

Reforma v oblasti výstavby a územného plánovania súvisí aj s digitalizáciou a optimalizáciou procesov a sprevádzkovaním jednotného informačného systému Urbion, ktorý by mal fungovať od 1. apríla 2024. Jednotný informačný systém Urbion bude zhromažďovať všetky stavebné procesy na jednom mieste. Procesy sa plne digitalizujú do 1. januára 2028 a funkcionality budú v intenciách, ktoré popisuje zákon. Od roku 2028 by malo byť stavebné konanie plne digitalizované, akékoľvek papierové konania sa skončia. Procesy budú transparentné a monitorovateľné, čo umožní digitalizácia územného plánovania a výstavby, ako aj následná postupná automatizácia procesov v systéme Urbion.

Pre výkon kompetencií Úradu bude potrebné zabezpečiť internú aj externú elektronickú komunikáciu pracovníkov úradu. Zároveň bude potrebné zabezpečiť prístup k zdrojom informačného systému tak z interného ako aj aj z externého prostredia, vrátane komunikačných potrieb so špeciálnymi stavebnými úradmi.

Identifikácia základných potrieb

V súvislosti s horeuvedeným Úrad identifikoval nasledujúce základné potreby pre využívanie pevných dátových elektronických komunikačných služieb pre nasledujúce obdobie:

- ✓ vybudovanie a prevádzkovanie služieb privátnej dátovej siete pre vzájomnú internú komunikáciu Úradu a regionálnych úradov a špeciálnych stavebných úradov a iných súvisiacich organizácií s možnosťou flexibilného nárastu potrebných kapacít;
- ✓ vybudovanie a prevádzkovanie zabezpečeného centrálneho prestupu do siete Internet;
- ✓ integrácia prepojenia do siete Govnet (už zrealizované);
- ✓ vybudovanie a prevádzkovanie centrálneho zabezpečeného prístupu do privátnej siete pre interných a externých užívateľov;
- ✓ vybudovanie a prevádzkovanie LAN sietí na pracoviskách Úradu a regionálnych úradov;
- ✓ vybudovanie a prevádzkovanie WiFi sietí (pre internú aj externú potrebu) na pracoviskách Úradu a regionálnych úradov;
- ✓ vybudovanie a prevádzkovanie samostatného prístupu do siete Internet pre externých užívateľov WiFi sietí s logicky oddelenou prevádzkou od internej komunikačnej prevádzky;
- ✓ vybudovanie a prevádzkovanie podpornej infraštruktúry (dátové stojany / rozvádzače a záložné zdroje napájania UPS) na pracoviskách Úradu a regionálnych úradov;
- ✓ poskytovanie služieb multimediálnej komunikácie medzi jednotlivými pracoviskami;
- ✓ príprava na integráciu záložného dátového centra do privátnej dátovej siete;
- ✓ príprava na integráciu bezpečnostných a „office friendly“ riešení (kamerové systémy, interaktívne tabule, manažment fyzického vstupu do objektu, dochádzkový systém, a pod.) do LAN sietí na pracoviskách Úradu a regionálnych úradov;
- ✓ monitorovanie prevádzky a služieb privátnej dátovej siete;
- ✓ poskytovanie služieb bežnej prevádzkovej podpory a technickej podpory na vyžiadanie pri rozšírení služieb a/alebo zmene konfigurácie služieb.

Základné požiadavky

Verejný obstarávateľ má v úmysle obstarať služby, definované v tomto opise predmetu zákazky ako komplexné služby. Pod pojmom "komplexná služba" sa rozumie služba, ktorej zriadenie, prevádzkovanie, monitorovanie, správu a prípadný servis použitých koncových zariadení a komponentov zabezpečuje v plnom rozsahu Poskytovateľ služby počas celej doby trvania zmluvného vzťahu.

Verejný obstarávateľ požaduje, aby boli služby zriadené a poskytované prostredníctvom nových koncových zariadení. Novým zariadením je každé zariadenie, ktoré nebolo nikdy a nikde nainštalované, okrem vybalenia zariadenia a jeho prvotnej konfigurácie.

<u>Služby sieťovej konektivity</u>

Dátovú komunikačnú infraštruktúru Úradu a partnerských organizácií bude tvoriť dátová virtuálna privátna sieť vrátane jej komponentov a infraštruktúry na úrovni WAN aj LAN vo všetkých lokalitách, resp. pracoviskách. Dátové pripojenie bude určené na vzájomnú elektronickú komunikáciu s ostatnými pracoviskami navzájom a bude zabezpečovať pripojenie na externé siete Internet a GOVNET.

Požiadavky verejného obstarávateľa v tejto oblasti zahŕňajú predovšetkým:

- ✓ zriadenie, prevádzkovanie a správu virtuálnej privátnej dátovej komunikačnej siete na prepojenie koncových bodov verejného obstarávateľa pre potreby obojsmerného prenosu dát výhradne medzi lokálnymi počítačovými sieťami jednotlivých lokalít verejného obstarávateľa a partnerských organizácií;
- ✓ redundantné prepojenie lokalít verejného obstarávateľa a partnerských organizácií za účelom zabezpečenia vysokej dostupnosti prepojenia;
- ✓ dodávka, konfigurácia, správa a servis koncových komunikačných zariadení, nevyhnutných pre správne fungovanie služby a umiestnených v jednotlivých lokalitách verejného obstarávateľa a partnerských organizácií;
- ✓ zriadenie a poskytovanie bezpečného pripojenia do siete Internet;
- ✓ zriadenie a poskytovanie vzdialeného VPN prístupu do privátnej dátovej siete;
- ✓ integrácia pripojenia do siete GOVNET.

