Opis predmetu zákazky: Digitálna infraštruktúra škôl - Národný centrálny uzol (NCU)

„Definícia služieb NCU“

Príloha 01b

12.6.2025

Obsah

1 Úvod 4

1.1 Cieľ dokumentu a širší kontext 4

1.2 Obsah dokumentu 4

1.3 Definície a výklad pojmov 5

1.4 Spôsob kategorizácie služieb 7

1.4.1 Kontinuálne (priebežne poskytované) služby 7

1.4.2 Ad hoc služby 7

1.4.3 Pravidelné služby 7

1.5 Proaktívny a reaktívny vznik incidentu 7

1.5.1 Proaktívne meranie 7

1.5.2 Reaktívny vznik incidentu 7

2 Katalóg služieb 8

2.1 Zabezpečovanie základných parametrov a vlastností služieb NCU 8

2.2 Služby sieťovej bezpečnosti 10

2.2.1 Riadenie prístupu používateľov k sieti 11

2.2.2 Zabezpečovanie centrálneho firewall-u 13

2.2.3 Prevádzka služieb centrálneho filtrovania webového obsahu 15

2.2.4 Prevádzka služieb centrálnej aplikačnej podpory 18

2.2.5 Prevádzka služieb centrálnej antivírusovej a antimalvérovej ochrany 21

2.2.6 Prevádzka služieb centrálnej IDS/IPS ochrany 22

2.2.7 Prevádzka služieb centrálnej ochrany proti DDoS 24

2.2.8 RACI matica pre služby sieťovej bezpečnosti 26

2.3 Prevádzka sieťových služieb 28

2.3.1 Prevádzka služieb centrálneho pripojenia do siete Internet 29

2.3.2 Prevádzka služieb prepájania sietí 31

2.3.3 Prevádzka služieb centrálnej správy IP adries 32

2.3.4 Poskytovanie služieb centralizovaného riešenia správy a dohľadu NCU (NCU-CRSD) pre potreby RPŠ 34

2.3.5 Zaisťovanie nastavenia globálnych politík LAN/WLAN sietí 47

2.3.6 Zabezpečovanie prihlasovania používateľov do siete LAN/WLAN 52

2.3.7 Prevádzka služieb vzdialeného pripojenia 54

2.3.8 Prevádzka služieb pripojenia lokalít škôl k NCU a služby CPE 55

2.3.9 Prepájanie na Dátové centrum rezortu školstva 58

2.3.10 RACI matica pre sieťové služby 59

2.4 Služby monitoringu NCU 60

2.4.1 Poskytovanie služieb monitoringu NCU 60

2.4.2 RACI matica pre služby monitoringu NCU 62

2.5 Služby Reportingu 63

2.5.1 Vytváranie reportu dostupnosti a kvality služieb DigiNET 63

2.5.2 Vytváranie správy o výkone Service Desku a plnení SLA 65

2.5.3 Vytváranie správy o stave sieťovej bezpečnosti 67

2.5.4 Vytváranie správy o prevádzke sieťových služieb 68

2.5.5 RACI matica pre služby reportingu NCU 69

2.6 Služby Prevádzkovej podpory, NCU Service Desk a SOC 70

2.6.1 Poskytovanie služieb centrálneho NCU Service Desk pre sieť DigiNET 71

2.6.2 Riešenie incidentov 75

2.6.2.1 Oznamovanie a odsúhlasovanie plánovaných výpadkov 81

2.6.3 Poskytovanie služieb SOC 83

2.6.3.1 Povinnosti používateľa SOC 86

2.6.3.2 Povinnosti RPŠ 86

2.6.3.3 RACI matica zodpovedností SOC 86

2.6.4 Ďalšie služby NCU ServiceDesk 87

2.6.5 Meranie spokojnosti koncového používateľa služieb a náprava 90

2.6.6 Poskytovanie školení 92

2.6.7 RACI matica pre služby podpory, prevádzky 94

2.7 Služby hradené na základe spotrebovaného času – Riadenie zmien 96

2.7.1 Poskytovanie služieb na základe spotrebovaného času 96

3 Prílohy 99

3.1 Zoznam skratiek 99

3.2 Zoznam obrázkov 101

3.3 Zoznam tabuliek 101

# Úvod

## Cieľ dokumentu a širší kontext

Nižšie obsiahnutá špecifikácia definuje požiadavky na telekomunikačné služby poskytované školám v pôsobnosti NCU (Národný Centrálny Uzol) podľa špecifikácie obstarávateľa - **Ministerstvo školstva výskumu vývoja a mládeže SR** (ďalej len: MŠVVaM SR, MŠ, Ministerstvo, rezort, obstarávateľ) pre dosiahnutie požadovaných štandardov IKT (Informačné a komunikačné technológie). Telekomunikačné služby sú poskytované na komponentoch infraštruktúry ktoré tvorí aktívny prvok CPE vybraný a dodávaný centrálne z NCU a v lokalite školy zabezpečuje pripojenie riešenia LAN/WLAN od RPŠ k NCU pomocou WAN konektivity od RPŠ. CPE rovnako slúži na zabezpečenie najvyššej miery kompatibility riešenia LAN/WLAN a služieb RPŠ s NCU. Kompatibilita služieb LAN/WLAN s Národným Centrálnym uzlom je preverená akceptačným testovaním riešenia tak, aby boli spĺňané definované služby RPŠ a NCU so svojimi vlastnosťami a parametrami. Po akceptácii riešenia vykonaním akceptačného testovania a odstránením nedostatkov prechádza riešenie do režimu poskytovania služieb NCU na požadované obdobie. Špecifikácia rovnako upravuje zodpovednosti zainteresovaných strán formou RACI.

Verejný obstarávateľ požaduje na rozhraní prestupu zo siete DigiNET do externých sietí poskytovanie služieb Centrálneho uzla siete DigiNET. Centrálny uzol DigiNET implementuje služby riadenia dátovej prevádzky a zároveň monitoruje akúkoľvek dátovú komunikáciu zo siete DigiNET do externých sietí a z externých sietí do siete DigiNET.

Predmetom dodávky NCU sú telekomunikačné služby podľa tejto špecifikácie - Príloha 1b s ich parametrami a definovanými požiadavkami. NCU dodáva riešenie podľa Prílohy 1a. Zabezpečovanie centrálnych telekomunikačných služieb ako: centrálne služby bezpečnosti, služby prevádzky a údržby, služby centrálneho monitoringu a reportingu, poskytovanie služieb centralizovaného riešenia správy a dohľadu pre RPŠ prostredníctvom služieb NCU (NCU-CRSD), služby centrálneho riadenia kvality a nastavovanie pravidiel v spolupráci s rezortom, poskytovanie školení, testovanie, riadenie dokumentácie, administrácie a konfigurácie CPE, zavádzanie zmien a škálovanie služieb, spolupráca s RPŠ a rezortom pre dosahovanie parametrov služieb, ich dlhodobú funkčnosť spoľahlivosť, jednotnosť a bezpečnosť. Služby NCU primárne podporujú kapacitne dostatočne škálovaný, bezpečný a riadený prístup používateľov k službám v sieti.

## Obsah dokumentu

**Kategorizácia služieb –** Definuje typy poskytovaných služieb podľa spôsobu ich poskytovania:

* kontinuálne,
* pravidelné,
* ad-hoc,

**Katalóg služieb** - Špecifikácia požiadaviek na služby uvádza najmä definíciu poskytovaných služieb NCU metriky merateľných parametrov služieb a ostatné nevyhnutné požiadavky pre zabezpečovanie plynulej prevádzky.

## Definície a výklad pojmov

| **Pojem** | **Vysvetlenie** |
| --- | --- |
| **Udalosť** | Udalosťou rozumieme akúkoľvek zmena stavu infraštruktúry, ktorá môže mať vplyv na poskytovanie služieb. Môže byť plánovaná alebo neplánovaná, avšak nie vždy má priamy negatívny vplyv na služby. Slúži ako signalizácia potenciálnej situácie, ktorú je potrebné sledovať. Udalosť môže byť automaticky/proaktívne detegovaná (napr. výpadok spojenia automatickým monitorovacím systémom), nahlásená oprávnenou osobou používateľa siete alebo manuálne zadaná pracovníkom RPŠ, pracovníkom CU. Požiadavky oprávnenej osoby typu: žiadosť o informáciu, zmenu, sú rovnako evidované ako udalosť. |
| **Ticket** | Je akýkoľvek zaznamenaný záznam o interakcii medzi oprávnenou osobou používateľa a prevádzkovateľom služieb. Slúži ako základný nástroj na sledovanie, správu a riešenie rôznych udalostí. |
| **Problém** | Je podstatná príčina jedného alebo viacerých incidentov. Zatiaľ čo incident predstavuje konkrétny výskyt poruchy, problém je koreňová príčina týchto porúch. |
| **Incident** | Je akákoľvek neplánovaná udalosť, ktorá spôsobuje, alebo má potenciál spôsobiť, prerušenie alebo podstatné zníženie kvality požadovaných služieb, hodnoty parametrov služieb nedosahujú požadovanú úroveň, negatívny vplyv na používateľov pre porušenie definovaných požiadaviek na služby. |
| **Požiadavka na zmenu** | Je formálna žiadosť o autorizáciu na vykonanie zmeny v IT službách, systémoch alebo infraštruktúre. Táto zmena môže byť plánovaná alebo nútená a môže mať vplyv na kvalitu, dostupnosť alebo zabezpečovanie služieb. |
| **Požiadavka o informáciu** | Je formálna žiadosť na poskytnutie informácie o poskytovaných službách, ich nastavení parametrov služieb, atď. |
| **RPŠ – Service Desk** | Je súbor organizačných, technických a personálnych prostriedkov pre zabezpečenie poskytovania služieb podpory prevádzky a údržby riešenia v pôsobnosti RPŠ. |
| **NCU – Service Desk** | Je súbor organizačných, technických a personálnych prostriedkov pre zabezpečenie poskytovania služieb podpory prevádzky a údržby riešenia v pôsobnosti CU. Znamená aj súbor technických, organizačných a personálnych prostriedkov pre zabezpečenie poskytovania služieb kontaktu a podpory prostredníctvom hlasovej komunikácie s využitím verejnej telefónnej siete, pomocou internetového portálu a mailovej adresy. |
| **Centrálny ticketing portál (CTP)** | Centrálny portál zriadený a prevádzkovaný dodávateľom služieb CU. Portál slúži ako základný centrálny nástroj na sledovanie, správu a riešenie ticketov, reportovania kvality. Portál je dostupný cez štandardné webové rozhranie pre RPŠ agentov, CU agentov, ŠKOLY a rezort. |
| **Severity** | Definuje závažnosť nesúladu služby a vplyv nesúladu služby na používateľov. |
| **Pripájaný bod** | Je označenie pre každé miesto, ktoré poskytuje možnosť fyzického pripojenia do siete používateľa – RJ.45 v učebni a WiFi AP. |
| **Nesúlad služby** | V prípade že parametre služby nedosahuje požadované hodnoty alebo služba nie je v súlade s definíciou požiadaviek na službu. |
| **Čas nesúladu ()** | Predstavuje celkový čas trvania nesúladu služby v mesiaci počas prevádzkovej doby služby. Čas nesúladu služby sa počíta od vzniku udalosti/nahlásenia problému oprávnenou osobou používateľa, od času odhalenia nedostupnosti poskytovateľom služieb RPŠ, poskytovateľom služieb CU (podľa toho čo nastane skôr). Čas nesúladu končí obnovením súladu služby. Čas kedy hodnoty merateľných parametrov a definícia požiadaviek na službu neboli dodržané z:  1/príčin na strane objednávateľa alebo,  2/z dôvodu plánovaných prác ktoré sú v súlade s požiadavkami,  nebude započítavaný do času nedostupnosti služby. Časy sa počítajú na celé minúty. |
| **Súlad služby** | Služba spĺňa hodnoty merateľných parametrov a spĺňa definíciu požiadaviek na službu |
| **Prevádzkový čas služby ()** | Predstavuje celkový čas prevádzky služby v mesiaci v ktorom sa vyžaduje garancia dosahovania hodnôt parametrov služby a definovaných požiadaviek na službu. Časy sa počítajú na celé minúty. |
| **Busy Hour** | Predstavuje rozpätie hlavných prevádzkových hodín a s ním súvisiace vyťaženie komponentov NCU, vyhodnocované typicky mesačne, či meraná vyťaženosť prekračuje počas celej meranej periódy hodnotu 80% kapacity služieb. |
| **Čas opravy nesúladu (TTR)** | Predstavuje celkový čas od vzniku udalosti o nesúlade služby až po nápravu služby. Časy sa počítajú na celé minúty. |
| **Požadovaný čas opravy nesúladu (RTTR)** | Predstavuje požadovaný celkový čas od vzniku udalosti o nesúlade služby až po nápravu služby. Časy sa počítajú na celé minúty. Požadované časy sú definované podľa severity nesúladu. |
| **Dostupnosť služby** | Dostupnosť sa vyjadrí v % zaokrúhlene na dve desatinné miesta. |
| **Prevádzková doba poskytovania služieb** | Je časové obdobie v ktorom sa vyžaduje garancia dosahovania hodnôt parametrov služby a definovaných požiadaviek na službu |
| **Chrbticová sieť LAN** | Je sieť v lokalite školy medzi CPE a akýmkoľvek switchom, medzi switchmi |
| **Riešiteľ incidentu** | Rola obsadená aktuálne zodpovednou stranou za pridelený ticket. |
| **RACI matica** | Predstavuje rozdelenie zodpovedností pri plnení úloh. RACI matica rozdeľuje zodpovednosti medzi Školu, RPŠ, CU a MŠVVaM pričom prvky RACI matice predstavujú:   * **R** (Responsible) – je zodpovedný za danú činnosť * **A** (Accountable) - je zodpovedný za výsledok a overenie danej činnosti * **C** (Consulted) – je konzultovaný o činnosti * **I** (Informed) - je informovaný o výsledku, priebehu činnosti |

Tabuľka 1: Zoznam pojmov

## Spôsob kategorizácie služieb

### Kontinuálne (priebežne poskytované) služby

Kontinuálne služby sú také, ktoré dodávateľ poskytuje súvisle, počas celého trvania zmluvy. Objednávateľ uhrádza za tieto služby fixný poplatok pre dané obdobie (s možným znížením poplatku z dôvodu penalizácie).

### Ad hoc služby

Ad-hoc služby sú také, ktoré sa vykonávajú na vyžiadanie resp. sú spustené automaticky z dôvodu zaznamenania udalosti v sieti. Typicky ide o služby operačnej prevádzky riešenia, riešenia incidentov a požiadaviek. Takouto službou je aj zvýšená prevádzková podpora pri mimoriadnych situáciách.

### Pravidelné služby

Pravidelnú služby sú také, ktoré sú vykonávané na pravidelnej báze. Typicky služby generovania reportov, služby údržby (SW upgrade), reportovanie kvality vykonávaných služieb a vyhodnocovanie dostupnosti za uplynulé obdobie.

## Proaktívny a reaktívny vznik incidentu

V opise služieb nižšie je definovaný vznik incidentu na základe proaktívneho merania alebo reaktívne nahlásením.

### Proaktívne meranie

Proaktívne meranie predstavuje priebežné sledovanie stavu merateľných parametrov a požiadaviek na službu. Prebieha kontinuálne (v definovaných intervaloch) a automatizovane. Pri zistení nesúladu meraného parametra s dohodnutou úrovňou parametrov je automaticky otvorený ticket.

### Reaktívny vznik incidentu

Reaktívny vznik incidentu je na základe nahlásenej udalosti pri podozrení nesúladu služby s požadovanými parametrami.

Reaktívne riešenie incidentu je obvykle iniciované na základe podozrenia školy, prípadne aj NCU alebo RPŠ.

Priebeh riešenia je nasledovný:

1. Nahlásenie udalosti, evidencia vo forme nového ticketu.
2. Klasifikácia na úrovni NCU.
3. Začatie riešenia do 60 minút počas prevádzkovej doby na úrovni NCU alebo RPŠ (podľa toho komu bol pridelený).

# Katalóg služieb

Katalóg služieb je detailný popis požadovaných služieb, pričom sú tieto služby rozdelené do nasledujúcich základných kategórii:

* Služby sieťovej bezpečnosti
* Služby sieťového pripojenia
* Služby monitoringu
* Služby reportingu
* Služby zabezpečovania centralizovaného riešenia správy a dohľadu pre RPŠ prostredníctvom služieb NCU (NCU-CRSD)
* Služby prevádzkovej podpory, NCU Service Desk a SOC
* Služby hradené na základu spotrebovaného času -Riadenie zmien

## Zabezpečovanie základných parametrov a vlastností služieb NCU

Verejný obstarávateľ požaduje nasledovné základné vlastnosti Národného Centrálneho uzla počas prevádzkovej doby poskytovania služieb, počas ktorej poskytovateľ služieb NCU garantuje kvalitu parametrov služieb:

* vysoko dostupné a škálovateľné riešenie celého systému Národného Centrálneho uzla,
* služby NCU poskytované v georedundantnej konfigurácii so zabezpečovaním loadbalancing-u,
* umiestnenie Centrálneho uzla DigiNET nesmie byť v žiadnej lokalite verejného obstarávateľa,
* dátové pripojenie NCU do siete Internet na minimálnej úrovni 100 Gbps, a obstarávateľ pristupuje na možnosť postupného rozšírenia až na 200 a400 Gbps pri dosahovaní 80% aktuálnej kapacity v Busy Hour, z dôvodu aby poskytovateľ NCU nebol povinný zriaďovať služby NCU v plnej kapacite od prvého dňa pre začatie poskytovania služieb, avšak je povinný spĺňať požiadavky na služby a ich parametre.
* minimálnu dostupnosť služieb NCU DigiNET na úrovni 99,9%,
* celková priepustnosť služieb NCU DigiNET na úrovni 99,9%.

Vzhľadom na požadovanú funkcionalitu a priepustnosť pri využívaní všetkých požadovaných služieb, verejný obstarávateľ požaduje použiť dostatočne robustný hardvér a konfiguráciu v jadre NCU, aby sa počas prevádzky nestali práve komponenty Národného Centrálneho uzla DigiNET úzkym hrdlom celého riešenia. Poskytovateľ služieb NCU je povinný zabezpečovať rozširovanie maximálnych kapacít komponentov NCU podľa požiadaviek definovaných v tejto kapitole. Poskytovateľ služieb NCU je zároveň povinný začať plánovať rozširovanie jadra NCU a CPE komponentov pri dosiahnutí 80% maximálnej kapacity v Busy Hour.

V prípade potreby rozširovania rozsahu požadovaných služieb nad rámec opisu predmetu zákazky, napríklad nad kapacitné požiadavky tohto opisu predmetu zákazky, potreby zriadenia nových služieb, je poskytovateľ povinný iniciovať požiadavku na zmenové konanie voči verejnému obstarávateľovi pre potreby rozširovania rozsahu poskytovaných služieb dostatočne s predstihom. V prípade priepustnosti, kapacity pri dosiahnutí 80% aktuálnej kapacity. Obstarávateľ očakáva že poskytovateľ NCU zriaďuje služby centrálneho uzla v súlade s rozsahom predpokladaného počtu Pripájaných bodov, WAN lokalít, kapacít, priepustností a ostatných požadovaných služieb a ich parametrov.

Verejný obstarávateľ požaduje, aby prevádzkovateľ NCU vykonával pravidelné aktualizácie a aplikáciu bezpečnostných záplat všetkých prvkov siete NCU a mal zabezpečenú podporu výrobcom pre SW a HW podporu zariadení. Poskytovateľ NCU zabezpečí, že všetky zakúpené sieťové prvky CPE budú dodané s platnými softvérovými licenciami a zahrnutou technickou SW aj HW podporou od výrobcu na obdobie trvania zmluvy. Poskytovateľ NCU dodá všetky licenčné kľúče a doklady k CPE Obstarávateľovi s ktorým sa dohodne na forme a spôsobe odovzdania.

## Služby sieťovej bezpečnosti

Sieť DigiNET primárne zabezpečuje kapacitne dostatočne škálovaný, bezpečný a riadený prístup k službám v sieti, ktorý umožní používateľom s využitím najmodernejších technologických riešení flexibilne pristupovať k rôznym digitálnym zdrojom a nástrojom vo výchovno-vzdelávacom procese. Súčasťou služieb DigiNET ako prístupu k digitálnym službám je taktiež ich využitie pre riadenie digitálnej bezpečnosti na školách.

Súčasne so zavádzaním služieb siete DigiNET je potrebné riešiť aj riadenie prístupu používateľov do školských sietí LAN/WLAN a tým aj riadenie prístupu a využívanie digitálneho obsahu z externých zdrojov (obsah tretích strán vhodný pre výchovno-vzdelávací proces), kde je potrebné jeho overovanie, špecifikácia rozsahu a možnosti jeho využívania a certifikácia vhodnosti pre výchovno-vzdelávací proces a to aj vzhľadom na aktuálne bezpečnostné a vzdelávacie politiky rezortu.

Verejný obstarávateľ požaduje, aby smerovanie dátovej komunikácie medzi sieťou DigiNET a externými sieťami (napríklad sieťou Internet) prechádzalo službou centrálneho firewall systému. S ohľadom na veľký počet pripájaných lokalít ako aj očakávané rýchlosti pripojenia je mimoriadne dôležité, aby konfigurácia NCU siete DigiNET bola dostatočne dimenzovaná nielen na úvodné potreby projektu, ale aj s možnosťou rozširovania počas obdobia trvania prevádzky služieb.

Verejný obstarávateľ požaduje, v navrhovanom systéme možnosť overovania prístupov používateľov k sieti na základe MS365 mena a hesla prideleného používateľovi v tenante školy, ku ktorej pristupuje cez zariadenie školy alebo cez svoje vlastné zariadenie, do ktorého sa úspešne prihlásil svojim MS365 účtom.

Verejný obstarávateľ požaduje, v navrhnutom systéme možnosť nastavenia filtrovania obsahu a blokovania nevhodného obsahu.

Verejný obstarávateľ požaduje, aby komunikácia z Internetu prechádzala cez IDS/IPS systém (Intrusion Detection System / Intrusion Prevention System).

Na reguláciu šírky prenosového pásma pre menej dôležité aplikácie nesúvisiace s procesom výučby v školách musia byť aplikovateľné metódy regulácie šírky pásma (traffic shaping). Navrhnuté riešenie musí umožniť implementovať dátové profily, ktoré budú priradené jednotlivým školám na základe požiadaviek Verejného obstarávateľa (nastavenie vykoná Úspešný uchádzač). Tieto profily musí byť možné priraďovať aj na základe časového princípu s granulárnou škálovateľnosťou nastavenia parametrov.

V prípade že v pripájanej lokalite k službám NCU nie sú zabezpečovanú služby RPŠ (lokalita bez RPŠ), môže obstarávateľ objednať u poskytovateľa NCU pre takúto lokalitu zabezpečovanie nasledovných centrálnych služieb sieťovej bezpečnosti, pričom poskytovateľ NCU bude využívať existujúcu konektivitu používateľa služieb:

* Zabezpečovanie centrálneho firewall-u
* Prevádzka služieb centrálneho filtrovania webového obsahu
* Prevádzka služieb centrálnej aplikačnej podpory
* Prevádzka služieb centrálnej antivírusovej a antimalvérovej ochrany
* Prevádzka služieb centrálnej IDS/IPS ochrany
* Prevádzka služieb centrálnej ochrany proti DDoS

Takto poskytované služby, ktoré sú výhradne v rozsahu zodpovednosti poskytovateľa služieb NCU, musia rovnako spĺňať požiadavky na služby a ich parametre podľa opisu predmetu zákazky.

