# Vymezení předmětu plnění

## Předmět plnění

Předmětem plnění veřejné zakázky je zajištění bezpečnosti komunikačních sítí dle § 18 písm. a) – e) vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).

## Popis současného stavu

## Popis lokalit

Serverovny jsou rozmístěny ve dvou budovách v areálu Krajského úřadu Karlovarského kraje. V těchto lokalitách bude probíhat poskytování poptávaných služeb.

## Popis stávajícího HW prostředí

* TCKK je technicky i provozně navrženo, vybudováno a provozováno pro poskytování vysoce dostupných infrastrukturních ICT služeb Krajskému úřadu a jeho zřizovaným organizacím. Technologické centrum je napojeno na RKI – WAN na bázi optických vláken propojující významné úřady v kraji (vesměs obce s rozšířenou působností) a některé zřizované organizace kraje. Přenosová kapacity RKI páteřních spojů je 10 Gb/s.
* TCKK je tvořeno dvěma rovnocennými datovými centry, pouze zálohovací technologie jsou soustředěny pouze v jedné lokalitě.
* Serverová infrastruktura je tvořena dvěma Blade šasi HP c7000 osazených Blade servery Gen7 – Gen10. Šasi jsou vybavena redundantními 8Gb FC SAN přepínači, redundantními 1 GbE passtrought moduly a redundantními Virtual Connect Flex 10Gb moduly. 8 fyzických serverů je virtualizováno technologiemi VMware vSphere 7 Enterprise+. Všechny servery využívají k ukládání dat replikované datové úložiště Dell Unity.
* Datové úložiště se skládá z 2x Dell Unity 300 rozmístěné rovnoměrně do obou lokalit. Disková pole jsou doplněna odpovídající SAN FC 8 Gb infrastrukturou sestavenou z FC přepínačů Brocade. Délka optických tras mezi lokalitami je cca 300 metrů. Celková disková kapacita činí: 200 TB.
* V budově A Krajského úřadu je umístěn řídící a úložný server HP DL380 G8 zálohovacího systému Veeam Backup a Recovery Enterprise. Pro dlouhodobé ukládání záloh slouží pásková knihovna HPE MSL3040.
* Síťová vrstva je postavena na technologii Extreme Fabric Connect. V TCK je použita čtveřice přepínačů Extreme VSP 7400 a dvojicí Extreme 5420M propojené 100/25 GE linky a mezi Datacentry 40GE linky. Páteřní přepínače jsou dvojice přepínačů Extreme VSP 7400. Nacházejí se v rozvodných místnostech v budově A, B a jsou propojeny přes 40GE linky. Páteřní přepínače mají propojení do přepínačů Datacenter rovněž přes 40 GE a dále agregují linky z přístupových přepínačů z rozvodných míst jednotlivých budov areálu na rychlosti 10 Gbit/s. TCK je do RKI připojeno prostřednictvím redundantních centrálních prvků HPE 5900-AF.
* Inspekci a řízení internetového provozu zajišťuje perimetrový firewall Checkpoint, který slouží i pro publikaci některých služeb TCKK bez pokročilých ochran a autentizačních mechanismů.
* Publikace většiny služeb TCKK do Internetu a RKI je prováděno prostřednictvím F5 Big-IP.
* Distribuční a přístupová vrstva síťové infrastruktury využívá síťové prvky Extreme na technologii Extreme Fabric Connect. Pro bezdrátovou komunikaci jsou využívány prvky Extreme.
* Obě lokality jsou vybaveny motorgenerátory, překlenutí doby jejich náběhu a krátkodobých výpadků zajištují UPS EATON 9355.
* Datová centra jsou dále vybavena klimatizacemi, zhášecím systémem, IP kamerami a Rack management systémem (dále RMS) s kouřovými, pohybovým a vlhkostními čidly s možností zasílání varování přes SMS.

## Popis stávajícího SW prostředí

* Systémové služby jsou provozovány převážně na platformě Microsoft, jde zejména o následující systémy:
	+ Microsoft Windows Server Datacenter a Standard
	+ Microsoft SQL Standard
	+ Microsoft Exchange Standard
	+ Microsoft 365
* Verze systémů Microsoft jsou průběžně aktualizovány v konzervativním režimu, tj. jsou udržovány cca. 1-2 verze za aktuální verzí.
* Pro doručování aplikací uživatelům jsou využívány technologie Microsoft Remote Desktop Service
* Primární adresářovou službou je Active Directory provozovaná na redundantních replikovaných řadičích, které zajištují také služby DNS a DHCP.
* K ukládání sdílených souborů je kromě prostředků Windows serveru využívána NAS funkcionalita diskového pole Dell Unity.
* Virtualizační platformou TCKK je VMware vSphere 7 Enterprise+ řízená jedním vCentrem. Jsou implementovány a využívány pokročilé funkce vSphere – High availability, Dynamic Resource Scheduler, vMotion, virtuální switche apod.

