**Technická specifikace předmětu zakázky**

Obsah

[*1.* Systém pro pokročilý provozní dohled 4](#_Toc8902981)

[*2.* Systém podpory pokročilé segmentace sítě 12](#_Toc8902982)

[*3.* Zvýšení fyzického zabezpečení HTCK 26](#_Toc8902983)

[*4.* Sdílené služby kybernetické bezpečnosti 30](#_Toc8902984)

[*4.1.* Zaznamenávání a ukládání logů a detekce bezpečnostních událostí 30](#_Toc8902985)

[*4.2.* Analýza datových toků a detekce bezpečnostních událostí 36](#_Toc8902986)

[*4.3.* Dohledové centrum - SOC 41](#_Toc8902987)

[*5.* Služby poradenství a podpory, resp. „Služby spojené s implementací IS“ 46](#_Toc8902988)

[*5.1.* Předimplementační analýza 46](#_Toc8902989)

[*5.2.* Prováděcí dokumentace 46](#_Toc8902990)

[*5.3.* Projektové vedení dodávky 47](#_Toc8902991)

[*5.4.* Dokumentace 47](#_Toc8902992)

[*5.5.* Provádění prací 47](#_Toc8902993)

[*6.* Výkony nad rámec podpory 48](#_Toc8902994)

Předmětem veřejné zakázky je zajištění komplexního monitoringu ICT prostředků, kontrola činností všech registrovaných uživatelů na všech úrovních zpracování dat, sledování datového provozu informační infrastruktury, registrování útoků na prostředky ICT a průběžné odhalování případných interních a externích útočníků na ICT Krajského úřadu Středočeského kraje (dále také „KÚSK“). Za tím účelem budou v rámci veřejné zakázky pořízeny a v prostředí KÚSK implementovány odpovídající technologie a zajištěny vybrané služby externího dodavatele, a to v souladu se zákonem o kybernetické bezpečnosti a nařízením EP a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

Řešení veřejné zakázky je koncipováno tak, aby naplnilo následující technická opatření dle zákona o kybernetické bezpečnosti:

* § 17 Fyzická bezpečnost
* § 18 Bezpečnost komunikačních sítí
* § 22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů
* § 23 Detekce kybernetických bezpečnostních událostí
* § 24 Sběr a vyhodnocení kybernetických bezpečnostních událostí
* § 27 Zajišťování úrovně dostupnosti informací
* Sdílené dohledové centrum kybernetické bezpečnosti (SOC)

Dodavatelé, kteří se budou podílet na rozvoji, provozu nebo zajištění bezpečnosti významných informačních systémů, musí dle § 8 Vyhlášky 82/2018 Sb., vyhláška o kybernetické bezpečnosti, splňovat bezpečnostní požadavky pro dodavatele.

Záměrem zadavatele je nakoupit dodávky a služby zařazené do 5 celků:

1. **Systém pro pokročilý provozní dohled** – Jedná se o komplexní řešení pokročilého provozního dohledu informačních technologií KÚSK tak, aby plně navazoval na stávající řešení, kdy je využíváno ASW Nagios. Součástí dodávky je návrh architektury řešení, upgrade software na nejnovější verzi a provedení jeho konfigurace podle návrhu. Dále je součástí servisní podpora zadavatele při provozu systému včetně zajištění podpory výrobce po dobu 60 měsíců.
2. **Systém podpory pokročilé segmentace sítě** – Jedná se o komplexní řešení systému podpory a řízení pokročilé segmentace síťové infrastruktury KÚSK takovým způsobem, aby navazovalo na současně využívanou technologii infrastruktury. Součástí dodávky je návrh architektury řešení včetně potřebného HW a potřebného SW a implementace tohoto řešení včetně požadované integrace do prostředí Zadavatele. Dále je součástí servisní podpora zadavatele při provozu systému včetně zajištění podpory výrobce po dobu 60 měsíců.
3. **Zvýšení fyzického zabezpečení HTCK** - Jedná se o dodávku a instalaci klimatizační jednotky a dodávku a instalaci zhášecího zařízení na bázi plynů inergenů. Dále je součástí dodávky zajištění pravidelného servisu zařízení včetně zajištění podpory výrobce po dobu 60 měsíců.
4. **Sdílené služby kybernetické bezpečnosti** – Jedná se o komplexní dodávku dílčích služeb po dobu 60 měsíců:
   1. *Zaznamenávání a ukládání logů a detekce bezpečnostních událostí* – Dodavatel s využitím vlastních technologií zajistí sběr, ukládání, analýzu a bezpečné dlouhodobé uchování logů z vybraných systémů IT zadavatele. Současné dodavatel zajistí detekci bezpečnostních událostí v sledovaných systémech IT dodavatele a informování o nich.
   2. *Analýza datových toků a detekce bezpečnostních událostí* – Dodavatel s využitím vlastních technologií zajistí sledování datových toků na výskyt anomálií a podezřelých aktivit a měření výkonových parametrů datových přenosů v síti IT zadavatele. Současně dodavatel zajistí záznam a uložení informací o sledovaných datových tocích, detekovaných událostech a stavech a o výsledcích měření sledovaných veličin.
   3. *Dohledové centrum – SOC* – Dodavatel s využitím vlastních zdrojů zajistí provoz Bezpečnostního dohledového centra, které pro zadavatele bude provádět bezpečnostní dohled nad sledovanými systémy IT, identifikaci, hodnocení a řešení bezpečnostních incidentů včetně poskytnutí včasných informací odpovědným pracovníkům zadavatele, pravidelné reportování stavu kybernetické bezpečnosti sledovaných systémů IT a poskytování podpory v oblasti kybernetické bezpečnosti.
5. **Služby poradenství a podpory** – Jedná se o komplexní dodávku dílčích služeb, které směřují ke koordinaci a kvalitnímu provedení dodávky ostatních služeb:
   1. *Předimplementační analýza* – Dodavatel zpracuje analýzu prostředí IT kraje, ve které popíše a vyhodnotí stav z hlediska zajištění kybernetické bezpečnosti podle §17, §18, §22, §23, §24 a §27 vyhlášky o kybernetické bezpečnosti, identifikuje bezpečnostní rizika a slabá místa a navrhne opatření k odstranění neshod.
   2. *Prováděcí dokumentace* – Dodavatel zpracuje prováděcí dokumentaci s detailním návrhem cílového stavu, s popisem aktivit potřebných pro řádnou implementaci jednotlivých služeb včetně implementace opatření navržených v předimplementační analýze a s návrhem harmonogramu implementačních prací. Součástí dokumentace bude také popis potřebných integrací do prostředí IT kraje.
   3. *Projektové vedení dodávky* – Dodavatel zajistí řízení, koordinaci a dokumentaci postupu dodávky včetně řízení rizik a změn dodávky a poskytování pravidelných zpráv o průběhu dodávky.
   4. *Dokumentace skutečného provedení* – Dodavatel v průběhu celé dodávky zajistí zpracování dokumentace dodaných řešení v požadovaném rozsahu.
6. **Výkony nad rámec podpory dle čl. III odst. 5.3 Smlouvy o dílo**

## Systém pro pokročilý provozní dohled

*Realizace tohoto opatření naplní § 27 Zajišťování úrovně dostupnosti informací* Vyhlášky č.82/2018 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti v platném znění*.*

Jedná se o komplexní řešení pokročilého provozního dohledu informačních technologií KÚSK tak, aby plně navazoval na stávající řešení, kdy je využíváno ASW Nagios. Je požadováno provést upgrade na nejnovější verzi Nagios s GUI s licencí minimálně pro 1000 hostů. V současné době je využíván Nagios 3.3 s předplacenou roční podporou. Upgrade ASW Nagios na nejnovější verzi vytvoří robustní dohledové centrum, které má zajistit nepřetržité proaktivní monitorování činností a správu všech aktivních prvků instalovaných informačních technologií na KÚSK. Je nutné zajistit zasílání automatické zprávy správcům sítě při výpadku jakéhokoliv aktivního prvku nebo dle definovaného scénáře spustit automatickou akci k obnovení provozu aktivního prvku. Systém musí umožňovat rozšíření pomocí definic uživatelských funkcí (pluginů) a být schopen pokrýt monitoring velkého množství různorodých prvků informačních technologií. Systém uchovává historii záznamů z provozu prvků, podává informace o aktuálním stavu a dostupnosti aplikací a jednotlivých prvků provozované infrastruktury. Systém bude sloužit jako centrální zdroj informací pro efektivní řízení infrastruktury KÚSK. Systém bude nakonfigurován pro poskytování automatizovaných výstupů službě SOC, na kterou bude napojen.

**Požadovaný účel implementace systému:**

Povýšit funkčnost služby provozního dohledu infrastruktury KÚSK s možností detekce na úrovni jednotlivých služeb nebo informačních systémů včetně vzájemných závislostí a podporou reportování (SLA).