### Riadenie prístupu používateľov k sieti

| **Riadenie prístupu používateľov k sieti - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Riadenie prístupu používateľov k sieti |
| **Kategória** | | | | Služby sieťovej bezpečnosti |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Táto služba zabezpečuje centrálne riadenie prístupov používateľov k službám LAN/WLAN na základe Microsoft Entra ID alebo centrálneho registra identít žiakov a pedagógov škôl. |
| **Riadenie prístupu používateľov k sieti - detailná definícia požiadaviek na službu** | | | | |
| Služba zabezpečuje:   * riadenie prístupov k službám siete na úrovni používateľa podľa pridelenej role, * oprávneným používateľom digitálnych služieb školy, použitím inštitucionálnych (inventárnych) digitálnych zariadení v správe školy, cez ktoré sú využívané služby DigiNET, * oprávneným používateľom digitálnych služieb školy, použitím digitálnych zariadení vo vlastníctve používateľa, cez ktoré bude využívať služby DigiNET, * centrálne riadenie prístupov k službám a digitálnemu obsahu tretích strán (umožní jednoduché, bezpečné a riadené prepojenie so zdrojmi tretích strán) a obojstrannú garanciu riadeného prístupu (bude možné garantovať oprávnenosť pristupujúceho používateľa cez sieť DigiNET, ako aj bezpečnosť a relevantnosť údajov od tretej strany), * realizovať prepájanie existujúcich registrov používateľov, čo zjednoduší prístup k údajom pre jej používateľov, ale aj proces kontroly prístupu zo strany externého poskytovateľa služby alebo obsahu, * centralizované riadenie a možnosti prepojenia a integrácie v rámci rezortných a medzirezortných IS a riadenie základnej digitálnej bezpečnosti na školách,   Obstarávateľ uvažuje zabezpečovať tieto služby spôsobom, aby bolo v budúcnosti umožnené prepojiť overovanie s budúcim centrálnym registrom identít žiakov a pedagógov škôl spolu s pridelenými rolami. Použitie centrálneho registra môže byť upresnené počas implementácie projektu.  Používateľom sú prideľované nasledujúce role, podľa ktorých bude následne aplikovaný profil používateľa s rôznou úrovňou nastavenia filtrovania webového obsahu, aplikačnej kontroly a povolením prístupu do segmentov LAN a WLAN siete:   * žiak prvého stupňa základnej školy, * žiak druhého stupňa základnej školy alebo 1.-4. ročníka osemročného gymnázia, * žiak strednej školy alebo 5.-8. ročníka osemročného gymnázia, * pedagogický a nepedagogický personál.   Centrálne zabezpečovanie služieb riadenia prístupov používateľov k službám LAN/WLAN na základe MS365 účtov pedagógov a žiakov zriadených v tenante danej školy. Služba počíta s centrálnym overovaním prístupov voči MS tenantu školy, dimenziou kapacity tak, aby komfortne obslúžilo predpokladaný počet používateľov počas Busy Hour. Overovanie na základe MS365 prístupových údajov používateľa vyžaduje jeho overenie a riadenie prístupu používateľa zo zariadení:   * A/ v správe školy, určené na výučbu pre žiakov a smerované do samostatného segmentu LAN/WLAN určeného pre tento typ klientov, * B/ v správe školy, určené pre pedagógov a ostatných pracovníkov školy a smerované do samostatného segmentu LAN/WLAN určeného pre tento typ klientov, * C/ vo vlastníctve žiakov, určené na podporu vyučovacieho procesu a smerované do samostatného segmentu LAN/WLAN určeného pre tento typ klientov, * D/samostatné „periférne“ zariadenia v správe školy ako napríklad: tlačiareň, interaktívny monitor atď., smerované do samostatného segmentu LAN/WLAN určeného pre tento typ klientov.   Centrálne riadenie prístupu používateľov implementované v rámci služieb Centrálneho uzla DigiNET je jedným zo základných predpokladov pre nasadenie akýchkoľvek centrálne manažovaných služieb v sieti DigiNET.  V rámci definovanej stratégie pre informačné systémy rezortu, ktoré sú určené nielen pre interné potreby, ale najmä pre potreby používateľov inštitúcií, ktoré sú organizačne alebo funkčne, priamo alebo nepriamo previazané s MŠVVaM SR, je primárnym cieľom vytvorenie jednotného systému pre AAA mechanizmy a služby.  NCU využije informácie zo systému Microsoft Entra ID alebo centrálneho registra identít žiakov a pedagógov škôl, ktorý bude umožňovať jednotný prístup k všetkým zdrojom údajov, ako aj zabezpečí jednotnú autentifikačnú a autorizačnú platformu pre integrujúce sa služby a informačné systémy. Takto bude zabezpečený jednotný prístup a jednoznačná autentifikácia používateľov vo všetkých integrovaných IS a službách s nimi súvisiacich prostredníctvom AAA služby.  Použitie Microsoft Entra môže umožniť využívanie SSO funkcionalít (Single Sign On) prostredníctvom centrálneho manažmentu identít a centrálneho riadenia bezpečnosti prístupov k zdrojom elektronického obsahu, ak je rovnaký manažment identít používaný aj pri overovaní používateľov systému Windows na jednotlivých lokalitách.  Poskytovateľ služieb NCU úzko spolupracuje s poskytovateľmi RPŠ pre zabezpečenie E2E funkcionality. | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | Škola |
| **Iné zainteresované strany** | | | RPŠ |
| **Prevádzková doba** | | | | pracovné dni 6:00 – 18:00 |
| **Minimálna Dostupnosť služby** | | | | 99,9% - Na základe základných parametrov a vlastností služieb NCU |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | podľa služby: Riešenie incidentov |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Čas potrebný na pripojenie WiFi klientov s komponentami v pôsobnosti NCU |
| **Definícia** | | Maximálny čas medzi spustením pripojenia klienta k zvolenému SSID až po schopnosť komunikovať do siete internet, musí byť na prvkoch v pôsobnosti NCU zabezpečený tak aby E2E parameter v celej DigiNET sieti spĺňala požadovanú hodnotu 10 000 ms |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | ms |
| **Minimum** | Nie je obmedzené |
| **Maximum** | 15000 |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých škôl |

Tabuľka 2: Prevádzka služieb riadenia prístupu používateľov k sieti

### Zabezpečovanie centrálneho firewall-u

| **Centrálny firewall - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Služby zabezpečovania centrálneho firewall-u |
| **Kategória** | | | | Služby sieťovej bezpečnosti |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Služby Centrálneho firewall-u sú významným zabezpečovacím prvkom, ktorý má za úlohu chrániť sieť DigiNET pred externými aj internými bezpečnostnými rizikami. V riešení centrálneho firewall systému sú očakávané okrem základných firewall funkcionalít aj funkcie kombinovaného zabezpečenia s využitím funkcionalít IPS/IDS, web content filtering a aplikačnej kontroly. |
| **Centrálny firewall - detailná definícia požiadaviek na službu** | | | | |
| V rámci zabezpečovania služieb Národného Centrálneho uzla verejný obstarávateľ očakáva, že vybraný dodávateľ poskytuje prevádzku komplexnej služby súvisiacej so zabezpečením centrálneho firewallingu, s nasledujúcimi minimálnymi požiadavkami:   * priepustnosť firewallu v paketoch za sekundu: 1500 Mpps * počet paralelných TCP spojení: min. 175 miliónov pri kapacite 100 Gbps * počet paralelných TCP spojení: min. 350 miliónov pri kapacite 200 Gbps * počet paralelných TCP spojení: min. 700 miliónov pri kapacite 400 Gbps * počet nových TCP spojení za sekundu: min. 1,5 milióna spojení/s pri kapacite 100 Gbps * počet nových TCP spojení za sekundu: min. 3 milióny spojení/s pri kapacite 200 Gbps * počet nových TCP spojení za sekundu: min. 6 miliónov spojení/s pri kapacite 400 Gbps * počet firewall pravidiel: min. 175.000 pravidiel * latencia centrálneho firewallu pri veľkosti UDP paketov 64 byte: max. 8 μs * podpora site-to-site IPSec * podpora SSL inšpekcie * identifikácia aplikácie bez ohľadu na port, kryptovanie (SSL alebo SSH) alebo využitie evazívnych metód a techník * využitie aplikačnej vrstvy a nie portu ako základu pre výber správnej bezpečnostnej politiky a aplikáciu bezpečnostných opatrení (povoliť, zakázať, povoliť v časovom okne, limitovať šírku pásma alebo filtrovať nepovolený obsah) * kategorizácia neidentifikovaných aplikácií * forenznú analýzu * blokovanie na základe databáz známych hrozieb, vrátane expoitov, malware a spyware na všetkých portoch a bez ohľadu na spôsob alebo metódu prieniku * limitovanie a obmedzovanie neautorizovaného prenosu súborov alebo iných typov dát vrátane HTTP a HTTPS prenosov webového obsahu * identifikácia neznámych typov malware na základe aplikácie behaviorálnych analytických nástrojov * centrálny a škálovateľný IPv4 PAT (1:N) pre preklad privátnych IPv4 adries na verejné adresy pre užívateľov siete DigiNET * centrálny a škálovateľný IPv4 NAT (1:1) pre sieť DigiNET (požiadavka na minimálne 2 verejné IPv4 adresy pre každú lokalitu pripojenú do siete DigiNET) pre publikovanie zdrojov zo školských DMZ | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | Škola, NCU |
| **Iné zainteresované strany** | | | RPŠ |
| **Prevádzková doba** | | | | pracovné dni 6:00 – 18:00 |
| **Minimálna Dostupnosť služby** | | | | 99,9% - na základe základných parametrov a vlastností služieb NCU |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa služby: Riešenie incidentov |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Priepustnosť |
| **Definícia** | | Celková priepustnosť dátovej prevádzky siete DigiNET podľa definície služby |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne – bude sa merať performance |
| **Požadovaná hodnota** | **Jednotka** | % |
| **Minimum** | 99,9 - na základe základných parametrov a vlastností služieb NCU |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých škôl |

Tabuľka 3: Prevádzka služieb centrálneho firewallu – definícia požiadaviek na službu

### Prevádzka služieb centrálneho filtrovania webového obsahu

| **Centrálne filtrovanie webového obsahu - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Prevádzka služieb centrálneho filtrovania webového obsahu |
| **Kategória** | | | | Služby sieťovej bezpečnosti |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Služby filtrovania webového obsahu sú určené na filtrovanie internetovej komunikácie pre sieť DigiNET a pripojené školy. Tento systém umožní administrátorom nastaviť pravidlá a obmedzenia týkajúce sa prístupu k určitým typom webového obsahu na základe profilu priradenému koncovému používateľovi. Filtrovanie prebieha pomocou kategórií ako sú napríklad sociálne siete, hazardné stránky alebo nevhodný obsah, respektíve explicitným definovaním povolených a zakázaných lokalít (allowlist a blocklist). Týmto spôsobom sa zvyšuje bezpečnosť siete a znižuje riziko, že žiaci budú vystavení potenciálne škodlivým alebo nevhodným materiálom.  Filtrovanie webového obsahu je potrebné realizovať centrálne pre zachovanie integrity a nediskriminačného aspektu poskytovania služieb. Filtrovanie obsahu je potrebné realizovať primárne pre zdroje obsahu umiestnené mimo siete DigiNET a to najmä v sieti Internet. |
| **Centrálne filtrovanie webového obsahu - detailná definícia požiadaviek na službu** | | | | |
| V rámci zabezpečovania služieb Centrálneho uzla verejný obstarávateľ požaduje, že vybraný dodávateľ poskytuje prevádzku komplexnej služby súvisiacej so zabezpečením filtrovania webového obsahu, a to najmä:   * možnosť explicitne povoliť web stránky / zdroje elektronického obsahu, ktoré sú dôveryhodné a tie ponechať bez inšpekcie * možnosť vytvoriť zoznamy s web stránkami alebo URL / URI, alebo špeciálnych výrazov a kľúčových slov, ktoré budú podliehať inšpekcii * možnosť použiť preddefinované kategórie filtrov obsahu a podkategórie a tie podľa určenia blokovať alebo povoľovať * možnosť použiť verejne dostupné block listy a podľa nich blokovať alebo povoľovať obsah * možnosť regulovať šírku prenosového pásma pre obsah nesúvisiaci s procesom výučby * možnosť aktualizovať databázu kategórií a signatúr systému filtrovania minimálne 4-krát denne * možnosť pridať do databázy kategórií a signatúr nový záznam   Globálne nastavenie filtrovania obsahu musí byť realizované spôsobom blocklist prístupu k filtrovaniu, teda neznámy, nevhodný, nový a nedôveryhodný obsah je zakázaný na základe kategórií a dodaných blocklist URL na základe požiadaviek MŠVVaM SR, podľa uvedených kritérií:   * podľa času (vyučovací čas vs. ostatný čas), * podľa WiFi SSID alebo LAN pripojeného používateľa, * podľa skupín užívateľov (vek, žiak, učiteľ, návštevník), * podľa zdrojovej IP adresy alebo rozsahu adries.   Zároveň je nevyhnutné, aby bolo možné blokovanie granulárne definovať pre konkrétnu skupinu používateľov alebo podmienok podľa rovnakých kritérií.  Známy, dôveryhodný obsah by mal byť štandardne povolený. Takto nastavený proces filtrovania musí byť možné škálovať a individuálne nastavovať podľa bezpečnostných nastavení skupín z identity servera až do úrovne konkrétneho prihláseného používateľa.  **Kategórie pre služby filtrovania webového obsahu:**   |  |  | | --- | --- | | **Hlavné kategórie** | **Podkategórie (príklady)** | | Obsah určený pre dospelých | Alkohol, drogy, gambling, pornografia a nahota, spodné prádlo, tabakové výrobky, zbrane, zoznamky. | | Obsah náročný na kapacitu pripojenia | Dátové úložiská, internetové TV a rádiá, peer-to-peer zdieľanie súborov, streaming, úložiská freeware a software, zdieľanie súborov. | | Právne postihnuteľný obsah | Diskriminácia skupín obyvateľstva, ilegálny obsah, násilie, neetický obsah, obchádzanie sieťových proxy politík, plagiátorstvo, propagácia extrémizmu a extrémistických skupín, zneužívanie drog, zneužívanie maloletých. | | IT bezpečnosť | Dynamické DNS, nové domény, phishing, spam, webstránky a lokality so škodlivým obsahom. | | Všeobecný obsah | Aukčné servery, automobilizmus, bankovníctvo, cestovanie, financie, folklór, hosting, hry, instantné správy, IT, médiá a spravodajstvo, náboženstvo, nákupy, online stretnutia s možnosťou zdieľania obsahu kamery a obrazovky, organizácie, osobné stránky a blogy, ozbrojené zložky, politické organizácie, reality, reklama, stravovanie, sociálne siete, šport, vyhľadávače, vzdelávanie, vzdialený prístup, webové aplikácie, webový chat, webový email, zábava, zdravie a osobná starostlivosť, zdravotníctvo, životný štýl. | | Nehodnotený obsah | Webové lokality, ktoré doteraz neboli ohodnotené a kategorizované. | | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | Škola, NCU, RPŠ |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | pracovné dni 6:00 – 18:00 |
| **Minimálna Dostupnosť služby** | | | | 99,9% - na základe základných parametrov a vlastností služieb NCU |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Funkčné filtrovanie webového obsahu |
| **Definícia** | | Filtrovanie obsahu musí spĺňať všetky požiadavky na službu a musí byť plne funkčné |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne |
| **Požadovaná hodnota** | **Jednotka** | boolean |
| **Minimum** | ÁNO v súlade |
| **Maximum** | N/A |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých škôl |
| **Metrika 2** | **Názov:** | | Frekvencia aktualizácií DB kategórií a signatúr |
| **Definícia** | | Frekvencia s akou sa aktualizujú DB kategórií a signatúr |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne |
| **Požadovaná hodnota** | **Jednotka** | Frekvencia denne |
| **Minimum** | 4 |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých škôl |

Tabuľka 4: Centrálne filtrovanie webového obsahu - detailná definícia požiadaviek na službu

### Prevádzka služieb centrálnej aplikačnej podpory

| **Prevádzka služieb centrálnej aplikačnej podpory - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Prevádzka služieb centrálnej aplikačnej podpory |
| **Kategória** | | | | Služby sieťovej bezpečnosti |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Aplikačná kontrola aplikácií skúma sieťovú prevádzku generovanú aplikáciami. Jednotlivé aplikácie je možné povoľovať, blokovať alebo obmedziť prístup na určitú dobu. Umožňuje granulárne nastaviť pravidlá založené na type aplikácie pomocou kategórií aplikácií. Optimalizuje využitie šírky pásma v sieti tým, že uprednostňuje alebo blokuje prevádzku na základe kategórie aplikácií alebo konkrétnej aplikácie |
| **Prevádzka služieb centrálnej aplikačnej podpory - detailná definícia požiadaviek na službu** | | | | |
| Filtrovanie aplikácií je potrebné realizovať primárne pre zdroje obsahu umiestnené mimo siete DigiNET a to najmä v sieti Internet.  Požadované funkcie aplikačnej kontroly:  Globálne nastavenie filtrovania obsahu je realizované spôsobom blocklist prístupu k aplikáciám, teda neznáme aplikácie a aplikácie predstavujúce bezpečnostné riziko by mali byť zakázané na základe požiadaviek MŠVVaM SR, podľa:   * času (vyučovací čas, ostatný čas), * WiFi SSID/LAN, * skupín používateľov (vek, žiak, učiteľ, návštevník).   Známe a dôveryhodné aplikácie by mali byť štandardne povolené (ako napr. Office 365, antivírusové SW, Edupage, Windows update, atď.). Takto nastavený proces filtrovania musí byť možné škálovať a individuálne nastavovať podľa bezpečnostných nastavení skupín zo servera identít až do úrovne konkrétneho používateľa.  V rámci zabezpečovania služieb Centrálneho uzla verejný obstarávateľ očakáva, že vybraný dodávateľ poskytuje prevádzku komplexnej služby súvisiacej so zabezpečením centrálnej aplikačnej kontroly, a to najmä:   * možnosť explicitne povoliť kategórie aplikácií a ich komunikáciu na zdroje elektronického obsahu, ktoré sú dôveryhodné a tie ponechať bez inšpekcie * možnosť explicitne zakázať kategórie aplikácií a ich komunikáciu na zdroje elektronického obsahu, ktoré sú nedôveryhodné alebo nežiadané pre komunikáciu siete DigiNET do Internetu * vytváranie profilov nastavení aplikačnej kontroly na základe požiadaviek MŠVVaM SR a uplatniť ich až do úrovne konkrétneho používateľa * možnosť regulovať šírku prenosového pásma pre aplikácie nesúvisiace s procesom výučby * možnosť aktualizovať databázu kategórií a signatúr systému aplikačnej kontroly minimálne 1-krát týždenne * možnosť pridať do databázy kategórií a signatúr nový záznam   **Kategórie pre služby Centrálnej aplikačnej kontroly**   |  |  | | --- | --- | | **Kategória** | **Popis kategórie** | | Botnet | Škodlivé aplikácie, ktoré sa používajú na distribúciu škodlivého softvéru, útokov DDoS a iných škodlivých účelov | | Podnikanie | Aplikácie súvisiace s podnikaním, ako sú napr. office balíky | | Cloudové služby | Cloud aplikácie | | Kolaboračné nástroje | Aplikácie používané na zdieľanie pracovnej plochy, vzdialené stretnutia a inú spoluprácu | | Emailové služby | Aplikácie na odosielanie / prijímanie a spracovanie e-mailov | | Zdieľanie súborov | Aplikácie používané na zdieľanie súborov | | Hry | Hry | | Všeobecné | Nástroje všeobecného záujmu, aplikácie | | IM | Instant Messaging aplikácie | | Priemysel | Priemyselné aplikácie | | Mobilné služby | Komunikácia mobilných aplikácií | | Sieťové služby | Aplikácie používané pre sieťové služby a komunikáciu | | P2P aplikácie | Peer-to-Peer aplikácie používané na zdieľanie súborov | | Proxy aplikácie | Proxy a VPN aplikácie | | Vzdialený prístup | Aplikácie na vzdialený prístup na prenos súborov alebo na diaľkové ovládanie | | Sociálne médiá | Online aplikácie sociálnych médií | | Špeciálne aplikácie | Špeciálne aplikácie | | Úložiská súborov | Aplikácie na online ukladanie súborov a fotografií | | Aktualizácie | Komunikácia na aktualizáciu serverov pre rôzne aplikácie | | Video/Audio | Zdieľanie videa, streamovanie a vysielacie aplikácie | | VoIP | Aplikácie Voice over IP | | Web – ostatné | Webový prehliadač a ďalšie nástroje pre prehľadávanie webu | | Webové klientske aplikácie | Klientske aplikácie založených na protokole HTTP | | Neznáme | Ostatné aplikácie, ktoré zatiaľ nespadajú do žiadnej inej kategórie aplikácií | | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | NCU, RPŠ, Škola |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | pracovné dni 6:00 – 18:00 |
| **Minimálna Dostupnosť služby** | | | | 99,9% - na základe základných parametrov a vlastností služieb NCU |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Funkčné filtrovanie nežiadúcich aplikácií |
| **Definícia** | | Filtrovanie nežiadúcich aplikácií musí spĺňať všetky požiadavky na službu a musí byť plne funkčné |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne |
| **Požadovaná hodnota** | **Jednotka** | boolean |
| **Minimum** | ÁNO v súlade |
| **Maximum** | N/A |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých škôl |
| **Metrika 2** | **Názov:** | | Frekvencia aktualizácií DB kategórií a signatúr |
| **Definícia** | | Frekvencia s akou sa aktualizujú DB kategórií a signatúr |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne |
| **Požadovaná hodnota** | **Jednotka** | Frekvencia týždenne |
| **Minimum** | 1 |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých škôl |

Tabuľka 5: Prevádzka služieb centrálnej aplikačnej podpory - detailná definícia požiadaviek na službu

### Prevádzka služieb centrálnej antivírusovej a antimalvérovej ochrany

| **Prevádzka služieb centrálnej antivírusovej a antimalvérovej ochrany - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Prevádzka služieb centrálnej antivírusovej a antimalvérovej ochrany |
| **Kategória** | | | | Služby sieťovej bezpečnosti |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Centrálna antivírusová a antimalvérová ochrana pre sieť DigiNET je kľúčovým prvkom v boji proti škodlivému softvéru a kybernetickým hrozbám. Tento ochranný mechanizmus sa nachádza na perimetri siete ako funkcionalita bezpečnostnej brány (firewall) a poskytuje prvú líniu obrany proti rôznym typom malware, vrátane vírusov, trojanov, ransomvéru a spyware. |
| **Prevádzka služieb centrálnej antivírusovej a antimalvérovej ochrany - detailná definícia požiadaviek na službu** | | | | |
| V rámci zabezpečovania služieb Centrálneho uzla DigiNET verejný obstarávateľ očakáva, že vybraný dodávateľ poskytuje prevádzku komplexných služieb s súvislosti so zabezpečením antivírusovej a antimalvérovej ochrany, a to najmä:   * Aktualizácie definícií: Pravidelné aktualizácie definícií vírusov a malwaru sú dôležité pre včasnú identifikáciu nových a upravených variantov škodlivého softvéru. Aktualizovať databázu definícií systému antivírusovej a antimalvérovej ochrany musí byť možné minimálne 4-krát denne. * Behaviorálna analýza: Techniky behaviorálnej analýzy na detekciu neznámych hrozieb podľa ich správania a aktivít v sieti. * Blokovanie škodlivého obsahu: Ak sa zistí prítomnosť vírusu alebo malwaru, systém okamžite blokuje prístup k infikovaným súborom alebo stránkam, aby sa minimalizovala škoda. * Ochrana pred hrozbami z internetu: Centrálna bezpečnostná brána poskytuje aj ochranu pred rôznymi internetovými hrozbami, ako sú phishingové stránky, škodlivé odkazy a nebezpečné súbory. * Logovanie a správa: Ochranný systém zaznamenáva všetky udalosti týkajúce sa detekcie a blokovania malwaru, čo umožňuje administrátorom sledovať bezpečnostné udalosti a vyhodnocovať efektívnosť ochrany. | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | NCU, RPŠ, Škola |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | pracovné dni 6:00 – 18:00 |
| **Minimálna Dostupnosť služby** | | | | 99,9% - na základe základných parametrov a vlastností služieb NCU |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Funkčná ochrana pre vírusmi a malvérmi |
| **Definícia** | | Funkčná ochrana pre vírusmi a malvérmi podľa definície služby |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** |  |
| **Požadovaná hodnota** | **Jednotka** | boolean |
| **Minimum** | ÁNO v súlade |
| **Maximum** | N/A |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých škôl |
| **Metrika 2** | **Názov:** | | Frekvencia aktualizácií DB definícií AV a AM ochrany |
| **Definícia** | | Frekvencia s akou sa aktualizujú DB definícií AV a AM ochrany |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne |
| **Požadovaná hodnota** | **Jednotka** | Frekvencia denne |
| **Minimum** | 4 |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých škôl |

Tabuľka 6: Prevádzka služieb centrálnej antivírusovej a antimalvérovej ochrany - detailná definícia požiadaviek na službu

### Prevádzka služieb centrálnej IDS/IPS ochrany

| **Prevádzka služieb centrálnej IDS/IPS ochrany - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Prevádzka služieb centrálnej IDS/IPS ochrany |
| **Kategória** | | | | Služby sieťovej bezpečnosti |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Služby zabezpečovania Intrusion Detection System (IDS) / Intrusion Prevention System (IPS) chránia sieť DigiNET pred vonkajšími útokmi. Služby Centrálneho firewall-u majú dve techniky na riešenie týchto útokov: obranu založenú na anomáliách alebo obranu založenú na vzorkách. |
| **Prevádzka služieb centrálnej IDS/IPS ochrany - detailná definícia požiadaviek na službu** | | | | |
| Ochrana založená na anomáliách sa používa, keď sa samotná sieťová prevádzka je zneužitá a napríklad hostiteľ môže byť zaplavený oveľa väčším počtom požiadaviek, ako je schopný zvládnuť, čím sa stáva nedostupný. Ochrana za základe vzoriek (signatúr) sa používajú proti známych útokom voči zraniteľnostiach. Útočník v tomto prípade používa konkrétne príkazy alebo sekvencie príkazov a premenných na získanie prístupu. Signatúry pri IDS/IPS zahŕňajú tieto príkazové sekvencie, ktoré umožňujú centrálnemu firewallu detegovať a zastaviť útok. Tieto signatúry sú pravidelne aktualizované zo serverov výrobcu alebo sú zaslané proaktívne v prípade vzniku akútnej hrozby na centrálny firewall, aby sa zabránilo aj najnovším typom útokov hneď pri ich detekcii. IDS/IPS signatúry sú zlučované do prednastavených profilov inšpekcie komunikácie, ktoré sa aplikujú na komunikácie alebo skupiny komunikácií na centrálnom firewalle.  Generálne nastavenie IDS/IPS ochrany by malo byť realizované spôsobom nasadenia na všetky komunikácie zo siete Internet do siete DigiNET pre komunikácie na IP adresy DMZ serverov a služieb vystavených do siete Internet. Aplikácie definované s bezpečnostným rizikom úrovne „kritický“ by mal byť. Známe a dôveryhodné aplikácie by mali byť štandardne povolené. Takto nastavený proces filtrovania musí byť možné škálovať a individuálne nastavovať podľa bezpečnostných nastavení jednotlivých používateľských skupín.  V rámci zabezpečovania služieb Centrálneho uzla DigiNET verejný obstarávateľ očakáva, že vybraný dodávateľ poskytuje prevádzku komplexných služieb s súvislosti so zabezpečením IDS/IPS ochrany, a to najmä:   * Detekciu hrozieb: IDS/IPS analyzuje sieťovú prevádzku a identifikuje potenciálne hrozby a útoku, ako sú malware, phishing, prieniky do siete a iné. * Ochrana pred útokmi: Na základe detekcie hrozieb systém aktívne reaguje a blokuje alebo obmedzuje prístup k napadnutým zdrojom alebo sieťovým zariadeniam, čím minimalizuje škody spôsobené útokom. * Logovanie: IDS/IPS systém zaznamenáva všetky identifikované udalosti a poskytuje detailné záznamy o sieťovej prevádzke a aktivitách, ktoré sa môžu využiť v rámci pravidelných reportov. * Reakcia v reálnom čase: V prípade identifikácie aktívneho útoku systém okamžite reaguje, blokuje nežiadúcu komunikáciu a informuje administrátorov / SOC o aktívnom bezpečnostnom incidente. * Aktualizácie a správa: IDS/IPS systém je neustále aktualizovaný o vzorky nových hrozieb tak, aby bol schopný identifikovať aj najnovšie typy útokov. Možnosť pridať do databázy kategórií a signatúr nový záznam. | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | NCU, RPŠ, škola |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | pracovné dni 6:00 – 18:00 |
| **Minimálna Dostupnosť služby** | | | | 99,9% - na základe základných parametrov a vlastností služieb NCU |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Detection time |
| **Definícia** | | Maximálny čas, za ktorý systém identifikuje útok |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | proaktívne alebo reaktívne |
| **Požadovaná hodnota** | **Jednotka** | sekunda |
| **Minimum** | Nie je obmedzené |
| **Maximum** | 2 |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých škôl |
| **Metrika 2** | **Názov:** | | Protection time |
| **Definícia** | | Maximálny čas, za ktorý systém po detekcii útoku začne s ochranou napadnutého systému |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | proaktívne alebo reaktívne |
| **Požadovaná hodnota** | **Jednotka** | sekunda |
| **Minimum** | Nie je obmedzené |
| **Maximum** | 2 |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých škôl |