## Popis způsobu řešení incidentů

* Zadavatel pro řešení incidentů a podporu uživatelů používá interní HelpDesk vytvořený na zakázku.
* Incidenty a požadavky uživatelů se řeší formou ticketů v systému HelpDesk, uživatelé tak mají přehled o stavu řešení jejich požadavků. Zadavatel také zajišťuje podporu 1. úrovně a většinu běžných problémů jsou schopni vyřešit interní pracovníci Zadavatele.
* Incidenty a požadavky, které nevyřeší interní HelpDesk budou předávány do helpdeskového systému dodavatele provozní podpory. Hlášení incidentů a požadavků bude prováděno telefonicky, emailem nebo přímo zadáním ticketu/požadavku do helpdeskového systému dodavatele.

## Popis servisních oken

TCKK nemá pevně definovaná pravidelná servisní okna. Aplikace aktualizací a oprav virtuálních serverů provádějí zaměstnanci KÚKK dle potřeby a s přihlédnutím k minimalizaci omezení uživatelů.

## Požadavky na technické řešení

* 1. Základní požadavky

Cílem projektu zajištění bezpečnosti komunikačních sítí dle § 18 písm. a) – e) vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.

**Požadavky:**

* nabízené řešení bude obsahovat SW komponenty jednoho výrobce včetně managementu,
* podpora dodávaného řešení bude dodavatelem zajištěna na období 3 let včetně aktualizací funkcionalit
* součástí 3leté technické podpory dodavatele bude:
	+ odstranění náhlých závad na SW vybavení
	+ pravidelná měsíční kontrola stavu systému
	+ update systému (minor verze, patche) 2x ročně
	+ dodavatel poskytne objednateli přístup do svého ticketovacího systému (ServiceDesk), ve kterém bude prováděno hlášení závad nebo požadavků a dodavatel je povinen vést k těmto požadavkům objednatele v systému evidenci
	+ činnosti dodavatele v rámci technické podpory budou provozovány v režimu 5x8, tj. po dobu 5 pracovních dnů v týdnu v době mezi 8 a 16 h
	+ dodavatel oznámí objednateli jméno řešitele požadavku nejpozději do 1 hodiny od jeho nahlášení v tiketovacím systému dodavatele
	+ dodavatel zahájí činnosti spojené s odbavením požadavku zadavatele nejpozději následující pracovní den po nahlášení požadavku v ticketovacím systému (servicedesk) dodavatele
* nabízené řešení bude instalováno na tzv. koncová zařízení zadavatele,
* nabízené řešení bude spravováno z centrálního managementu,
* nabízené řešení, jehož součástí je EDR řešení musí obsahovat agenta minimálně do prohlížeče Chrome, Firefox, Brave, Edge,
* nabízené řešení musí být schopno současného provozování různých verzí agenta, tzn. dle požadavku zadavatele může být na určitém typu koncových zařízeních nainstalována jiná verze než na jiném typu koncových zařízeních,
* nabízené bezpečnostní řešení EDR bude provádět nepřetržitý sběr dat a analýzu s hlášením do centralizovaného systému. To poskytne bezpečnostnímu týmu plný přehled o stavu koncových bodů sítě,
* nabízené bezpečnostní řešení EDR bude provádět automatizovaný sběr a zpracování dat a určité činnosti odezvy. To umožní bezpečnostnímu týmu rychle získat kontext týkající se potenciálního bezpečnostního incidentu a rychle podniknout kroky k jeho nápravě,
* nabízené bezpečnostní řešení umožní automatické aktivní reakce na incidenty na základě předem definovaných pravidel. To umožní zablokovat nebo rychle reagovat na nežádoucí aktivity. Průběžný sběr a analýza dat řešení EDR poskytuje detailní přehled o stavu koncových stanic.
	1. Centralizovaný nástroj pro správu

**Požadované funkcionality:**

* centrální správa dodaného SW, prostřednictvím centrálního management v Cloudu nebo On premise v DC zadavatele,
* přiřazení uživatelských oprávnění dle rolí,
* dlouhodobé uchování záznamů alespoň 90 dnů,
* rozhraní pro reporting – vytváření reportů o provozu z uchovaných záznamů.
	1. Požadavky na funkcionality řešení

**Požadované funkcionality:**

**Threat Intelligence:**

Požadujeme prevenci hrozeb založenou na kombinaci informací o hrozbách ze sdílených databází (tzn. výrobce SW musí mít přístup k databázi sdílené s jinými poskytovateli) kombinovanou s pokročilými technologie umělé inteligence, aby byla navýšena oblast prevence. Požadujeme schopnost řešení přidávat Indikátory kompromitace IoC pro domény, IP adresy, URL, MD5 Hash klíče a SHA1 Hash klíče, které umožní řešení jejich automatickou blokaci.

**Access Control:**

Požadujeme spolupráci s naším řešení FW Check Point tak, aby pravidla brány firewall přijímaly nebo rušily síťový provoz do a z koncových bodů na základě IP adres, domén, portů a protokolů.