Bezpečnostné služby

Privátna dátová sieť poskytne bezpečnú komunikáciu. Pripojenie sa požaduje šifrované a prostredníctvom šifrovacích protokolov sa požaduje selektívne definovať bezpečnostné parametre, definovať spôsob utajenia prenosu, spôsob verifikácie odosielateľa a spôsob algoritmického zabezpečenia celistvosti prenášaných dát. Požaduje sa IPSEC protokol medzi aktívnymi WAN prvkami, v konfigurácií SiteToSite. Pripojenie pre vybraných koncových používateľov do privátnej dátovej siete bude možné aj z Internetu cez IPSEC VPN klienta. Funkcionalita sieťovej bezpečnosti je požadovaná aj s ochranou voči organizovaným útokom typu DDoS. DDoS ochrana je požadovaná na elimináciu nelegitímneho dátového toku, keď je sieťová prevádzka postihnutá útokom typu DDoS a požadované je presmerovať, alebo inak efektívne a s veľkou účinnosťou odfiltrovať útok.

Požiadavky verejného obstarávateľa v tejto oblasti zahŕňajú predovšetkým:

- ✓ zriadenie, prevádzkovanie a správa služby zabezpečujúcej šifrovanú komunikáciu medzi uzlami privátnej dátovej siete;
- ✓ zriadenie, prevádzkovanie a správa služby zabezpečujúcej služby riadenia a vyhodnocovania toku dát s funkcionalitami, spĺňajúcimi definíciu Next Generation Firewall;
- ✓ zriadenie, prevádzkovanie a správa služby zabezpečujúcej ochranu pred neželaným únikom dát z interného prostredia verejného obstarávateľa (DLP);
- ✓ zriadenie, prevádzkovanie a správa služby zabezpečujúcej bezpečné vzdialené pripojenie užívateľov do privátnej siete verejného obstarávateľa (VPN);
- ✓ zriadenie, prevádzkovanie a správa služby zabezpečujúcej ochranu voči organizovaným útokom typu DDoS.

Služby na úrovni lokálnych sietí

Súčasťou poskytovanej privátnej siete na úrovni lokálnej siete bude prenájom a prevádzka aktívnych prvkov LAN a WiFi infraštruktúry v jednotlivých lokalitách.

Požiadavky verejného obstarávateľa v tejto oblasti zahŕňajú predovšetkým:

- ✓ zriadenie, prevádzkovanie a správu zariadení LAN siete typu prepínač slúžiaceho pre pripojenie koncových zariadení typu PC/NTB, VoP SIP telefón, WiFi AP a iné;

- ✓ zriadenie, prevádzkovanie a správu zariadení LAN siete typu WiFi access point (WiFi AP) slúžiaceho pre zabezpečené pripojenie koncových zariadení pracovníkov užívateľa typu mobil, tablet, NTB, a iné;
- ✓ zriadenie, prevádzkovanie a správu zariadení LAN siete typu WiFi access point (WiFi AP) slúžiaceho pre verejné pripojenie koncových zariadení externých užívateľov typu mobil, tablet, NTB, a iné;
- ✓ zriadenie, prevádzkovanie a správu zariadení LAN siete typu WiFi kontroler slúžiaceho na riadenie príslušných priradených WiFi AP;
- ✓ zriadenie, prevádzkovanie a správu zariadení podpornej infraštruktúry typu UPS slúžiaceho pre zálohovanie napájania koncových zariadení typu smerovač, LAN prepínač a WiFi AP;
- ✓ zriadenie, prevádzkovanie a správu zariadení podpornej infraštruktúry typu technologický stojan slúžiaceho pre umiestnenie a primárne napájanie koncových zariadení typu smerovač, LAN prepínač a UPS.

<u>Služby správy, administrácie, monitoringu a prevádzkovej podpory</u>

Verejný obstarávateľ požaduje nepretržitý 24 hodinový/365 dňový monitoring privátnej dátovej siete (vrátane koncových zariadení) a služieb s možnosťou okamžitého prehľadu o stave privátnej dátovej siete a služieb poskytovaných privátnou dátovou sieťou. Riešenie poruchových stavov musí byť v súčinnosti so zodpovedajúcimi organizačnými zložkami verejného obstarávateľa, resp. ním poverenej tretej strany. Súčasťou poskytovaných komunikačných služieb musí byť správa a údržba dodaných a prevzatých koncových zariadení.

Súčasťou prevádzkovej podpory privátnej dátovej siete bude aj aktivácia doplnkových služieb a poskytovanie služieb expertnej technickej podpory na vyžiadanie.

Požiadavky verejného obstarávateľa v tejto oblasti zahŕňajú predovšetkým:

- ✓ zriadenie, prevádzkovanie a správa služby, zabezpečujúcej služby centralizovaného logovania kritických komponentov komunikačnej infraštruktúry a bezpečnostných komponentov;
- ✓ riadenie, prevádzkovanie a správa služby, zabezpečujúcej služby centrálneho dohľadu a monitoringu poskytovaných služieb;
- ✓ poskytovanie služieb technickej podpory pri odstraňovaní porúch a zaistení garantovanej kvality poskytovanej služby SLA v režime 24 hodín / 365 dní;
- ✓ poskytovanie služieb technickej podpory pri riešení minoritných nezávažných porúch neohrozujúcich garantované SLA počas pracovnej doby verejného obstarávateľa v režime min. 8 hodín / 5 pracovných dní;
- ✓ poskytovanie služieb expertnej technickej podpory pri zriaďovaní a prevádzke horeuvedených služieb.

Podrobná špecifikácia predmetu zákazky

Služby sieťovej konektivity

Miesta a typy koncových bodov pre poskytovanie služieb

Koncové body komunikačnej infraštruktúry verejného obstarávateľa sa nachádzajú výhradne na území SR v intraviláne miest a obcí s výnimkami uvedenými nižšie.