Tabuľka 7: Prevádzka služieb centrálnej IDS/IPS ochrany - detailná definícia požiadaviek na službu

### Prevádzka služieb centrálnej ochrany proti DDoS

| **Prevádzka služieb centrálnej ochrany proti DDoS- detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Prevádzka služieb centrálnej ochrany proti DDoS |
| **Kategória** | | | | Služby sieťovej bezpečnosti |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Centralizovaná ochrana pred distribuovanými sieťovými útokmi (DDoS) je kritickým prvkom zabezpečenia, ktorý poskytuje ochranu pred masívnymi volumetrickými útokmi na sieťovú infraštruktúru a sieťové služby. Ochrana pred DDoS sa nachádza na perimetri Centrálneho uzla a monitoruje všetky prichádzajúce a odchádzajúce sieťové dáta, aby identifikovala potenciálne DDoS útoky a minimalizovala ich vplyv na prevádzku DigiNET siete. |
| **Prevádzka služieb centrálnej ochrany proti DDoS- detailná definícia požiadaviek na službu** | | | | |
| V rámci zabezpečovania služieb Centrálneho uzla DigiNET verejný obstarávateľ požaduje, že vybraný dodávateľ poskytuje prevádzku komplexných služieb s súvislosti so zabezpečením ochrany pred DDoS útokmi, a to najmä:   * Detekcia DDoS útokov: Systém neustále monitoruje sieťové toky a metadáta z centrálnych zariadení a zariadení CPE a analyzuje správanie tak, aby identifikoval neobvyklé vzory a indikátory DDoS útokov, ako sú nadmerné množstvá prichádzajúcich žiadostí o spojenie alebo zvýšený tok dát. Identifikuje taktiež botnetové aktivity a škodlivé sieťové toky. * Filtrovacie mechanizmy: Systém používa rôzne filtračné mechanizmy, ako sú filtrovanie na základe zdrojovej IP adresy alebo cieľovej IP adresy, prípadne sieťového protokolu. * Automatické akcie: V prípade detekcie DDoS útoku systém automaticky spúšťa protiopatrenia (mitigáciu) na minimalizáciu jeho vplyvu na prevádzku DigiNET siete. Tieto kroky môžu zahŕňať presmerovanie alebo blokovanie tokov, respektíve filtrovanie konkrétnych požiadaviek smerujúcich do DigiNET siete, prípadne izolovanie siete * Požadované kapacitné parametre sú:   + minimálna kapacita mitigácie v paketoch za sekundu: 37 Mpps   + minimálny podporovaný počet TCP spojení: 60 miliónov   + maximálny čas, za ktorý systém začne s mitigáciou: 2 sekundy od prvého detekovaného paketu | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | NCU, RPŠ, škola |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | pracovné dni 6:00 – 18:00 |
| **Minimálna Dostupnosť služby** | | | | 99,9% - na základe základných parametrov a vlastností služieb NCU |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Čas mitigácie |
| **Definícia** | | Maximálny čas, za ktorý systém po detekcii útoku začne s mitigáciou |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Sekunda |
| **Minimum** | Nie je obmedzené |
| **Maximum** | 2 |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých škôl |

Tabuľka 8: Prevádzka služieb centrálnej ochrany proti DDoS- detailná definícia požiadaviek na službu

### RACI matica pre služby sieťovej bezpečnosti

| **Popis činnosti** | **Škola** | **RPŠ** | **NCU** | **MŠVVaM** |
| --- | --- | --- | --- | --- |
| Identifikácia, odstraňovanie a náprava bezpečnostných hrozieb, nedostatkov a incidentov v riešení v pôsobnosti NCU | I | C | A,R | I |
| Dodržiavanie požadovanej hodnoty merateľného parametra: Čas potrebný na pripojenie klienta WiFi na prvkoch v pôsobnosti RPŠ | I | A,R | C | I |
| Dodržiavanie požadovanej hodnoty merateľného parametra: Čas potrebný na pripojenie klienta WiFi na prvkoch v pôsobnosti NCU | I | C | A,R | I |
| Poskytovanie vzdialeného prístupu do siete školy podľa potrieb školy | C | C | A,R |  |
| Prepnutie na záložnú konektivitu v prípade výpadku primárnej linky. V prípade že RPŠ odovzdáva primárnu a záložnú konektivitu na dvoch samostatných rozhrania v lokalite školy poskytovateľovi služieb NCU ktorý ich pripája do CPE | I | R | A,R | I |
| Prepnutie na záložnú konektivitu v prípade výpadku primárnej linky. V prípade že RPŠ odovzdáva primárnu a záložnú konektivitu na jednom spoločnom rozhraní poskytovateľovi služieb NCU ktorý ho pripája do CPE | I | A,R | C,I | I |
| Zabezpečovanie záložnej dátovej konektivity v príslušných častiach siete LAN/WLAN pre ktoré je táto záloha konektivity výhradne určená. | C | R | A,R | N/A |
| Dohoda s poskytovateľmi pripojenia a prevádzkovateľmi pokrytia na adrese školy | C | A,R | C | N/A |
| Konfigurácia centrálneho filtrovania webového obsahu |  |  | R | A |
| Metodické usmernenie filtrovania obsahu |  |  |  | A |
| Nahlasovanie lokálnych výnimiek z filtrovania obsahu | R |  |  | A |
| Konfigurácia centrálnej aplikačnej kontroly |  |  | R | A |
| Metodické usmernenie aplikačnej kontroly |  |  |  | A |
| Nahlasovanie lokálnych výnimiek z aplikačnej kontroly | R |  |  | A |

Tabuľka 9: RACI matica pre služby sieťovej bezpečnosti

## Prevádzka sieťových služieb

Sieť a služby DigiNET sú primárne určené pre prístup k digitálnemu edukačnému obsahu. Tento obsah je však dostupný nielen z interných zdrojov v sieti DigiNET ale taktiež zo zdrojov v sieti Internet. Pre prístup k zdrojom v sieti Internet, ako aj pre možnosť využívania pripojenia k sieti DigiNET pre sprístupnenie vlastných zdrojov, je potrebné zabezpečiť služby centrálneho prekladu IP adries. Preklad adries môže byť dynamický v režime 1:N, ale aj statický v režime 1:1. Prestup je kontrolovaný a sú aplikované bezpečnostné pravidlá podľa definície verejného obstarávateľa.

Riešenie prestupu do iných sietí mimo sieť DigiNET je vykonávané centrálnou bezpečnostnou bránou rovnako ako prestup do siete Internet. Prestup je kontrolovaný a sú aplikované bezpečnostné pravidlá podľa definície verejného obstarávateľa.

**Popis služieb**

V rámci celkovej funkčnosti služieb poskytovaných prostredníctvom riešenia siete DigiNET je potrebné zabezpečiť aj komunikáciu mimo privátnej siete, napríklad do siete Internet a do prepojených sietí.

**Charakteristika pripojenia do siete Internet:**

* vysoko dostupné a zabezpečené pripojenie do siete Internet prostredníctvom Centrálneho uzla
* centrálny preklad privátnych IPv4 adries na verejné IPv4
* centrálne DNS služby

**Charakteristika pripojenia do iných sietí :**

* vysoko dostupné a zabezpečené pripojenie do iných sietí prostredníctvom Centrálneho uzla
* centrálny preklad privátnych IPv4 adries na verejné IPv4

Súčasťou sieťových služieb NCU je poskytovanie centralizovaného riešenia správy a dohľadu NCU (NCU-CRSD) pre potreby RPŠ. Tieto služby NCU sprostredkúva RPŠ pre zabezpečovanie služieb RPŠ - manažmentu a monitoringu siete LAN/WLAN prostredníctvom NCU-CRSD.

V prípade že v pripájanej lokalite k službám NCU nie sú zabezpečovanú služby RPŠ (lokalita bez RPŠ), môže obstarávateľ objednať u poskytovateľa NCU pre takúto lokalitu zabezpečovanie nasledovných sieťových služieb, pričom poskytovateľ NCU bude využívať existujúcu konektivitu používateľa služieb:

* Prevádzka služieb centrálneho pripojenia do siete Internet
* Prevádzka služieb centrálnej správy IP adries
* Prevádzka služieb vzdialeného pripojenia
* Prevádzka služieb pripojenia lokalít škôl k NCU a služby CPE
* Prepájanie na Dátové centrum rezortu školstva

Takto poskytované služby, ktoré sú výhradne v rozsahu zodpovednosti poskytovateľa služieb NCU, musia rovnako spĺňať požiadavky na služby a ich parametre podľa opisu predmetu zákazky.

### Prevádzka služieb centrálneho pripojenia do siete Internet

| **Prevádzka služieb centrálneho pripojenia do siete Internet - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Prevádzka služieb centrálneho pripojenia do siete Internet |
| **Kategória** | | | | Prevádzka sieťových služieb |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Zabezpečovanie vysoko dostupného pripojenia do siete internet prostredníctvom NCU |
| **Prevádzka služieb centrálneho pripojenia do siete Internet - detailná definícia požiadaviek na službu** | | | | |
| Verejný obstarávateľ požaduje:   * dátové pripojenie Centrálneho uzla do siete Internet na úrovni 100 Gbps, s podporou rozšírenia na nasledujúce kapacity pri zabezpečovaní všetkých služieb opisu predmetu zákazky:   + 200 Gbps   + 400 Gbps * pri dosiahnutí 80% kapacity v 5 minútovej vzorke po dobu troch za sebou idúcich dní Prevádzkovej doby garancie parametrov služieb, je prevádzkovateľ NCU povinný iniciovať zmenový proces potreby navýšenia kapacity v spolupráci s Verejným obstarávateľom, poskytovateľ služieb NCU je teda povinný proaktívne spolupracovať s obstarávateľom v prípade potreby navýšenia aktuálnej kapacity na vyššiu úroveň ktorú si obstarávateľ u poskytovateľa NCU následne objedná, * poskytovateľ služieb NCU je povinný do troch mesiacov od požiadavky obstarávateľa navýšiť kapacitu na vyššiu úroveň, * poskytovateľ služieb NCU zabezpečuje plne geograficky redundantné prepojenie tak, aby v prípade výpadku jednej lokality Národného Centrálneho uzla neprišlo k obmedzeniu alebo degradácii poskytovanej služby, * aby akákoľvek dátová komunikácia medzi sieťou Internet a sieťou DigiNET prechádzala cez bezpečnostné komponenty NCU. Dátové prevádzka žiadnej pripojenej lokality DigiNET nesmie byť smerovaná priamo do siete Internet, * pripojenie do siete Internet na úrovni protokolov IPv4, aj IPv6 bez prekladu adries a protokolov, * minimálne 2 verejné IPv4 adresy pre každú lokalitu pripojenú do siete DigiNET, * poskytovanie centrálnej služby DNS pre všetkých používateľov a všetky zariadenia na každej lokalite. | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | RPŠ, škola |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | pracovné dni 6:00 – 18:00 |
| **Minimálna Dostupnosť služby** | | | | 99,9% - na základe základných parametrov a vlastností služieb NCU |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Priepustnosť |
| **Definícia** | | Priepustnosť do siete internet na úrovni 100 Gbps |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | proaktívne |
| **Požadovaná hodnota** | **Jednotka** | % |
| **Minimum** | 99,9 |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých škôl |
| **Merateľné parametre** | **Metrika 2** | **Názov:** | | Priepustnosť |
| **Definícia** | | Priepustnosť do siete internet na úrovni 200 Gbps |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | proaktívne |
| **Požadovaná hodnota** | **Jednotka** | % |
| **Minimum** | 99,9 |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých škôl |
| **Merateľné parametre** | **Metrika 4** | **Názov:** | | Priepustnosť |
| **Definícia** | | Priepustnosť do siete internet na úrovni 400 Gbps |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | proaktívne |
| **Požadovaná hodnota** | **Jednotka** | % |
| **Minimum** | 99,9 |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých škôl |

Tabuľka 10: Prevádzka služieb centrálneho pripojenia do siete Internet - detailná definícia požiadaviek na službu

### Prevádzka služieb prepájania sietí

| **Prevádzka služieb prepojenia sietí, dátovej bezpečnosti a integrity prostredia - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Prevádzka služieb prepojenia sietí, dátovej bezpečnosti a integrity prostredia |
| **Kategória** | | | | Prevádzka sieťových služieb |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Zabezpečovanie bezpečnej výmeny a spracovania dát |
| **Prevádzka služieb prepojenia sietí, dátovej bezpečnosti a integrity prostredia - detailná definícia požiadaviek na službu** | | | | |
| Verejný obstarávateľ požaduje, aby vybraný uchádzač technicky zabezpečil peeringové lokality pre prepájanie sietí zúčastnených strán.  V rámci zabezpečovania služieb Národného centrálneho uzla DigiNET bude pre prepájanie sietí použité peeringové centrum SIX (Slovak Internet eXchange) z dôvodu naplnenia nasledujúcich požiadaviek:   * Je požadované, aby prenos dát medzi NCU, RPŠ a MŠVVaM SR prebiehal výhradne prostredníctvom Slovenského peeringového centra SIX, pričom je nevyhnutné zabezpečiť, aby spomínaný prenos neopúšťal územie Slovenskej republiky. V kontexte zabezpečovania poskytovania služieb RPŠ je každý zmluvný poskytovateľ služieb RPŠ pripojený v peeringovom centre SIX. Uvedená skutočnosť, vytvára jednotné technické prostredie, ktoré zabezpečuje integritu dátových prenosov, efektívnu integrovateľnosť celého systému a efektívnu prevádzku služieb. Tento prístup je zásadný z hľadiska ochrany citlivých a regulovaných informácií, bezpečnosti ako aj z pohľadu zabezpečenia dátovej suverenity štátu. * Infraštruktúra na prenos a spracovanie dát medzi NCU, RPŠ a MŠVVaM SR musí byť umiestnená v rámci národného prostredia výlučne na území Slovenskej republiky, aby sa zabezpečila schopnosť rýchlej reakcie na kybernetické hrozby. Dátová prevádzka prostredníctvom služieb musí prebiehať v národnom peeringovom centre, ktoré poskytuje technickú izoláciu kritických častí infraštruktúry od globálnych sieťových pripojení. Táto izolácia je zásadná pre minimalizáciu rizika prenosu hrozieb z vonkajších zdrojov a na efektívne monitorovanie, analýzu a riešenie bezpečnostných incidentov. Zároveň je potrebné, aby centrum podliehalo právnemu rámcu Slovenskej republiky a strategickým bezpečnostným požiadavkám v oblasti informačných technológií a kybernetickej bezpečnosti. * V prípade že poskytovateľ služieb NCU využíva pre poskytovanie svojich služieb cloudové služby alebo služby typu „sandboxing“ je nevyhnutné zabezpečiť, aby vybrané dátové súbory, ktoré obstarávateľ označí za citlivé, neboli spracovávané mimo územia Slovenskej republiky. Tieto technické a organizačné opatrenia musia zabezpečiť, že dotknuté dáta zostanú pod jurisdikciou Slovenskej republiky. | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | NCU, RPŠ, MŠVVaM SR |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | 24/7 |
| **Minimálna Dostupnosť služby** | | | | 99,9% |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Zabezpečovanie dátovej bezpečnosti a integrity prostredia |
| **Definícia** | | V súlade s požiadavkami popísaných v definícii služby vyššie |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne alebo Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | boolean |
| **Minimum** | ÁNO v súlade |
| **Maximum** | N/A |
| **Severita nesúladu služby** | | Severity 1 |

Tabuľka 11: Prevádzka služieb prepojenia sietí, dátovej bezpečnosti a integrity prostredia - detailná definícia požiadaviek na službu

### Prevádzka služieb centrálnej správy IP adries

| **Prevádzka služieb centrálnej správy IP adries - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Prevádzka služieb centrálnej správy IP adries |
| **Kategória** | | | | Prevádzka sieťových služieb |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Centrálna správa IP adries |
| **Prevádzka služieb centrálnej správy IP adries - detailná definícia požiadaviek na službu** | | | | |
| V rámci centrálne manažovaného riešenia je požadovaná aj centrálna správa IP adries v dostatočnom rozsahu až do úrovne LAN a WLAN sietí. Tento centrálny IP manažment musí obsahovať aj vlastný centrálny DHCP server, ktorého vlastnosti musia podporovať minimálne nasledovné funkcionality:   * statický IP to MAC binding, * podpora pre 802.1X, * podpora pre IPv4 a IPv6.   Sú požadované minimálne 2 verejné IPv4 adresu pre každú lokalitu pripojenú do siete DigiNET.  Centrálny uzol DigiNET musí na základe údajov z AD / LDAP vytvoriť vlastnú databázu používateľov, ktorá bude neustále priebežne aktualizovaná z AD / LDAP. Táto vlastná databáza musí byť integrovaná s IP manažmentom a centrálnym DHCP serverom a cez vlastné administračné webové rozhranie umožňovať minimálne nasledovné funkcionality:   * prehľad a manažment lokalít podľa geografického členenia (obdobne ako pri monitoringu a reportingu) pre zástupcov z MŠVVaM SR, * globálny manažment IP adries a prepojenie s centrálnym DHCP serverom, * pre každú lokalitu prideľovanie administrátora lokality, ktorý bude viazaný na používateľa v AD / LDAP, * manažment používateľov a zariadení lokality administrátorom lokality nasledovne:   + prideľovanie IP adries a MAC adries zariadeniam v LAN sieťach (IP-to-MAC binding),   + vytváranie zoznamov MAC adries zariadení pre prístup z LAN sietí (MAC Authentication Bypass),   + možnosť vlastných názvov pre zariadenia.   V rámci globálneho adresného manažmentu musia byť zástupcom z MŠVVaM SR dostupné všetky funkcionality minimálne v read-only móde. | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | RPŠ, škola, MŠVVaM SR |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | 24/7 |
| **Minimálna Dostupnosť služby** | | | | 99,9% - na základe základných parametrov a vlastností služieb NCU |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Prevádzka služieb centrálnej správy IP adries |
| **Definícia** | | Prevádzka služieb centrálnej správy IP adries je vykonávaná v súlade s definíciou služby |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne alebo Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | boolean |
| **Minimum** | ÁNO v súlade |
| **Maximum** | N/A |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých škôl |

Tabuľka 12: Prevádzka služieb centrálnej správy IP adries - detailná definícia požiadaviek na službu

### Poskytovanie služieb centralizovaného riešenia správy a dohľadu NCU (NCU-CRSD) pre potreby RPŠ

Súčasťou sieťových služieb NCU je poskytovanie centralizovaného riešenia správy a dohľadu NCU (NCU-CRSD) pre potreby RPŠ. Tieto služby NCU sprostredkúva RPŠ pre zabezpečovanie služieb RPŠ - manažmentu a monitoringu siete LAN/WLAN prostredníctvom NCU-CRSD v lokalitách škôl.