**Základní požadavky implementace systému:**

Požadavky zadavatele jsou uvedeny ve sloupci „Minimální technické požadavky, které zadavatel požaduje“. Dodavatel je povinen vyplnit, zda jím nabízený produkt / řešení tyto požadavky splňuje, a to v sloupci „Splnění požadavků zadavatele“ (dodavatel doplní prohlášení ANO nebo NE podle skutečnosti). Ve sloupci „Odkaz do nabídky“ dodavatel uvede odkaz na konkrétní část nabídky, ve které je možné ověřit splnění uvedeného požadavku. Následná smlouva s vybraným dodavatelem může být v této části upravena tak, aby obsahovala již pouze dodavatelem nabídnuté zařízení a jeho technické parametry.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Minimální technické požadavky, které zadavatel požaduje | | Splnění požadavků zadavatele (ANO/NE) | Odkaz do nabídky dodavatele, kde je možné ověřit splnění požadavku | Public/NDA |
| Část | **Popis** |
| Upgrade stávajícího řešení, administrace | | | |  |
| Rozsah | * Řešení umožňuje připojit infrastrukturu KÚSK. |  |  | public |
| Upgrade Nagios 3.3 | * Provést upgrade na nejvyšší možnou verzi stávající a stabilní verzi s GUI (komerční provedení). * Provést upgrade grafického rozhraní systému Nagios. * Vytvořit řešení on−premise. |  |  | public |
| Administrace a uživatelský přístup | * Realizovat výhradně přes jednotné GUI a to formou webové aplikace s podporou prohlížečů Internet Explorer verze 11 a Mozilla Firefox v. 45 příp. dalších vyšších verzí. |  |  | public |
| Mobilita administrace | * Podporovat možnosti využití verzi aplikace pro mobilní zařízení na platformách Google Android a Apple iOS v libovolném počtu. |  |  | public |
| Integrita | * Systém obsahuje všechny požadované funkcionality, není možné jej sestavit z vícero různých komponent od různých výrobců software. |  |  | public |
| Virtualizace | * Řešení se požaduje jako samostatný virtuální stroj do infrastruktury VMware (virtuální server bude zajištěn zadavatelem). |  |  | public |
| Podpora monitoringu | | | |  |
| Nativní podpora | * Podpora nativního monitoringu standardních technologií – Microsoft Windows, SQL Server, VMware, Linux, grafické platformy (např. Integraph technologie), FalconStor, MS Exchange, SW Symantec, Networker atd. |  |  | public |
| Autodiscovery | * Přidávat další monitorované systémy a služby s rozeznáním vyjmenovaných aktivních síťových služeb. |  |  | public |
|  | * Vytvářet vlastní scripty nebo pluginy pro jednotlivé prováděné kontroly. |  |  | public |
| Šablony v GUI | * Možnost vytváření vlastních šablon zařízení, tak aby pokud je takováto šablona přiřazena ke všem vhodným prvkům v infrastruktuře, byly služby definované v této šabloně sledovány dle parametrů zadaných přímo v šabloně. Pokud je následně v šabloně provedena jakákoli změna služeb, musí se toto projevit i na prvcích, které tuto šablonu využívají bez dalších nutných kroků administrátorů. Šablony lze vytvářet nebo upravovat výhradně přes GUI. |  |  | public |
| Monitoring služeb | * Návrh řešení obsahuje možnosti monitoringu služeb, které zajišťuje Odbor informatiky (OINF). Každá služba, např. email je složena z jednotlivých komponent, např. SMTP gateway, Internetová konektivita apod. Každá z těchto sub−komponent obsahuje další podřízené sub−komponenty, např. zatížení CPU, využití disku, apod. Systém umožňuje nastavení takových vazeb mezi komponentami a sub−komponentami služby, aby v případě degradace komponenty v nejnižší hierarchii byl tento stav promítnut do celé struktury služeb až po službu samotnou. Zároveň v tomto případě musí být jasně definováno, které jednotlivé části jsou tímto ovlivňovány. |  |  | public |
| Reporting | | | |  |
| Reporting SLA | * Řešení nabízí možnosti reportingu SLA u jednotlivých služeb poskytovaných IT, a to na základě parametrů nastavovaných pověřeným uživatelem. |  |  | public |
| * Sledované komponenty je možné nastavit do režimu plánovaného výpadku, kdy nedochází k notifikacím a ke změně daného SLA. |  |  | public |
| Časové sledování služeb | * U jednotlivých sledovaných služeb musí být k dispozici adekvátní graf parametru služby ve zvoleném časovém úseku. |  |  | public |
| Topologické mapy | * Řešení musí obsahovat možnost vytváření interaktivních topologických map, např. mapu síťové konektivity v místě, přičemž při kliknutí na jakýkoliv interaktivní prvek uživatel uvidí detail tohoto prvku v samotném systému řešení. * Zobrazení či pohled, kde se graficky znázorňuje celková mapa implementované sítě, jsou označeny spoje mezi jednotlivými body infrastruktury. |  |  | public |
| Zobrazení | * Poskytovat přehled všech monitorovaných služeb, kde jejich aktuální stav je barevně odlišen; * Poskytovat přehled všech monitorovaných zařízení, kde jejich aktuální stav je barevně odlišen; * Poskytovat souhrnný výpis všech monitorovaných zařízení, rozdělený do jednotlivých skupin; * Poskytovat souhrnný výpis všech monitorovaných služeb, rozdělený do jednotlivých skupin. |  |  | public |
| Dashboard, přehledy | * Vytvořit/revidovat základní přehled stavů (dashboard) všech monitorovaných služeb a zařízení. |  |  | public |
| Reporty, výčet, příklady | * Vytvářet reporty vybraného zařízení nebo služby a jejich problémových stavů; * Vytvářet grafické reporty o stavu zařízení nebo služby v čase, kde lze stanovit časový interval; * Generovat souhrnné reporty o stavu sledovaných služeb a zařízení za zvolený časový interval * Zpracovávat výpis logu se zaznamenanými událostmi; * Vytvářet report o dostupnosti a vyhodnocení stavu služeb a zařízeních v časovém období |  |  | public |
| GUI, nastavení | | | |  |
| Konfigurace | * V rámci GUI umožňovat uživatelsky měnit rozložení pracovní plochy a konfiguraci jednotlivých prvků GUI, které se týkají výstupů z monitoringu. |  |  | public |
| Notifikace | * Systém disponuje možnostmi notifikace pomocí emailů nebo SMS při určitých stavech zjištění. Samotné notifikační šablony musí být editovány prostřednictvím jednotného GUI včetně možnosti rozesílání kontaktním skupinám. |  |  | public |
| Autentizace | * Součástí nabízeného řešení je možnost řízení uživatelského a administrátorského přístupu k řešení prostřednictvím LDAP/AD/IDM. |  |  | public |
| * Řízení autentizace bude dodán jako samostatný virtuální stroj do infrastruktury VMware. Dodávka obsahuje vlastní operační systém. Systém zajistí možnosti automatické i manuální aktualizace samotného operačního systému, tak i vlastní aplikace výhradně přes jednotné GUI. |  |  | public |
| Implementace monitoringu | | | |  |
| Dohledování HW | * Na HW zařízeních budou dohledovány relevantní parametry, příklady:   + Síťové prvky.   + Utilizace CPU.   + Utilizace paměti RAM.   + Teplota.   + Utilizace šířky pásma rozhraní, interní.   + Případně další dle typu. * Servery   + Utilizace RAM.   + Utilizace CPU.   + Utilizace síťových rozhraní.   + Utilizace disků.   + Služby/procesy.   + Případně další dle typu. |  |  | public |
| Dohledování SW | * Pro jednotlivé monitorované SW budou definovány dle jeho účelu užití sledované parametry, které budou nakonfigurovány do řešení. |  |  | public |
| * Definovat a rozdělit zařízení a služby do skupin tykajících se příslušných primárních aktiv; V případě aktiva, které disponuje rozdělením na produkční, testovací a případně vývojové prostředí je nutné provést seskupení dle těchto prostředí. |  |  | public |
| * Sledovat aktuální síťové stavy prostřednictvím webového rozhraní, zobrazení historií událostí, logovacích souborů atd. |  |  | public |
| * Pro každé primární aktivum definovat relevantní služby, které budou monitorovány. Pro každou službu definovat alespoň stavy OK, Warning (HARD, SOFT) a Critical (HARD, SOFT) včetně definovaných prahových hodnot s provedením následné konfigurace. |  |  | public |
| * Zařízení primárních aktiv budou monitorována. Pro doporučené parametry zařízení definovány stavy OK, Warning (HARD, SOFT) a Critical (HARD, SOFT) včetně definovaných prahových hodnot s provedením následné konfigurace. |  |  | public |
| * Dále budou definovány vazby mezi jednotlivými službami (service dependency) a zařízeními (host dependency) v rámci primárního aktiva. Poté budou definovány vazby mezi jednotlivými primárními aktivy. Veškeré diagramy budou součástí dokumentace pro každé aktivum a napříč aktivy. Diagramy budou odevzdány v editovatelné podobě specifikované zadavatelem. Veškeré vazby budou nakonfigurovány. |  |  | public |
| * Provádět monitorování síťových služeb všech systémů vystavených na internet a interních systémů/služeb, které jsou klasifikovány z míry dostupnosti vysoká a vyšší. |  |  | public |
| * Provádět monitorování hostitelských zdrojů (vytíženost procesoru, využití disku a pamětí, běžící procesy, logovací soubory atd.). |  |  | public |
| * Disponovat schopností definovat síťovou hostitelskou hierarchii, umožňující zjištění rozdílu mezi zařízením (službou), které je vypnuté a které nedostupné. |  |  | public |
| * Připravit vnější příkazové rozhraní, které dovoluje za provozu modifikovat monitorování a chování celého systému. |  |  | public |
| * Uchovávat stav zařízení a služeb i po restartu Nagiosu. |  |  | public |
| * Připravit prostředí pro potvrzení problémů přes webové rozhraní. |  |  | public |
| * Pro specifikované události disponovat schopností definované akce na událost (např. při nedostupnosti restartuj službu apod.). |  |  | public |
| * Provést implementaci vlastnosti Predictive Checks. |  |  | public |

**Obecné informace:**

Zadavatel v rámci upgrade systému verze Nagios 3.3 na vyšší verzi nepožaduje přenesení naimplementovaných funkcionalit v rámci stávajícího systému na nový. V rámci dodávky bude zajištěno úvodní a průběžné školení administrátorů v rozsahu 20 MD.

**Dílčí cíle implementace systému:**

* Navrhnout řešení dle požadavků výše.
* Navrhnout a popsat architekturu včetně potřebného HW a potřebného SW včetně požadované integrace do prostředí Zadavatele.
* Naplnění požadavků pro významné informační systémy pro řešenou oblast ze zákona č. 181/2014 Sb. o kybernetické bezpečnosti a příslušných vyhlášek v platném znění a souvisejících část normy ČSN ISO/IEC 27001:2014 (nebo rovnocenné řešení).
* Implementovat řešení podle návrhu schváleného Zadavatelem
* Servisní podpora v režimu 12/5/365 tj. v pracovní dny od 7-19 hodin s reakcí do 4 hodin.

**Podpora výrobce:**

Zadavatel požaduje zajištění upgrade a update dodaného SW po dobu 60 měsíců. Dodavatel se zavazuje, že součástí dodávky bude služba upgrade a update poskytována výrobcem Nagios na 36 měsíců, a že v průběhu plnění 5leté podpory tento dokoupí tuto službu ke své tíži na dalších 24 měsíců, jakmile to bude možné a to tak, aby byla zajištěna kontinuální podpora výrobce Nagios po dobu 60 měsíců. Dodavatel zajistí upgrade a update vždy při vydání nové verze (tzv. main release) a zajistí její implementaci do testovacího a produkčního prostředí. Testovací prostředí bude vytvořeno dodavatelem z důvodu možnosti testování před nasazením do produkčního provozu. Zadavatel si vyhrazuje právo schválit či odmítnout plánovaný upgrade.

## Systém podpory pokročilé segmentace sítě

*Realizace tohoto opatření naplní § 18 Bezpečnost komunikačních sítí* Vyhlášky č.82/2018 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti v platném znění*.*

Jedná se o komplexní řešení systému podpory pokročilé segmentace síťové infrastruktury KÚSK takovým způsobem, aby navazovalo na současně využívanou technologii infrastruktury. Navržené řešení bude obsahovat reportovací nástroj, který bude poskytovat základní provozní informace o infrastrukturních prvcích (dodávaných firewallech, WiFi access pointech a switchích). Reportovací nástroj bude obsahovat veškeré informace o nestandardních stavech a detekovaných hrozbách v infrastruktuře, které bude zasílat automaticky oprávněným uživatelům dle pozic definovaných bezpečnostní politikou informačních technologií KÚSK.