V závislosti od komunikačných potrieb a garancie SLA sú koncové body pre poskytovanie služieb rozdelené do nasledujúcich typov:

- ✓ Typ 1 – pracovisko centrály – SLA 1 (Bratislava)
- ✓ Typ 2 – pracovisko pobočky – SLA 1 (regionálny úrad, partnerská organizácia v krajskom meste)
- ✓ Typ 3 – pracovisko pobočky – SLA 2 (regionálny úrad, partnerská organizácia v okresnom meste)
- ✓ Typ 4 – pracovisko pobočky detašované – SLA 2 (regionálny úrad, partnerská organizácia)
- ✓ Typ 5 – pracovisko pobočky mobilné – SLA 3 (regionálny úrad, partnerská organizácia)

Spôsob a kapacita pripojenia koncových bodov privátnej siete

Verejný obstarávateľ požaduje vybudovať privátnu sieť technológiou IP MPLS s možnosťou komunikácie medzi všetkými vzájomne prepojenými privátnymi sieťami verejného obstarávateľa a s možnosťou nastavenia obmedzení v smerovaní tokov dát podľa Požiadaviek verejného obstarávateľa.

Primárne pripojenie jednotlivých koncových bodov je možné realizovať výhradne jednou z nasledovných technológií (ak nie je uvedené inak):

- ✓ pripojenie prostredníctvom optického prenosového média;
- ✓ pripojenie prostredníctvom metalického prenosového média;
- ✓ rádiové pripojenie v licencovanom pásme.

Prístupová kapacita primárneho pripojenia musí byť plne symetrická a musí zodpovedať definovaným kapacitným požiadavkám pre daný typ koncového bodu (uvedené v tabuľke nižšie). Navýšenie prístupovej kapacity na minimálnu požadovanú úroveň musí byť zrealizované bez potreby výmeny prístupovej technológie s minimálnym dopadom na dostupnosť služby.

Záložné pripojenie jednotlivých lokalít je možné realizovať výhradne jednou z nasledovných technológií (ak nie je uvedené inak):

- ✓ pripojenie prostredníctvom optického prenosového média
- ✓ pripojenie prostredníctvom metalického prenosového média
- ✓ rádiové pripojenie v licencovanom pásme
- ✓ asymetrické pripojenie technológiou xDSL (aplikovateľné len pre Typ 4)
- ✓ bezdrôtové pripojenie technológiou 4G/LTE/5G (aplikovateľné len pre Typ 4).

Prístupová kapacita záložného pripojenia musí byť plne symetrická (s výnimkou pripojenia xDSL a 4G/LTE/5G) a musí zodpovedať definovaným kapacitným požiadavkám pre daný typ koncového bodu (uvedené v tabuľke nižšie).

Typ pripojenia	Základná kapacita primárneho pripojenia	Navýšená kapacita primárneho pripojenia	Kapacita záložného pripojenia	Typ SLA
Typ 1	500 Mbit/s	1GBit/s	500 Mbit/s	SLA 1
Typ 2	200 Mbit/s	500 Mbit/s	200 Mbit/s	SLA 1
Typ 3	100 Mbit/s	200 Mbit/s	100 Mbit/s	SLA 2
Typ 4	20 Mbit/s	50 Mbit/s	20 Mbit/s	SLA 2
Typ 5	10 Mbit/s	20 Mbit/s	n/a	SLA 3

Záložné pripojenie jednotlivých lokalít musí byť realizované na inom type prenosového média, aké bude použité pre primárne pripojenie a je nutné realizovať ho geograficky nezávislou trasou, ktorá nesmie byť v súbehu s primárnou trasou. V prípade, že je primárne pripojenie realizované prostredníctvom optického prenosového média, je pre záložné pripojenie akceptované aj pripojenie prostredníctvom optického prenosového média realizovaného geograficky nezávislou trasou od vstupu do objektu.

Pripojenie lokalít (ak nie je uvedené inak) musí byť realizované v režime vysokej dostupnosti (high availability). V prípade výpadku primárneho pripojenia musí byť záložné pripojenie aktivované automaticky.

Každý použitý typ prístupu musí garantovať poskytnutie požadovaných parametrov a nesmie byť obmedzený zdieľaním prenosovej kapacity s inými účastníkmi siete poskytovateľa.

Služba pripojenia musí zahŕňať aj možnosť prioritizovať vybrané typy komunikácie (QoS).

Služba pripojenia musí zahŕňať aj dodávku a správu koncových zariadení typu smerovač s podporou QoS pre aplikácie a zdroje poskytované z dátového centra a smerovač musí byť dostatočne výkonný odpovedajúci parametrom pripojení v tabuľke vyššie.

<u>Centralizovaný bezpečný prestup do siete Internet</u>

Centralizovaný prestup do siete Internet a smerovanie v privátnej dátovej sieti musí byť realizovaný v priestoroch dátových centier Poskytovateľa tak, aby bola zabezpečená vysoká dostupnosť služby. Prenosová kapacita musí byť v súlade s požiadavkami na prenosové kapacity jednotlivých lokalít, prepojených v rámci siete IP MPLS, vrátane požiadaviek na kapacitu pripojenia do siete Internet.

Služba bezpečného prístupu do siete Internet bude ukončená na zariadení typu Next Generation Firewall (NGFW). Pripojený aktívny prvok centralizovaného prístupu Internet bude podporovať protokol BGP a prenosové rýchlosti min. 1Gbps.

Smerovanie prevádzky do siete Internet z privátnej dátovej siete bude realizované prostredníctvom zariadení NGFW s dvoma nezávislými trasami, každá s prenosovou kapacitou min. 1Gbit/s symetricky.