| **Poskytovanie služieb centralizovaného riešenia správy a dohľadu NCU (NCU-CRSD) pre potreby RPŠ - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Poskytovanie centralizovaného riešenia správy a dohľadu NCU-CRSD |
| **Kategória** | | | | Prevádzka sieťových služieb |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Národné centralizované riešenie správy a dohľadu (ďalej len NCU - CRSD), súvisí s prevádzkou, monitorovaním, správou, údržbou sieťového riešenia, atď. Takáto služba umožní čo najefektívnejšie nasadenie riešenia, jeho správu, monitorovanie a diagnostiku. |
| **Poskytovanie služieb centralizovaného riešenia správy a dohľadu NCU (NCU-CRSD) pre potreby RPŠ - detailná definícia požiadaviek na službu** | | | | |
| **Poskytovanie služieb NCU-CRSD**  Poskytovanie centralizovaného riešenia správy a dohľadu (ďalej len NCU-CRSD), súvisiaceho s prevádzkou, správou a údržbou sieťového riešenia.  Centralizovanou službou sa myslí spravidla jedno grafické prostredie (GUI) poskytujúce ucelenú funkcionalitu, dostupné vzdialene a on-line pre všetky relevantné organizácie prostredníctvom web klienta (štandardný internetový browser).  Služba je zabezpečovaná podľa nasledujúcich kritérií:   * Je neprípustné v kombinácii so službami NCU umiestňovanie serverov alebo akýchkoľvek dedikovaných kontrolérov do prostredia/lokality školy. NCU môže NCU-CRSD vybudovať alebo inak zabezpečiť jeho prevádzku napríklad v private cloud prostredí, resp. On-premises dátové centrum alebo public cloud prostredí. Predložené CRSD riešenie musí podporovať:   + garantované vo funkčnom stave a podporujúce pridávanie funkcionality do produktov WiFi AP a switche zo strany ich výrobcov (ak títo budú pridávať nové vlastnosti) po celú dĺžku trvania prevádzky,   + prevádzkované na lokalitách určených NCU – napr. private cloud, on-premises dátové centrum, na náklady NCU,   + pri prevádzkovaní v public cloud prostredí, garantujúcom požadovanú dostupnosť, na náklady NCU,   + dostupná vzdialene v reálnom čase, pričom musí byť možný prístup do grafického GUI prostredia zabezpečujúci management, prevádzku a ostatné prevádzkové funkcionality určené pre RPŠ na zabezpečenie služieb prevádzky v lokalitách škôl minimálne pre nasledovných určených pracovníkov:     - zamestnanci a administrátori RPŠ,     - zamestnanci NCU,   + dostupná vzdialene v reálnom čase, pričom musí byť možný prístup do grafického GUI prostredia zabezpečujúci náhľad prevádzkových a výkonnostných parametrov minimálne pre nasledovných určených pracovníkov:     - zamestnanci školy/poverení pracovníci školy,     - zamestnanci zriaďovateľa školy,     - zamestnanci MŠVVaM SR a poverená osoba pre prípadný audit,     - zamestnanci poskytovateľa NCU.   **NCU-CRSD** služba musí vykonávať funkcie WiFi kontroléra – tzn., musí:   * vykonávať registráciu WiFi prístupových bodov, * zabezpečovať centrálne konfiguráciu všetkých AP, * zbierať informácie od jednotlivých AP vo vzťahu k frekvenciám použitých susedným AP, * minimalizovať interferenciu, nastavovať vysielací výkon a kanál, * vykonávať rádiofrekvenčné plánovanie (RRM) s cieľom maximalizovať kvalitné pokrytie signálom, * v prípade výpadku kontroléra zabezpečovať aby aktuálne pripojení klienti/používatelia nestratili prístup k službám WLAN.   RPŠ je povinný sa o dodané prvky infraštruktúry – WiFi a Switche starať pomocou NCU-CRSD v súlade s metodickým usmernením NCU, a to minimálne z pohľadu nastavenia,  úpravy a optimalizácií nastavení v čase, upgrade-ov OS/firmware aktívnych prvkov, dohľadu a monitoringu a riešení problémov.  Vzhľadom na očakávanú veľkosť projektu sa požaduje, aby NCU-CRSD nástroj podporoval API RESTFUL služby, ktoré musia:   * byť verejne zdokumentované, * dostupné počas celej doby trvania zmluvného vzťahu, * byť dostupné vzdialene a real-time, * poskytnúť informácie o konfiguráciách (WiFi AP a prepínačov), * poskytnúť informácie o pripojených zariadeniach v sieti (klientov), * chránené unikátnym API kľúčom s možnosťou revokácie.   **Služba onboardingu zariadení LAN/WLAN**  Z dôvodu jednoduchosti a rýchlosti nasadenia, budúceho rozširovania, urýchlenia výmen pokazených zariadení, minimalizácie ľudskej chyby ako aj ďalších dôvodov sa požaduje, aby dodané sieťové zariadenia - WiFi access point-y (indoor a outdoor) a switche podporovali a boli nasadené v režime ZTP – Zero Touch Provisioning.  Režimom ZTP sa myslí najmä:   * Schopnosť nového zariadenia bez predchádzajúcej konfigurácie sa po zapnutí a pripojení ku sieti poskytujúcej DHCP pridelenie adresy automatizovaným a zabezpečeným spôsobom prihlásiť do NCU-CRSD a stiahnuť si svoju konfiguráciu s ktorou má byť prevádzkované, bez potreby vykonávania predchádzajúcej konfigurácie (bez potreby tzv. pre-staging-u). Zároveň je možné vytvárať konfiguračné šablóny, zabezpečujúce konzistenciu konfigurácií. * Pri onboardingu zariadení sa navyše musia automaticky stiahnuť potrebné aktualizácie firmvéru a bezpečnostné záplaty, odporúčané výrobcom týchto zariadení. * Dodané riešenie NCU-CRSD musí za týmto účelom takéto ZTP služby umožňovať.   **Služba konfigurácie zariadení LAN/WLAN**  NCU-CRSD musí poskytovať centralizovanú službu správy konfigurácii umožňujúcu minimálne nasledovné:   * kompletnú konfiguráciu WiFi AP a switchov, * priradiť zariadeniam popisné označenie/meno, * priradiť Ethernet rozhraniam switchov popisné označenia, * konfigurovať zariadenia:   + individuálnym spôsobom   + prostredníctvom konfiguračných šablón umožňujúcich aplikovať zvolené nastavenia hromadným spôsobom – napr. pre všetky AP, prepínače * špecificky pre WiFi musí byť možné nastaviť hromadne:   + pre skupinu zvolených AP:     - frekvenčné pásmo na ktorom sú dostupné dané SSID – 2.4 Ghz, 5Ghz, obe, band steering,     - vysielací výkon v zvolenom frekvenčnom pásme,     - maximálnu povolenú rýchlosť,     - šírku pásma vysielacieho kanálu – 20/40/80 Mhz (5Ghz pásmo),   + pre každé SSID individuálne parametre:     - časový harmonogram dostupnosti zvoleného SSID,     - či je zvolené SSID verejne inzerované alebo skryté,     - na ktorých AP je SSID inzerované,     - bezpečnostné parametre:       * PSK / IEEE 802.1X,       * WPA2 /WPA3,       * Vynucovanie DHCP pridelenej IP adresy klienta od definovaných DHCP serverov     - do ktorej VLAN je bridge-ované,   + povolenie/zakázanie L2 izolácie klientov,   + ACL umožňujúci dodatočné blokovanie zvolených cieľov – IP adresa, Protokol, Port   + shaping dátovej prevádzky umožňujúci na jednotlivé SSID definovať kapacitné limity, ktoré umožnia:     - možnosť definovať download a upload maximá pripojených klientov k danému SSID,     - definovať download a upload maximá agregovane pre jednotlivé SSID, * špecificky pre Switche musí byť možné nastaviť hromadne:   + zapnutie/vypnutie skupiny portov,   + povolenie/zakázanie PoE skupiny portov,   + časový harmonogram zapínania/vypínania skupiny portov,   + Access VLAN ID resp. Trunk a povolené VLAN ID, Native VLAN ID skupiny portov,   + rýchlosť, duplex skupín portov,   + Rapid STP mechanizmy: BPDU Guard, Loop Guard, Root Guard skupiny portov,   + Prístupovú politiku skupiny portov:     - Radius IEEE802.1X, MAB, MAB fallback ak zlyhá 802.1X,     - Radius accounting,     - Režim: Single Host, Multi Domain, Multi Auth,     - VLAN ID pri zamietnutí autentifikácie,     - VLAN ID pri nedostupnosti Radius servera. * Viditeľnosť a topológia siete a prvkov, ich dostupnosť atď..   Služba musí byť schopná obsluhovať od predpokladaných 50.000 pripájaných bodov LAN/WLAN. Verejný obstarávateľ predpokladá že počet obsluhovaných PB nebude nižší ako 50 000 avšak negarantuje ich minimálny a maximálny počet.  V prípade jeho nedostupnosti NCU-CRSD verejný obstarávateľ požaduje, aby:   * už autentikovaní používatelia ostali pripojení, * dátová komunikácia prebiehala bez prerušenia, * používatelia mohli byť prepájaný medzi pripájanými bodmi typu AP * skupinové a bezpečnostné politiky ostali v platnosti a boli naďalej aplikované, * RF vlastnosti bezdrôtovej siete boli bez prerušenia.   Služba musí automatizovane vytvárať typologické zobrazenie aktuálneho zapojenia sieťovej infraštruktúry, umožňujúce jednoducho identifikovať:   * topológiu zapojenia s menom/popisom zariadení, * chybový stav zariadenia (ak taký nastal), * ktoré zariadenia sú vzájomne prepojené, * konkrétny port na prepínači, kde je pripojené AP so zobrazením:   + rýchlosť portu,   + vyťaženie portu, * Služba topológie musí byť okrem pre RPŠ dostupná cez GUI štandardných browserov aj pre poverených pracovníkov školy, MŠVVaM SR a NCU. A to v minimálne kapacite počtu prístupov v počte 33% obsluhovaných lokalít škôl. * Interferencie a cudzie prvky:   + Pre bezproblémovú prevádzku najmä WLAN siete je kľúčové byť schopný odhaliť prítomnosť rušenia (interferencie) a cudzích prvkov. Za týmto účelom je vhodné vykonávať periodickú spektrálnu analýzu, ktorá jednak tieto zdroje rušenia identifikuje, ale poskytuje tiež údaje potrebné k automatickému alebo manuálnemu preladeniu na iný kanál, prípadne úpravu výkonu. Vzhľadom na časovú náročnosť spektrálnej analýzy je požadované aby túto funkciu vykonávala oddelená časť WiFi AP, aby nedochádzalo k ovplyvňovaniu užitočnej prevádzky. Ďalšou úlohou je pri identifikácii cudzích prvkov aj schopnosť posúdiť, či predstavujú bezpečnostnú hrozbu.   + Štandardom služby je:   + dedikované rádio pre 2,4 Ghz, Dedikované rádio pre 5 Ghz,   + spektrálna analýza 2,4 a 5 Ghz pásma (real-time, bez ovplyvnenia dátovej prevádzky WiFi klientov) a schopnosť odhaliť interferencie ako aj kvantifikovať mieru využitia (utlizácie) všetkých kanálov príslušného spektra 2.4 a 5 Ghz, priemerovanú za min. posledných 60 sekúnd,   + meranie a zobrazovanie interferencií v pásme 2.4 a 5 Ghz v reálnom čase, bez dopadu na obsluhovanie WiFi klientov schopné určiť prítomnosť zdrojov rušenia v blízkosti zvoleného AP a tieto zdroje (ak sú to WiFi AP) identifikovať – SSID, BSSID (MAC), * Wireless IDS – intrusion detection system:   + nepretržitá klasifikácia WiFi AP ako autorizované, susedné alebo neautorizované (rogue), pričom služba umožňuje:     - detegovať:       * pripojenie neautorizovaného WiFi AP do spravovanej siete LAN,       * vyžarovanie rovnakého SSID aké poskytuje služba WiFi neautorizovaným WiFi AP,       * DOS útoky spôsobený zasielaním nadmerného množstva de-autentifikačných, disasociačných a manažment rámcov,     - reagovať:       * zamedzením pripojenie sa na neautorizované WiFi AP,       * zablokovaním prístupu k neovereným SSID definovaným školou, ktoré sú detegované spravovanými WiFi AP v rámci sieťovej infraštruktúry školy,       * zaslaním emailu zodpovedným osobám, Syslog informácie, zaznamenaním eventu v manažmente WLAN riešenia.   Správa inventára   * Inventory manažment poskytuje v rámci služby detailný prehľad o všetkých inštalovaných LAN, WLAN zariadeniach, prípadne licenciách, nevyhnutných pre centralizovanú správu siete RPŠ. Okrem potreby RPŠ slúžia tieto informácie na účely auditu inštalácie a tiež kontroly dodržania regulačných požiadaviek (napr. inštalované WiFi AP sú v súlade s požiadavkami TÚ SR/ETSI). * V rámci služby Inventory manažmentu je nevyhnutné poskytnúť nasledovné informácie o zariadeniach: * MAC adresa, sériové číslo, model, aktuálny firmware, stav pripojenia, licencia. * Pre účely kontroly prístupu k monitoringu a manažmentu siete je nevyhnutné, aby služba umožňovala rozdelenie kompetencií v rámci administrátorských účtov. Služba teda definuje, aký typ administrátora má k inventarizácií zariadení prístup. * Služba musí byť prístupná real-time online formou GUI prostredníctvom štandardných browserov pre poverených zamestnancov RPŠ, školy, NCU a MŠVVaM SR. Musí tiež umožňovať tieto dáta exportovať (priamo z GUI a tiež formou API) aspoň v jednom z formátov CSV, XML, JSON, pre potreby archivácie a ďalšieho spracovania.   Monitoring  Služba musí umožňovať centralizovaný vzdialený online dohľad aktívnych sieťových prvkov – WiFi AP indoor, WiFi AP outdoor, prepínače prostredníctvom web klienta (štandardný internetový prehliadač) a používateľov.  Služba musí umožňovať centralizovaný vzdialený online zber monitoring informácii WiFi AP indoor, WiFi AP outdoor, prepínače prostredníctvom štandardizovaného rozhrania.  Monitoring Služba NCU-CRSD pozostáva z nasledovných kategórií:   * monitorovanie dostupnosti a stavu prvkov infraštruktúry, * stav aktívnych prvkov (WiFi AP, prepínače),   Monitoring prepínačov:   * zobrazenie dostupnosti / nedostupnosti zariadenia, * zobrazenie grafickej reprezentácie prepínača s rozmiestnením portov zodpovedajúcim realite, na ktorom je zrejmé:   + ktoré porty sú aktuálne pripojené, odpojené porty,   + ktoré pripojené porty poskytujú PoE napájanie, * zobrazenie mena/popisu prepínača, * počet aktuálne pripojených klientov, * zobrazenie zoznamu pripojených zariadení (wired klientov) za zvolené časové obdobie, min. 30 dní spätne, * zoznam pripojených zariadení musí poskytovať minimálne nasledovné informácie:   + port prepínača, MAC adresa klienta, VLAN ID,   + zobrazenie informácií o nastavení a štatistikách portov switchu, minimálne nasledovné informácie:     - vlan ID, Trunk a native vlan ID a zoznam povolených VLAN (ak je zapnutý trunk),     - administratívny stav (port zapnutý/vypnutý), výsledná rýchlosť linky, duplex, alokácia PoE výkonu, * informácie o Spanning-Tree-protokole – min:   + či je port v stave prepúšťajúci alebo blokujúci používateľskú prevádzku,   + Spanning-Tree Root – ktorý switch je root, * počítadlá za zvolené časové obdobie, min. 30 dní spätne:   + prenesený objem dát na porte v smere prijatom,   + prenesený objem dát na porte v smere odoslanom, * LLDP zoznam susedov, * množstvo alokovaného PoE výkonu z celkového PoE budgetu prepínača.   Monitoring WiFi AP:   * zobrazenie dostupnosti / nedostupnosti zariadenia, * zobrazenie prevádzky Uplink/Downlink v reálnom čase pre vybrané AP, * zobrazenie informácií pre aktuálne pripojených klientov, ako napr.:   + meno zariadenia, IP adresa, MAC adresa, VLAN, asociované SSID,   + dĺžka pripojenia, množstvo prenesených dát, sila signálu, aktuálny kanál a jeho šírka,   + percentuálne vyťaženie jednotlivých kanálov v 2.4Ghz a 5 Ghz pásme,   + zobrazenie aktuálne spotreby AP, dĺžky prevádzky AP, * pre vybrané SSID je dôležité sledovať nasledovné údaje o výkone bezdrôtovej služby WiFi s dopadom na vybrané problematické AP a klientov:   + schopnosť prešetriť čas potrebný na pripojenie k prístupovému bodu,   + sledovanie priemernej latencie, straty paketov a kvalitu signálu SNR pre klientov,   + monitorovanie dostupnosti služieb ako RADIUS, DNS.   Bezpečnostný monitoring:   * Udalosti súvisiace prevádzkou 802.1x, napríklad:   + autentifikácia používateľa,   + deautentikáciou používateľa,   + vypršanie času odozvy (time-out) RADIUS servera,   + vypršanie času odozvy (time-out) klienta,   + zlyhanie autentifikácie,   + detekcia a upozorňovanie na pokusy o neoprávnený prístup.   Reaktívne monitorovanie používateľa pripojeného v sieti:   * vyhľadanie konkrétneho zariadenia (klienta) aby bolo možné pre WiFi určiť:   + na ktoré AP je pripojené,   + od kedy je pripojené,   + ako vyťažuje sieť za zvolené časové obdobie,   + na ktoré destinácie komunikuje a koľko na ne prenieslo dát,   + na ktoré SSID, pásmo (2.4 Ghz alebo 5 Ghz), silu signálu s ktorou je zariadenie videné zo strany AP,   + vyhľadanie konkrétneho zariadenia (klienta) aby bolo možné pre wired určiť:     - na ktorý switch a port je pripojené,     - od kedy je pripojené,     - ako vyťažuje sieť za zvolené časové obdobie,     - na ktoré destinácie komunikuje a koľko na nich prenieslo dát.   Monitorovanie používateľských aktivít:   * koľko bolo za zvolené časové obdobie pripojených zariadení pomocou WiFi, * koľko bolo za zvolené časové obdobie pripojených zariadení cez drôtový ethernet, * ktoré pripojené WiFi zariadenia preniesli koľko dát za zvolené časové obdobie, * ktoré pripojené drôtové zariadenia preniesli koľko dát za zvolené časové obdobie, * ktoré zariadenie prenieslo za zvolené časové obdobie najviac dát, * IP adresa pripojených zariadení, * typ zariadenia a jeho OS, * zobrazenie aktívnych aj neaktívnych zariadení, ktoré sa pripojili za posledných 30 dní.   Poznámka: v prípade zberu reportinových dát z NCU-CRSD môže RPŠ spolupracovať s NCU na príprave a vytváraní reportov v jednotnom formáte.  **Upozornenia**  NCU-CRSD monitoring musí umožňovať na definované ciele na základe metodického usmernenia Ministerstva zasielať upozornenia týkajúce sa najmä zmien, výpadkov a kritických stavov. Medzi monitorované udalosti, v reakcii na ktoré sú zasielané upozornenia musí patriť:   * zmena konfiguračných parametrov AP, switchov a firewallu, * detekcia cudzieho WiFi AP, * WiFi AP sa stalo nedostupným, * switch sa stal nedostupným, * bola zistená prítomnosť nelegitímneho DHCP servera.   Medzi definované ciele, na ktoré je možné odosielať upozornenia musí patriť:   * definovaný zoznam emailových adries – napríklad adresy zvolených zamestnancov školy, * minimálne 2 Webhook HTTPS adresy, kde budú notifikácie odosielané formou HTTP POST metódy.   **Ochrana centrálneho monitoring nástroja**  Centralizované riešenie správy a dohľadu (NCU-CRSD) siete obsahuje dôveryhodné informácie, ktoré sú určené pre vybraných správcov a zainteresované osoby podľa príslušného rozdelenia právomocí. Dodaná služba preto musí poskytnúť zabezpečenie takéhoto nástroja kombináciou viacvrstvovej bezpečnosti. Tieto opatrenia garantujú dôveru používateľov.  V rámci zabezpečovania služieb RPŠ očakávame, že vybraný dodávateľ poskytne zabezpečený prístup do RPŠ monitoring nástroja nasledovne:   * všetka komunikácia medzi používateľmi a NCU-CRSD je šifrovaná (šifrovanie data in-motion), * NCU-CRSD podporuje dvojfaktorovú autentifikáciu, ktorá pridáva dodatočnú vrstvu ochrany tým, že vyžaduje nielen heslo, ale aj druhý faktor, ako je potvrdenie identity pomocou mobilnej aplikácie alebo kódom, obdržaným cez SMS/email, * služba podporuje SAML SSO, čo umožňuje integráciu s externými autentifikačnými systémami a centralizovanú správu prístupu, * prístup k nástroju je riadený na základe rolí (RBAC – Role based access control), čo umožňuje priradiť rôzne úrovne prístupu používateľom podľa ich úlohy a zodpovedností, a to nasledovne:   + privilégia na zmeny (read-write), privilégia na čítanie (read-only) pre rôznych používateľov – zamestnanci RPŠ, zamestnanci NCU, zamestnanci školy a pod.,   + aby bolo možné zriadiť administrátora, ktorý bude mať prístup do monitoring nástroja pre celú školu: WiFi AP a prepínače na všetkých adresách školy,   + administrátora, ktorý bude mať prístup do monitoring nástroja pre WiFi AP a switche na len danej adrese školy,   + pre zvolených pracovníkov školy, zriaďovateľa a MŠVVaM SR, musí byť možné zriadiť read-only prístupy, * prístup k dátam **NCU-CRSD** je možné poskytnúť pomocou API prístupu, ktorý je zabezpečený unikátnym API kľúčom (s možnosťou odvolať/zrušiť už vytvorený kľúč), * možnosťou zadefinovať IP adresné rozsahy, z ktorých je povolené prihlásenie sa do monitoring-ového nástroja, * dáta obsiahnuté v monitorovacom nástroji sú šifrované (šifrovanie data at-rest), navyše monitoring spĺňa požiadavky GDPR (General Data Protection Regulation), * audit Log - NCU-CRSD automatizovane zaznamenáva všetky prístupy a akcie vykonané používateľmi, čo umožňuje administrátorom sledovať aktivity a identifikovať potenciálne bezpečnostné incidenty.   **Audit Log**  Za účelom editovateľnosti vykonaných konfiguračných zmien spolu s autorom zmien musí NCU-CRSD automatickým spôsobom tieto zmeny zaznamenávať – Audit Log.  Štandardom služby pritom je:   * držanie záznamov o administratívnych zmenách vykonaných za obdobie min. 3 mesiacov spätne, * záznamy musia jasne definovať ktorý konkrétny používateľ vykonal ktorú zmenu, * popis čoho sa zmena týkala, * detail pôvodného nastavenia, * detail nového (zmeneného nastavenia), * export Audit Logu do jedného z formátov: XML, JSON, CSV.   **NCU-CRSD podporuje minimálne integráciu nasledovných prvkov**   |  |  | | --- | --- | | **Fortinet WLAN** | | | **Model zariadenia** | **Špecifikácia** | | **802.11be Wi-Fi 7** |  | | FAP-441K | 4x4 Indoor quad-radio 11be 6Ghz Capable APs | | FAP-443K | 4x4 Indoor quad-radio 11be 6Ghz Capable APs | | FAP-241K | 2x2 Indoor quad-radio 11be 6Ghz Capable APs | | FAP-243K | 2x2 Indoor quad-radio 11be 6Ghz Capable APs | | **802.11ax Wi-Fi 6E** |  | | FAP-431G | 4x4 Indoor tri-radio 11ax 6Ghz Capable APs | | FAP-432G | 4x4 Ruggedized Tri-radio indoor/outdoor 11ax (6Ghz) Capable APs | | FAP-433G | 4x4 Indoor tri-radio 11ax 6Ghz Capable APs | | FAP-231G | 2x2 Indoor tri-radio 11ax 6Ghz Capable APs | | FAP-233G | 2x2 Indoor tri-radio 11ax 6Ghz Capable APs | | FAP-234G | 2x2 Ruggedized Tri-radio indoor/outdoor 11ax (6Ghz) Capable APs | | **802.11ax Wi-Fi 6** |  | | FAP-831F | 8x8 Indoor tri-radio 11ax AP | | FAP-433F | 4x4 Indoor tri-radio 11ax APs | | FAP-432F | 4x4 Ruggedized indoor/outdoor tri-radio 11ax AP | | FAP-431F | 4x4 Indoor tri-radio 11ax APs | | FAP-234F | 2x2 Ruggedized indoor/outdoor tri-radio 11ax AP | | **Fortinet LAN** | | | **Model zariadenia** | **Špecifikácia zariadenia a portov** | | FortiSwitch-108F | 7x GE RJ45, 1x GE/POE-PD RJ45 + 2x GE SFP | | FortiSwitch-108F-POE | 8x (802.3af/at) GE RJ45 + 2x GE SFP | | FortiSwitch-108F-FPOE | 8x (802.3af/at) GE RJ45 + 2x GE SFP | | FortiSwitch-108E-FPOE | 8x (802.3af/at) GE RJ45 + 2x GE SFP | | FortiSwitch-110G-FPOE | 2x 5G/2.5G/1G/100M [PoE bt], 8x 2.5G/1G/100M/10M RJ45 [PoE at/af], 4x 10G/1G/100 SFP+/SFP | | FortiSwitch-124F | 24x GE RJ45 and 4x 10GE SFP+ | | FortiSwitch-124F-POE | 24x GE RJ45 and 4x 10GE SFP+ [12x 802.3af/at] | | FortiSwitch-124F-FPOE | 24x GE RJ45 and 4x 10GE SFP+ [24x 802.3af/at] | | FortiSwitch-148F | 48x GE RJ45 and 4x 10GE SFP+ | | FortiSwitch-148F-POE | 48x GE RJ45 and 4x 10GE SFP+ [24x 802.3af/at] | | FortiSwitch-148F-FPOE | 48x GE RJ45 and 4x 10GE SFP+ [48x 802.3af/at] | | **CISCO WLAN** | | | **Model zariadenia** | **Špecifikácia** | | **Catalyst** |  | | 9105AX (I/W) | Wi-Fi 6 (802.11ax), 2x2 UL/DL MU-MIMO with two spatial streams | | 9115AX (I/E) | Wi-Fi 6 (802.11ax), 4x4 DL MU-MIMO with four spatial streams | | 9120AX (I/E/P) | Wi-Fi 6 (802.11ax), 4x4 DL MU-MIMO with four spatial streams | | 9130AX (I/E) | Wi-Fi 6 (802.11ax), 8x8 UL/DL MU-MIMO with eight spatial streams | | 9136 (I) | Wi-Fi 6E (802.11ax), 8x8 UL/DL MU-MIMO with eight spatial streams | | 9162 (I) | Wi-Fi 6E (802.11ax), 2x2 UL/DL MU-MIMO with two spatial streams | | 9164 (I) | Wi-Fi 6E (802.11ax), 4x4 UL/DL MU-MIMO with four spatial streams | | 9166 (I/D1) | Wi-Fi 6E (802.11ax), 4x4 UL/DL MU-MIMO with four spatial streams | | 9124AX (I/D/E) | Wi-Fi 6 (802.11ax), 4x4:4 UL/DL MU-MIMO with four spatial streams | | 9163 (E) | Wi-Fi 6E (802.11ax), 2x2 DL MU-MIMO with two spatial streams | | IW9167 (I/E) | Wi-Fi 6E (802.11ax), 4x4 UL/DL MU-MIMO with four spatial streams | | **Aironet** |  | | 1815 (I/W/M/T) | 802.11ac Wave 2 with 2x2:2 MU-MIMO | | **CISCO LAN** | | | **Model zariadenia** | **Špecifikácia** | | Catalyst C9200L-24P-4G | 24-port full PoE+, 4 x 1G fixed uplinks | | Catalyst C9200L-24T-4G | 24-port data only, 4 x 1G fixed uplinks | | Catalyst C9200L-48P-4G | 48-port full PoE+, 4 x 1G fixed uplinks | | Catalyst C9200L-48T-4G | 48-port data only, 4 x 1G fixed uplinks | | Catalyst C9200L-48PL-4G | 48-port partial PoE+, 4 x 1G fixed uplinks | | Catalyst C9200L-24P-4X | 24-port full PoE+, 4 x 1/10G fixed uplinks | | Catalyst C9200L-24T-4X | 24-port data only, 4 x 1/10G fixed uplinks | | Catalyst C9200L-48P-4X | 48-port full PoE+, 4 x 1/10G fixed uplinks | | Catalyst C9200L-48T-4X | 48-port data only, 4 x 1/10G fixed uplinks | | Catalyst C9200L-48PL-4X | 48-port partial PoE+, 4 x 1/10G fixed uplinks | | Catalyst C9200CX-8P-2X2G | 8-port full PoE+; 2x 1G copper, 2x 10G SFP+ fixed uplinks | | Catalyst C9200CX-12P-2X2G | 12-port PoE+; 2x 1G copper, 2x 10G SFP+ fixed uplinks | | Catalyst C9200CX-12T-2X2G | 12-port data only; 2x 1G copper, 1x 1G CU PD 802.3bt Class 6, 2x 10G SFP+ fixed uplinks | | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU, RPŠ |
| **Používateľ** | | | RPŠ, Škola, NCU, MŠVVaM SR |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | 24/7 |
| **Minimálna Dostupnosť služby** | | | | 99,9% |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1 krát mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Poskytovanie centralizovaného riešenia správy a dohľadu |
| **Definícia** | | Zabezpečovanie služieb nástroja NCU-CRSD podľa definície a jeho GUI, API, služieb exportovania, ochrany, atď pre potrebnú kapacitu pripájaných bodov |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne |
| **Požadovaná hodnota** | **Jednotka** | % |
| **Minimum** | 99,9% |
| **Maximum** | N/A |
| **Severita Nesúladu služby** | | Severita 1 |
| **Metrika 2** | **Názov:** | | Poskytovanie zabezpečeného prístup do NCU-CRSD |
| **Definícia** | | Zabezpečovanie dostatočnej kapacity počtu prístupov používateľom |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne alebo reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Počet |
| **Minimum** | 33% z počtu obsluhovaných lokalít škôl |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Severita 2 |
| **Metrika 3** | **Názov:** | | Poskytovanie zabezpečeného prístup do NCU-CRSD |
| **Definícia** | | Zabezpečovanie dostatočnej kapacity konkurentných prístupov |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne alebo reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Počet |
| **Minimum** | 33% z počtu obsluhovaných lokalít škôl |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Severita 2 |

Tabuľka 13: Poskytovanie služieb centralizovaného riešenia správy a dohľadu NCU (NCU-CRSD) pre potreby RPŠ - detailná definícia požiadaviek na službu