**Požadovaný účel implementace systému:**

Povýšit stávající systém kontroly propojení segmentu tak, aby umožňoval pokročilou kontrolu propojení mezi jednotlivými segmenty sítě prostředí KÚSK až na aplikační úrovni. Zajistit vysoký výkon řešení firewallů s cílem využití jako tzv. interní segmentační firewally a to na 10 Gbps síti s požadavkem zajištění alespoň L2/L3 stavového firewallu v plné propustnosti sítě. Zajistit vysoký výkon v IPSEC VPN s cílem přípravy na budoucí zvyšování požadavků na šifrování provozu na vysokorychlostních sítích pro připojení podřízených organizací a složek i pro vybrané interní toky.

**Základní požadavky implementace systému:**

Požadavky zadavatele jsou uvedeny ve sloupci „Minimální technické požadavky, které zadavatel požaduje“. Dodavatel je povinen vyplnit, zda jím nabízený produkt / řešení tyto požadavky splňuje, a to v sloupci „Splnění požadavků zadavatele“ (dodavatel doplní prohlášení ANO nebo NE podle skutečnosti). Ve sloupci „Odkaz do nabídky“ dodavatel uvede odkaz na konkrétní část nabídky, ve které je možné ověřit splnění uvedeného požadavku. Následná smlouva s vybraným dodavatelem může být v této části upravena tak, aby obsahovala již pouze dodavatelem nabídnuté zařízení a jeho technické parametry.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Minimální technické požadavky, které zadavatel požaduje | | Splnění požadavků zadavatele (ANO/NE) | Odkaz do nabídky dodavatele, kde je možné ověřit splnění požadavku | Public/NDA |
| Část | **Popis** |
| Obecné | | | |  |
| Řešení | * On−premise. |  |  | public |
| Správa – obecné požadavky na nabízené systémy | * Syslog. * CLI (Command Line Interface) konzole. * SSHv2 konzole. * SMNPv3 a vyšší. * Podpora protokolu RADIUS. * RBAC (Role Based Access Control). * Synchronizace času prostřednictvím NTP. |  |  | public |
| Komponenty | | | |  |
| Firewally | * Počet komponent: 2 * Hardware appliance o velikosti 1RU instalovatelné do racku 19“ s podporou duálního napájení * Min 8 x 10/100/1000 Mbps 2x SFP+ 10Gb, 8x SFP 1Gb. * Konzolový port RS232, management port RJ 45 * Podpora IPv4 a IPv6. * Minimální propustnost firewallu pro IPv4 i IPv6 provoz je 30 Gbps (měřeno na UDP komunikaci). Při měření na provozu tvořeným mixem různě velkých paketů, nebo při měření na malých (64B) paketech, nesmí výkonnost poklesnout pod 20 Gbps * Propustnost funkce IPS min. 5 Gbps (měřeno na tzv. enterprise mix provozu) * Propustnost funkce SSL inspekce alespoň 5 Gbps (měřeno na tzv. enterprise mix provozu). * Propustnost při zapnutí všech bezpečnostních funkcí ochrany před hrozbami (IPS, L7 analýza aplikací, ochrana proti malware) min 3,8 Gbps (měřeno na tzv. enterprise mix provozu). * Latence firewallu < 4 μs. * Počet souběžných spojení alespoň 5mil. * Počet nových spojení alespoň 200 tis/s. * SSL−VPN souběžných spojení alespoň 500. * Podpora pro L2TP over IPSEC, IPSEC VPN. * Propustnost IPSEC VPN alespoň 10 Gbps (při použití AES256-SHA256). * Podpora NAT/PAT. * Podpora HA řešení (active−active, active−passive). * Podpora virtuálních kontextů (min. 10 v ceně nabídky), každý z virtuálních kontextů může pracovat buď v L2 režimu (transparentní režim inspekce) nebo L3 režimu * Podpora bezpečnostní funkce ochrany před škodlivým kódem podle databáze vzorků škodlivého kódu pravidelně aktualizované výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (tzv. mobile malware), detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak), podpora sanitarizace aktivního obsahu office dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby); podpora sandboxovací funkce (dynamická analýza přenášených souborů na výskyt dosud nepopsaných variant škodlivého kódu) s integrací s nabízeným řešením pro část „Ochrana neznámých hrozeb“ * Podpora bezpečnostních funkcí: ochrana proti spamu, IPS/IDS, kategorizace webových stránek, IP reputační database, DNS filtering, ochrana před únikem citlivých informací data leak prevention). * Podpora bezpečnostní funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 2000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace * Podpora bezpečnostní funkce pro ochranu práce s populárními cloudovými aplikacemi pro sdílení a ukládání souborů na principu sledování aktivit aktivních uživatelů přes API daného provozovatele včetně funkcí monitoringu, detekce compliance pravidel a bezpečnostních kontrol (DLP, antivirus včetně sandboxingu) s ohledem na minimalizaci šíření sítových hrozeb; minimálně podpora pro Google, Amazon, Microsoft Azure, Dropbox * Podpora funkce SSL inspekce pro webové a poštovní protokoly s možností whitelistingu určitých domén či kategorií webových stránek * Funkce rozpoznání typu a druhu koncového zařízení (Windows OS, Linux OS, Mac OS, iOS, Android, mobilní zařízení, tablety) s možností aplikace do bezpečnostní politiky * Funkce QoS, traffic shaping * Ověřování identity uživatelů (možnost napojení na MS Active Directory), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign On * Funkce klientská VPN (přístup do vpn v tunelovém režimu s vpn klientem a přístup do vpn přes webový portál; možnost aplikace identit uživatele ve smyslu definice bezpečnostní politiky vpn uživatelů) * Funkce site-to-site ipsec VPN s podporou statického i dynamického routování * Podpora dvoufaktorové autentizace za pomoci HW tokenů i aplikace pro mobilní telefony (minimálně Android, iOS) s podporou autentizace administrátorů při přístupu k firewalu a pro 2FA autentizaci uživatelů do VPN. Funkce může být integrována do firewallu, nebo dodána jako samostatné řešení. Součástí dodávky budou 4ks HW tokenů pro přístup administrátorů. Řešení bude podporovat budoucí možné rozšíření na VPN uživatele (tj. podpora pro nejméně 500 tokenů) * Podpora 802.3ad * Certifikace výrobce ICSA Labs minimálně pro IPSec VPN a Network Firewall, Advanced Threat Defense (ATD), Anti−virus, SSL−TLS, IPS. * Umístění výrobce zařízení v NSS LABS NEXT GENERATION FIREWALL testu v roce 2017 nebo 2018 nadprůměrně v obou posuzovaných parametrech * Dodavatel garantuje demonstraci dosažení minimálních výkonových parametrů propustností vybraných funkcí na vyžádání. Zadavatel si vyhrazuje právo na otestování výkonových parametrů. * 1x Reportovací nástroj stejného výrobce jako FW – přípustná je 1ks fyzická appliance, 1 ks virtuální appliance s podporou Vmware. Minimální velikost úložiště 4 TB, min příjem 100 GB logů denně |  |  | NDA |
|  | * Dodavatel zajistí implementaci a konfiguraci nových FW tak, aby bylo možné aktuální zařízení odpojit, popř. využít k jinému účelu. V současné době je využíváno cca 500 aktivních pravidel na stávajících technologiích FortiGate a Check Point. |  |  | NDA |
| Ochrana neznámých hrozeb | * Počet komponent: 1 * 4x 1 GE SFP, 4 x RJ45 10/100/1000Mbps. * Úložiště 2 x 1 TB * 2 x redundantní zdroj napájení * Hardware appliance instalovatelná do racku 19“ maximálně 1RU * Alespoň 5000 souborů za hodinu prověřených antivirem. * Alespoň 150 souborů za hodinu prověřených VM sandboxingem. * Technologie VM OS Sandbox nebo obdobná včetně podpory souběžných instancí OS MS Windows 7, 8 a vyšší. * Minimální počet současně běžících VM 10 * Možnost vytvořit simulovanou síť pro oddělené scanování souborů * Podpora typ souborů: .7z, .ace, .apk, .arj, .bz2, .dll, .doc, .docm, .docx, .dot, .dotm, .dotx, .exe, .gz, .izh, .msi, .pdf .ppsx, .ppt, .pptm, .pptx, .rar, .rtf, .tar, .tgz, .xls, .xlsb, .xlsm, .xlsx, .zip a dalších. * Podpora statického směrování. * Podpora HA clusteru. * Možnost instalace v režimu neviditelného snífování a integrace s dodávaným firewallem. * Hloubková inspekce alespoň protokolů SMTP, POP3, IMAP, HTTP, FTP, SMB * Možnost SSL/TLS inspekce. * Možnost white/black listingu pro kontrolní součet souboru * Anti−evasion technik: alespoň sleep calls. * Detekce botnetů, rootkitů atd. * Dashboard s aktuálními informacemi. |  |  | NDA |
| Směrovače | * Počet komponent: 2. * Hardware appliance instalovatelné do racku 19“ max 1RU * Propojení High−availability. * 2 x SFP+ 10Gbe port, 24 x RJ45 10/100/1000Mbps. * L2 a L3 směrovací výkon alespoň 1Gbps. * IEEE 802.1Q VLAN encapsulation. * Link Aggregation Control Protocol (LACP): IEEE 802.3ad. * Jumbo frames na všech portech. * Podpora IPv4 a IPv6. * Podpora Multicast. * Směrovací protokoly: Statické, Routing Information Protocol Version 2 (RIPv2), Open Shortest Path First Version 2 (OSPFv2), Border Gateway Protocol (BGP). * IPv6 routing protocols: Static, OSPFv3, BGPv6. * Policy−Based Routing (IPv4 and IPv6). * ACL L4 včetně. * Podpora MVRP dle standardu 802.1ak pro distribuci VLAN * STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+) * Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675 * Podpora technologie MACsec * Podpora RADIUS včetně RADIUS CoA (RFC3576) * Podpora REST API pro automatizaci nastavení sítě. * Podpora Zero Touch Provisioning (ZTP) * Funkce mDNS brány pro distribuci a filtraci multicast služeb napříč IP subenty. (Apple Bonjour Gateway) * Automatická konfigurace portu podle připojeného zařízení (automatické nastavení tagged a untagged VLAN, QoS a ACL) * Podpora IP SLA pro měření zpoždění provozu VoIP |  |  | public |
| Segmentace WIFI sítě pro všechny uživatele KÚSK | * Pokrytí všech prostor budovy KÚSK pro využití HW prostředků s Wifi připojením pro pracovníky KÚSK, zastupitelstvo, klienty úřadu v oblasti využití vazby na registrované VISy KÚSK. * WiFi síť s duální frekvencí 2,4 a 5 GHz s podporou WiFi 6 (standardy 802.11n/ax), řízená controlery v HA (High Availability – režim vysoké dostupnosti). * Technická specifikace bude vypracována na základě proměření budovy na prostupnost signálu v součinnosti se zadavatelem. * Dodávku řešení a pro implementace zabezpečení sítě dle standardu 802.1x, včetně řešení pro inteligentní správu zařízení, které standard 802.1x nepodporují (tiskárny, IP kamery apod.) + BYOD (Bring Your Own Device − ověřování zařízení, které nejsou v doméně, např. telefony, tablety včetně licence na min. 500 zařízení. Přípustné je řešení formou 2ks HW appliance v HA režimu nebo 1ks virtuální appliance s podporou Vmware. Implementace řešení musí zahrnovat kompletní implementaci ověřování 802.1x pro bezdrátovou síť mimo konfigurace klientů a přípravu řešení pro drátovou síť včetně odpovídající konfigurace dodávaných switchů. * 121 x Access Point s minimálními parametry:   + Určený pro instalaci na strop/podhled   + Integrované všesměrové antény (v horizontální rovině) pro obě pásma   + Dvě samostatná rádia pro paralelní provoz ve 2,4GHz a 5GHz pásmech   + Konfigurace rádií: 4x4:4 pro 5GHz a 2x2:2 pro 2,4GHz   + Přenosové rychlosti: až 4,8Gbps pro 5GHz a 575Mbps pro 2,4GHz   + Podpora standardů 802.11a/b/g/n, 802.11ac wave 2 a 802.11ax   + Certifikace Wi-Fi Aliance: Wifi Enhanced Open   + Certifikace Wi-Fi Alliance: WiFi WPA3 Enterprise (včetně CNSA, SAE, OWE)   + Záruka výrobce za dodatečnou certifikaci Wi-Fi Alliance: WiFi 6 (včetně případné výměny necertifikovaných zařízení)   + Minimální počet inzerovaných SSID (BSSID) per radio: 16   + Podpora mechanismu pro optimalizaci fáze vysílaného bezdrátového signálu - Transmit Beam Forming (TxBF)   + Podpora víceuživatelského vícenásobného vstup a výstupu (MU-MIMO)   + Automatizovaná migrace klientů na optimální frekvenci, AP či rádio s využitím min. těchto parametrů: kategorie daného klienta, SNR, schopnosti klienta, kvalita signálu, zhodnocení dostupných AP z pohledu klienta   + Podpora přenosu řídících i uživatelských dat skrze controller v tzv. tunelovém režimu   + Podpora operačního režimu AP umožňujícího formování clusteru AP, který se následně chová jako kontrolér – tedy synchronizuje konfiguraci AP a zajišťuje centrální funkce (např. automatické plánování kanálů, aktivní roaming, band steering atp.) AP musí být schopna formovat clustery nejméně o velikosti 100AP.   + Hardwarová podpora šifrovaní řídících i uživatelských dat přenášených mezi AP a controllerem   + AP uzavřené konstrukce, bez větracích otvorů a ventilátoru   + Podpora přímého přístupu na příkazovou řádku AP přes serial konzoli a přes IPv4 a IPv6 pomocí Telnet a SSH   + Napájení AP pomocí 802.3at/af PoE   + USB 2.0 port využitelný pro záložní LTE uplink zapojením LTE modemu   + 2,5Gbps ethernet rozhraní dle standardu 802.3bz a NBase-T   + Bluetooth rozhraní pro navigační a management účely   + Podpora spektrální analýzy pro monitoring non-WIFI rušení   + Podpora ověření AP do sítě pomocí 802.1x suplikanta * 2 x WiFi controllery zapojené do HA clusteru s minimálními parametry:   + Dedikované HW appliance s 2x SFP+ 10 Gbe porty   + Je vyžadováno, aby HW appliance byly vybaveny specializovanými CPU či ASIC pro odbavování a zpracování síťového provozu, nikoliv generickými x86 procesory.   + Podpora pro 802.11u, 802.11v, 802.11k a 802.11w   + Podpora XML a REST API pro automatizovanou konfiguraci kontroléru   + Klasifikace klientských zařízení do tříd na základě typu nebo OS zařízení a následné uplatnění definovaných politik pro danou třídu   + Podpora STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)   + Podpora OSPF   + Podpora rozpoznavani aplikací na 7. vrstvě (aplikace typu: Youtube, Facebook, Dropbox, BitTorrent, Skype, Office365, apod.). Možnost jejich povolování, zakazování, prioritizace nebo omezování s možnosti vytvořit minimálně 20 souběžných aplikačních pravidel k ošetření provozu konkrétních aplikací.   + Podpora Bonjour services gateway, zpracování mDNS paketů, možnost filtrování služeb mezi subnety   + Podpora WIPS pro detekci a zamezení útoků na bezdrátovou síť   + Podpora monitoringu IP telefonních a UCC komunikačních spojení – přehled o proběhlých hovorech a zhodnocení z hlediska jejich kvality a SLA   + Automatické dynamické rozpoznání a prioritizace hlasových protokolů jako SIP, SCCP, VOCERA a SVP pomocí funkce DPI a jejich SLA monitoring   + Podpora protokolů RADIUS a TACACS+ pro ověřování administrátorů a uživatelů do sítě včetně CoA dle RFC3576 a RadSec (Radius Over TLS)   + Podpora tunelového režimu propojení s nabízenými AP s transportem veškerého i uživatelského provozu přes controller a možností jeho šifrování * 18 x L2 switch (min. 8 x 10/100/1000 Mbps + 2x SFP 1Gb) a 1 x L2 switch (min. 24 x 10/100/1000 Mbps + 2x SFP 1 Gb) s minimálními parametry:   + Podpora PoE+ 802.3at na všech metalických portech a 802.1x ověřování   + Podpora MVRP dle standardu 802.1ak pro distribuci VLAN   + STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)   + Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675   + Podpora RADIUS včetně RADIUS CoA (RFC3576)   + Podpora REST API pro automatizaci nastavení sítě.   + Podpora Zero Touch Provisioning (ZTP)   + Funkce mDNS brány pro distribuci a filtraci multicast služeb napříč IP subenty. (Apple Bonjour Gateway)   + Automatická konfigurace portu podle připojeného zařízení (automatické nastavení tagged a untagged VLAN, QoS a ACL) * 3 x PoE injektor dle 802.3af 1Gpbs. * 1x Sjednocená management platforma pro dodávané WiFi řešení a switche (přípustná je 1ks fyzická appliance nebo 1 ks virtuální appliance s podporou Vmware)   + Podpora upgrade firmware switchů   + Podpora zálohování a zpětné nahrávání konfigurací zařízení   + Monitorování a sběr aplikačních toků ze sítě minimálně po 30 dní   + Monitorování a sběr historie bezdrátové sítě a připojených klientů minimálně 180 dní   + Vizualizace fyzické topologie sítě (automatická-bez nutnosti manuálního zadávání zařízení)   + Sledování a vyhodnocení kvality a spolehlivosti síťových služeb: DNS, DHCP, RADIUS   + Možnost importu mapových podkladů a zakreslení rozmístění AP. Následná simulace pokrytí prostoru signálem a zobrazení připojených klientů lokalizační metodou triangulace pomocí RSSI. * 1x Reportovací nástroj pro WiFi řešení a dodávané switche – přípustná je 1ks fyzická appliance nebo 1 ks virtuální appliance s podporou Vmware. Minimální velikost úložiště (pro HW appliance v RAID) 4 TB. Může být společný pro firewally, WiFi access pointy a switche. Může být sloučen se sjednocenou management platformou. * Licence pro všechny části řešení po dobu udržení projektu. * Instalace strukturované kabeláže z technických místností k AP tunelem pod stropem. Pro instalaci bude dle kvalifikovaného odhadu zadavatele potřeba minimálně 2800 m UTP kabelu a 50 m lišt. |  |  | public |