Štandardná služba centralizovaného Internet pripojenia obsahuje najmenej:

- ✓ vysokokapacitné pripojenie a redundantné pripojenie (redundancia je požadovaná aj pre pripojenie, aj pre aktívne prvky);
- ✓ poskytovanie záložného DNS (menného) servera v redundantnej konfigurácií;

- ✓ službu registrátora doménového mena;
- ✓ službu poskytnutia verejného IP adresného rozsahu (IPV4) v minimálnom počte 14 pevných verejných IP adries.

Vzdialený VPN prístup do privátnej dátovej siete

Verejný obstarávateľ požaduje nasadenie a správu technológie, umožňujúcej bezpečný vzdialený prístup užívateľov verejného obstarávateľa do jeho privátnej dátovej siete. Služba je požadovaná ako bezpečné pripojenie do privátnej dátovej siete pre zamestnanca pracujúceho mimo stáleho pracovisko a/alebo pracovníkov partnerských organizácií s využitím ľubovoľného prístupu do siete Internet. Služba vzdialeného prístupu musí byť vysoko dostupná, plne manažovaná a zahŕňa vybudovanie a prevádzkovanie zariadenia typu VPN koncentrátor. Redundantný aktívny prvok bezpečného prístupu do VPN musí poskytovať vzdialený šifrovaný prístup z koncového zariadenia používateľa (PC, notebook) pripojeného v ľubovoľnom bode siete Internet do privátnej dátovej siete verejného obstarávateľa.

Služba vzdialeného VPN prístupu do privátnej dátovej siete musí umožňovať paralelné pripojenie min. 200 užívateľov s možnosťou rozšírenia až na 1000 užívateľov bez potreby výmeny hardvéru.

Integrácia pripojenia do siete GOVNET

Požaduje sa zabezpečenie integrácie služieb existujúceho dátového prepojenia so sieťou GOVNET v súlade s pravidlami stanovenými správcom siete GOVNET. Ide o prevádzkovanie zabezpečeného lokálneho prepojenia služieb privátnej dátovej siete s infraštruktúrou siete GOVNET. Požaduje sa zabezpečiť samostatný fyzický port na prestupovom aktívnom WAN prvku v danej lokalite. Prístup do siete GOVNET je už v súčasnosti zriadený a poskytovaný.

NASES, ako správca siete GOVNET určuje podmienky pripojenia v zmysle svojich interných prevádzkových predpisov. Pre veľkokapacitné uzly je štandardom redundancia všetkých aktívnych prvkov aj pripojenia WAN prípojky a pripojenie na aktívny bezpečnostný prvok dátovej privátnej siete.

Pripojený aktívny prvok s FW funkcionalitou centralizovaného prístupu GOVNET do WAN bude podporovať protokol BGP a prenosové rýchlosti min. 2x1Gbps.

Miestom pripojenia do siete GOVNET je centrála privátnej dátovej siete (Tomášikova 14366/64A, 831 04 Bratislava).

Bezpečnostné služby

Šifrovaná komunikácia medzi uzlami privátnej dátovej siete

Privátna dátová sieť poskytne bezpečnú komunikáciu. Pripojenie sa požaduje šifrované a prostredníctvom šifrovacích protokolov sa požaduje selektívne definovať bezpečnostné parametre, definovať spôsob utajenia prenosu, spôsob verifikácie odosielateľa a spôsob algoritmického zabezpečenia celistvosti prenášaných dát. Ďalej sa požaduje selektívne definovať bezpečnostné

parametre v súlade s aktuálnou bezpečnostnou politikou a príslušnej legislatívy, najmä v zmysle Zákona o Kybernetickej bezpečnosti a príslušných vyhlášok.
Požaduje sa IPSEC protokol medzi aktívnymi WAN prvkami, v konfigurácií SiteToSite. Pripojenie pre vybraných koncových užívateľov do VPN bude možné aj z Internetu cez VPN klienta.

Next generation firewall (NGFW)

Verejný obstarávateľ požaduje nasadenia a správu technológie Next Generation Firewall (NGFW) za účelom granulárneho riadenia dátovej komunikácie medzi privátnou dátovou sieťou verejného obstarávateľa, sieťou Internet a sieťami externých dodávateľov a partnerov verejného obstarávateľa. Účelom nasadenia technológie Next Generation Firewall je dosiahnutie najvyššieho možného stupňa ochrany vonkajšieho perimetra siete verejného obstarávateľa a ochranu jeho privátnych sietí pred neoprávneným prístupom. Služba má byť plne manažovaná Poskytovateľom a prevádzkovaná v dátovom centre Poskytovateľa v režime vysokej dostupnosti.

Služba Next Generation Firewall má podporovať nasledovné funkcionality:

Schopnosť rozpoznania aplikácií – podporovať schopnosť rozpoznať a následne umožniť, zakázať alebo požadovaným spôsobom limitovať dátovú komunikáciu, prináležiacu konkrétnej aplikácii a bez ohľadu na použitý komunikačný protokol a port, cez ktorý aplikácia komunikuje;
Schopnosť rozpoznania identity užívateľov – podporovať schopnosť rozpoznania identity užívateľov za účelom granulárnej kontroly prístupu ku konkrétnym aplikáciám na základe užívateľa, skupiny užívateľov resp. zariadení, z ktorých je realizovaný prístup k systémom verejného obstarávateľa;
Centralizovaný manažment, administrácia, logovania a reporting – podporovať možnosť centralizovaného manažmentu prostredníctvom web rozhrania;
Stavová inšpekcia paketov - podporovať možnosť stavovej inšpekcie dát v reálnom čase min. v rozsahu 2-7 vrstvy OSI modelu;
Hĺbková inšpekcia paketov (Deep packet inspection - DPI) – podporovať možnosť hĺbkovej inšpekcie za účelom identifikovania a následného blokovania prípadných chýb, anomálií a známych typov útokov v dátovej komunikácii;
Ochrana proti prieniku (Intrusion Detection/Prevention System - IDS/IPS) – podporovať integrovanú ochranu proti prieniku do siete verejného obstarávateľa s možnosťou automatického zablokovania alebo notifikácie o prebiehajúcej neželanej resp. abnormálnej dátovej komunikácii;
Možnosť inšpekcie šifrovanej komunikácie – podporovať možnosť nahliadať do obojsmerne prebiehajúcej šifrovanej dátovej komunikácie min. pre protokol SSL;
Možnosť integrácie s inými bezpečnostnými riešeniami – podporovať možnosť integrácie min. so systémom SIEM, bezpečnostným reportingovým nástrojom a službou viacfaktorovej autentifikácie;
Vstavaná antivírová a antibot ochrana – podporovať zabudovaný mechanizmus ochrany proti vírusom a botom so schopnosťou identifikácie infikovaných súborov min. pre protokoly HTTP, HTTPS, FTP, POP3, SMTP a SMB;