### Zaisťovanie nastavenia globálnych politík LAN/WLAN sietí

| **Zaisťovanie nastavenia globálnych politík LAN/WLAN sietí - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Zaisťovanie nastavenia globálnych politík LAN/WLAN sietí - detailná definícia požiadaviek na službu |
| **Kategória** | | | | Prevádzka sieťových služieb |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Centrálny uzol musí zabezpečiť globálne politiky nastavenia LAN sietí tak, aby boli uniformné pre každého RPŠ. Metodickými usmerneniami a pre NCU- CRSD |
| **Zaisťovanie nastavenia globálnych politík LAN/WLAN sietí - detailná definícia požiadaviek na službu** | | | | |
| **LAN**  Centrálny uzol musí zabezpečiť globálne politiky nastavenia LAN sietí tak, aby boli uniformné pre každého RPŠ. Týmto je zabezpečené jednoduchšie prechádzanie učiteľov medzi jednotlivými školami, ako aj jednoduchšie riešenie prevádzkových problémov, ak nastanú.  Je nevyhnutné nastaviť rozdelenie dátovej prevádzky, pričom ju je potrebné konfigurovať a rozdeliť do rôznych segmentov. To znamená aplikovať špecifické nastavenia pre jednotlivé LAN segmenty nasledujúcim spôsobom:   |  |  | | --- | --- | | **Typ LAN** | **Popis využitia LAN** | | **LAN 1** | **Určená pre pripojenie učiteľov a zamestnancov škôl** | | **LAN 2** | **Určená na pripojenie učební a výpočtovej techniky** | | **LAN 3** | **Určená ako DMZ pre pripojenie serverov a ďalších zariadení** | | **LAN 4** | **Určená pre kritické situácie, ako je vykonávanie eTestov, eMaturít, školských Monitorov, a podobne** |   Nasledujú bližšie popisy jednotlivých LAN segmentov.  LAN 1:  Táto LAN sieť bude slúžiť na pripojenie infraštruktúry slúžiacej pre pedagogický a nepedagogický personál škôl, pričom prístup k nej budú mať iba používatelia s príslušnou pridelenou rolou. Táto sieť bude pre týchto používateľov dostupná aj prostredníctvom WLAN SSID 1. Okrem toho umožní prístup k prostriedkom aj v sieťach LAN 2 a LAN 3, ako aj k digitálnemu edukačnému obsahu v sieti.  LAN 2:  Táto LAN sieť bude slúžiť na pripojenie učební a výpočtovej techniky, ktorá je prístupná aj žiakom. Z tejto siete môžu používatelia pristupovať k vybraným prostriedkom v sieti LAN 3 a k digitálnemu edukačnému obsahu v sieti. Prístup do LAN 2 je regulovaný na základe zaradenia do príslušnej používateľskej role. Táto LAN sieť je dostupná pre pedagogický a nepedagogický personál aj prostredníctvom WLAN SSID 1.  LAN 3:  Táto LAN sieť bude slúžiť ako demilitarizovaná zóna (DMZ) a je navrhnutá tak, aby primárne umožnila pripojenie serverov a zdieľaných zariadení, ktoré budú prístupné všetkým používateľom v LAN 1, LAN 2 a používateľom pripojeným k WLAN sieťam, okrem WLAN SSID 2. Táto LAN sieť bude tiež dostupná pre pedagogický a nepedagogický personál prostredníctvom WLAN SSID 1. Z tejto LAN siete bude možné komunikovať iba s vybranými zdrojmi údajov v sieti DigiNET podľa špecifických požiadaviek, ako sú napríklad aktualizačné servery. DMZ slúži ako ochranná zóna, ktorá zabezpečuje, že externí používatelia môžu pristupovať len k určitým verejným službám bez priameho prístupu k interným zdrojom siete.  LAN 4:  Táto LAN sieť bude slúžiť na pripojenie zariadení, ktoré budú používané počas tzv. kritických situácií a to na vyžiadanie verejným obstarávateľom alebo jeho podliehajúcimi organizáciami, napríklad počas elektronického testovania a iných špecifických potrieb. V normálnom režime nebude táto LAN aktívna.  **WLAN**  Centrálny uzol musí zabezpečiť globálne politiky nastavenia WLAN sietí tak, aby boli uniformné pre každého RPŠ. Týmto je zabezpečené jednoduchšie prechádzanie učiteľov medzi jednotlivými školami, ako aj jednoduchšie riešenie prevádzkových problémov, ak nastanú.  Aby sa dosiahlo pripojenie rovnaké ako pri pevnej LAN, je nevyhnutné dodržať podobné nastavenia a rozdelenie dátovej prevádzky. V rámci tohto riešenia je potrebné konfigurovať a rozdeliť dátovú prevádzku do rôznych sietí, čo v prípade WiFi technológií znamená aplikovať špecifické nastavenia pre jednotlivé SSID nasledujúcim spôsobom:   |  |  | | --- | --- | | **Typ SSID** | **Popis využitia SSID** | | **SSID 1, určené pre prihlásenie žiakov, učiteľov a zamestnancov škôl** | **Ekvivalent k pevnej LAN 1 a LAN 2** | | **SSID 2, pre hostí školy** | **Špeciálny, limitovaný prístup pre návštevníkov škôl** | | **SSID 3, určené pre sieťové tlačiarne** | **Pripojenie tlačiarní a multifunkčných zariadení** | | **SSID 4, pre kritické situácie, ako vykonávanie eTestov, eMaturít, školských Monitorov, a podobne** | **Ekvivalent k pevnej LAN 4** |   Nasledujú bližšie popisy jednotlivých SSID.  SSID 1:  Hlavnou úlohou SSID 1 je zabezpečiť autentifikáciu, autorizáciu a následné pripojenie používateľa k sieti. Autentifikácia sa vykonáva prostredníctvom používateľského mena a hesla. Až po úspešnej autentifikácii a autorizácii sa aplikujú bezpečnostné profily a nastavenia. Tento proces podlieha štandardu 802.1x, čo umožňuje efektívne oddeľovanie a tagovanie používateľov do samostatných VLAN, čím sa zabezpečuje ich transport v sieti na základe predchádzajúcej autentifikácie a autorizácie. Pre plnú funkcionalitu je nevyhnutné, aby boli používatelia po autentifikácii oddeľovaní, resp. označovaní na základe autorizačných profilov.  SSID 2:  Hlavnou úlohou SSID 2 je umožniť pripojenie k sieti a sprístupniť základný rozsah digitálneho vzdelávacieho obsahu. Cieľom tejto siete je poskytnúť žiakom a návštevníkom školy bezpečný prístup k verejne dostupnému digitálnemu vzdelávaciemu obsahu bez potreby autentifikácie a autorizácie. Pri pripojení na toto SSID sa používateľovi zobrazí upozornenie o obmedzenom prístupe k dostupným webovým a iným dátovým službám. Toto SSID môže byť na požiadanie školy na danej lokalite aj deaktivované.  SSID 3:  Hlavnou úlohou SSID 3 je umožniť pripojenie tlačiarní a iných multifunkčných zariadení k sieti v prípadoch, keď nie je možné tieto zariadenia pripojiť priamo pomocou kábla do siete DMZ. Cieľom tejto siete je zabezpečiť bezpečné a pohodlné pripojenie pre zariadenia, ktoré používajú používatelia z rôznych VLAN sietí na danej lokalite. Toto SSID môže byť na žiadosť školy na danej lokalite aj deaktivované a zároveň je tiež možné individuálne nastaviť potrebné prechody medzi VLAN v tejto lokalite.  SSID 4:  Hlavnou úlohou SSID 4 je zabezpečiť autentifikáciu a pripojenie používateľských zariadení k sieti počas tzv. špeciálneho režimu. Toto SSID bude aktívne len na vyžiadanie obstarávateľom alebo jeho podliehajúcimi organizáciami napríklad počas elektronického testovania a iných špecifických potrieb. V normálnom režime nebude toto SSID aktívne. Autentifikácia sa uskutoční pomocou mena a hesla. Aplikácia bezpečnostných profilov a nastavení sa vykoná až po úspešnej autentifikácii a autorizácii používateľa alebo zariadenia. Proces autentifikácie bude prebiehať podľa štandardu 802.1x, rovnako ako pri SSID 1.  **LAN a WLAN – prestupy medzi sieťami LAN/WLAN**  V tejto časti sú zadefinované povolené a zakázané prestupy medzi jednotlivými sieťami v rámci jednej školy.  Definícia povolených a zakázaných prestupov medzi jednotlivými sieťami: | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | RPŠ, Škola, MŠVVaM SR |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | 24/7 |
| **Minimálna Dostupnosť služby** | | | | 99,9% |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Globálne politiky LAN/WLAN sietí |
| **Definícia** | | V súlade s požiadavkami popísaných v definícii služby vyššie |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Reaktívne a Proaktívne |
| **Požadovaná hodnota** | **Jednotka** | boolean |
| **Minimum** | ÁNO v súlade |
| **Maximum** | N/A |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých škôl |

Tabuľka 14: Zaisťovanie nastavenia globálnych politík LAN/WLAN sietí - detailná definícia požiadaviek na službu

### Zabezpečovanie prihlasovania používateľov do siete LAN/WLAN

| **Zabezpečovanie prihlasovania používateľov do siete LAN/WLAN - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Zabezpečovanie prihlasovania používateľov do siete LAN/WLAN **-** |
| **Kategória** | | | | Prevádzka sieťových služieb |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Centrálna implementácia služieb zabezpečujúcich jednotné a bezpečné prihlasovanie používateľov do siete LAN/WLAN v lokalitách škôl s vysokou úrovňou spokojnosti používateľov. |
| **Zabezpečovanie prihlasovania používateľov do siete LAN/WLAN - detailná definícia požiadaviek na službu** | | | | |
| V prostredí siete DigiNET sa bude overovanie používateľov pri prístupe k pevnej sieti LAN realizovať cez protokol 802.1x. Proces zahŕňa overovanie používateľov pristupujúcich cez prvky v správe RPŠ voči serveru umiestneného v Centrálnom uzle prostredníctvom servera RADIUS (Remote Authentication Dial-In User Service) a rovnomenného protokolu. Povinnosťou NCU je v spolupráci s RPŠ zabezpečiť a udržiavať v lokalitách škôl definovaný proces spôsobu riadenia prístupov používateľov k sieti, zabezpečovať homogenitu a kompatibilitu na prvkov vo svojej správe s prvkami RPŠ pre zabezpečovanie týchto služieb  **Postup prihlasovania do pevných sietí LAN:**   1. Používateľ sa pripojí k sieťovej zásuvke RJ45: Po pripojení počítača do LAN siete pomocou ethernetového kábla sa spustí proces autentifikácie cez 802.1x. 2. Žiadosť o overenie: prepínač, ku ktorému je používateľ pripojený pošle žiadosť o overenie identity do RADIUS servera NCU DigiNET. 3. RADIUS server obdrží žiadosť a preverí identitu používateľa voči serveru, kde sú uložené všetky autentifikačné údaje. 4. Povolenie alebo odmietnutie prístupu: Ak je autentifikácia úspešná, prepínač povolí prístup používateľa do siete a nakonfiguruje port do správnej siete VLAN. Ak autentifikácia zlyhá, prístup je zamietnutý.   V prostredí siete DigiNET sa bude overovanie používateľov pri prístupe k bezdrôtovej sieti WLAN realizovať cez protokol 802.1x. Proces zahŕňa overovanie používateľov pristupujúcich cez prvky v správe RPŠ voči serveru umiestneného v Centrálnom uzle prostredníctvom servera RADIUS (Remote Authentication Dial-In User Service) a rovnomenného protokolu.  **Postup prihlasovania do bezdrôtových sietí WLAN:**   1. Používateľ sa pripojí k WLAN: Keď sa používateľ pokúsi pripojiť k WLAN sieti, jeho zariadenie (napr. notebook, telefón alebo tablet) vyšle žiadosť o overenie. 2. Žiadosť o overenie: WLAN prístupový bod pošle žiadosť o overenie identity do RADIUS servera Centrálneho uzla DigiNET. 3. RADIUS server obdrží žiadosť a preverí identitu používateľa voči LDAP serveru, kde sú uložené všetky autentifikačné údaje. 4. Povolenie alebo odmietnutie prístupu: Ak je autentifikácia úspešná, prepínač povolí prístup používateľa do siete a nakonfiguruje port do správnej siete VLAN. Ak autentifikácia zlyhá, prístup je zamietnutý. | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | Škola |
| **Iné zainteresované strany** | | | RPŠ |
| **Prevádzková doba** | | | | 24/7 |
| **Minimálna Dostupnosť služby** | | | | 99,9% |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Zabezpečovanie prihlasovania používateľov do siete LAN/WLAN |
| **Definícia** | | V súlade s požiadavkami popísaných v definícii služby vyššie |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne |
| **Požadovaná hodnota** | **Jednotka** | boolean |
| **Minimum** | ÁNO je zabezpečovaná |
| **Maximum** | N/A |
| **Severita nesúladu služby** | | Podľa rozsahu postihnutých škôl |

Tabuľka 15: Zabezpečovanie prihlasovania používateľov do siete LAN/WLAN - detailná definícia požiadaviek na službu

### Prevádzka služieb vzdialeného pripojenia

| **Prevádzka služieb vzdialeného pripojenia - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Prevádzka služieb vzdialeného pripojenia |
| **Kategória** | | | | Prevádzka sieťových služieb |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Zabezpečovanie služieb vzdialeného prístupu pre používateľov |
| **Prevádzka služieb vzdialeného pripojenia - detailná definícia požiadaviek na službu** | | | | |
| Verejný obstarávateľ požaduje, aby vybraný uchádzač technicky zabezpečil bezpečný vzdialený prístup pre používateľov siete DigiNET do internej siete školy (remote access VPN).  V rámci zabezpečovania služieb Centrálneho uzla DigiNET verejný obstarávateľ očakáva, že vybraný dodávateľ poskytuje prevádzku komplexných služieb v súvislosti so zabezpečením vzdialeného prístupu užívateľov siete DigiNET, a to najmä:   * Centrálne overovanie užívateľov totožné s overovaním pri pripájaní do LAN a WLAN sietí * Klientska časť VPN riešenia musí byť kompatibilná s OS Windows, Mac OS a Linux * Klientska časť VPN riešenia musí byť kompatibilná s mobilným OS Android a iOS   Pripojený používateľ musí mať prístup iba na explicitne povolené ciele v rámci internet siete DigiNET | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | Škola |
| **Iné zainteresované strany** | | | RPŠ |
| **Prevádzková doba** | | | | 24/7 |
| **Minimálna Dostupnosť služby** | | | | 99,9% |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Prevádzka služieb vzdialeného pripojenia |
| **Definícia** | | V súlade s požiadavkami popísaných v definícii služby vyššie |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne alebo reaktívne |
| **Požadovaná hodnota** | **Jednotka** | boolean |
| **Minimum** | ÁNO je zabezpečovaná |
| **Maximum** | N/A |
| **Severita nesúladu služby** | | Podľa rozsahu postihnutých škôl |

Tabuľka 16: Prevádzka služieb vzdialeného pripojenia - detailná definícia požiadaviek na službu

### Prevádzka služieb pripojenia lokalít škôl k NCU a služby CPE

| **Prevádzka služieb pripojenia lokalít škôl k NCU a služby CPE - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Prevádzka služieb pripojenia lokalít škôl k NCU a služby CPE |
| **Kategória** | | | | Prevádzka sieťových služieb |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Pripájanie lokalít škôl k sieti DigiNET |
| **Prevádzka služieb pripojenia lokalít škôl k NCU a služby CPE - detailná definícia požiadaviek na službu** | | | | |
| Pripojenie školskej lokality do siete digiNET sa realizuje prostredníctvom CPE zariadenia, ktorého typ definuje, zabezpečuje a distribuuje dodávateľ riešenia Národného Centrálneho uzla tak, aby bolo plne kompatibilné a integrovateľné s riešením Národného Centrálneho uzla. Z hľadiska funkcionality musí byť zvolené CPE schopné zabezpečiť:   * smerovanie dátovej prevádzky do Národného Centrálneho uzla, * vytvorenie šifrovaného tunela (na úrovni protokolu AES256 alebo ekvivalentného) do Centrálneho uzla DigiNET, kde musí byť tento tunel ukončovaný na koncentrátore VPN, * základnú sieťovú bezpečnosť v rámci lokality (zabezpečiť prístup na implementované zariadenia v lokalite, zakázanie nepotrebných služieb ako sú ident, finger, MOP, PAD, TCP a UDP small servers, implementácia VLAN sietí v rámci lokality a filtrov na zamedzenie/reštrikciu komunikácie medzi nimi, implementácia BPDU a STP Root Guard), * Zabezpečovať „otvorenosť“ riešenia pre zabezpečený prístup RPŠ k lokalite školy potrebný pre zabezpečovanie služieb a prevádzku LAN/WLAN služieb škole * QoS podľa typy aplikácie, * DHCP server / relay pre lokálnych používateľov.   CPE je centrálne spravované z Centrálneho uzla a úzko integrované s celým riešením.  Z hľadiska parametrov CPE požaduje verejný obstarávateľ podporu minimálne:   * Rozhrania: minimálne 2 WAN RJ45 rozhrania (pripojenie voči sieti RPŠ) a 2 LAN rozhrania RJ45 smerom do infraštruktúry školy s podporovanými priepustnosťami do 1Gbps na rozhranie * Požadovaná minimálna priepustnosť smerovača musí zodpovedať minimálne požadovanej rýchlosti pripojenia lokality počas celého definovaného obdobia poskytovania služieb, minimálne po dobu 5 rokov * Podpora stavového firewallu a ACL * Požadovaná je podpora nasadenia firewallu v režime smerovania * Požadovaná je podpora nasadenia firewallu v režime transparentného L2 bridge * Požadovaný minimálny počet súčasných spojení cez firewall je 500.000 * Požadovaný minimálny počet nových spojení cez firewall za sekundu je 25.000 * Podpora statického a dynamického smerovania s protokolmi OSPF a BGP * Podpora protokolov IPv4 a IPv6 * Podpora DHCP klient, DHCP server a DHCP relay na minimálne 20 virtuálnych sieťach * Požadovaná je podpora pre preklad adries NAT * Podpora site-to-site IPSec pre minimálne 2 paralelne zostavené tunely s priepustnosťou do maximálnej rýchlosti konkrétnej školy * Podpora 802.1q a minimálny počet VLAN 20 * Požadovaný minimálny počet VPN spojení je 8 * Podpora SNMPv3, Syslog, RADIUS * Podpora NetFlow * Podpora MAC filtering * Podpora Port Security * Podpora automatickej detekcia MDI/MDIX * Podpora pre mechanizmy QoS (DiffServ, LLQ, WFQ, CBWFQ, mapovanie CoS-DSCP) * Formát montovateľný do 19“ rozvádzača * Aktualizácie a správa: CPE je spravovateľné z Centrálneho uzla a umožňuje automatizovaný upgrade softvéru   Úvodnú konfiguráciu zabezpečuje dodávateľ riešenia Centrálneho uzla DigiNET, či už prostredníctvom predkonfigurovania konkrétneho kusu CPE, alebo vlastným riešením Zero Touch Provisioningu (ZTP) tak, aby RPŠ po správnom pripojení CPE na lokalite nemusel realizovať žiadne ďalšie konfiguračné zásahy na CPE. | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | Škola, RPŠ |
| **Iné zainteresované strany** | | | RPŠ |
| **Prevádzková doba** | | | | 24/7 |
| **Minimálna Dostupnosť služby** | | | | 99,9% |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Prevádzka služieb CPE |
| **Definícia** | | V súlade s požiadavkami popísaných v definícii služby vyššie |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne |
| **Požadovaná hodnota** | **Jednotka** | boolean |
| **Minimum** | ÁNO je zabezpečovaná |
| **Maximum** | N/A |
| **Severita nesúladu služby** | | Severity 1 |
| **Merateľné parametre** | **Metrika 2** | **Názov:** | | Priepustnosť |
| **Definícia** | | Priepustnosť minimálne na požadovanej rýchlosti pripojenia lokality počas celého definovaného obdobia poskytovania služieb, počas celej doby prevádzky |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne |
| **Požadovaná hodnota** | **Jednotka** | % |
| **Minimum** | 99,9 |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Severity 1 |

Tabuľka 17: Prevádzka služieb pripojenia lokalít škôl k NCU a služby CPE - detailná definícia požiadaviek na službu

### Prepájanie na Dátové centrum rezortu školstva

| **Prepájanie na Dátové centrum rezortu školstva - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Prepájanie na Dátové centrum rezortu školstva |
| **Kategória** | | | | Prevádzka sieťových služieb |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Prepájanie na Dátové centrum rezortu školstva pre zabezpečovanie prístupu k centrálnemu obsahu |
| **Prepájanie na Dátové centrum rezortu školstva - detailná definícia požiadaviek na službu** | | | | |
| Dátové centrum rezortu školstva poskytuje aplikácie a digitálny obsah pre školy, zabezpečuje testovanie. Verejný obstarávateľ požaduje, aby Dátové centrum rezortu školstva bolo pripojené do virtuálnej privátnej siete DigiNET minimálne prístupom 10Gbps, rozšíriteľným na 2x 10Gbps. | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | Škola, RPŠ |
| **Iné zainteresované strany** | | | RPŠ |
| **Prevádzková doba** | | | | pracovné dni 6:00 – 18:00 |
| **Minimálna Dostupnosť služby** | | | | 99,9% |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Priepustnosť |
| **Definícia** | | Priepustnosť na požadovanej rýchlosti |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | proaktívne |
| **Požadovaná hodnota** | **Jednotka** | % |
| **Minimum** | 99,9 |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých škôl |

Tabuľka 18: Prepájanie na Dátové centrum rezortu školstva - detailná definícia požiadaviek na službu

### RACI matica pre sieťové služby

| **Popis činnosti** | **Škola** | **RPŠ** | **NCU** | **MŠVVaM** |
| --- | --- | --- | --- | --- |
| Dodržiavanie požadovanej hodnoty merateľného parametra: Čas potrebný na pripojenie klienta WiFi na prvkoch v pôsobnosti RPŠ | I | A,R | C | I |
| Dodržiavanie požadovanej hodnoty merateľného parametra: Čas potrebný na pripojenie klienta WiFi na prvkoch v pôsobnosti NCU | I | C | A,R | I |
| Odstraňovanie nedostatkov identifikovaných na strane školy | A,R | C | I | I |
| Odstraňovanie nedostatkov identifikovaných na strane RPŠ | C | A,R | I | I |
| Odstraňovanie nedostatkov identifikovaných na strane NCU | C | I | A,R | I |
| Odstránenie cudzieho zariadenia spôsobujúceho nameranú interferenciu v priestoroch školy | A,R | C | I | N/A |
| Konfigurácia, správa a údržba prvkov riešenia NCU | I,C | C | A,R | N/A |
| Identifikácia, odstraňovanie a náprava bezpečnostných hrozieb, nedostatkov a incidentov v riešení v pôsobnosti NCU | I | A,R | C | I |
| Dodanie CPE na centrálny sklad NCU a zapečenie potrebných kusov na distribúciu pre RPŠ, distribúcia na RPŠ v požadovanom počte, vrátane náhradných dielov | N/A | C | A,R | N/A |
| Dodanie CPE do lokality, Inštalácia CPE v centrálnom rozvádzači a napájanie CPE a pripojenie CPE na škole | I | A,R | C | N/A |
| Konfigurácia a správa CPE | I,C | C | A,R | N/A |
| Sprevádzkovanie a oživenie CPE a WAN |  | A,R | R |  |
| IP adresácia CPE – spolupráca pri prideľovaní adresného priestoru |  | R | A |  |

Tabuľka 19: RACI pre sieťové služby

## Služby monitoringu NCU

### Poskytovanie služieb monitoringu NCU

| **Poskytovanie služieb monitoringu NCU - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Poskytovanie služieb monitoringu NCU - detailná definícia požiadaviek na službu |
| **Kategória** | | | | Služby monitoringu NCU |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Monitoring aktívnych prostriedkov zabezpečujúcich prevádzku služieb siete DigiNET musí umožňovať sledovanie stavu jednotlivých prostriedkov, ich aktuálnych vlastností a stavu vyťaženia. Tieto údaje musia byť použiteľné na detekciu stavu služby, resp. identifikáciu a následnú nápravu vzniknutých problémov. |
| **Prevádzka služieb vzdialeného pripojenia - detailná definícia požiadaviek na službu** | | | | |
| Monitoring je službou, ktorá je využívaná pre zabezpečenie nasledujúcich požiadaviek na centrálny uzol:   * monitoring všetkých aktívnych zariadení v centrálnom uzle * monitoring všetkých aktívnych CPE zariadení v rámci služieb lokálnej infraštruktúry škôl * korelácie udalostí z jednotlivých aktívnych zariadení v sieti centrálneho uzla a v rámci lokálnej infraštruktúry škôl z pohľadu CPE zariadení * správu zoznamu zariadení   V rámci služieb tejto časti riešenia sú zahrnuté všetky služby súvisiace s monitorovaním a dohladovaním služieb CPE na lokalitách školských zariadení. V rámci centrálneho monitoringu sa od navrhnutého riešenia očakávajú nasledovné funkcionality z pohľadu lokality školského zariadenia:   * centrálny monitoring dostupnosti služieb CPE na lokalitách školských zariadení * centrálny monitoring dostupnosti služieb prístupu k sieti DigiNET na lokalitách školských zariadení * centrálny monitoring kvality služieb CPE na lokalitách školských zariadení * centrálny monitoring kvality služieb prístupu k sieti DigiNET na lokalitách školských zariadení   Centrálny monitoring musí poskytovať všeobecný prehľad o aktuálnom stave lokalít a služieb v lokalitách, v kombinácii so základnými notifikačnými prvkami ako poslanie notifikačného emailu / SMS kontaktnej osobe pre vybranú lokalitu, prípadne zasielanie hromadných notifikácií pri výpadkoch s väčším plošným dopadom (napr. výpadok konektivity v okrese/kraji…).  Jednotlivé časti centrálneho monitoringu služieb na lokalitách školských zariadení budú slúžiť na zabezpečenie kontinuálneho procesu výuky žiakov a pre služby súvisiace s prevádzkou školského zariadenia. Výstupy z centrálneho monitoringu budú zároveň podkladom pre analýzy a redizajn služieb za účelom neustáleho zvyšovania kvality služieb, ako aj pre aplikáciu nastavení, ktoré zabezpečia rovnaké nediskriminačné podmienky pre využívanie služieb pre jednotlivé kategórie užívateľov.  Centrálny monitoring CPE zariadení na lokalitách verejného obstarávateľa musí zabezpečovať:   * implementáciu koncových zariadení CPE do monitorovacieho systému Poskytovateľa, * sledovanie management nástrojov jednotlivých komponentov riešenia, * proaktívne riešenie vznikajúcich problémov, * read-only SNMP prístup na CPE zariadenia na splnenie podmienky vzdialenej diagnostiky, * konfiguračný management pre tieto zariadenia, zmena konfigurácie na požiadanie, * dohľad dostupnosti konektivity všetkých koncových bodov, * o vzniknutých problémoch súvisiacich s poskytovaním služieb týkajúcich sa verejného obstarávateľa, resp. lokalít musí úspešný uchádzač informovať verejného obstarávateľa minimálne raz mesačne formou reportov a adhoc formou štruktúrovaných emailov, * v prípade výpadku služieb CPE je povinný informovať oprávnenú osobu školy.   Poskytovateľ služieb NCU môže za účelom zefektívnenia prevádzkovej činnosti a riešenia udalostí v sieti využiť prístup do centralizovaného riešenia správy a dohľadu (CRSD) od RPŠ. CRSD nie je v tomto prípade zabezpečované samotným NCU tzv. NCU-CRSD.  V prípade že v pripájanej lokalite k službám NCU nie sú zabezpečované služby RPŠ (lokalita bez RPŠ), vykonáva poskytovateľ služieb NCU len tie relevantné požiadavky na služby monitoringu, ktoré sú výhradne v rozsahu jeho zodpovednosti. | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | NCU, MŠVVaM SR |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | 24/7 |
| **Minimálna Dostupnosť služby** | | | | 99,9% |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Poskytovanie centralizovaného riešenia správy a dohľadu |
| **Definícia** | | V súlade s požiadavkami popísaných v definícii služby vyššie |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne alebo reaktívne |
| **Požadovaná hodnota** | **Jednotka** | boolean |
| **Minimum** | ÁNO je zabezpečovaná |
| **Maximum** | N/A |
| **Severita nesúladu služby** | | N/A |

Tabuľka 20: Poskytovanie služieb monitoringu NCU - detailná definícia požiadaviek na službu

### RACI matica pre služby monitoringu NCU

| **Popis činnosti** | **Škola** | **RPŠ** | **NCU** | **MŠVVaM** |
| --- | --- | --- | --- | --- |
| Monitorovanie napĺňania kritérií a požiadaviek služieb DigiNET | I | R | A,R | I |
| Merania napĺňania kritérií a požiadaviek služieb RPŠ | I | R | A | I |
| Poskytovanie parametrov služieb RPŠ pre NCU | N/A | R | A | I |
| Škola je povinná akceptovať dočasné prerušenie WAN konektivity v čase vykonávania mimoriadneho intruzívneho merania | A,R | N/A | N/A | N/A |
| Vykonávanie intruzívneho merania WAN konektivity | C,I | A,R | C,I | N/A |
| V prípade že bude objednaná - Prevádzka a monitoring systémov pre poskytovanie služieb centralizovaného riešenia správy a dohľadu poskytovaná RPŠ prostredníctvom služieb NCU-CRSD |  | C,I | A,R |  |

Tabuľka 21: RACI matica pre služby monitoringu NCU

## Služby Reportingu

Prevádzka služieb reportingu poskytuje komplexné správy a analýzy týkajúce sa výkonu siete, stavu zariadení, používaní siete klientami a kvality poskytovaných služieb. NCU odovzdáva reporty MŠVVaM SR na určenú sieťovú lokalitu v požadovanom formáte podľa metodického usmernenia Ministerstva.