**Obecné informace:**

Pokud zadavatel vyžaduje jako parametr některých prvků optické SFP/SFP+, zadavatel k tomu konstatuje, že v rámci budovy má vybudovány MM optické trasy a že optické transceivery jsou vyžadovány jako součást nabídky. V rámci dodávky bude zajištěno úvodní a průběžné školení administrátorů v rozsahu 20 MD.

**Dílčí cíle implementace systému:**

* Navrhnout řešení dle požadavků výše.
* Navrhnout a popsat architekturu včetně potřebného HW a potřebného SW včetně požadované integrace do prostředí Zadavatele.
* Naplnit požadavky pro významné informační systémy pro řešenou oblast ze zákona č. 181/2014 Sb. o kybernetické bezpečnosti a příslušných vyhlášek v platném znění a souvisejících část normy ČSN ISO/IEC 27001:2014 (nebo rovnocenné řešení).
* Implementovat celé řešení podle návrhu schváleného Zadavatelem včetně migrace stávajícího řešení firewallů na nové.
* Servisní podpora v režimu 12/5/365 tj. v pracovní dny od 7-19 hodin s reakcí do 4 hodin.

**Záruka a podpora (maintenance) výrobce:**

Minimální záruka a podpora (maintenance) garantovaná výrobcem na dodané systémy je požadována v délce 60 měsíců. Pokud výrobce neumožňuje nákup záruky a podpory na 60 měsíců dopředně, zavazuje se dodavatel, že v rámci dodávky nabídne a dodá záruku a podporu na dobu co nejbližší 60 měsícům a poté bude tyto periodicky nakupovat ke své tíži tak, aby zajistil pro zadavatele záruku a podporu poskytovanou kontinuálně na požadovaných 60 měsíců.

## Zvýšení fyzického zabezpečení HTCK

*Realizace tohoto opatření naplní § 17 Fyzická bezpečnost* Vyhlášky č.82/2018 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti v platném znění*.*

Jedná se o pořízení klimatizační jednotky, která bude umístěna ve vyhrazených prostorách OINF v místnosti budovy KÚSK 038 a dodávku zhášecího zařízení na bázi plynů inergenů umístěného ve vyhrazeném prostoru OINF v místnosti č. 2106 budovy KÚSK. Dodávkou těchto zařízení docílíme zvýšení technické dostupnosti služeb informačních technologií nastavením standardního teplotního prostředí v prostorách UPS TCK a omezíme vzniklé škody na zařízení informačních technologií instalovaných v místnosti 2106 KÚSK v případě zahoření.

**Požadovaný účel implementace technologických zařízení:**

Zvýšení dostupnosti služeb informačních technologií regulací teploty a omezení škod při zahoření prostor s instalovanými HW prvky informačních technologií KÚSK.