Minimálne požadované výkonové parametre pre službu Next Generation Firewall:

Redundancia – požaduje sa plná redundancia zariadení, zabezpečujúcich službu;
Priepustnosť firewallu – priepustnosť 1,6 Gb/s v prípade IPv4/IPv6 UDP paketov s veľkosťou 1518 bitov;
Priepustnosť IPSec VPN – priepustnosť 1 Gb/s pri paketoch s veľkosťou 512 bitov pri použití šifrovania AES256-SHA256;
Priepustnosť SSL inšpekcie – priepustnosť 1 Gb/s pre HTTPS spojenia;

Priepustnosť SSL VPN – priepustnosť 1 Gb/s (pri TLS v1.2 s AES256-SHA šifrovaní vrátane podpory TLS v1.3)

Data Loss Prevention (DLP) - systém na prevenciu pred únikom citlivých dát

Verejný obstarávateľ požaduje nasadenie a správu technológie Data Loss Prevention (DLP) - systému na zabránenie únikom citlivých dát z interného prostredia verejného obstarávateľa pre 2000 počet koncových bodov. Verejný obstarávateľ požaduje prístup ku manažment konzole DLP systému za účelom vytvárania, modifikácie a rušenia bezpečnostných politík, získania prehľadu o incidentoch a celkovom stave systému v reálnom čase a za účelom reportingu. Verejný obstarávateľ požaduje mať v prípade potreby k dispozícii možnosť prevzatia manažmentu celého riešenia do svojej vlastnej správy.

Služba Data Loss Prevention (DLP) má podporovať nasledovné funkcionality:

Bezpečnostný audit dát – podporovať auditovanie historických dát, vrátane dát z externých zariadení, webových uploadov, emailov, instant messagingu, tlače a cloudových úložísk;
Podpora auditovania pre Office 365 – podporovať auditovanie operácii so súbormi a odchádzajúcich emailov prostredníctvom služby MS Office 365;
Podpora bezpečnostných noriem a regulácií – podpora pre bezpečnostné normy a regulácie, min. v rozsahu GDPR;
Klasifikácia inšpektovaného obsahu – klasifikovať senzitívne súbory a emaily pomocou preddefinovaných vzorov a pravidiel;
Detekcia podozrivých aktivít – detekcia a notifikácia podozrivých aktivít v reálnom čase;
Ochrana siete a emailov – podporovať ochranu pre emaily, webové uploady, instant messaging a zdieľané sieťové disky;
Ochrana zariadení a tlače – podporovať ochranu dát ukladaných na externé úložné zariadenia a taktiež ochranu pred neželaným vytlačením dát na tlačiarňach všetkých typov;
Ochrana vzdialeného prístupu – schopnosť zabrániť únikom dát cez vzdialený prístup k pracovnej ploche;
Pokročilá klasifikácia dát – detegovať a označovať senzitívne dáta na základe pôvodu alebo typu súboru prostredníctvom uložených metadát;
Vytváranie kópií podozrivých dát – schopnosť vytvárať šifrované kópie podozrivých dát z incidentov za účelom forenznej analýzy;
Správa riešenia – podporovať správu prostredníctvom web rozhrania v plnom rozsahu;
Kontrola pracovnej plochy – podporovať ochranu pracovnej plochy s možnosťou zabrániť únikom dát vytváraním kópií obrazovky;
Podpora pre BitLocker – podporovať šifrovanie BitLocker;
Ochrana synchronizácie dát na cloudové úložiská – podporovať ochranu dát, ktoré sú synchronizované na externé cloudové úložiská typu OneDrive, GoogleDrive, DropBox a pod.;
Ochrana pre Office 365 – podporovať ochranu proti neželanému zdieľaniu dokumentov Office 365 a SharePoint prostredníctvom cloudovej služby;
Podpora pre integráciu s doménou – podporovať integráciu s Active Directory;
Integrácia s NGFW – podporovať integráciu s ponúkaným Next Generation Firewallom za účelom automatizácie vybraných operácií.

Vzdialený VPN prístup používateľov

Verejný obstarávateľ požaduje nasadenie a správu technológie, umožňujúcej bezpečný vzdialený prístup používateľov verejného obstarávateľa do jeho privátnej siete.