Všetky požadované reporty musí NCU pripraviť za daný kalendárny mesiac najneskôr do termínu špecifikovaného nižšie Verejný obstarávateľ má právo vyžiadať si ďalšie reporty konsolidovaných dát aj mimo pravidelný interval generovania reportov.

V prípade že v pripájanej lokalite k službám NCU nie sú zabezpečované služby RPŠ (lokalita bez RPŠ) zabezpečuje poskytovateľ služieb NCU len tie relevantné požiadavky na služby reportingu, ktoré sú výhradne v rozsahu jeho zodpovednosti.

### Vytváranie reportu dostupnosti a kvality služieb DigiNET

| **Vytváranie správy o dostupnosti a kvality služieb - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Report dostupnosti a kvality služieb DigiNET |
| **Kategória** | | | | Služby reportingu |
| **Typ** | | | | Pravidelná |
| **Cieľ** | | | | Súhrnná správa slúži na kontrolu plnenia SLA a výkone služieb Service desku. |
| **Vytváranie správy o dostupnosti a kvality služieb - detailná definícia požiadaviek na službu** | | | | |
| **NCU vypracuje mesačné report dostupnosti a kvality služieb, ktorý budú obsahovať:**   * report o dostupnosti a kvalite služieb NCU * konsolidovať reportov RPŠ zo sietí a služieb RPŠ * spolupracovať s RPŠ pri príprave reportov a obstarávateľ odporúča NCU v maximálnej miere automatizovať generovanie konsolidovaných reportov. Rovnako je cieľom aby mal NCU dostatočné informácie o službách a ich kvalite. * centrálny reporting dostupnosti a kvality služieb prístupu k sieti DigiNET na lokalitách školských zariadení * reporting dostupnosti a kvality služieb prístupu k sieti Internet * reporting dostupnosti a kvality služieb prístupu k zdrojom MŠVVaM SR * reporting dostupnosti a kvality služieb centrálneho uzla DigiNET   **Požadované sú reporty dostupnosti poskytovaných služieb vyjadrené v percentách a reporty kvality poskytovaných služieb vyjadrené v utilizácii dodávaných prenosových kapacít, resp. v utilizácii maximálnych hardwarových alebo licenčných limitov.**   * NCU vypracuje všetky požadované reporty dostupnosti a kvality služieb a odovzdá ich MŠ najneskôr v piaty pracovný deň nasledujúceho mesiaca po skončení príslušného zúčtovacieho obdobia. Formát v akom budú reporty odovzdávané špecifikuje MŠ. Report bude obsahovať aj posúdenie zhody s požadovanými hodnotami parametrov a dostupnosti. * V prípade nedodržania parametra dostupnosti ku ktorému sú dohodnuté pokuty NCU vypočíta a uvedie aj príslušnú pokutu. V prípade nedodržania parametra pre službu Riešenia incidentov, nesúlad sa vypočítava na základe časov podľa ticketov v centrálnom portály riadenia ticketov prevádzkovaného poskytovateľom služieb NCU. * MŠ reporty skontroluje a zašle prípadné pripomienky najneskôr 8. pracovný deň nasledujúceho mesiaca po skončení príslušného zúčtovacieho obdobia NCU. V prípade že najneskôr 8. pracovný deň nasledujúceho mesiaca po skončení príslušného zúčtovacieho obdobia NCU nedostane pripomienky, považuje sa report za schválený.   Poskytovateľ NCU je zodpovedný za kontrolu parametrov služieb celej siete DigiNET, v prípade nedodržiavania kvalitatívnych parametrov je povinný oznamovať MŠVVaM SR nesúlad služieb DigiNET s požiadavkami v opise predmetu zákazky na služby NCU a RPŠ. Pre tento účel využíva reporty RPŠ a informácie o ticketoch. | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | Škola, NCU, MŠVVaM SR |
| **Iné zainteresované strany** | | | RPŠ |
| **Prevádzková doba** | | | | 24/7 |
| **Minimálna Dostupnosť služby** | | | | 99,9% |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Dostupnosť reportov |
| **Definícia** | | Príprava a zaslanie reportu podľa požiadaviek na službu |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Počet |
| **Minimum** | 1x mesačne |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Eskalácie |

Tabuľka 22: Vytváranie správy o dostupnosti a kvality služieb - detailná definícia požiadaviek na službu

### Vytváranie správy o výkone Service Desku a plnení SLA

| **Vytváranie správy o výkone Service Desku a plnení SLA - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Vytváranie správy o výkone Service Desku a plnení SLA |
| **Kategória** | | | | Služby reportingu |
| **Typ** | | | | Pravidelná |
| **Cieľ** | | | | Súhrnná správa slúži na kontrolu plnenia SLA a výkone služieb Service desku. |
| **Vytváranie správy o výkone Service Desku a plnení SLA - detailná definícia požiadaviek na službu** | | | | |
| **NCU vypracuje mesačné report služieb Service Desk a plnenia SLA, ktorý budú obsahovať:**   * Prehľad ticketov pre servisných prípadov v zodpovednosti NCU * Zoznam ticketov NCU pri ktorých bolo porušené SLA * Výpočet pokút za nedodržanie SLA * Manažérske zhrnutie prevádzky NCU plnenie SLA   **Report kvality služieb prevádzky**   * NCU vypracuje všetky požadované reporty a odovzdá ich MŠ najneskôr v piaty pracovný deň nasledujúceho mesiaca po skončení príslušného zúčtovacieho obdobia. Formát v akom budú reporty odovzdávané špecifikuje MŠ. Report bude obsahovať aj posúdenie zhody s požadovanými hodnotami parametrov a dostupnosti. * V prípade nedodržania parametra dostupnosti ku ktorému sú dohodnuté pokuty NCU vypočíta a uvedie aj príslušnú pokutu. V prípade nedodržania parametra pre službu Riešenia incidentov, nesúlad sa vypočítava na základe časov podľa ticketov v centrálnom portály riadenia ticketov prevádzkovaného poskytovateľom služieb NCU. * MŠ reporty skontroluje a zašle prípadné pripomienky najneskôr 8. pracovný deň nasledujúceho mesiaca po skončení príslušného zúčtovacieho obdobia NCU. V prípade že najneskôr 8. pracovný deň nasledujúceho mesiaca po skončení príslušného zúčtovacieho obdobia NCU nedostane pripomienky, považuje sa report za schválený. | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | Škola, NCU, MŠVVaM SR |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | 24/7 |
| **Minimálna Dostupnosť služby** | | | | 99,9% |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Dostupnosť reportov |
| **Definícia** | | Príprava a zaslanie reportu podľa požiadaviek na službu |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Počet |
| **Minimum** | 1x mesačne |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Eskalácie |

Tabuľka 23: Vytváranie správy o výkone Service Desku a plnení SLA - detailná definícia požiadaviek na službu

### Vytváranie správy o stave sieťovej bezpečnosti

| **Vytváranie správy o stave sieťovej bezpečnosti - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Report o stave sieťovej bezpečnosti |
| **Kategória** | | | | Služby reportingu |
| **Typ** | | | | Pravidelná |
| **Cieľ** | | | | Súhrnná správa slúži na kontrolu plnenia služieb sieťovej bezpečnosti |
| **Vytváranie správy o stave sieťovej bezpečnosti - detailná definícia požiadaviek na službu** | | | | |
| NCU vypracúva mesačné report dostupnosti a kvality služieb, ktorý obsahuje:   * početnosť zaznamenaných a odvrátených útokov na sieť DigiNET, * početnosť zablokovaných rizikových aplikácií, malwareov, spywareov, botnetov, vírusov, podvodných webstránok, * početnosť zablokovaných a povolených pokusov o prístup na webové lokality zobrazená v čase, * TOP 20 blokovaných webových kategórií, * TOP 10 blokovaných podvodných webových lokalít, vírusov, malwareov, * TOP 10 zablokovaných pokusov o prienik do siete DigiNET (názov a typ zraniteľnosti, kritikalita, početnosť), * štatistiky systému IPS podľa kritikality vyjadrené v čase. | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | Škola, NCU, MŠVVaM SR |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | 24/7 |
| **Minimálna Dostupnosť služby** | | | | 99,9% |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Dostupnosť reportov |
| **Definícia** | | Príprava a zaslanie reportu podľa požiadaviek na službu |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Počet |
| **Minimum** | 1x mesačne |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Eskalácie |

Tabuľka 24: Vytváranie správy o stave sieťovej bezpečnosti - detailná definícia požiadaviek na službu

### Vytváranie správy o prevádzke sieťových služieb

| **Vytváranie správy o prevádzke sieťových služieb - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Vytváranie správy o prevádzke sieťových služieb |
| **Kategória** | | | | Služby reportingu |
| **Typ** | | | | Pravidelná |
| **Cieľ** | | | | Súhrnná správa slúži na kontrolu prevádzky sieťových služieb |
| **Vytváranie správy o prevádzke sieťových služieb - detailná definícia požiadaviek na službu** | | | | |
| **NCU vypracuje mesačné report prevádzky sieťových služieb, ktorý bude obsahovať:**   * objemy prenesených dát v prichádzajúcom aj odchádzajúcom smere na WAN rozhraní v čase, po školách * objemy prenesených dát v jednotlivých LAN segmentoch, celkovo a po školách * objemy prenesených dát v jednotlivých WLAN segmentoch, celkovo a po školách * TOP 100 SSID podľa prenesených dát * TOP 100 SSID podľa počtu pripojených klientov * TOP 100 WiFi prístupových bodov podľa prenesených dát (AP, škola, objem dát) * TOP 100 WiFi prístupových bodov podľa priemerného počtu pripojených klientov (AP, škola, počet) * TOP 100 WiFi prístupových bodov podľa maximálneho počtu pripojených klientov (AP, škola, počet) * TOP 100 používateľov podľa prenesených dát (škola, zdroj, objem dát) * TOP 10 aplikácií podľa prenesených dát * TOP 10 operačných systémov podľa prenesených dát * TOP 10 operačných systémov podľa počtu pripojených klientov | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | Škola, NCU, MŠVVaM SR |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | 24/7 |
| **Minimálna Dostupnosť služby** | | | | 99,9% |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Dostupnosť reportov |
| **Definícia** | | Príprava a zaslanie reportu podľa požiadaviek na službu |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Počet |
| **Minimum** | 1x mesačne |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Eskalácie |

Tabuľka 25: Vytváranie správy o prevádzke sieťových služieb - detailná definícia požiadaviek na službu

### RACI matica pre služby reportingu NCU

| **Popis činnosti** | **Škola** | **RPŠ** | **NCU** | **MŠVVaM** |
| --- | --- | --- | --- | --- |
| Reportovanie napĺňania kritérií a požiadaviek služieb RPŠ | I | R | A | I |
| Reportovanie napĺňania kritérií a požiadaviek služieb NCU | I | C | A | I |
| Poskytovanie parametrov pre NCU reporting | N/A | R | A | I |
| Definovanie štruktúry reportov | N/A | C | A,R | C |
| Príprava reportov v požadovanej štruktúre | N/A | A,R | C | N/A |
| Zasielanie reportov do NCU podľa požadovanej štruktúry do požadovaného adresára | N/A | R | A | C |
| Poskytovanie rozhrania pre NCU na zber dát pre reportovanie | N/A | A,R | C | C |
| Schvaľovanie reportov | I | I | A,R | R |

Tabuľka 26: RACI matica pre služby reportingu NCU

## Služby Prevádzkovej podpory, NCU Service Desk a SOC

Prevádzkovú podporu koordinuje NCU v spolupráci s RPŠ a školami, prevažne prostredníctvom Service desku NCU. Hlavnou úlohou Service desku je prijímať, spracovávať a riešiť požiadavky a problémy používateľov týkajúce sa služieb siete škôl.

Udalosti sú vo forme ticketov ako prvý kontakt s používateľmi zaznamenávané a riadené v centrálnom ticketing portály (CTP) ktorý prevádzkuje NCU Service Desk. NCU Service Desk je centrálnym bodom, ktorý poskytuje okrem iných služieb aj centrálnu podporu používateľom siete ako prvý bod kontaktu a centrálny nástroj pre riadenie a evidenciu udalostí. Jeho hlavnou úlohou je prijímať, spracovávať a riešiť požiadavky, otázky a problémy používateľov v súvislosti s prevádzkou služieb siete.

V prípade že v pripájanej lokalite k službám NCU nie sú zabezpečované služby RPŠ (lokalita bez RPŠ) vykonáva poskytovateľ služieb NCU len tie relevantné služby Prevádzkovej podpory, NCU Service Desk a SOC, ktoré sú výhradne v rozsahu jeho zodpovednosti a to podľa definície požiadaviek a parametrov:

* Poskytovanie služieb centrálneho NCU Service Desk
* Riešenie incidentov NCU
* Poskytovanie služieb SOC
* Ďalšie služby NCU Service Desk

### Poskytovanie služieb centrálneho NCU Service Desk pre sieť DigiNET

Service Desk je centrálnym bodom, ktorý poskytuje podporu používateľom školskej siete DigiNET, RPŠ a MŠVVaM SR. Jeho hlavnou úlohou je prijímať, spracovávať a riešiť, resp. distribuovať na regionálnych partnerov (RPŠ) požiadavky, otázky a problémy používateľov v súvislosti s prevádzkou školskej siete a riešiť incidenty a problémy.

Služby NCU Service Desku sú najmä nasledovné:

* prevádzka CTP a sprístupnenie pre RPŠ
* správa a evidencia priebehu riešenia udalostí, incidentov, problémov prostredníctvom ticketov v CTP,
* riadenie incidentov,
* riadenie žiadostí o služby a informácie,
* riadenie problémov,
* riadenie zmien,
* správa znalostí,
* logovanie,
* reporting a výpočet kreditov za nedodržanie SLA,
* správu plánovaných prác a výpadkov,
* eskalácia podľa dohodnutých eskalačných postupov,
* technická podpora pre NCU,
* služby SOC.

Detailnejší popis požiadaviek je uvedený nižšie.

Na riešení incidentov sa podieľa NCU aj RPŠ podľa toho, v koho kompetencii je identifikovaná príčina nesúladu.

Verejný obstarávateľ požaduje, aby bola služba Service Desku poskytovaná odo dňa pripojenia prvej lokality do siete DigiNET.

| **Poskytovanie služieb centrálneho NCU Service Desk pre sieť DigiNET - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Poskytovanie služieb centrálneho NCU Service Desk pre sieť DigiNET |
| **Kategória** | | | | Služby Prevádzkovej podpory, NCU-Service Desk a SOC |
| **Typ** | | | | Ad-hoc |
| **Cieľ** | | | | Služby prevádzkovej podpory sú koordinované a poskytovaná najmä prostredníctvom operačného strediska NCU Service Desk. Jeho hlavnou úlohou je prijímať, spracovávať a riešiť požiadavky, otázky a problémy používateľov v súvislosti s prevádzkou služieb siete. |
| **Poskytovanie služieb centrálneho NCU Service Desk pre sieť DigiNET - detailná definícia požiadaviek na službu** | | | | |
| NCU prevádzkuje službu správy a evidencie priebehu riešenia udalostí, incidentov, problémov v reálnom čase prostredníctvom ticketov využívaním CTP. CTP je webový nástroj prístupný cez štandardný webový prehliadač. NCU zabezpečí pre RPŠ prístupy do nástroja CTP v dostatočnej kapacite podľa požiadaviek RPŠ  NCU vystaví API na ktoré sa môže RPŠ integrovať pre implementáciu automatizácie preberania a aktualizácie ticketov z vlastného nástroja.  NCU poskytne dokumentáciu rozhrania, stavov ticketov a ich prechodov a poskytne integračnú podporu RPŠ.  CTP umožňuje:   * zadanie udalosti Centrálnym uzlom, samotným RPŠ, oprávnenou osobou školy, ministerstvom * kategorizácia udalosti, * informácie o stave udalosti, riešení, aktivitách a uzavretí, * informácia o stave pridelenie riešenia udalosti (NCU, ktorý RPŠ) * tvorbu reportov na požiadanie užívateľom, * filtrovanie ticketov podľa rôznych kritérií (čas, typ, kategória, oblasť, škola, typ zariadenia, stav atď...) * komentovanie priebehu riešenia udalosti, zmena stavu a časove stopy každej zmeny, * sledovanie stavu riešenia ticketu v reálnom čase pre školu, MŠ a RPŠ * ďalšie primerané funkcie a parametre podľa potrieb.   Služby NCU Service desku prevádzky sú poskytované v Slovenskom jazyku.  Každá udalosť je zaevidovaná v CTP a pridelené jej číslo ticketu, pod ktorým bude zaznamenaný celý priebeh riešenia. Udalosť môže vzniknúť:   * nahlásením na centrálny portál NCU Service Desk, * automaticky/proaktívne RPŠ alebo NCU (napr. automatickou detekciou výpadku, proaktívny monitoring), * manuálne operátorom RPŠ, manuálne operátorom NCU.   Po zaevidovaní udalosti, ju operátor Service desku klasifikuje (ak už nebol klasifikovaný operátorom RPŠ – Service Desk) a začne riešiť v zmysle dohodnutého postupu. Udalosť môže byť klasifikovaná ako:   * incident, * problém, * žiadosť o informáciu, * žiadosť o zmenu, * plánovaný výpadok * iná požiadavka.   Povinnosťou NCU je okrem prevádzkovania služieb CTP, prijímať, zadávať a aktualizovať udalosti z a do centrálneho ticketing portálu.  V prípade nahlasovania udalosti telefonicky je poskytovateľ NCU povinný prevziať hovor do 30s v 90% nahlasovaných udalostí.  V prípade že operátor NCU Service desku počas kategorizácie zistí že riešenie je v pôsobnosti RPŠ, nastaví v CTP príslušný príznak a v riešení pokračuje príslušný zodpovedný RPŠ a naopak RPŠ môže zmeniť zodpovedného za riešenie späť na NCU.  Každá zmena stavu ticketu je zaznamená na centrálnom portáli. Dotknutá škola bude informovaná aj mailom o podstatných zmenách stavu riešenia ticketu a jeho uzatvorení aj o plánovaných prácach začatí prác a ich ukončení. Kontaktné informácie a oprávnené osoby nahlasuje škola pri akceptácii riešenia, informácie je RPŠ povinný odovzdať NCU.  **Ostatné služby – Service review meetings**  Service Review Meeting (SREV) slúži na pravidelné hodnotenie a zlepšovanie poskytovaných služieb. Jeho cieľom je zabezpečiť, aby služby spĺňali očakávania škôl a objednávateľa. Predmetom stretnutia bude najmä:   * hodnotenie kvality dodaných služieb, analýza kľúčových ukazovateľov výkonnosti, porovnanie s cieľmi a identifikácia odchýlok, * zhrnutie spätnej väzby získanej od škôl, identifikácia oblastí na zlepšenie, * analýza incidentov: preskúmanie významných incidentov, identifikácia príčin a navrhovanie preventívnych opatrení, * hodnotenie nových požiadaviek: diskusia o nových požiadavkách, * plánovanie zmien: diskusia o plánovaných zmenách v službách a ich vplyve, * stretnutie iniciuje NCU a bude sa konať mesačne počas prvých 6 mesiacov poskytovania služieb a následne štvrťročne. NCU zabezpečí primeranú účasť pracovníkov zodpovedných za poskytované služby. Mimoriadne Service review meeting môže iniciovať MŠVVaM SR v prípade opakovaných, podstatných porušení hodnôt parametrov a definície služieb.   Z každého stretnutia bude vytvorený zápis so zhrnutím obsahu, zoznamom identifikovaných problémov a príležitostí, prijatých rozhodnutí, zoznamom úloh, zodpovedných osôb a termínov. | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | RPŠ, Škola, NCU, MŠVVaM SR |
| **Iné zainteresované strany** | | | NCU |
| **Prevádzková doba** | | | | pracovné dni 6:00 – 18:00 |
| **Minimálna Dostupnosť služby** | | | | 99,9% |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | N/A |
| **Doba vyhodnocovania** | | | | N/A |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | NCU Service Desk |
| **Definícia** | | Je zabezpečovaná podľa požiadaviek vyššie |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | N/A |
| **Požadovaná hodnota** | **Jednotka** | boolean |
| **Minimum** | ÁNO je zabezpečovaná |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | N/A |
| **Merateľné parametre** | **Metrika 2** | **Názov:** | | Doba spracovania ticketu |
| **Definícia** | | Čas od prijatia, prevzatia do zaevidovania a kategorizácie |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | minúta |
| **Minimum** | Nie je obmedzené |
| **Maximum** | 60 |
| **Severita Nesúladu služby** | | Service review meeting eskalácia |

Tabuľka 27: Poskytovanie služieb centrálneho NCU Service Desk pre sieť DigiNET  **-** detailná definícia požiadaviek na službu