**Základní požadavky implementace systému:**

Požadavky zadavatele jsou uvedeny ve sloupci „Minimální technické požadavky, které zadavatel požaduje“. Dodavatel je povinen vyplnit, zda jím nabízený produkt / řešení tyto požadavky splňuje, a to v sloupci „Splnění požadavků zadavatele“ (dodavatel doplní prohlášení ANO nebo NE podle skutečnosti). Ve sloupci „Odkaz do nabídky“ dodavatel uvede odkaz na konkrétní část nabídky, ve které je možné ověřit splnění uvedeného požadavku. Následná smlouva s vybraným dodavatelem může být v této části upravena tak, aby obsahovala již pouze dodavatelem nabídnuté zařízení a jeho technické parametry.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Minimální technické požadavky, které zadavatel požaduje | | Splnění požadavků zadavatele (ANO/NE) | Odkaz do nabídky dodavatele, kde je možné ověřit splnění požadavku | Public/NDA |
| Část | **Popis** |
| Klimatizační jednotka | * Celoroční chlazení serverovny invertní klimatizací (2 jednotky) s centrálním ovládáním. * Automatická regulace teploty v závislosti zatížení tepelným výkonem. * Signalizace provozu a výpadku administrátorům klimatizovaných prostor, napojení na centrální alarm budovy. * Filtrace antibakteriální standardní. * Chladící/topný výkon kW/hod, − stanoví výpočtem dodavatel. * Vnitřní jednotka nástěnná * Ovládání IR (infra) nebo kabelový ovladač * Záruka na dodané zařízení min. 60 měsíců. * Čištění klimatizační jednotky nejméně 2 x ročně. |  |  | NDA |
| Parametry místnosti | * VxŠXH: 270x260x590, sklepní místnost. * Okna: nejsou; jen vývod pro vzduchotechniku pod úrovní terénu. * Dveře: obyčejné plechové, nutno utěsnit – návrh na dodávku bezpečnostních dveří. * Omezení instalace: venkovní klimatizační jednotky – nutno najít prostor k umístění (vchod „C“ do úřadu). * Napájení: samostatný přívod el. energie jištění dieselagregátem a automatickým přiřazováním. * UPS: 3x EATON 9355−30−NHS−7−2x9Ah, output: 30kVA 27 KW (stávající řešení, není součástí zadání) Výkon se bude navyšovat minimálně 2x. * Nenapojeno na centrální alarm budovy. * Rozměrový náčrt místnosti s umístěnými technologiemi vydá zadavatel na vyžádání. |  |  | NDA |
| Automatický zhášecí systém | * Okamžitá reakce na dým (zajištěno optickokouřovým hlásičem). * Zaplavení celého prostoru pří výskytu dýmu, uhašení vzniklého požáru s následným ochlazením chráněného prostoru. * Spuštění hasícího systému musí signalizovat zvukové a elektronické signalizační zařízení. * Spuštěním hasícího systému musí být automaticky ukončeno větrání místnosti, aby nedošlo k úniku plynu potřebného k hašení. * V případě výpadku elektrické energie musí být zařízení vybaveno záložním systémem spuštění v případě zahoření. * Použité hasivo nesmí být toxické a při určité koncentraci hašení nesmí ohrozit obsluhu zařízení. * Zhášecí zařízení nesmí překročit procentní obsah ve vzduchu, který povoluje norma a nesmí obsluhu ohrozit na životě. * Zhášecí zařízení musí být certifikováno pro použití v ČR. * Výstup pro relé na větrání. * Zajištění servisu zařízení po dobu 60 měsíců v rozsahu minimálně jednou za 12 měsíců:   + Prohlídka zařízení s kontrolou jednotlivých částí.   + Kontrola úniku hasiva detektorem s jeho převážením.   + Kontrola vnitřního tlaku nezávislým manometrem.   + Kontrola funkce hlásiče a záložního systému spouštění hasiva.   + Kontrola funkce ventilu bez vypuštěného hasiva.   + Vystavení protokolu o kontrole do evidence KÚSK. |  |  | NDA |
| Parametry místnosti | * Celková VxŠxH: 350 x 280 x 680. * VxŠxH: zdvojené podlahy: 26 x 280 x 360. * Okno: 1 rozměr 170 x 235. * Dveře: bezpečnostní dveře s těsněním. * Omezení instalace: dvojitá podlaha. * Napájení: samostatný přívod el. energie jištěný UPS a dieselagregátem. * Napájeno na centrální alarm budovy, požární čidla. * 2 centrální klimatizace, dvě náhradní a vzduchotechnika. * Technicky místnost odpovídá standardu pro serverovny. * Technická zdvojená podlaha. |  |  | NDA |

**Obecné požadavky na realizaci:**

Venkovní jednotka klimatizace bude umístěna na zdi ve dvoře v 1.NP, jednotka bude přichycena konzolí na zeď, vzdálenost cca 20 m.

Stavební prostupy včetně začištění a protipožárního utěsnění budou součástí předmětu plnění ze strany vybraného dodavatele v součinnosti s hospodářskou správou Zadavatele.

**Dílčí cíle implementace systému:**

* Navrhnout řešení dle požadavků výše.
* Implementovat celé řešení včetně potřebných úprav stavebních prostupů.
* Servisní podpora v režimu 12/5/365 tj. v pracovní dny od 7-19 hodin s reakcí do 4 hodin.

**Záruka a servis:**

Minimální záruka garantovaná výrobcem a servis na dodaný systém dodavatelem je požadována v délce 60 měsíců. Pokud výrobce neumožňuje nákup záruky a servisu na 60 měsíců dopředně, zavazuje se dodavatel, že v rámci dodávky nabídne a dodá záruku a servis na dobu co nejbližší 60 měsícům a poté bude tyto periodicky nakupovat ke své tíži tak, aby zajistil pro zadavatele záruku a servis kontinuálně poskytovaný na požadovaných 60 měsíců.

## Sdílené služby kybernetické bezpečnosti

Součástí služby jsou následující činnosti:

* 1. zaznamenávání a ukládání logů a detekce bezpečnostních událostí
  2. analýza datových toků a detekce bezpečnostních událostí
  3. dohledové centrum - SOC

## Zaznamenávání a ukládání logů a detekce bezpečnostních událostí

*Realizace tohoto opatření naplní, dle* Vyhlášky 82/2018 Sb., *§22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů, § 24 Sběr a vyhodnocování kybernetických bezpečnostních událostí.*

Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů zajistí tzv. log management. Mimo sběru logů řeší log management i zajištění jejich uložení v nezměněné podobě minimálně po zákonem definovanou dobu.

Security Information and Event Management (dále jen „SIEM“) je jedním ze základních stavebních prvků, který zajišťuje nutné bezpečnostní informace pro plnění povinností vyplývajících ze Zákona o kybernetické bezpečnosti a příslušných vyhlášek. Bez SIEM nástroje nelze reálně splnit požadavek na vyhodnocování kybernetických bezpečnostní události a následného hlášení kybernetického bezpečnostního incidentu dle § 7 a § 8 zákona 181/2014 Sb.

Poptávané řešení bude dodáno formou rozšíření služby SOC o sběr, uložení, vyhodnocování logů a detekce kybernetických událostí, musí umožňovat efektivně reagovat na již proběhlé bezpečnostní incidenty.

Dále služba umožní dlouhodobé ukládání dat v nezpochybnitelné podobě pro potřeby shody s předpisy, požadavky pro forenzní analýzu, případné bezpečnostní audity a orgány ČR. Systém poskytuje i informace pro operační a provozní úseky, kterým bude umožněno snadnými dotazy proti uložené databázi s logy nalézat například podstatu možného bezpečnostního incidentu u aplikačního nebo infrastrukturního systému, okamžitě identifikovat podstatu identifikované hrozby, včetně rychlého dohledání událostí popisujících její příčinu. Poptávané řešení musí poskytovat vysokou dostupnost sběru a transportu logů minimálně na úrovni sběračů logů.

Navazující rozšiřující službou bude SIEM, který v reálném čase vyhodnotí bezpečnostní výjimky z uložené databáze a prezentuje data ve formě předdefinovaných reportů. Systém bude podporovat sběr všech potenciálních událostí a logů vznikajících v informačním systému KÚSK a zajistí jejich ukládání do centrálního zabezpečeného úložiště. Od systému bude požadováno, aby rychle vyhodnocoval velké množství dat, které okamžitě zpracuje.

Rozsahy a formy poskytovaných rozšiřujících služeb nesmí být pevně svázána s rozsahem a formou poskytované služby SOC.

Nabízené rozšíření služby SOC zajistí provozování celého systému tak, aby odpovídal všem relevantním zákonným normám a aktuálním trendům v dané oblasti a zadavatel nemusel investovat do dalších lidských zdrojů pro administraci, správu a podporu řešení.

**Požadovaný účel služby:**

Poskytnout komplexní službu pro zaznamenávání logů vznikajících na infrastruktuře KÚSK s důrazem na autonomní detekci bezpečnostních událostí v oblasti provozovaných VIS KÚSK na serverové části včetně možnosti jejich uložení do neměnné databáze. Zajistit poskytování služby dodavatelem v souladu s požadavky zadavatele a trendy v oboru.