Služba vzdialeného VPN prístupu má podporovať nasledovné funkcionality:

Bezpečnosť – podporovať vzdialený prístup pomocou protokolov min. IPSec VPN / L2TP VPN;
Viacfaktorová autentifikácia – okrem štandardného prihlasovania prostredníctvom prihlasovacieho mena a hesla musí podporovať aj viacfaktorovú autentifikáciu prostredníctvom softvérového tokenu, generujúceho jednorazové číselne kódy, dostupného pre všetky bežne používané OS a mobilné platformy;
Správa VPN používateľov – umožňovať správu VPN používateľov (min. v rozsahu vytvárania, rušenia a dočasného zablokovania účtu, priradenia tokenu používateľovi, možnosti definovania pravidiel a politík, vymedzujúcich prístup vzdialených používateľov na konkrétne zariadenie resp. služby vo vnútornej sieti verejného obstarávateľa) prostredníctvom web rozhrania;
Overovanie používateľov – podporovať overovanie používateľov prostredníctvom samostatného autentizačného servera, bezpečne oddeleného od vnútornej infraštruktúry verejného obstarávateľa aj od Internetu;
Autorizácia používateľov – podporovať možnosť autorizácie vzdialených používateľov s funkcionalitou reportingu o udalostiach, týkajúcich sa prihlasovania sa používateľov do VPN a využívania vzdialeného pripojenia;
Logovanie prístupov – podporovať centralizované logovanie vzdialených VPN prístupov používateľov za účelom zisťovania problémov a bezpečnostných incidentov;
Kompatibilita – VPN klient musí byť dostupný pre všetky bežne používané OS a mobilné platformy.

Služby na úrovni lokálnych sietí

LAN prepínače

Verejný obstarávateľ požaduje nasadenie a správu technológie typu LAN prepínač umožňujúcej pripojenie koncových zariadení typu PC/NTB, VoP SIP telefón, WiFi AP prípadne iných typov s využitím funkcionality napájania týchto koncových zariadení prostredníctvom PoE, resp. PoE+.

V závislosti od komunikačných potrieb sú požadované nasledovné typy LAN prepínačov:

Typ A: 8-portové aktívne prvky (prepínače): min. 8 down-link portov 10/100/1000 RJ45
Typ B: 24-portové aktívne prvky (prepínače): min. 24 down-link portov 10/100/1000 RJ45
Typ C: 48-portové aktívne prvky (prepínače): min. 48 down-link portov 10/100/1000 RJ45
Typ D: 24-portové aktívne prvky (prepínače): min. 24 down-link portov SFP+ (10G/25G) – non-PoE

Požiadavky na up-link porty:
Typ A: min. 2 SFP porty/sloty 1Gbps použiteľné ako pre optickú tak aj pre metalickú kabeláž
Typ B: min. 2 SFP+ porty/sloty 10Gbps použiteľné ako pre optickú tak aj pre metalickú kabeláž
Typ C: min. 4 SFP+ porty/sloty 10Gbps použiteľné ako pre optickú tak aj pre metalickú kabeláž
Typ D: min. 4 SFP+ porty/sloty 25/40Gbps pre optickú kabeláž

Požiadavky na L2 funkcionalitu:
- podpora IEEE 802.3x Flow Control,
- podpora jumbo (min. 9000B) rámcov,
- podpora monitorovania a záznamu o dátových tokoch v hardvéri,
- podpora IEEE 802.3ad (LACP),
- podpora IEEE 802.3az (Energy Efficient Ethernet),
- podpora IEEE 802.1q, hlasových aj dynamických VLAN,
- podpora IEEE 802.1d (Spanning Tree Protocol),
- podpora IEEE 802.1s MST,
- podpora IEEE 802.1w RSTP,
- podpora IEEE 802.1ab LLDP,
- ochrana STP Protokolu pred zmenou koreňového prepínača, filtrovanie BPDU,
- ochrana pri vzniku jednosmerných liniek,
- podpora lokálneho aj vzdialeného zrkadlenia dátových tokov.

Požiadavky na bezpečnosť:
- riadenie bezpečnostných funkcií pomocou IPv4 aj IPv6 prístupových filtrov,
- podpora IPv6 first hop security - min. funkcia RA guard, DHCPv6 guard, IPv6 Source Guard,
- podpora RADIUS CoA,
- podpora Dynamic ARP Inspection, DHCP Snooping, IP Source Guard,
- podpora IEEE 802.1x s dynamickým priradením VLAN, Podpora IEEE 802.1x s dynamickým priradením ACL,
- podpora IEEE 802.1x s MAB,
- podpora IEEE 802.1x pre dátovú aj hlasovú VLAN súčasne na jednom fyzickom porte,
- podpora webovej autentifikácie pre non-802.1x klientov,
- podpora IEEE 802.1x Guest VLAN, Auth-fail VLAN, Auth-bypass VLAN,
- podpora Wake-on-LAN spolu s 802.1x,
- ochrana riadiacej jednotky pred DoS útokmi,
- podpora IEEE 802.1ae macsec 128 (neplatí pre 8 port. zariadenie).

Požiadavky na manažment zariadení:
- samostatný konzolový port a/alebo samostatný 10/100 Ethernet network manažment port,
- podpora SSHv2, HTTPS,
- podpora SNMPv3 (s autentifikáciou a šifrovaním).

Požiadavky na riadenie kvality služieb QoS:
- riadenie kvality poskytovaných služieb (QoS) pre prenos dát hlasu a videa, prioritný queueing, traffic shaping, traffic policing, DSCP remarking,
- klasifikácia / Marking / Policing / Queueing,
- klasifikácia podľa 802.1p CoS / ToS / DSCP / MAC / L3 ACL / L4 ACL.

<u>WiFi AP a WiFi kontroler</u>

Verejný obstarávateľ požaduje nasadenie a správu technológie typu WiFi access point (WiFi AP) v spojení so zariadeniami typu WiFi kontrolér (centrálny riadiaci prvok) na riadenie bezdrôtových prístupových sietí.

Na WiFi kontrolér sú definované všetky sieťové a bezpečnostné parametre. Systém musí mať funcionalitu „captive portal“ resp. „hot spot“ s automatickým odpájaním užívateľov. Tento riadiaci prvok musí mať minimálne 2Gpbs priepustnosť, podporu pre pripojenie až do 256 WiFi AP.