### Riešenie incidentov

| **Riešenie incidentov NCU Service Desk - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Riešenie incidentov NCU - Service Desk |
| **Kategória** | | | | Služby Prevádzkovej podpory, NCU Service Desk a SOC |
| **Typ** | | | | Ad-hoc |
| **Cieľ** | | | | Služby riadenia/riešenia incidentov |
| **Riešenie incidentov NCU Service Desk** **- detailná definícia požiadaviek na službu** | | | | |
| Riadenie incidentov zahŕňa najmä:   * registráciu a kategorizáciu podľa severity: zaznamenávanie všetkých nahlásených udalostí, * priorizácia: určenie naliehavosti incidentov na základe ich dopadu na zákazníka a prevádzku, * riešenie: podľa potreby vzdialené, na mieste, výmenu zariadenia za nové, výjazd servisného technika apod. a sledovanie ich riešenia až do úplného vyriešenia, * komunikácia: informovanie zákazníkov o stave a zmene stavu ich požiadaviek a poskytovanie pravidelných aktualizácií. * Proaktívne informovanie používateľov pri proaktívne vytvorenom incidente z monitoringu RPŠ pri identifikovaní Nesúladu so službou taktiež pri podstatnej zmene stavu incidentu   Incidenty sú podľa závažnosti Nesúladu služby a vplyv Nesúladu služby na používateľov definované takto:   * Severity 1: Viac ako 25% škôl bez pripojenia alebo podstatný nesúlad služieb školách. * Severity 2: Viac ako 5% škôl bez pripojenia alebo podstatný nesúlad služieb školách. * Severity 3: Menej ako 5% škôl bez pripojenia alebo podstatný nesúlad služieb školách. * Severity 4: Výpadok bezpečnostných funkcií NCU, výpadok iných služieb priamo neovplyvňujúci pripojenie škôl alebo bezpečnostné funkcie (monitoring, CTP, reporting, Servicedesk.   NCU začne s diagnostikou a  odstraňovaním incidentu do 60 minút (viď metrika služby NCU-ServiceDesk) od jeho nahlásenia alebo detekcie. Stav riešenia a vykonané kroky budú priebežne aktualizované v tickete v CTP.  NCU si vytvorí primerané skladové zásoby náhradných dielov pre potreby výmeny chybných zariadení NCU.  **Požiadavky na odstraňovanie Nesúladu služby podľa severity:**  **Incident severity 1**: RTTR - Odstránenie do 3 hodín od identifikácie/nahlásenia.  **Incident severity 2**: RTTR - Odstránenie do 5 hodín od identifikácie/nahlásenia  **Incident severity 3**: RTTR - Odstránenie nasledujúci pracovný deň od identifikácie/nahlásenia  **Incident severity 4**: RTTR - Odstránenie nasledujúci pracovný deň od identifikácie/nahlásenia  Časy uvedené vyššie sa predlžujú:   * o dobu neposkytnutia súčinnosti na základe povinností RPŠ alebo školy, * o plánované výpadky podľa definície požiadaviek na služby plánovania výpadkov, * o dočasné prerušenie poskytovania služby na žiadosť Používateľa/Objednávateľa, * o dočasné prerušenie poskytovania služby z dôvodu zmeny prevádzkových parametrov okruhu resp. služby na žiadosť Používateľa/Objednávateľa (zmena rýchlosti a pod.), * z dôvodu prekládky služieb na žiadosť Používateľa/Objednávateľa a pod., * o prerušenie spôsobené Používateľom alebo dôvodom na strane Používateľa napr. spôsobené nevhodným používaním zariadení RPŠ alebo ich odpojením, spôsobené výpadkom elektrického napájania, * neumožnenie prístupu technických pracovníkov poskytovateľa služieb do priestorov, v ktorých je umiestnená infraštruktúra alebo pripájaný bod, * o dobu zapríčinenú nefunkčnosťou (aj opakujúcou sa) koncových zariadení, ktoré sú v správe školy, * o prerušenie z dôvodu nepredvídateľných a neodvrátiteľných udalostí (Vis Major).   Povinnosti používateľa  Poverená osoba školy je povinná poskytovať súčinnosť pri odstraňovaní incidentu podľa požiadaviek NCU. Súčinnosť môže spočívať vo vzdialenej podpore (napr. telefonicky poskytne informáciu o výpadku el. energie, stave kontroliek na zariadení, vizuálnej kontrole zariadení, kabeláže a pod). Súčinnosť pri podpore na mieste môže spočívať v sprístupnení budovy a miest inštalácie, uskladnení zariadení a pod.  V prípade neposkytovania potrebnej súčinnosti sa budú časy uvedené v RTTR predlžovať o dobu neposkytovania súčinnosti a takéto predĺženie nebude považované za porušenie RTTR (napr. ak kontaktná osoba neberie telefón, nie je na mieste a nie je schopná poskytnúť súčinnosť, nie je ochotná sprístupniť v požadovanom čase miesto inštalácie a pod).  **Riadenie problémov (Problém manažment)**  Cieľom riadenia problémov je identifikácia a odstránenie základných príčin opakujúcich sa incidentov NCU, prevencia budúcich incidentov a zlepšenie celkovej dostupnosti a spoľahlivosti služieb.  NCU musí mať implementovaný systém riadenia problémov v zmysle ITIL alebo obdobný, ktorý zahŕňa minimálne:   * analýzu incidentov a identifikácia opakujúcich sa incidentov, * identifikáciu základnej príčiny (root cause), * navrhovanie a implementácia trvalých riešení, * aktualizácia znalostnej bázy, * implementácia prípadných potrebných zmien v konfigurácii, * preventívne opatrenia.   **Eskalácie**  Pravidlá pre eskalácie definujú postup, ako sa bude riešiť situácia, keď poskytované služby NCU nespĺňajú dohodnuté parametre. Cieľom eskalácií je urýchlenie procesu identifikácie a odstránenia porúch, zvýšenie transparentnosti, zlepšenie komunikácie, vytvorenie jasných kanálov komunikácie medzi poskytovateľom a zákazníkom a minimalizácia negatívnych dôsledkov výpadkov alebo zhoršenia kvality služieb.  Eskalačné postupy sa aplikujú pre incidenty Severity 1 a Severity 2 po uplynutí stanovenej doby po nesplnení parametrov pre daný incident alebo pri značnom množstve dotknutých škôl, hromadných výpadkoch.  Eskalácia 1. úrovne:   * Eskalácia na vedúceho Servis desku * Incident Severity 1 neodstránený v dohodnutom čase   Eskalácia 2. úrovne:   * Eskalácia na CTO alebo obdobné * Incident Severity 1 neodstránený 3 hodiny po dohodnutom čase, alebo * Incident Severity 2,3,4 neodstránený nasledujúci pracovný deň   Eskalácia 3. úrovne:   * Eskalácia na CEO NCU * Incident Severity 1 neodstránený 6 hodín po dohodnutom čase, alebo * Incident Severity 2,3,4 neodstránený druhý pracovný deň   O eskalácii bude upovedomený mailom zodpovedná oprávnená osoba školy ako aj Ministerstvo a uvedením kontaktov na vedúceho pracovníka ktorému bola situácia eskalovaná. | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | Škola |
| **Iné zainteresované strany** | | | RPŠ |
| **Prevádzková doba** | | | | pracovné dni 6:00 – 18:00 |
| **Minimálna Dostupnosť služby** | | | | N/A |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa času v tickete |
| **Doba vyhodnocovania** | | | | Po uzavretí ticketu |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | RTTR Merateľné ukazovatele pre odstraňovanie Nesúladu služby podľa severity |
| **Definícia** | | Severity 1 |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | N/A |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | hodiny od nahlásenia/identifikácie |
| **Minimum** | Nie je obmedzené |
| **Maximum** | 3 |
|  | |  |
| **Metrika 2** | **Názov:** | | RTTR Merateľné ukazovatele pre odstraňovanie Nesúladu služby podľa severity |
| **Definícia** | | Severity 2 |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | N/A |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | hodiny od nahlásenia/identifikácie |
| **Minimum** | Nie je obmedzené |
| **Maximum** | 5 |
|  | |  |
| **Metrika 3** | **Názov:** | | RTTR Merateľné ukazovatele pre odstraňovanie Nesúladu služby podľa severity |
| **Definícia** | | Severity 3 |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | N/A |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | pracovný deň od nahlásenia/identifikácie |
| **Minimum** | Nie je obmedzené |
| **Maximum** | Nasledujúci pracovný deň |
|  | |  |
| **Metrika 4** | **Názov:** | | RTTR Merateľné ukazovatele pre odstraňovanie Nesúladu služby podľa severity |
| **Definícia** | | Severity 4 |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | N/A |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | pracovný deň od nahlásenia/identifikácie |
| **Minimum** | Nie je obmedzené |
| **Maximum** | Nasledujúci pracovný deň |
|  | |  |

Tabuľka 28: Riešenie incidentov NCU Service Desk - detailná definícia požiadaviek na službu

A group of white labels

Description automatically generated

Obrázok 1: Proces spracovania incidentu

#### Oznamovanie a odsúhlasovanie plánovaných výpadkov

| **Oznamovanie a odsúhlasovanie plánovaných výpadkov - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | **Oznamovanie a odsúhlasovanie plánovaných výpadkov** |
| **Kategória** | | | | Služby Prevádzkovej podpory, NCU-Service Desk a SOC |
| **Typ** | | | | Ad-hoc |
| **Cieľ** | | | | Táto časť definuje požiadavky na úrovne služieb v súvislosti s plánovanými výpadkami. Cieľom je zabezpečiť, aby plánované výpadky mali minimálny vplyv na prevádzku škôl a aby boli všetky relevantné informácie poskytnuté včas a transparentne. |
| **Oznamovanie a odsúhlasovanie plánovaných výpadkov - detailná definícia požiadaviek na službu** | | | | |
| **Plánovaný výpadok:** Dočasné prerušenie/Nesúlad poskytovania aspoň časti služieb, ktoré je vopred naplánované a ohlásené NCU.  **Okno údržby:** Časový úsek, počas ktorého môže dôjsť k plánovanému výpadku:   * pracovné dni medzi 16:00 a 06:00 a počas víkendov 00:00 – 23:59   **Oznámenie o plánovanom výpadku:** Informácie poskytuje NCU Service Desk, vytvorí príslušný typ udalosti v CTP o nadchádzajúcom plánovanom výpadku, ktorá obsahuje dátum, čas začiatku a predpokladaný čas ukončenia výpadku.  Oznámenie o plánovanom výpadku bude obsahovať nasledujúce informácie:   * dátum a čas začiatku plánovaného výpadku, * predpokladaný čas ukončenia plánovaného výpadku, * dôvod plánovaného výpadku, * vplyv plánovaného výpadku na poskytované služby, * kontaktné informácie pre prípad otázok.   **Urgentný plánovaný výpadok:** V mimoriadnych situáciách, keď s bezpečnostných alebo iným závažných dôvodov nie je možné dodržať časy uvedené vyššie. Ak to urgencia vyžaduje, vo výnimočných prípadoch je ho možné zrealizovať aj mimo Okna údržby. Oznámenie potom musí obsahovať aj zdôvodnenie Urgentného plánovaného výpadku.  Po ukončení výpadku NCU oznámi ukončenie plánované výpadku.  V prípade že navrhovaný čas plánovaného výpadku bude pre školu v značne nevyhovujúcom čase, môže požiadať zmenu času vykonania plánovanej práce a NCU zváži možnosť vyhovieť požiadavke.  V prípade že výpadok bude oznámený podľa podmienok, nebude podliehať pokutám inak sa bude na neho nahliadať ako na Incident ak nastane v prevádzkovej dobe služby. | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | Škola, RPŠ |
| **Iné zainteresované strany** | | | RPŠ |
| **Prevádzková doba** | | | | 24/7 |
| **Minimálna Dostupnosť služby** | | | | N/A |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa času v tickete |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Oznámenie o plánovanom výpadku vopred |
| **Definícia** | | Požadovaný čas oznámenia plánovaného výpadku |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | N/A |
| **Požadovaná hodnota** | **Jednotka** | hodina |
| **Minimum** | 72 vopred |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Servce review meeting |
| **Merateľné parametre** | **Metrika 2** | **Názov:** | | Oznámenie o urgentnom plánovanom výpadku vopred |
| **Definícia** | | Požadovaný čas oznámenia urgentného plánovaného výpadku |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | N/A |
| **Požadovaná hodnota** | **Jednotka** | hodina |
| **Minimum** | 2 vopred |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Servce review meeting |
| **Merateľné parametre** | **Metrika 3** | **Názov:** | | Požiadavka na trvanie plánovaného výpadku |
| **Definícia** | | Maximálna dĺžka plánovaného výpadku |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | pracovné dni medzi 16:00 a 06:00 a počas víkendov 00:00 – 23:59 |
| **Spôsob** | N/A |
| **Požadovaná hodnota** | **Jednotka** | hodina |
| **Minimum** | Nie je obmedzené |
| **Maximum** | 5 |
| **Severita Nesúladu služby** | | Podľa služby: Riešenie incidentov; a teda rozsahu počtu postihnutých bodov v prípade že plánovaný výpadok presiahol okno údržby do štandardnej prevádzkovej doby služieb. |

Tabuľka 29: Oznamovanie a odsúhlasovanie plánovaných výpadkov – definícia požiadaviek na službu

### Poskytovanie služieb SOC

| **Poskytovanie služieb SOC - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Poskytovanie služieb SOC |
| **Kategória** | | | | Služby Prevádzkovej podpory, NCU-Service Desk a SOC |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Prevádzka Bezpečnostného operačného centra (SOC) |
| **Poskytovanie služieb SOC - detailná definícia požiadaviek na službu** | | | | |
| Service desk NCU bude prevádzkovať aj Bezpečnostné operačné centrum (SOC), ktoré zabezpečí monitorovanie, detekciu a reakciu na bezpečnostné hrozby v sieti DigiNET. SOC sa skladá z tímu bezpečnostných expertov a využíva nástroje a technológie Centrálneho uzla na sledovanie a ochranu siete. Požiadavky na služby SOC sú:   * Monitorovanie bezpečnostných udalostí: SOC monitoruje sieťové toky a systémové udalosti na všetkých lokalitách, aby identifikoval potenciálne bezpečnostné hrozby a incidenty. * Triage upozornení: Automatizované klasifikovanie a priorizovanie upozornení na základe závažnosti a kontextu * Analýza bezpečnostných udalostí: SOC analyzuje zaznamenané udalosti a vyhodnocuje ich mieru rizika a závažnosti (severity), aby určil, či ide o skutočnú hrozbu. * Automatizácia reakcie na incidenty: Zefektívnenie pracovných postupov reakcie na incidenty na zníženie času reakcie a zvýšenie efektivity. * Reakcia na incidenty: V prípade zistenia bezpečnostného incidentu SOC okamžite reaguje a prijíma opatrenia v spolupráci s RPŠ na jeho riešenie a minimalizáciu škôd. * Správa prípadov: Riadenie bezpečnostných incidentov ako prípadov, sledovanie pokroku a zabezpečenie včasného riešenia prostredníctvom automatizovaných pracovných postupov. * Eskalácia incidentov: Automatizovaná eskalácia incidentov na základe definovaných kritérií na zabezpečenie primeraných úrovní reakcie. * Hľadanie hrozieb: Automatizácia procesov hľadania hrozieb na proaktívne vyhľadávanie indikátorov kompromitácie v prostredí. * Ochrana pred útokmi: SOC vykonáva aktívne opatrenia na ochranu siete pred rôznymi typmi útokov, ako sú malvérové útoky, útoky na dáta alebo phishing. Vyrozumenie dotknutých používateľov a poskytnutie vzdelávacích zdrojov o rozpoznávaní malvéru a phishingu. * Analýza sieťovej prevádzky: Automatizované monitorovanie sieťovej prevádzky na anomálie, ktoré môžu naznačovať bezpečnostný incident. Detekcia nezvyčajného správania v sieti, ako je napríklad skenovanie portov. Detekcia nezvyčajných vzorcov používania VPN, prístup z viacerých miest alebo v nezvyčajných časoch. Detekcia nezvyčajného správania periférnych zariadení (napr. tlačiarní, interaktívnych tabúľ, kamier) v sieti. * Detekcia pokusu o získanie neoprávnených administrátorských práv k systému. * Zabezpečovanie súladu: SOC zabezpečuje dodržiavanie bezpečnostných predpisov a noriem voči zákonom a reguláciám, ako aj interným bezpečnostným politikám a postupom. * Analýza trendov a prevencia: Na základe zaznamenaných incidentov a analýzy trendov SOC vyvíja stratégie na prevenciu budúcich bezpečnostných hrozieb a zlepšenie celkovej bezpečnosti siete. * Správa zraniteľností: Automatizované identifikovanie, hodnotenie a náprava zraniteľností v celej sieti. * SOC tiež spravuje špecializované bezpečnostné komponenty Centrálneho uzla, ako sú centrálny firewall, AntiDDoS alebo analyzátor sieťovej prevádzky. Taktiež nastavuje automatizované reakcie na systémami identifikované incidenty. Takýmito reakciami môžu byť napríklad vygenerovanie alarmu v dohľadovom systéme, správa o incidente do emailu alebo SMS, ale aj obmedzenie klientskeho zariadenia alebo používateľského účtu, a jeho izolácia od zvyšku siete (tzv. karanténa). Následne identifikácia a umiestnenie do karantény akýchkoľvek ďalších zariadení, ktoré komunikovali s infikovaným zariadením. * V kompetencii SOC je tiež konsolidácia bezpečnostných správ a reportov z Centrálneho uzla, a príprava pravidelných mesačných reportov a správ o incidentoch pre objednávateľa. Tieto reporty je možné poskytnúť aj na požiadanie. * Správa a analýza protokolov: Centralizácia a automatizácia zbierania a analýzy protokolov z rôznych zdrojov pre lepšiu viditeľnosť * SOC poskytuje správy o výkone svojej činnosti mesačne   **Povinnosti prevádzkovateľa SOC**   * Reagovať na nahlasovanie bezpečnostných incidentov zo školy: Pokiaľ sa jedná o bezpečnostný incident zaznamenaný školou, bude eskalovaný na SOC, kde sa bude špecialista venovať prevereniu incidentu a jeho závažnosti, následne budú vykonané zmeny, aby bola minimalizovaná škoda, a zamedzilo sa opakovaniu takéhoto incidentu. Každý takýto incident bude súčasne zahrnutý do mesačného SOC bezpečnostného reportu poskytovaného objednávateľovi služby. * Monitorovať sieťovú prevádzku prostredníctvom špecializovaných nástrojov a včas reagovať na všetky incidenty aj hrozby. * Monitorovať správanie používateľov a včas identifikovať a aktívne preveriť anomálie. * Monitorovať stav operačných systémov a firmvérov v koncových zariadeniach a pripravovať odporúčania pre školy na aplikácie bezpečnostných záplat a aktualizáciu operačných systémov a aplikácií. * Vykonávať bezpečnostné kontroly na zistenie zraniteľností. * Automaticky blokovať sieťové hrozby a podozrivé IP adresy. * Automaticky izolovať postihnuté zariadenia alebo IP rozsahy v sieti. * Poskytovať vzdelávacie zdroje o predchádzaní incidentom (napr. o zabezpečení účtu, o rozpoznávaní phishingu, a pod.). * Komunikovať škole identifikované incidenty v jej sieti podľa závažnosti ihneď alebo v rámci mesačného reportu. Týka sa to napríklad používateľov alebo používateľských zariadení zaradených do karantény, používateľov ktorí nesprávne klikli na phishingovú alebo spearingovú správu alebo klientske zariadenia, ktoré generujú neúmerný objem prevádzky nesúvisiaci s potrebami školy, typicky prostredníctvom aplikácií v peer-to-peer sieti alebo dátových úložísk. * Reportovať bezpečnostné incidenty a riziká objednávateľovi v rámci pravidelného mesačného reportu alebo na požiadanie. | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | RPŠ, škola, MŠVVaM SR |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | pracovné dni 8:00 – 17:00 |
| **Minimálna Dostupnosť služby** | | | | 99,9% - na základe základných parametrov a vlastností služieb NCU |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Požiadavky na služby SOC |
| **Definícia** | | Prevádzka služieb SOC podľa definície služby |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne alebo Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | boolean |
| **Minimum** | ÁNO v súlade |
| **Maximum** | N/A |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých škôl |

Tabuľka 30: Poskytovanie služieb SOC - definícia požiadaviek na službu

#### Povinnosti používateľa SOC

* Poverený pracovník školy je povinný nahlasovať incidenty na Service Desk.
* Škola musí umožniť prístup pri inštalácií, údržbe a výmene prvkov siete.
* Škola musí aktívne spolupracovať s prevádzkovateľom pri riešení bezpečnostných incidentov, ako napríklad spolupracovať pri identifikácii koncového zariadenia, spolupracovať pri identifikácii a kontaktovaní používateľa, poskytovať súčinnosť pri aplikácii bezpečnostných záplat, aktualizácii operačných systémov a aplikácií, odvírovaní alebo odinštalovaní nebezpečného softvéru (botnetov a podobne) zo serverov a klientskych zariadení.
* Škola musí rešpektovať návrhy a odporúčania prevádzkovateľa SOC na update a upgrade operačných systémov a firmvérov koncových zariadení a v prípade, že to nebude spôsobovať iné prevádzkové problémy, tieto zahrnúť do svojho plánu aktualizácií a bezpečnostných záplat, a vo svojej sieti aj realizovať.

#### Povinnosti RPŠ

* Poskytnúť podporu škole pri identifikácii klientskych zariadení na základe hlásení a reportov SOC.
* Poskytnúť podporu škole pri tvorbe a realizácii plánu aktualizácií a aplikácie bezpečnostných záplat podľa odporúčania SOC. Toto sa týka klientskych zariadení, ale aj iných zariadení v sieti, ako napríklad sieťových kamier, tlačiarní alebo serverov.
* Aktualizovať firmvér v sieťových zariadeniach podľa odporúčania SOC.
* Na požiadanie SOC identifikovať a odpojiť klientske zariadenie alebo časť siete zasiahnutej alebo podieľajúcej sa na prebiehajúcom bezpečnostnom incidente.

#### RACI matica zodpovedností SOC

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Popis činnosti** | **Škola** | **RPŠ** | **NCU** | **MŠVVaM** |
| **Monitorovanie sieťovej prevádzky** |  |  | **A, R** | **I** |
| **Monitorovanie správania používateľov** |  |  | **A, R** | **I** |
| **Vykonávanie bezpečnostných kontrol** |  |  | **A, R** | **I** |
| **Blokovanie sieťových hrozieb** | **I** | **I** | **A, R** | **I** |
| **Izolovanie postihnutých zariadení alebo IP rozsahov** | **I** | **I** | **A, R** | **I** |
| **Poskytnutie vzdelávacích zdrojov o rozpoznávaní hrozieb** | **I** |  | **A, R** |  |
| **Poskytovanie podpory školám** | **I** | **A, R** |  |  |
| **Fyzická podpora pre SOC pri riešení incidentov a eliminácii identifikovaných hrozieb** | **I** | **R** | **A** |  |
| **Nahlasovanie incidentov** | **R** | **R** | **A** |  |
| **Umožnenie fyzického prístupu na školu** | **A, R** |  |  |  |

Tabuľka 31: RACI matica zodpovedností SOC

### Ďalšie služby NCU ServiceDesk

| **Požiadavky na Ďalšie služby NCU Service desk - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Ďalšie služby NCU Service Desk |
| **Kategória** | | | | Služby Prevádzkovej podpory, NCU-Service Desk a SOC |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Zabezpečenie ďalších služieb NCU Servicedesk |
| **Požiadavky na Ďalšie služby NCU Service desk - detailná definícia požiadaviek na službu** | | | | |
| **Zabezpečovanie aktualizácii a testovania**  NCU musí mať zavedený systém pre riadenie záplat (patchov) a aktualizácií. Systém musí zabezpečiť pravidelné sledovanie publikovaných aktualizácie prevádzkované prvky infraštruktúry a rozhodnúť o ich nasadení. Okrem sledovania vydaných aktualizácií sa musia pravidelne (minimálne raz za mesiac) monitorovať a posudzovať ich zraniteľnosti.  Aktualizácie sa nasadzujú na základe vyhodnotenia rizík a kontrolovaným spôsobom. Inštalácia aktualizácií musí byť riadená iba Špecialistom/Administrátorom zodpovedným za daný systém a to kontrolovaným spôsobom tak, aby bezpečnostná záplata nespôsobila funkčné výpadky služieb. Nasadenie zmien musí byť riadne otestované. Aktualizácie a meny musia byť pred inštaláciou adekvátne otestované za účelom overenia ich funkčnosti a vplyvu na prevádzku a bezpečnosť. Zároveň musí byť pripravená aj stratégia vrátenia zmeny v prípade neočakávaných problémov.  NCU pred implementáciou opráv softvéru, implementácie zmien HW, SW, konfigurácie v sieti vykoná všetky potrebné testy. V prípade požiadavky oprávnenej osoby školy, Ministerstva, poskytne správu o testovaní. Zástupcovia školy, Ministerstva, NCU majú právo zúčastniť sa testov ak o to požiadajú.  **Prevádzka informačného systému a komunikačného prostredia**  Úspešný uchádzač sa prevádzkovať pre verejného obstarávateľa informačný systém, v ktorom úspešný uchádzač bude pravidelne aktualizovať a zdieľať údaje súvisiace s projektom. Informačný systém môže byť samostatný alebo súčasťou CTP.  Bude slúžiť najmä na:   * sledovanie plnenia časového harmonogramu projektu, * sledovanie historických údajov o jednotlivých lokalitách (od zapojenia do siete DigiNET, cez všetky vykonané zmeny a žiadosti o zvýšenie rýchlosti, o prekládku, o dodatočné IKT zariadenia, až po prípadné zrušenie školy, resp. odpojenie zo siete DigiNET, * kontrolu údajov pre účely verifikácie oprávnenosti faktúr, * vytváranie exportov štatistických údajov podľa zvolených kritérií (počet zapojených škôl vo zvolenom období, počet zapojených škôl podľa krajov, podľa typu pripojenia, atď.), štatistiky a filtrované údaje bude možné vyexportovať do súboru excel, * sledovanie stavu vybavenosti požiadaviek škôl (žiadosť o zapojenie do projektu, zvýšenie rýchlosti, prekládka), * poskytnutie a prístup k systému Service Desk, ktorým uchádzač sleduje, vyhodnocuje a odstraňuje servisné prípady (napr. výpadok virtuálnej privátnej siete, poruchy koncových zariadení, nefunkčnosť internetového pripojenia), * archívne úložisko všetkých vystavených a uhradených/neuhradených faktúr a vystavených objednávok.   Tiež bude slúžiť ako úložisko v rámci riadenia dokumentácie ako napríklad:   * Detailný popis riešenia a služieb NCU * Návody pre užívateľov, RPŠ, MŠ * Dokumentácia súvisiaca s riadením rizík * Dokumentácia zaslaná RPŠ   K informačnému systému a jeho funkcionalitám vytvorí úspešný uchádzač pre verejného obstarávateľa používateľský manuál.  **Zabezpečovanie súladu s metodickými usmerneniami**  NCU bude koordinovať konfigurácie služieb/nastavenia služieb v súlade s metodickými usmerneniami Ministerstva s cieľom zabezpečenia homogenity nastavení a udržateľnosti zmien v školských sieťach. Úlohou poskytovateľa služieb NCU je formalizovať prevádzkový a konfiguračný poriadok ktorý formálne schvaľuje Ministerstvo a úlohou RPŠ je sa ním riadiť.  Zabezpečovanie súladu dokumentácie  Súčasťou služieb NCU je priebežne aktualizovať dizajn a dokumentáciu riešenia a služieb NCU.  Dokumentácia odovzdaná pri akceptácii riešenia do prevádzky musí byť aktualizovaná po každej významnej zmene v systéme počas nasadzovania a životného cyklu projektu.  Zabezpečovať správu licencii ktoré prislúchajú k nainštalovaným prvkom riešenia.  Všetky časti dokumentácie sú aktualizované v digitálnej podobe na lokalite definovanej Ministerstvom. Dokumentácia musí byť v Slovenskom jazyku.  **Kontrola reportov RPŠ**  NCU Service desk bude zodpovedný za primárnu kontrolu mesačných reportov RPŠ. Postup bude nasledovný:  RPŠ vypracuje všetky požadované reporty a odovzdá ich Centrálnemu uzlu najneskôr v tretí pracovný deň nasledujúceho mesiaca. Formát v akom budú reporty odovzdávané špecifikuje NCU. Report bude obsahovať aj posúdenie zhody s požadovanými hodnotami parametrov a dostupnosti a výpočet zmluvných pokút.  NCU report skontroluje a najneskôr piaty pracovný deň zašle RPŠ schválenie reportu alebo pripomienky, ktoré RPŠ bez odkladne odstráni a zašle opravený report. Kontrola bude zameraná najmä na dodržiavanie parametrov SLA a výpočet zmluvných pokút.  NCU zašle reporty 5. pracovný deň MŠ, ktoré zašle prípadné pripomienky najneskôr 10. pracovný deň RPŠ. V prípade že najneskôr 10. pracovný deň, RPŠ nedostane pripomienky považuje sa report za schválený.  Žiadosť o informáciu  Škola môže požiadať prostredníctvom NCU Service desku o rôzne ďalšie relevantné informácie súvisiace poskytovanými službami. NCU žiadosť zaeviduje v tickete, priamo odpovie alebo presunie riešenie na RPŠ.  **Mimoriadne situácie**  Mimoriadna situácia je vopred ohlásené časové obdobie v ktorom sú požadované zvýšené nároky na dostupnosť a kvalitu služieb zo strany NCU. V prípade mimoriadnej situácie môže Ministerstvo žiadať o spustenie posilnenia prevádzky. Ide napríklad o prevádzku v čase volieb v budove školy, maturít, testovania deviatakov, živelných katastrof a odstraňovania ich následkov a podobne.  Mimoriadna situácia môže byť vyhlásená na jednej, niekoľkých alebo aj všetkých školách.  Mimoriadnu situáciu oznámi Ministerstvo alebo Škola NCU a to minimálne 1 mesiac vopred, o výnimočných prípadoch urgentnej mimoriadnej situácie aj v skrátenej lehote.  Počas trvania mimoriadnej situácie NCU zabezpečí prednostné spracovanie na ServiceDesk-u, prednostné odstraňovanie incidentov na mieste a ďalšie požadované primerané opatrenia.  Počas mimoriadnej situácie môže Ministerstvo žiadať o zmenu konfigurácie v sieti tak aby bol uprednostňovaný istý typ služby, časť siete resp. zapnutá časť siete a ostatné blokované a zabezpečená zmena smerovania v sieti. | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | RPŠ, škola |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | Ako NCU Servicedesk |
| **Minimálna Dostupnosť služby** | | | | 99,9% - na základe základných parametrov a vlastností služieb NCU |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Ďalšie služby NCU Servicedesk |
| **Definícia** | | Prevádzka ďalších služieb NCU Servicedesku |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | proaktívne |
| **Požadovaná hodnota** | **Jednotka** | boolean |
| **Minimum** | ÁNO v súlade |
| **Maximum** | N/A |
| **Severita nesúladu služby** | | Podľa rozsahu postihnutých škôl |