**Základní požadavky na službu:**

Požadavky zadavatele jsou uvedeny ve sloupci „Minimální technické požadavky, které zadavatel požaduje“. Dodavatel je povinen vyplnit, zda jím nabízená služba tyto požadavky splňuje, a to v sloupci „Splnění požadavků zadavatele“ (dodavatel doplní prohlášení ANO nebo NE podle skutečnosti). Ve sloupci „Odkaz do nabídky“ dodavatel uvede odkaz na konkrétní část nabídky, ve které je možné ověřit splnění uvedeného požadavku. Následná smlouva s vybraným dodavatelem může být v této části upravena tak, aby obsahovala již pouze dodavatelem nabídnutou službu a její technické parametry.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Minimální technické požadavky, které zadavatel požaduje** | | **Splnění požadavků zadavatele (ANO/NE)** | **Odkaz do nabídky dodavatele, kde je možné ověřit splnění požadavku** | **Public/NDA** |
| *§22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů*  *§24 Sběr a vyhodnocování kybernetických bezpečnostních událostí* | | | | |
| 1. | Řešení musí být funkčně i technicky odděleno od ostatních částí systému SIEM |  |  | public |
| 2 | Řešení nesmí nijak zasahovat do sbíraných systémů. |  |  | public |
| 3 | Řešení musí být schopno trvale zpracovávat 10000 EPS |  |  | public |
| 4 | Řešení musí umožnit uchování log záznamů (RAW formát) po dobu minimálně 13 měsíců |  |  | public |
| 5 | Řešení musí poskytnout vysokou dostupnost sběru logů (sběračů). |  |  | public |
| 6 | Řešení musí podporovat (sbírat, zpracovat a interpretovat) všechny typy logu a protokolů nezbytné pro zpracování dle vyhlášky 82/2018 Sb.  Jmenovitě musí podporovat zejména následující typy logů a protokolů:  TCP/UDP Syslog, WMI, SQL, FTP, S/TP/SCP, SNMP, ODBC/JDBC, CP-LEA, SDEE, log file protokol RAW, CEF, JSON RFC7159 a další.  Windows Events Collection (WinRM/ RPC) - MS Windows Vista SP2 a vyšší, MS windows Server 2008 a vyšší, MS SQL 2008 a vyšší. |  |  | public |
| 7 | Řešení musí podporovat bezagentový sběr logů (sběr bez nutnosti instalovat agenta na cílový systém) |  |  | public |
| 8 | Řešení musí podporovat načítání log souborů (jedno a víceřádkové textové logy), kde tyto soubory budou mít stanovenou strukturu a význam dat. |  |  | public |
| 9 | Komponenta sbírající logy je posílá dále zašifrovaně a komprimovaně a umožňuje regulovat šířku užívaného pásma. |  |  | public |
| *§ 24 Sběr a vyhodnocování kybernetických bezpečnostních událostí.* | | | | |
| 10 | Licence pro trvalé zpracování 1000 EPS v rámci celodenního průměru, která musí být rozšířitelná na 5000 EPS v celodenním průměru. |  |  | NDA |
| 11 | Architektura produktu obsahuje realtime procesory pro sběr a analýzu událostí včetně fulltext databáze pro ukládání a analýzu dat. |  |  | public |
| 12 | Řešení zvládá krátkodobé výkonové špičky (trvání 24 hodin) o objemu 7500 EPS. |  |  | NDA |
| 13 | Řešení musí podporovat současnou práci minimálně 5 administrátorů či operátorů. |  |  | public |
| 14 | Řešení musí obsahovat možnost minimálně 1000 sběrných konektorů |  |  | public |
| 15 | Řešení nebude licenčně omezeno úložnou kapacitou. |  |  | public |
| 16 | Licence umožňuje dočasné překročení EPS limitu na dobu několika minut bez ztráty přijímaných událostí. |  |  | public |
| 17. | Možnost definovat na základě rolí uživatelům přístup k jednotlivým zařízením, jejich skupinám či síťovým segmentům. |  |  | public |
| 18. | Možnost uložení uživatelem vytvořených pohledů na data (dashboardů, pojmenovaných dotazů) pro budoucí zpracování. |  |  | public |
| 19 | Systém umožňuje tvorbu pravidelných reportů podporujících řízení bezpečnosti podle standardu ISO 27001 s tím, že úroveň reportování bude specifikována v průběhu provozu SOC. |  |  | public |
| 20 | Služba splňuje požadavky kladené evropskými a českými bezpečnostními normami – ISO 27001, GDPR a zákon 181/2014 Sb. - Zákon o kybernetické bezpečnosti. |  |  | public |
| 21 | Řešení Služby bude poskytovat automaticky backup/recovery procesu. |  |  | public |
| 22 | Poskytovat interní kontroly stavu zařízení (healthcheck) a upozornění uživatele v případě problému. |  |  | public |
| 23 | Poskytování analytické a korelačních funkcí bez dalších zásahů a činností (out-of-the-box). |  |  | public |
| 24 | Systém musí umožňovat definici vlastního parseru pro jednotlivé zdroje logů a tím, že uživatelská konfigurace vlastních parserů pomocí vizuálního programovacího jazyka. |  |  | public |
| 25 | Požadujeme zajištění integrity nasbíraných dat, kdy data jsou kontrolována před neoprávněnou změnou nebo smazáním. |  |  | public |
| 26 | Požadujeme možnost nastavit více filtrů retenčních politik pro různé zdroje dat |  |  | public |
| 27 | Near-real-time analýza událostí |  |  | public |
| 28 | S ohledem k nastavení a provádění procesu získávání, zaznamenání a zpracování logů je přípustná detekce bezpečnostních událostí v řádu minut. |  |  | public |
| 29 | Analýza dlouhodobých trendů událostí |  |  | public |
| 30 | Pokročilé "drill-down" dohledávání v případě potřeby |  |  | public |
| 31 | Vyhledávací rozhraní systému správy logů musí poskytovat podporu jak pro zadání dotazu s použitím Booleovy logiky, tak pro zadání regulárními výrazy |  |  | public |
| 32 | Poskytování alertů na detekované anomálie, změny chování sítě a změny v generování logů a událostí |  |  | public |
| 33 | Korelační modul musí poskytovat již po instalaci (out-of-the-box) metody korelačních pravidel, která automatizují zjišťování incidentů |  |  | public |
| 34 | Korelační systém musí využívat i externí on-line reputační databázi pro vyhodnocování bezpečnostních rizik. |  |  | public |
| 35 | Systém musí být schopen využít detekované anomálie a informace ze sítě pro korelaci s logy do jednotných incidentů, pro zpřesnění kontextu a snížení false-positives |  |  | public |
| 36 | Řešení musí poskytnout alerting vycházející z detekovaných bezpečnostních hrozeb od monitorovaných zařízení |  |  | public |
| 37 | Požadujeme schopnost samostatného “učení” normálního stavu. Podle nastavené bezpečnostní politiky pak reagovat na vznik skupinových nebo kontextuálních anomálií. |  |  | public |
| 38 | Vykonávání akci v závislosti na přijatém logu jako např. zaslat email, notifikaci nebo spustit předem definovaný skript |  |  | public |
| 39 | Schopnost pracovat s IP geolokacemi (botnet kanály atp.) |  |  | public |
| 40 | Generování alertu při výpadku logů z konkrétního zařízení |  |  | public |
| 41 | Vestavěný mechanismus na klasifikaci systémů podle typu (např. mail server vs. databázový server) |  |  | public |
| 42 | Poskytování rozhraní pro reporting, pomocí kterého lze vytvářet nové sestavy bez nutnosti sestavovat SQL dotazy |  |  | public |
| 43 | Požadujeme pravidelnou, plánovanou tvorbu takových reportů minimálně ve formátech PDF a CSV + podporu alespoň jednoho běžně používaného formátu pro strojové čtení (XML či JSON) |  |  | public |
| 44 | Řešení musí obsahovat nativní podporu vysoké dostupnosti (HA) bez rozšiřujících komponent/software třetích stran. |  |  | public |
| 45 | Řešení musí nabízet přístup k datům skrze otevřené REST API pro integraci s dalšími systémy. |  |  | public |
| 46 | Řešení musí uchovávat logy v normalizovaném formátu, tak i „raw“ formátu. |  |  | public |
| 47 | Řešení musí obsahovat funkcionalitu pro výměnu standardizovaných informací informačně bezpečnostního charakteru, jako jsou STIX nebo TAXII. |  |  | public |
| 48 | Řešení musí být navázáno na národní centrum kybernetické bezpečnosti CSIRT a publikovat v konzoli jím aktuálně uveřejněné hrozby. |  |  | public |
| 49 | SIEM použitý v řešení musí být zařazen do 5 posledních studií agentury Gartner (tzv. magických kvadrantů) |  |  |  |

**Další požadavky na rozšiřující službu SOC:**

* Nabízená služba detekce bezpečnostních událostí musí:
  + naplnit požadavky pro významné informační systémy pro řešenou oblast ze zákona č. 181/2014 Sb. o kybernetické bezpečnosti a příslušných vyhlášek v platném znění a souvisejících část normy ČSN ISO/IEC 27001:2014 (nebo rovnocenné řešení).
  + zajistit dlouhodobé uschování logů pro předložení organizacím zabývajícím se bezpečností, zejména NBÚ a orgánům činným v trestním řízení.
  + zajistit v rámci poskytování služby SIEM napojení „Primárních aktiv“, kterými jsou významné informační́ systémy (VIS) Krajského úřadu Středočeského kraje, pokud tato aktiva poskytují využitelné výstupy, které lze automatizovaně zpracovat:
    1. Spisová služba
    2. Ekonomický systém
  + zajistit v rámci poskytování služby SIEM napojení „Podpůrných aktiv“, kterými jsou bezpečnostní systémy a veškeré ICT prvky pro zajištění provozní dostupnosti, důvěrnosti a integrity informací:
    1. Ochrana perimetru a přístupy k perimetru sítí Internet/DMZ/LAN/WiFi
    2. Komponenty datové sítě (switch, router, hub, access point)
    3. Network Behavior Analyzer
    4. Autentizační a autorizační systémy
    5. Anti (mallware, spam, adware) systémy
    6. Vulnerability management systém
    7. Databázové systémy
    8. Provozní dohledové systémy (Servery, Storage, Datová síť, Energy infrastruktura, Zálohování dat)
    9. Zálohovací systémy
    10. Operační systémy serverů – Unix a Windows
    11. Virtualizační infrastruktura

**Záruka a podpora (maintenance) výrobce:**

Poskytovatel služby zajistí, že po celou dobu poskytování služby budou veškeré využité části kryté zárukou a podporou ze strany výrobce. Z tohoto důvodu zadavatel nepřipouští open sourcové řešení.

**Doba poskytování služby:**

Služba bude poskytována po dobu 60 měsíců.

## Analýza datových toků a detekce bezpečnostních událostí

*Realizace tohoto opatření naplní § 23 Detekce kybernetických bezpečnostních událostí* Vyhlášky č.82/2018 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti v platném znění*.*

Jedná se o komplexní službu pro monitorování sítě KÚSK na základě datových toků, kterou umožní nástroje pro sledování provozu a zabezpečení sítě. Služba bude podporovat následná řešení vyskytujících se problémů a nestandardních stavů v síti, monitoring aktivit uživatelů a provozovaných SW aplikací. Služba umožní správcům pohled na využití síťového provozu na infrastruktuře KÚSK. Služba disponuje funkcí, která umožní sledovat výkonové parametry sítě a technologií analýzy datových toků včetně vyhodnocování chování sítě v návaznosti na aktuální hrozby a nestandardní stavy.

Rozsahy a formy poskytovaných rozšiřujících služeb nesmí být pevně svázána s rozsahem a formou poskytované služby SOC.

Nabízené rozšíření služby SOC zajistí provozování celého systému tak, aby odpovídal všem relevantním zákonným normám a aktuálním trendům v dané oblasti a zadavatel nemusel investovat do dalších lidských zdrojů pro administraci, správu a podporu řešení.

**Požadovaný účel služby:**

Poskytnout komplexní službu pro zaznamenávání aplikačních logů vznikajících na infrastruktuře KÚSK s důrazem na autonomní detekci bezpečnostních událostí v oblasti provozovaných VIS KÚSK na serverové části včetně možnosti jejich uložení do neměnné databáze. Zajistit poskytování služby dodavatelem v souladu s požadavky zadavatele a trendy v oboru.