Požadované funkcionality pre WiFi kontrolér:

Podpora RF manažment signálu s aktívnou identifikáciou a zmierňovaním rušenia signálu.
Podpora bezdrôtových štandardov: IEEE 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11w, 802.11ac, 802.1Q, 802.1X.
Podpora bezpečnostných štandardov: WPA2™ AES, WPA3™ AES s 802.1x alebo preshared key, Web Captive Portal, MAC blocklist & allowlist: EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST.

Požadované funkcionality pre WiFi AP:

- dual-band802.11a/g/n/ac/ax
- podpora 802.11ac Wave 2
- certifikácia Wifi Alliance Wifi6 a WPA3
- inteligentné riadenie prevádzkového režimu 2.4GHz, 5GHz, 6GHz,
- podpora 802.3at PoE,
- podpora multigigabit-ethernet 2.5Gbps IEEE802.3bz
- min. počet LAN portov 1x 10/100/1000Base-T
- analýza 7 aplikačnej vrstvy s možnosťou prioritizácie a blokovania jednotlivých aplikácií
- podpora asistovaného roamingu 802.11k, 802.11r, 802.11v

<u>Záložný zdroj napájania UPS</u>

Verejný obstarávateľ požaduje nasadenie a správu technológie typu UPS slúžiaceho pre zálohovanie napájania koncových zariadení typu smerovač, LAN prepínač a WiFi AP.

V závislosti od komunikačných potrieb a potrieb na distribuovanú alokáciu prvkov LAN siete sú požadované nasledovné typy UPS zariadení:

Typ A: záložné napájanie koncového bodu privátnej komunikačnej siete Typ 1 (WAN smerovač, 4 x LAN prepínač Typ C, 4 x WiFi AP) minimálne pod dobu 60 minút;
Typ B: záložné napájanie koncového bodu privátnej komunikačnej siete Typ 2 a Typ 3 (WAN smerovač, 1 x LAN prepínač Typ C, 2 x WiFi AP) minimálne pod dobu 60 minút;
Typ C: záložné napájanie koncového bodu privátnej komunikačnej siete Typ 4 (WAN smerovač, 1 x LAN prepínač Typ B, 1 x WiFi AP) minimálne pod dobu 60 minút;
Typ D: záložné napájanie distribuovaného uzla LAN siete (1 x LAN prepínač Typ C, 2 x WiFi AP) minimálne pod dobu 30 minút;

<u>Technologický stojan (rack)</u>

Verejný obstarávateľ požaduje nasadenie a správu technológie typu technologický stojan (rack) slúžiaceho pre umiestnenie a primárne napájanie koncových zariadení typu smerovač, LAN prepínač a UPS.

Aktívne prvky je potrebné umiestniť do racku (oceľový rám so štandardným 19‘‘ uchytením), ktorý bude obsahovať centrálnu napájaciu lištu, z ktorej budú primárne napájané aktívne zariadenia. Rack musí byť uzatvorený a uzamykateľný.

V závislosti od komunikačných potrieb a potrieb na distribuovanú alokáciu prvkov LAN siete sú požadované nasledovné typy technologických stojanov:
Typ A: min. 42 U
Typ B: min. 20 U

Služby správy, administrácie, monitoringu a prevádzkovej podpory

Služby správy, administrácie, monitoringu

Verejný obstarávateľ požaduje nepretržitý 24 hodinový/365 dňový monitoring privátnej dátovej siete (vrátane koncových zariadení) a služieb s možnosťou okamžitého prehľadu o stave privátnej dátovej siete a služieb poskytovaných privátnou dátovou sieťou. Poskytovateľ služby zabezpečuje správu a administráciu privátnej dátovej siete a zároveň všetkých aktívnych koncových zariadení, ktoré sú poskytované ako súčasť služby (smerovače, LAN prepínače, WiFi AP a kontroler, UPS).

Služba centralizovaného monitoringu musí byť vysoko dostupná a musí spĺňať nasledovné funkcionality:

Alerting – podpora automatického vyhodnocovania chybových stavov a následná možnosť alertingu, hlásenia incidentov a prevádzkových problémov;
Reporting – podpora automatického reportingu aktuálnych dát v reálnom čase a tiež historických dát s min. granularitou deň/týždeň/mesiac/rok;
Prístup – pre technický personál verejného obstarávateľa sa požaduje zabezpečenie prístupu k dashboardu monitorovacieho nástroja min. v móde read only, t.j. na sledovanie štatistík systému v reálnom čase a archívnych dát bez možnosti zmeny konfigurácie systému;
Informácia o plnení SLA – od monitorovacieho nástroja sa požaduje možnosť automaticky vyhodnocovať nastavené parametre SLA a následne spracovať report o plnení SLA parametrov.

Služby prevádzkovej podpory

Od Poskytovateľa sa požaduje poskytnutie služby nepretržitej prevádzkovej podpory a odstraňovania prípadných poruchových stavov. Poskytovateľ musí disponovať centrom prevádzkovej a technickej podpory s nepretržitým režimom 24 hodín/365 dní. Toto kontaktné miesto môže používateľ použiť v prípade akýchkoľvek problémov alebo otázok súvisiacich s poskytovanou službou v prípade poruchy.

Pre potreby klarifikácie technických otázok súvisiacich s poskytovaním služby a pri riešení minoritných nezávažných porúch neohrozujúcich garantované SLA musí Poskytovateľ disponovať centrom podpory „HELP DESK“ počas pracovnej doby verejného obstarávateľa v režime min. 8 hodín / 5 pracovných dní.