Tabuľka 32: Požiadavky na Ďalšie služby NCU Service desk

### Meranie spokojnosti koncového používateľa služieb a náprava

| **Meranie spokojnosti koncového používateľa služieb, objektívna analýza - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Meranie spokojnosti koncového používateľa služieb, objektívna analýza |
| **Kategória** | | | | Služby Prevádzkovej podpory, NCU-Service Desk a SOC |
| **Typ** | | | | Pravidelná |
| **Cieľ** | | | | Prevádzka služieb merania spokojnosti koncového používateľa sa vykonávala za účelom zistenia kvality služieb a následného zlepšenia služieb poskytovaných koncovým používateľom (školám). Nasledovná definícia uvádza pre celkový kontext definíciu služieb poskytovateľa NCU aj RPŠ. |
| **Meranie spokojnosti koncového používateľa služieb, objektívna analýza - detailná definícia požiadaviek na službu** | | | | |
| Služby súvisiacich meraním spokojnosti koncového používateľa, zahŕňajú nasledujúce činnosti:   * zber a analýza údajov používateľskej skúsenosti – subjektívna analýza, * zber a analýza údajov používateľskej skúsenosti – objektívna analýza, * reporty z analýzy, * optimalizácia siete na základe analýzy.   Štandardom služby pritom je:   * subjektívna analýza - pravidelný dotazníkový zber používateľskej skúsenosti na základe ich subjektívneho hodnotenia, realizovaný poskytovateľom služieb NCU:   + min. 2x ročne, rovnomerne rozdelené,   + formou odoslania internetového linku na formulár (zo strany NCU), ktorý následne rozpošle riaditeľ školy na zamestnancov, ktorí sa zapájajú na dobrovoľnej báze, * formulár musí skúmať spokojnosť a používateľskú skúsenosť používateľov s DigiNET min. vo vzťahu k WLAN konektivite a LAN konektivite, sieťovej bezpečnosti, prihlasovaním do siete na škále od 1 – 5 (5=najlepšia skúsenosť) a to minimálne s ohľadom na:   + rýchlosť WLAN,   + pokrytie WLAN,   + rýchlosť LAN,   + rýchlosť práce s Internetom,   + skúsenosť so sieťovou bezpečnosťou   + skúsenosť s prihlasovaním sa do siete * formulár musí tiež dávať priestor vložiť ku každej otázke vlastný text, a obsahovať časť s voľným textovým poľom, * vyhodnotenie dotazníkov musí NCU po spracovaní zasielať poverenej osobe na MŠVVaM SR a RPŠ, * za účelom štandardizácie zberu dát má MŠVVaM SR právo zmeniť a určiť presné formulácie dotazníkových otázok resp. znenie celého formuláru, aby boli tieto porovnateľné pre všetky školy, * v prípade, že používatelia vo vzťahu k skúmaným otázkam udelia počet bodov 1 a 2, opakovane dva krát po sebe vo vzťahu k príbuznej veci k službám v správe NCU, musí NCU pristúpiť k objektívnej analýze, * objektívna analýza – objektívny zber parametrov kvality práce používateľov formou získavania metrík z reálnej používateľskej prevádzky ako aj formou syntetickej (umelo generovanej) dátovej prevádzky:   + min. v trvaní 10 dní, v reakcii na nízky počet bodov (1 a 2), * Výsledkom vyhodnotenia objektívnej analýzy musí byť potvrdenie resp. vyvrátenie hlásených problémov a implementácia zmien, ktoré budú týmto problémom predchádzať, pokiaľ tieto nie sú preukázateľne mimo kompetencie NCU a RPŠ. Výsledky skúmania a zmien musí NCU do 30 dní po skončení Objektívnej analýzy oznámiť, oprávnenej osobe školy a MŠVVaM SR na pripomienkovanie, prípadne ďalej riešiť na eskalačných stretnutiach. | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | RPŠ, Škola, MŠVVaM SR |
| **Iné zainteresované strany** | | | RPŠ |
| **Prevádzková doba** | | | | pracovné dni 6:00 – 18:00 |
| **Minimálna Dostupnosť služby** | | | | Podľa výsledkov merania prieskumu viď definícia vyššie |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | Podľa výsledkov merania prieskumu viď definícia vyššie |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Objektívna analýza |
| **Definícia** | | Objektívna analýza na základe merania reálnej a syntetickej prevádzky podľa popisu vyššie |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne a reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Počet |
| **Minimum** | Definované podľa nízkeho bodového hodnotenia zo subjektívnej analýzy |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa severity ticketu |
| **Merateľné parametre** | **Metrika 2** | **Názov:** | | Pravidelný dotazníkový zber používateľskej skúsenosti |
| **Definícia** | | Vykonávanie zberu a anlýza používateľskej skúsenosti podľa definície služby |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Počet |
| **Minimum** | 2 x ročne |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Eskalácie |

Tabuľka 33: Meranie spokojnosti koncového používateľa služieb, objektívna analýza – definícia požiadaviek na službu

### Poskytovanie školení

| **Poskytovanie školení - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Poskytovanie školení |
| **Kategória** | | | | Podporné služby |
| **Typ** | | | | Pravidelná |
| **Cieľ** | | | | Poskytovanie školení s cieľom zabezpečovania vyškolenia pracovníkov používateľa služieb DigiNET v záujme zabezpečovania kvality, rozvoja, spolupráce s MŠVVaM SR. |
| **Poskytovanie školení - detailná definícia požiadaviek na službu** | | | | |
| NCU vypracúva tréningové materiály služieb v správe NCU pre potreby školení RPŠ pre zástupcov škôl. NCU spolupracuje s RPŠ pri návrhu rozsahu a materiálov školení. Tieto sú vypracované 15 pracovných dní pred realizáciou akceptácie služieb na prvej škole a odovzdané na komentár RPŠ. NCU na základe komentárov doplní/upraví materiály v požadovanom rozsahu do 5tich pracovných dní.  NCU vypracúva tréningové materiály pre služby DigiNET a zabezpečuje pre poverených pracovníkov používateľa služieb - MŠVVaM SR pravidelné školenia k poskytovaným službám NCU  Školenia budú realizované podľa nasledovného harmonogramu:   * prvé školenie pred akceptáciou zriadenia služieb NCU a 3 mesiace po spustení služieb, * ďalšie školenie minimálne 1x ročne podľa predošlej dohody s MŠVVaM SR, * mimoriadne školenia v prípade potreby po dohode s MŠVVaM SR,   Školenia sú zamerané aj na:   * celkové technické riešenie, základné funkčné bloky, schéma prepojenia, NCU, RPŠ * základné poučenie podmienkach zmluvy a SLA zodpovednosti školy, RPŠ a NCU, * oboznámenie sa s nástrojmi monitoringu, reportingu, Service Desk * oboznámenie sa so službami ktoré NCU poskytuje * udržiavanie, zabezpečovanie kvality služieb DigiNET * Performance a kvalitatívne parametre * Správy sieťovej bezpečnosti a jej rozvoja a hrozieb * Návrhy rozvoje a aktivít služieb DigiNET * postup pri bežných situáciách * postupy pri eskalácii, * zásady pre bezpečnosť, funkcie a prevádzka SOC.   Organizačné požiadavky na školenia:   * Školenia budú prebiehať minimálne online dištančnou formou s možnosťou otázok a diskusie. V prípade potreby budú školenia realizované aj v priestoroch poskytovateľa NCU. * Rozsah školenia bude minimálne 2 hodiny. * Termíny školenia poskytovateľ NCU poskytne 2 z ktorých jeden potvrdzuje MŠVVaM SR ) a to minimálne 3 týždne pred navrhovaným termínom školenia. * Školiace materiály budú sprístupnené aj v elektronickej podobe. * MŠVVaM SR na žiadosť poskytovateľa NCU nominuje účastníkov školenia. * NCU pripraví protokol a prezenčnú listinu zo školenia. | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | RPŠ, MŠVVaM SR |
| **Iné zainteresované strany** | | | RPŠ |
| **Prevádzková doba** | | | | pracovné dni 8:30 – 17:00 |
| **Minimálna Dostupnosť služby** | | | | 99,9% |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | Ročne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Príprava školiacich materiálov a výkon školení |
| **Definícia** | | Podľa požiadaviek na službu |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Počet ročne |
| **Minimum** | 1 |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Eskalácia |

Tabuľka 34: Poskytovanie školení - detailná definícia požiadaviek na službu

### RACI matica pre služby podpory, prevádzky

| **Popis činnosti** | **Škola** | **RPŠ** | **NCU** | **MŠVVaM** |
| --- | --- | --- | --- | --- |
| Bezodkladné nahlasovanie udalosti používateľom | A,R | I | I | n/a |
| Poskytovanie súčinnosti používateľa pri klasifikácii a riešení udalostí 8.00 – 17.00 počas pracovných dní | A,R | C | C | n/a |
| Prevádzka NCU – Service Desku | N/A | N/A | A,R | N/A |
| Evidencia udalostí, aktuálnosť informácií ticketov | I | R | A,R | I |
| Klasifikácia udalosti | C | R | A,R | I |
| Detekcia udalostí v pôsobnosti NCU | I | R | A,R | I |
| Spolupráca s NCU pri riešení problémov | N/A | A,R | C | N/A |
| Spolupráca s RPŠ pri riešení problémov | N/A | C | A,R | N/A |
| Odstránenie incidentu v pôsobnosti RPŠ | I | R | A,I | I |
| Odstránenie incidentu v pôsobnosti NCU | I | I | A,R | I |
| Vzdialená podpora, súčinnosť, podpora na mieste | R | C | C | A |
| Sklad HW, výmena HW na mieste, RMA, výjazd servisného technika | I | A,R | I | I |
| Oznámenie o plánovanom výpadku služieb NCU | I | C | A,R | I |
| Oznámenie o neplánovanom výpadku služieb NCU | I | I | A,R | I |
| Meranie spokojnosti koncového používateľa služieb | R | C | A,R | I |

Tabuľka 35: RACI matica pre služby podpory, prevádzky NCU

## Služby hradené na základe spotrebovaného času – Riadenie zmien

Cieľom služby Riadenie zmien je zabezpečiť, aby zmeny v IT infraštruktúre a službách či už na požiadavku používateľa alebo s dôvodu údržby a aktualizácie zo strany NCU boli plánované, schválené a implementované kontrolovaným spôsobom, minimalizujúc pritom riziká a negatívne dopady na prevádzku.

### Poskytovanie služieb na základe spotrebovaného času

O zmenu môže požiadať riaditeľ školy, ním poverená osoba alebo zástupca obstarávateľa.

Po prijatí žiadosti o zmenu NCU (alebo RPŠ) vytvorí ticket, kde bude evidovaná žiadosť, následná komunikácia, realizácia zmeny až po jej akceptáciu.

NCU posúdi žiadosť o zmenu, klasifikuje ju podľa ich potenciálneho vplyvu na prevádzku (nízky, stredný, vysoký) z dôvodu prispôsobenia procesu schvaľovania a kontroly jednotlivým typom zmien, vykoná hodnoteniu rizík, aby sa identifikovali potenciálne negatívne dopady a prijali potrebné opatrenia na ich minimalizáciu.

Následne v primeranom čase, maximálne však do 20 pracovných dní v prípade potreby komplexnejšej analýzy požiadavky, zašle žiadateľovi ponuku s navrhovanou cenou, počtom MD práce, časom realizácie a zhodnotením rizík a dopadov na prevádzku.

Ponuku na zmenu žiadateľ posúdi a po schválení zašle objednávku NCU.

NCU zmenu zrealizuje, otestuje a odovzdá do prevádzky. Testovanie musí NCU vykonať v súčinnosti s RPŠ ak sa jedná o dotknuté služby zabezpečované oboma stranami. Testovanie musí preukázať plnú funkčnosť riešenia po aplikovaní zmeny.

V prípade že v pripájanej lokalite k službám NCU nie sú zabezpečované služby RPŠ (lokalita bez RPŠ) vykonáva poskytovateľ služieb NCU len tie relevantné služby Prevádzkovej podpory, NCU Service Desk a SOC, ktoré sú výhradne v rozsahu jeho zodpovednosti a to pre:

Služby hradené na základe spotrebovaného času môžu byť zabezpečované aj pre pripájané lokality k službám NCU kde nie sú zabezpečované služby RPŠ (lokalita bez RPŠ).

| **Parameter služby** | | | | **Hodnota** |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Poskytovanie služieb na základe spotrebovaného času |
| **Kategória** | | | | Služby hradené na základe spotrebovaného času |
| **Typ** | | | | Na požiadanie |
| **Cieľ** | | | | Zabezpečiť, aby zmeny v infraštruktúre a službách boli plánované, schválené a implementované kontrolovaným spôsobom, minimalizujúc pritom riziká a negatívne dopady na prevádzku. |
| **Definícia požiadaviek na službu** | | | | 1. Zmeny musia prechádzať jasne definovaným procesom, ktorý zahŕňa podanie žiadosti o zmenu, hodnotenie, schvaľovanie, plánovanie, implementáciu, testovanie a zavedenie do prevádzky. 2. Zmeny sú klasifikované podľa ich potenciálneho vplyvu na prevádzku (nízky, stredný, vysoký) z dôvodu prispôsobenia procesu schvaľovania a kontroly jednotlivým typom zmien. 3. Každá zmena musí byť podrobená dôkladnému hodnoteniu rizík, aby sa identifikovali potenciálne negatívne dopady a prijali potrebné opatrenia na ich minimalizáciu. 4. Zmeny musia byť schválené oprávnenými osobami, ktoré majú potrebné znalosti a autoritu. 5. Pre každú zmenu musí byť vypracovaný detailný plán, ktorý špecifikuje všetky potrebné činnosti, zdroje a časové harmonogramy. 6. Zmeny musia byť implementované podľa schváleného plánu. 7. Po implementácii musí byť vykonané primerané testovanie. 8. Po úspešnom testovaní je zmena zavedená do pravidelnej prevádzky. 9. Celý proces riadenia zmien musí byť dôkladne zdokumentovaný v príslušnom tickete, aby bolo možné sledovať históriu zmien a vyhodnocovať ich účinnosť. 10. O zmenách musia byť primerane informovaní zástupcovia školy, MŠVVaM SR a poskytovateľ služieb NCU. |
| **Účastníci** | **Poskytovateľ** | | | NCU |
| **Používateľ** | | | Škola, MŠVVaM SR |
| **Iné zainteresované strany** | | | RPŠ |
| **Prevádzková doba** | | | | N/A |
| **Merateľné parametre** | **Metrika 1** | **Názov** | | Čas na vyjadrenie k žiadosti o zmenu |
| **Definícia** | | Posúdenie žiadosti o zmeny RPŠ, zhodnotenie rizík, vypracovanie ponuky a navrhované časového harmonogramu |
| **Meranie** | **Vykonávateľ** | NCU |
| **Čas** | N/A |
| **Spôsob** | Evidencia v tickete a e-mailoch |
| **Požadovaná hodnota** | **Jednotka** | Dni |
| **Minimum** | Čas primeraný rozsahu zmeny |
| **maximum** | Čas primeraný rozsahu zmeny, maximálne však do 20 pracovných dní |
| **Metrika 2** | **Názov** | | Cena a čas realizácie zmeny |
| **Definícia** | | Navrhovaná cena (cena zariadení, počet dní práce) a doba realizácie zmeny |
| **Meranie** | **Vykonávateľ** | NCU |
| **Čas** | N/A |
| **Spôsob** | N/A |
| **Požadovaná hodnota** | **Jednotka** | EUR, MD, dní |
| **Minimum** | N/A |
| **Maximum** | Cena rovnaká ako pri dodávke a realizácii prvotnej inštalácie školy, počet MD a doba realizácie primeraná rozsahu zmeny |
| **Metrika 3** | **Názov** | | Dodržanie dohodnutého času a rozsahu realizácia zmeny |
| **Definícia** | | Realizácia zmeny po objednávke podľa dohodnutého rozsahu a v dohodnutom čase |
| **Meranie** | **Vykonávateľ** | NCU |
| **Čas** | Podľa objednávky |
| **Spôsob** | Akceptácia zástupcom školy, Evidencia v tickete a e-mailoch |
| **Požadovaná hodnota** | **Jednotka** | N/A |
| **Minimum** | N/A |
| **Maximum** | Dodržaný čas a cena podľa objednávky |
| **Dostupnosť služby** | | **Minimálna dostupnosť** | N/A | |
|  |  | |

Tabuľka 36:Poskytovanie služieb na základe spotrebovaného času – definícia požiadaviek na službu

# Prílohy

## Zoznam skratiek

| **Skratka** | **Vysvetlenie** |
| --- | --- |
| ACL | Access Control List |
| AP | Access Point |
| API | Application Programming Interface |
| API RESTful | Representational State Transfer Application Programming Interface |
| BPDU | Bridge Protocol Data Unit |
| BSSID | Basic Service Set Identifier |
| CEO | Chief Executive Officer |
| CoPP | Control Plane Policing |
| CPE | Customer Premises Equipment |
| CRSD | Centralizované riešenie správy a dohľadu |
| CSV | Comm-aSeparated Values |
| CTO | Chief Technology Officer |
| CTP | Centrálny Ticketing Portál |
| NCU | Národný Centrálny Uzol |
| DDoS | Distributed Denial of Service |
| DFS | Dynamic Frequency Selection |
| DHCP | Dynamic Host Configuration Protocol |
| DMZ | Demilitarized Zone |
| DNS | Domain Name System |
| EoL | End of Life |
| EoS | End of Service |
| ETSI | European Telecommunications Standards Institute |
| EUR | Euro |
| GDPR | General Data Protection Regulation |
| GUI | Graphical User Interface |
| HECC | Highly Equipped and Connected Classroom |
| HTTP | HyperText Transfer Protocol |
| HTTPS | HyperText Transfer Protocol Secure |
| HW | Hardvér |
| ID | Identifikátor |
| IDS | Intrusion Detection System |
| IEEE | Institute of Electrical and Electronics Engineers |
| IKT | Informačné a Komunikačné Technológie |
| IP | Internet Protocol |
| IPSEC | Internet Protocol Security |
| IT | Informačné Technológie |
| ITIL | Information Technology Infrastructure Library |
| JSON | JavaScript Object Notation |
| LAN | Local Area Network |
| LLDP | Link Layer Discovery Protocol |
| MAB | Media Access Control Authentication Bypass |
| MAC | Media Access Control |
| MD | Man-Day |
| MIB | Management Information Base |
| MŠVVaM SR | Ministerstvo školstva výskumu vývoja a mládeže SR |
| MU-MIMO | MultiUser Multiple Input Multiple Output |
| N/A | Not Applicable |
| NBAR | NetworkBased Application Recognition |
| NTBK | Notebook |
| OID | Object Identifier |
| OS | Operačný Systém |
| OWE | Opportunistic Wireless Encryption |
| PAT | Port Address Translation |
| PC | Osobný Počítač |
| PoE | Power over Ethernet |
| POST | PowerOn SelfTest |
| PSK | PreShared Key |
| RADIUS | Remote Authentication Dial-In User Service |
| RAM | Random Access Memory |
| RBAC | RoleBased Access Control |
| RFC | Request for Comments |
| RPŠ | Regionálny Partner Školy |
| RSSI | Received Signal Strength Indicator |
| RX-SOP | Receiver Start of Packet |
| SLA | Service Level Agreement |
| SMS | Short Message Service |
| SN | Serial Number |
| SNMP | Simple Network Management Protocol |
| SNR | Signal-to-Noise Ratio |
| SR | Slovenská Republika |
| SREV | Service Review Meeting |
| SSH | Secure Shell |
| SSID | Service Set Identifier |
| SSL | Secure Sockets Layer |
| STP | Spanning Tree Protocol |
| SW | Softvér |
| SYSLOG | System Logging Protocol |
| TBD | To Be Determined |
| TÚ SR | Telekomunikačný Úrad Slovenskej Republiky |
| U-APSD | Unscheduled Automatic Power Save Delivery |
| UL/DL | Upload/Download |
| URI | Uniform Resource Identifier |
| URL | Uniform Resource Locator |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| WiFi | Wireless Fidelity |
| WLAN | Wireless Local Area Network |
| WMM | WiFi Multimedia |
| WPA | WiFi Protected Access |
| XML | eXtensible Markup Language |
| ZTP | Zero Touch Provisioning |

Tabuľka 37: Zoznam skratiek

## Zoznam obrázkov

[Obrázok 1: Proces spracovania incidentu 80](#_Toc198499049)

## Zoznam tabuliek

[Tabuľka 1: Zoznam pojmov 6](#_Toc198499050)

[Tabuľka 2: Prevádzka služieb riadenia prístupu používateľov k sieti 13](#_Toc198499051)

[Tabuľka 3: Prevádzka služieb centrálneho firewallu – definícia požiadaviek na službu 15](#_Toc198499052)

[Tabuľka 4: Centrálne filtrovanie webového obsahu - detailná definícia požiadaviek na službu 18](#_Toc198499053)

[Tabuľka 5: Prevádzka služieb centrálnej aplikačnej podpory - detailná definícia požiadaviek na službu 21](#_Toc198499054)

[Tabuľka 6: Prevádzka služieb centrálnej antivírusovej a antimalvérovej ochrany - detailná definícia požiadaviek na službu 22](#_Toc198499055)

[Tabuľka 7: Prevádzka služieb centrálnej IDS/IPS ochrany - detailná definícia požiadaviek na službu 24](#_Toc198499056)

[Tabuľka 8: Prevádzka služieb centrálnej ochrany proti DDoS- detailná definícia požiadaviek na službu 26](#_Toc198499057)

[Tabuľka 9: RACI matica pre služby sieťovej bezpečnosti 27](#_Toc198499058)

[Tabuľka 10: Prevádzka služieb centrálneho pripojenia do siete Internet - detailná definícia požiadaviek na službu 31](#_Toc198499059)

[Tabuľka 11: Prevádzka služieb prepojenia sietí, dátovej bezpečnosti a integrity prostredia - detailná definícia požiadaviek na službu 33](#_Toc198499060)

[Tabuľka 12: Prevádzka služieb centrálnej správy IP adries - detailná definícia požiadaviek na službu 34](#_Toc198499061)

[Tabuľka 13: Poskytovanie služieb centralizovaného riešenia správy a dohľadu NCU (NCU-CRSD) pre potreby RPŠ - detailná definícia požiadaviek na službu 48](#_Toc198499062)

[Tabuľka 14: Zaisťovanie nastavenia globálnych politík LAN/WLAN sietí - detailná definícia požiadaviek na službu 52](#_Toc198499063)

[Tabuľka 15: Zabezpečovanie prihlasovania používateľov do siete LAN/WLAN - detailná definícia požiadaviek na službu 54](#_Toc198499064)

[Tabuľka 16: Prevádzka služieb vzdialeného pripojenia - detailná definícia požiadaviek na službu 55](#_Toc198499065)

[Tabuľka 17: Prevádzka služieb pripojenia lokalít škôl k NCU a služby CPE - detailná definícia požiadaviek na službu 58](#_Toc198499066)

[Tabuľka 18: Prepájanie na Dátové centrum rezortu školstva - detailná definícia požiadaviek na službu 59](#_Toc198499067)

[Tabuľka 19: RACI pre sieťové služby 60](#_Toc198499068)

[Tabuľka 20: Poskytovanie služieb monitoringu NCU - detailná definícia požiadaviek na službu 62](#_Toc198499069)

[Tabuľka 21: RACI matica pre služby monitoringu NCU 63](#_Toc198499070)

[Tabuľka 22: Vytváranie správy o dostupnosti a kvality služieb - detailná definícia požiadaviek na službu 65](#_Toc198499071)

[Tabuľka 23: Vytváranie správy o výkone Service Desku a plnení SLA - detailná definícia požiadaviek na službu 67](#_Toc198499072)

[Tabuľka 24: Vytváranie správy o stave sieťovej bezpečnosti - detailná definícia požiadaviek na službu 68](#_Toc198499073)

[Tabuľka 25: Vytváranie správy o prevádzke sieťových služieb - detailná definícia požiadaviek na službu 70](#_Toc198499074)

[Tabuľka 26: RACI matica pre služby reportingu NCU 70](#_Toc198499075)

[Tabuľka 27: Poskytovanie služieb centrálneho NCU Service Desk pre sieť DigiNET  **-** detailná definícia požiadaviek na službu 75](#_Toc198499076)

[Tabuľka 28: Riešenie incidentov NCU Service Desk - detailná definícia požiadaviek na službu 79](#_Toc198499077)

[Tabuľka 29: Oznamovanie a odsúhlasovanie plánovaných výpadkov – definícia požiadaviek na službu 83](#_Toc198499078)

[Tabuľka 30: Poskytovanie služieb SOC - definícia požiadaviek na službu 86](#_Toc198499079)

[Tabuľka 31: RACI matica zodpovedností SOC 87](#_Toc198499080)

[Tabuľka 32: Požiadavky na Ďalšie služby NCU Service desk 89](#_Toc198499081)

[Tabuľka 33: Meranie spokojnosti koncového používateľa služieb, objektívna analýza – definícia požiadaviek na službu 92](#_Toc198499082)

[Tabuľka 34: Poskytovanie školení - detailná definícia požiadaviek na službu 94](#_Toc198499083)

[Tabuľka 35: RACI matica pre služby podpory, prevádzky NCU 95](#_Toc198499084)

[Tabuľka 36:Poskytovanie služieb na základe spotrebovaného času – definícia požiadaviek na službu 98](#_Toc198499085)

[Tabuľka 37: Zoznam skratiek 101](#_Toc198499086)