**Základní služby:**

Požadavky zadavatele jsou uvedeny ve sloupci „Minimální technické požadavky, které zadavatel požaduje“. Dodavatel je povinen vyplnit, zda jím nabízená služba tyto požadavky splňuje, a to v sloupci „Splnění požadavků zadavatele“ (dodavatel doplní prohlášení ANO nebo NE podle skutečnosti). Ve sloupci „Odkaz do nabídky“ dodavatel uvede odkaz na konkrétní část nabídky, ve které je možné ověřit splnění uvedeného požadavku. Následná smlouva s vybraným dodavatelem může být v této části upravena tak, aby obsahovala již pouze dodavatelem nabídnutou službu a její technické parametry.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Minimální technické požadavky, které zadavatel požaduje | | Splnění požadavků zadavatele (ANO/NE) | Odkaz do nabídky dodavatele, kde je možné ověřit splnění požadavku | Public/NDA |
| Část | **Popis** |
| Řešení | * V rámci monitoringu infrastruktury KÚSK se předpokládá využití:   + 1x Kolektor a detekční moduly.   + 2x Modul sonda.   + Dále jako zdroj budou připojeny alespoň 2x core přepínače. |  |  | NDA |
| Obecné | | | |  |
| Monitorování sítě | * Schopnost analyzovat provoz ze SPAN portu centrálních switchů, TAP zařízení nebo zdrojů NetFlow dat. * Protokoly NetFlow v9 a IPFIX nebo ekvivaletní. * Podpora pro IPv4, IPv6, VLAN, MPLS * Neviditelné na L3 vrstvě (monitorovací porty nemají IP, je zcela pasivní. * Zaznamenávání vybrané komunikace do formátu PCAP z celé sítě. * Řešení, které významným způsobem nezatíží datové linky zadavatele (nárůst provozu o max 5%) |  |  | public |
| Komponenty | | | |  |
| Modul NetFlow kolektor | * Záznamy dat 12 měsíců zpětně na RAID poli. * Dedikovaná kapacita je alespoň 48TB dat. * Zabezpečená vzdálená správa, dohled a konfigurace. |  |  | NDA |
| Modul NetFlow sonda | * 2 kusy sondy * Realizováno hardware komponentami s instalaci do 19“ racku, každá sonda max. 1RU. * Zabezpečená vzdálená správa, dohled a konfigurace. * Podpora standardu NSEL, monitorování MAC adres. * Fyzická monitorovací rozhraní minimálně 2x 10Gbps pro každou sondu * Sondy poskytnou na každém monitorovacím portu monitorování v rychlosti 10 Gbps * Podpora pro příjem a analýzu HTTP/HTTPS provozu. * Pasivní zapojení monitorovacích portů přes TAP. * Zpracování všech FLOWs – nesamplované. * Monitoring zpoždění sítě a odezvy aplikace. |  |  | public |
| Modul detekce anomálií na síti | * Nástroj bude poskytován na kolektoru, kde bude dostupné grafické rozhraní a které bude i zdrojem pro reporting událostí pro rozšiřující službu SIEM. * Sběr a zpracování statistik o síťovém provozu. * Sbírání informací z netflow sond. * Detekce nežádoucích vzorů chování na síti (útoky, anomálie datového provozu, nežádoucí aplikace, detekce virů a botnetů ve vnitřní síti, detekce odchozího spamu, provozních problémů). * Detekce anomálií vzhledem k dlouhodobému profilu chování zařízení na síti. * Předdefinovaná sada pravidel pro odhalování obecných anomálií v síti. * Vyhodnocování na základě implementace standardu Bidirectional flows (RFC 5103). * Integrace informací ze služeb DNS, DHCP, WHOIS, geolokační služby. |  |  | public |
| Modul analýzy a monitorování komunikace aplikací a systémů | * Pro naplnění zákona č.101/2000 Sb. v aktuálním znění má řešení detekovat a lokalizovat aktuální změny komunikace systémů, aplikací a uživatelů pracujících se zákonně klasifikovanými informacemi, tj.:   + Sledování komunikace systémů   + Sledování komunikace aplikací |  |  | public |
| Modul analýzy a monitorování výkonosti | * Sledování provozní výkonnosti datové sítě, minimálně Round Trip Time * Sledování provozní výkonnosti všech aplikací z provozu datové sítě, především reakce databází a WWW strojů. |  |  | public |
| Správa | | | |  |
| Víceuživatelský přístup | * Možnost definovat k jakým datům má jednotlivý uživatel přístup i v jednotlivých aplikačních modulech. |  |  | public |
| Webové rozhraní | * Uživatelsky definovat dashboard. * Správu provádět prostřednictvím webového rozhraní. |  |  | public |
| Aktualizace | * Zařízení pravidelně samostatně aktualizuje znalostní bázi. |  |  | public |
| Reporty | | | |  |
| Generování | * Vytvářet krátkodobé i dlouhodobé grafy a přehledy s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (http, IMAP, SSH), aplikačních protokolů atp. * Generování statistik a podrobných výpisů nad volitelnými časovými intervaly. * Export reportů a grafů alespoň do PDF. |  |  | public |
| Zasílání logů do SIEM | * Zasílání logů o detekovaných událostech ze všech detekčních modulů s možností uživatelské konfigurace přes GUI * Konfigurovatelný obsah logů |  |  | public |

**Dílčí cíle služby:**

* Navrhnout řešení služby dle požadavků výše.
* Navrhnout a popsat architekturu, včetně potřebného HW a potřebného SW, včetně požadované integrace do prostředí Zadavatele.
* Naplnit požadavky pro významné informační systémy pro řešenou oblast ze zákona č. 181/2014 Sb. o kybernetické bezpečnosti a příslušných vyhlášek v platném znění a souvisejících část normy ČSN ISO/IEC 27001:2014 (nebo rovnocenné řešení).

**Záruka a podpora (maintenance) výrobce:**

Poskytovatel služby zajistí, že po celou dobu poskytování služby budou veškeré využité části kryté zárukou a podporou ze strany výrobce. Z tohoto důvodu zadavatel nepřipouští open sourcové řešení.

**Doba poskytování služby:**

Služba bude poskytována po dobu 60 měsíců.

## Dohledové centrum - SOC

Předmětem poptávky je komplexní řešení pro centralizovanou správu, ukládání a vyhodnocování logů v nezměnitelné podobě z libovolných síťových aktivních prvků, operačních systémů a používaného aplikačního software provozované formou služby Sdíleného dohledového centra kybernetické bezpečnosti (SOC – Security Operation Centra). Implementace systému bude v provedena v souladu s § 22 a § 24 Vyhlášky č.82/2018 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti v platném znění.

**Požadovaný účel implementace opatření:**

Zajištění externě provozované / dodávané služby dohledového ICT bezpečnostního centra - SOC.