Súčasťou prevádzkovej podpory privátnej dátovej siete bude aj aktivácia doplnkových služieb uvedených nižšie a poskytovanie služieb expertnej technickej podpory pri rozšírení a/alebo zmene konfigurácie privátnej dátovej siete na vyžiadanie verejným obstarávateľom.

Doplnkové služby

Verejný obstarávateľ môže požadovať poskytovanie doplnkových služieb, ktoré by boli poskytované ako rozšírenie existujúcich základných služieb privátnej dátovej siete o nové funkcionality, resp. by boli poskytované formou expertnej technickej podpory. Poskytovateľ musí poskytovať nasledujúci minimálny rozsah doplnkových služieb:

- ✓ Zriadenie novej alebo presťahovanie existujúcej lokality Typ 2, Typ 3, alebo Typ 4;
- ✓ Navýšenie kapacity pripojenia pre primárny prístup pre lokalitu Typ 1
- ✓ Navýšenia kapacity pripojenia pre záložný prístup pre lokalitu Typ 1
- ✓ Navýšenie kapacity pripojenia pre primárny prístup pre lokality Typ 2 až Typ 5;
- ✓ Zriadenie a prevádzkovanie nového zariadenia LAN prepínač a jeho začlenenie do existujúcej siete;
- ✓ Zriadenie a prevádzkovanie nového WiFi AP a jeho začlenenie do existujúcej siete pod príslušný WiFi kontroler;
- ✓ Poskytovanie služieb expertnej technickej podpory.

Garantovaná kvalita poskytovaných služieb SLA

Garantovaná kvalita poskytovaných služieb (ďalej tiež „SLA“, t.j. Service Level Agreement) je definovaná skupinou merateľných hodnôt, ktoré majú podstatný vplyv na prevádzku a kvalitu poskytovaných verejných telekomunikačných služieb. Tieto hodnoty vyjadrujú minimálnu úroveň, ktorú sa Poskytovateľ zaväzuje verejnému obstarávateľovi poskytnúť ako záruku za dodržanie medzných hodnôt dohodnutej skupiny parametrov. Zárukou je dohodnutá finančná náhrada, na ktorú má užívateľ nárok v prípade, že medzné parametre služby nie sú v danom období dodržané.

Prípojný bod služby (ďalej tiež „PBS“) je fyzické rozhranie charakterizované funkčnými, mechanickými, elektrickými a protokolovými vlastnosťami, ktoré umožňuje pripojenie koncového zariadenia verejného obstarávateľa.

Porucha je taký stav, ktorý znemožňuje riadne používanie služby v dohodnutom rozsahu a kvalite. Za poruchu sa nepovažuje dočasné prerušenie poskytovania služby počas plánovanej a odsúhlasenej údržby. Akákoľvek údržba, ktorá nebola naplánovaná a odsúhlasená verejným obstarávateľom a ktorá spôsobí nedostupnosť služby, bude považovaná za poruchu. Pokiaľ porucha presahuje z jedného do nasledujúceho kalendárneho mesiaca, považuje sa iba za jednu poruchu a započítava sa do kalendárneho mesiaca, v ktorom vznikla.

Doba opravy (TTR) - je garantovaná doba opravy poruchy vyjadrená v minútach alebo hodinách a počíta sa ako doba medzi nahlásením poruchy (telefonicky, e-mailom, prostredníctvom Helpdesku poskytovateľa) účastníkom operátorovi servisného strediska a okamihom obnovenia prevádzky, potvrdeným účastníkom.

Dostupnosť služby (ďalej tiež „SA“, t.j. Service Availability) je garantovaná dostupnosť služby vyjadrená ako podiel času, počas ktorého môže verejný obstarávateľ používať službu v dohodnutom rozsahu a kvalite, k dĺžke celého sledovaného obdobia. Sledované obdobie je kalendárny mesiac (vyjadrený v minútach) a výsledná hodnota dostupnosti služby sa vyjadruje v percentách so zaokrúhlením na dve desatinné miesta smerom nahor.

SA bude počítaná podľa nasledovného vzorca:

$$SA\ [\%] = \frac{(\Sigma \text{ minút/mesiac} - \Sigma \text{ minút nedostupnosti/mesiac})}{\Sigma \text{ minút/mesiac}} \times 100\%$$

Doba nedostupnosti služby (vyjadrená v minútach) je doba, počas ktorej nemohla byť služba používaná v dohodnutej kvalite.

Dĺžka sledovaného obdobia: 1 mesiac.

Počet dní v mesiaci	Počet minút v mesiaci
28	40320
29	41760
30	43200
31	44640

Kategórie SLA a garantované parametre:

Pre poskytovanie služieb privátnej dátovej siete sú definované nasledovné kategórie SLA a k nim prislúchajúce garantované parametre:

Kategória SLA	Dostupnosť služby SA (v %)	Doba opravy TTR (v hod.)
SLA 1	99,9 %	Do 4 hodín
SLA 2	99,5 %	Do 8 hodín
SLA 3	99,0 %	Do 8 hodín NBD

Poznámka: NBD (Next Business day) znamená nasledujúci pracovný deň.

Sankcie za nedodržanie SLA:

Poskytovateľ sa zaväzuje, že v prípade zavineného porušenia ľubovoľného parametra SLA z jeho strany, poskytne objednávateľovi kredit za obdobie dotknutého kalendárneho mesiaca, vyjadrený v zľave z pravidelného poplatku za predmetnú službu za obdobie dotknutého kalendárneho mesiaca avšak maximálne do výšky 20% z mesačného poplatku, nasledovne:

Za každú aj začatú hodinu výpadku prekračujúcu tolerovanú dobu nedostupnosti služby	**1,00 %** z pravidelného mesačného poplatku za služby
Za každú aj začatú hodinu nad garantovanú dobu opravy poruchy	**0,50 %** z pravidelného mesačného poplatku za služby