**Základní požadavky implementace systému:**

Požadavky zadavatele jsou uvedeny ve sloupci „Minimální technické požadavky, které zadavatel požaduje“. Dodavatel je povinen vyplnit, zda jím nabízený produkt / řešení tyto požadavky splňuje, a to v sloupci „Splnění požadavků zadavatele“ (dodavatel doplní prohlášení ANO nebo NE podle skutečnosti). Ve sloupci „Odkaz do nabídky“ dodavatel uvede odkaz na konkrétní část nabídky, ve které je možné ověřit splnění uvedeného požadavku. Následná smlouva s vybraným dodavatelem může být v této části upravena tak, aby obsahovala již pouze dodavatelem nabídnuté zařízení a jeho technické parametry.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Minimální technické požadavky, které zadavatel požaduje** | | **Splnění požadavků zadavatele (ANO/NE)** | **Odkaz do nabídky dodavatele, kde je možné ověřit splnění požadavku** | **Public/NDA** |
| **Požadavky na SOC** | | | |  |
| 1. | Poskytovatel prokazatelně doloží, že provozuje CSIRT (CERT), který je registrovaný v databázi TF – CSIRT Trusted Introducer. |  |  | public |
| 2. | Poskytovatel musí uvést adresu, kde jsou ukládána data SOC k prokázání zpracování dat v působnosti právních norem ČR |  |  | public |
| 3. | Informace o provozu a potenciálních zranitelnostech informačních systémů umožní zavádění preventivních opatření a předcházení případným bezpečnostním incidentům. |  |  | public |
| 4. | Zavedením systému zadavatel získá schopnost detekce bezpečnostních incidentů a informace pro jejich rychlejší a efektivnější řešení. |  |  | public |
| 5. | Reporty systému budou sloužit pro přehlednou kontrolu stavu a chování informačních systémů a uživatelů za určité období (typicky 1 měsíc) a ke kontrole dodržování compliance („jednání v souladu s pravidly") organizace zadavatele. |  |  | public |
| 6. | Pro případné auditní akce ze strany zadavatele systém umožní provádění tzv. NBA (Network Behavioral Analysis), tj. automatického trvalého monitorování síťového provozu nad prostředím sdíleného dohledového centra kybernetické bezpečnosti. Ze stejného důvodu bude nad významnými součástmi služby provozován nástroj pro audit a monitoring aktivit uživatelů. |  |  | public |
| 7. | Data uložená v systému a systémem archivovaná budou zajištěna a zabezpečena před neoprávněnou změnou i pro účely vyšetřování případného bezpečnostního incidentu.  Data / logy budou uskladněna v prostředí poskytnutém dodavatelem, a to minimálně na dobu požadovanou zákonem. |  |  | public |
| 8. | Vytvoření bezpečného sdíleného uložiště pro sdílení kompletních materiálů k poskytované službě. |  |  | public |
| 9. | Detailní analýza bude zahrnovat identifikaci zdrojů dat, jejichž provozně bezpečnostní informace bude nutné, popř. vhodné sbírat, korelovat a analyzovat. Analýza bude podléhat schválení zadavatelem. |  |  | public |
| 10. | Zdroje dat budou vybrány z tzv. primárních a podpůrných (technických) aktiv zadavatele (zejm. se jedná o systémy a řešení poptávané v této veřejné zakázce). K jejich určení bude využito vyhlášky č. 82/2018 Sb. o významných informačních systémech a jejich určujících kritérií přiměřeně uzpůsobených a aplikovaných na prostředí zadavatele (zadavatel provozu celkem 4 významné informační systémy – GINIS, e-mail, elektronickou spisovou službu a Service Desk). Dále bude pro určení zdrojů dat využito vstupního osobního setkání (workshopu) se správci provozovaných informačních a komunikačních systémů v rozsahu jednoho pracovního dne. |  |  | public |
| 11. | Předimplementační analýza bude obsahovat následující oblasti specifické pro SOC:   * + - * 1. specifikace profilu pro každý napojovaný zdroj dat, včetně určení vhodné úrovně detailu logování, odpovídající jeho roli v infrastruktuře,         2. klasifikaci zdrojů informací pro stanovení priority události (stejná událost z různých zdrojů může mít různou prioritu) a z hlediska poskytovaných logů (obsažené informace, struktura logu),         3. doporučení nastavení logování pro jednotlivé zdroje,         4. výběr událostí a parametry jejich záznamů a metody sběru z jednotlivých zdrojů,         5. návrh parserů pro zdroje, které nebudou systémem přímo podporovány,         6. návrh doplňování logovaných informací z dalších zdrojů pro zlepšení jejich relevantnosti či srozumitelnosti,         7. metody a pravidla identifikace, zpracování a vyhodnocování událostí, návrhy korelací,         8. pravidla pro vznik varováni, upozornění, incidentů včetně priority,         9. doporučenou strukturu oprávnění a řízení přístupových práv         10. proaktivní a reaktivní procesy (aktivity, role, výstupy, doba odezvy) v případě výskytu varování, upozornění, incidentu a apod.         11. popis zajištění autentičnosti logů,         12. definice pohledů na události v konzoli uživatelů (např. setřídění událostí podle zdroje, typu, priority, stupně důležitosti, času vzniku apod.),         13. návrh zálohování konfigurace a dat,         14. návrh průběhu Zkušebního provozu pro ověření funkčnosti systému v reálném provozu,         15. návrh retence logů a archivů,         16. návrh způsobu napojení řešení na monitorovací systém dodavatele a definice procesů reakce, které jsou v souladu s platnou legislativou a bezpečnostní politikou ISKÚ,         17. popis monitorovaných aktivit přispívajících k naplnění požadavků dle zákona č.101/2000 Sb. v aktuálním znění a k naplnění požadavků dle nařízení Evropského parlamentu a Rady (EU) 2016/679 (GDPR). |  |  | public |
| 12. | Součástí dodávky bude návrh změn konfigurací dotčených a souvisejících systémů, koordinace provedení změn s provozovateli systémů a ověření správné konfigurace. |  |  | public |
| 13. | Součástí dodávky bude návrh a provedení funkčních testů (musí zahrnovat výkonové testy, testy archivace/obnovy logů a ověření detekce neoprávněně modifikace logů). Návrh podléhá schválení zadavatele. |  |  | public |
| **Požadovaná podpora SOC** | | | |  |
| 14. | Průběžné monitorování IT prvků dodaných v rámci této veřejné zakázky, popř. prvků IT, které mohou ovlivnit jejich chod. Počet sledovaných parametrů nesmí být prakticky omezen (min. stovky). |  |  | public |
| 15. | Monitoring bude probíhat minimálně dle výstupů ze služby pro zaznamenávání a ukládání logů a detekce bezpečnostních událostí (SIEM), systému analýzy datových toků a detekce bezpečnostních událostí, systému pro pokročilý provozní dohled a firewallů zadavatele. |  |  | public |
| 16. | Helpdeskový systém s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení. |  |  | public |
| 17. | Rozšířený monitoring a specifické služby provozního zajištění komodity SOC:   * + - * 1. Provádění monitoringu systému a zpracovávaných dat v rozsahu potřebném pro provádění následujících služeb.         2. Informování odpovědných osob zadavatele o vzniku bezpečnostního incidentu v reálném čase za pomocí základních komunikačních nástrojů (mail / SMS / tel).         3. Zahájení řešení bezpečnostního incidentu do 4 hodin od vzniku, řízení souvisejících činností správců a případných dalších dotčených osob.         4. Zakládání tiketů, proaktivní komunikace o jejich řešení. Komunikace s třetí stranou jako NBÚ, NUKIB, CSIRT atd.         5. Rozšířený reporting – detailní report o událostech a incidentech s návrhy systematických opatření 1x měsíčně. Vzdálená prezentace reportu např. formou videokonference.         6. Kontinuální skenování aktiv definovaných danou sítí/sítěmi a zranitelností relevantních pro daná aktiva. Minimálně na začátku poskytování služby budou provedeny plné skeny a dále vždy 1x měsíčně skeny rozdílové.         7. Přístup administrátorů zadavatele ke sledovaným parametrům alespoň v režimu čtení prostřednictvím grafického rozhraní (GUI – dashboard apod.). |  |  | public |
| 18. | Dodavatel zpracuje a poskytne zadavateli každý měsíc Report, ve kterém je popsán průběh realizace Plnění za uplynulé období, provedené služby a návrh doporučených opatření pro další období pro zvýšení bezpečnosti, dostupnosti a prevenci incidentů. |  |  | public |
| **SLA** |  |  |  | public |
| 19. | Přístup k podpoře služby - HotLine/Ticket systém – 24 x 7 |  |  | public |
| 20. | Přístup k webovému portálu služby – 24 x 7 |  |  | public |
| 21. | Reakční čas na změnu konfigurace služby mimo Incident Response – 12x5 do 4 hodin |  |  | public |
| 22. | Reakční čas na mimořádnou událost – do 15 minut |  |  | public |
| 23. | **Služba Monitoringu a detekce - Zajištění Operátorské úrovně**  Průběžné sledování provozu prostředí objednatele.  Real-time analýza situace v napojených zařízeních podle skupin, kategorií zařízení a podle kontextu log záznamů nebo událostí.  Posouzení kontextu anomálie a příčin vzniku situace s případnou eskalací problému objednatele na analytického specialistu dodavatele. |  |  | public |
| 24. | **Služba reakce na nestandardní situace v provozu bezpečnostních systémů – Zajištění analytické úrovně**  Zpracování analytických scénářů na aktuální kybernetické hrozby.  Posouzení eskalovaného problému objednatele analytickým specialistou.  Detekce a vyhodnocení závažnosti identifikovaných anomálií.  Posouzení a ve spolupráci se Zadavatelem případná eskalace nestandardní situace v provozu objednatele na službu včasné výstrahy a reakce na incident v rámci bezpečnostních struktur ČR.  1x za měsíc předání analytického reportu za uplynulé období do 10 pracovního dne v následném měsíci interpretující stav bezpečnosti prostředí, účinnost nápravných opatření a seznam eskalace incidentů. |  |  | public |

**Doba poskytování služby:**

Dohledové centrum bude poskytováno formou služby po dobu 60 měsíců.

## Služby poradenství a podpory, resp. „Služby spojené s implementací IS“

## Předimplementační analýza

**Před implementací řešení zpracuje dodavatel předimplementační analýzu, minimálně pro následující oblasti a pro oblasti specifické pro jednotlivé dodávané produkty a služby:**

1. Detailní popis stávajícího stavu, identifikaci slabých míst a bezpečnostních rizik, včetně vazeb na HW a SW systémy TCK.
2. Způsob začlenění nabízených komodit do prostředí TCK, popis začlenění nabízených / dodávaných služeb do procesů zadavatele.
3. Síťová infrastruktura ve vztahu k plánovanému využití.
4. SAN infrastruktura ve vztahu k plánovanému využití.
5. Virtualizační infrastruktura (serverová, disková) ve vztahu k plánovanému využití.
6. Integrace nabízených softwarových systémů.
7. Rekonfigurace stávajících systémů.
8. Dopady implementace na dostupnost a funkčnost stávajících služeb.
9. Požadované součinnosti zadavatele a jejich rozsah.
10. Návrh opatření k odstranění neshod zjištěných v průběhu analýzy.

**Výstupem předimplementační analýzy bude písemná zpráva, která podléhá schválení zadavatelem.**

## Prováděcí dokumentace

**Po schválení předimplementační analýzy zpracuje dodavatel prováděcí dokumentaci minimálně pro následující oblasti a pro oblasti specifické pro jednotlivé dodávané produkty a služby:**

1. Dodavatel před zahájením implementačních prací zpracuje prováděcí dokumentaci, která bude vycházet ze schválené předimplementační analýzy a bude zahrnovat všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění veřejné zakázky do stávajícího prostředí TCK.
2. Prováděcí dokumentace musí být před zahájením prací schválena zadavatelem.
3. Prováděcí dokumentace musí zohlednit podmínky stávajícího stavu, požadavky cílového stavu a musí obsahovat minimálně tyto části:
   1. Detailní popis cílového stavu včetně funkcionalit jednotlivých částí dodávky.
   2. Nutné a doporučené optimalizační a konfigurační změny dodávaných systému i všech navázaných systémů TCK (vSphere, LAN, SAN, zálohování, monitorování atd.).
   3. Způsob zajištění potřebného HW a SW.
   4. Způsob zajištění koordinace realizace předmětu plnění s běžným provozem.
   5. Detailní návrh a popis postupu implementace předmětu plnění.
   6. Detailní popis zajištění bezpečnosti informací.
   7. Detailní harmonogram realizace včetně uvedení kritických milníků.
   8. Návrh designu síťového a bezpečnostního řešení a jeho konfigurace.
   9. Návrh designu aplikačních řešení.
   10. Vazby na stávající systémy a jejich konfigurace.
   11. Návrh akceptačních kritérií a akceptačních testů.

**Výstupem prováděcí dokumentace bude písemná zpráva, která podléhá schválení zadavatelem.**

## Projektové vedení dodávky

**V průběhu celého plnění veřejné zakázky (dodávka řešení) zajistí dodavatel projektové vedení dodávky:**

S ohledem na rozsah projektu a dopad jeho zavedení do produkčního provozu je požadováno aplikování základních principů projektového řízení ze strany dodavatele. Jedná se o následující aktivity:

1. Řízení projektových prací v souladu s uzavřenou smlouvu s ohledem na:
   1. věcné plnění dané smlouvou,
   2. řízení postupu prací s ohledem na závazný harmonogram projektu,
   3. dodržování termínů a milníků harmonogramu.
2. Zpracování pravdivých, úplných a věcně jasných a vypovídajících zápisů z konzultačních schůzek a pracovních jednání.
3. Prezenční účast odpovědné osoby dodavatele na kontrolních dnech v sídle zadavatele, případně se souhlasem obou smluvních stran formou videokonference nebo telekonference.
4. Reporting projektu na úrovni pravidelných dvoutýdenních písemných zpráv směrem k odpovědné osobě zadavatele.
5. Řízení rizik projektu.
6. Řízení změn na projektu – v případě odsouhlasení změn spolupráce při implementaci změn do projektu, komunikace s realizačním týmem.

## Dokumentace

**Zadavatel požaduje v rámci plnění zpracování a dodání konečné a úplné dokumentace k dodanému řešení v následující skladbě:**

1. Uživatelská dokumentace – v rozsahu konkrétních nasazených funkcionalit u zadavatele.
2. Administrátorská dokumentace – správa a konfigurace v rozsahu konkrétního (nasazeného) řešení. Dokumentace musí být zpracována v takovém rozsahu, který umožní odborným IT pracovníkům zadavatele systémy spravovat a udržovat bez jakékoliv součinnosti dodavatele (s výjimkou mimořádných událostí a chyb v dodaném SW a HW).
3. Bezpečnostní dokumentace – příručka bezpečnostního správce informačních systémů.
4. Integrační dokumentace – dokumentace všech nasazených a dodaných rozhraní k informačním systémům.

## Provádění prací

**Zadavatel požaduje, aby v rámci plnění zakázky práce probíhaly:**

1. V souladu se všemi běžnými zákonnými předpisy týkajícími se bezpečnosti práce
2. Dle zadavatelem schválené prováděcí dokumentace
3. Byly vždy řádně dokumentovány
4. A práce, které generují riziko pro technologie, infrastrukturu, či prostředí zadavatele, byly explicitně schvalovány pověřenou osobou zadavatele

## Výkony nad rámec podpory

Jedná se o služby upravené v čl. III odst. 5.3) smlouvy o dílo.