Požadujeme možnost omezit přístup k síti pro konkrétní aplikace tak, aby bylo možno definovat, zda povolit, blokovat nebo ukončit aplikace a procesy.

Požadujeme, aby řešení umožnilo zajistit pro koncové body dodržování bezpečnostních pravidel organizace. Koncové body, které pravidla nebudou splňovat se zobrazí jako „nesouladné“ a správce na ně může použít omezující zásady.

**Threat Prevention:**

Požadované řešení musí neustále monitorovat chování specifické pro ransomware a identifikovat nelegitimní šifrování souborů bez signatury. Musí detekovat a uplatňovat karanténu všech prvků útoku ransomwaru, které jsou identifikovány forenzní analýzou.

Požadujeme zajištění plné kontinuity provozu tak, aby šifrované soubory byly automaticky obnoveny ze snapshotů.

Požadujeme funkcionalitu Intel TDT – Implementace ochrany na úrovni procesoru pomocí technologie Intel Threat Defense.

Požadované řešení musí chránit před malwarem resp. před všemi druhy malwarových hrozeb, červů, trojských koní a adware.

Řešení musí být schopnou funkce Anti-Bot, kdy požadujeme zabránění dopadům infekce Bot na koncové body.

Požadujeme ochranu před útoky založenými na exploitech, které ohrožují legitimní aplikace, a požadované řešení zajistí, že tyto zranitelnosti nelze zneužít.

Požadujeme, aby řešení detekovalo a blokovalo mutace malwaru podle jejich chování v reálném čase.

Požadujeme ochranu portů tím, že řešení bude vyžadovat autorizaci pro přístup k úložným zařízením a dalším vstupně/výstupním zařízením.

**Analytické funkce:**

Požadujeme, aby se po detekci škodlivé události automaticky spustila forenzní analýza a celá sekvence útoku byla prezentována jako forenzní zpráva.

Požadujeme tzv. mapování MITRE, kdy řídicí panel MITRE ATT&CK poskytuje přehled o všech technikách pozorovaných aplikací pro ochranu koncového bodu v reálném čase a mapuje všechny události na MITRE taktiky, techniky a postupy (TTPs).

**Ochrana prohlížeče:**

Součástí řešení musí být agent do prohlížeče minimálně pro Chrome,Firefox, Brave, Edge a musí:

* detekovat phishingove webové stránky,
* umožňovat CDR (Content Disarm and Reconstruction) stahovaných souborů,
* detekce použití firemních přístupových údajů při přihlášení na 3rd party webové služby,
* vynutit "safe search",
* podporovat URL filtering,
* možnost rožšíření o podporu DLP funkcionality pro upload souborů,
* možnost rožšíření o DLP nad GenAI (ChatGPT a další GenAI produkty).

Zajistit Zero-Phishing ochranu v reálném čase před neznámými zero-day phishingovými stránkami. Statická a heuristická detekce podezřelých prvků na webových stránkách, které vyžadují soukromé informace.

Vynutit ochranu firemních přihlašovacích údajů tzn. detekovat opakované použití firemních přihlašovacích údajů na externích stránkách.

Umožnit filtrování URL díky plugin prohlížeče, který povoluje/blokuje přístup k webovým stránkám v reálném čase s plným přehledem o provozu HTTPS.

Zajistit bezpečné vyhledávání. Tzn. z našeho pohledu funkci přidanou do vyhledávačů, která funguje jako automatizovaný filtr pro potenciálně urážlivý a nevhodný obsah.

Možnost rozšíření o zabezpečení DLP a GenAI funkce, což zahrnuje možnost skenování nahrávání a stahování, ovládání schránky a tisku a bezpečnostní nástroje GenAI pro detekci a prevenci ztráty dat v reálném čase. To vše s více než 700 předdefinovanými datovými typy a Microsoft Tagging option.

**Posture Management:**

Požadujeme funkce tzv. Posture Managementu, které obsahují Vulnerability Management and Patch Management, kdy tyto funkcionality poskytují automatickou detekci zranitelností, stanovují priority a opravy, pro snížení rizika narušení dat nebo jiného bezpečnostního incidentu.

* 1. Obecné požadavky

Na veškeré produkty, které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky:

* mají plnou záruku od výrobce,
* mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,
* obsahují všechny nezbytné licence na používání příslušného softwaru,
* jsou v databázi výrobce uvedeny jako prodaná kupujícímu,
* jsou určeny pro provoz v České republice.
* Zadavatel si vyhrazuje právo na zjištění původu výrobků při jejich předávání, a to dle příslušných sériových čísel a právo podpisu akceptačního protokolu, osvědčujícího převzetí dodávky, až po ověření původu výrobku.
* Veškerá dokumentace vytvořená v rámci realizace veřejné zakázky, musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standardních formátech (např. MS Office, Open Office, PDF) používaných zadavatelem. Struktura i forma dokumentace musí být před předáním předána ke kontrole a výslovně schválena zadavatelem.
* Navržené řešení musí být tvořeno komponentami podle uvedených požadavků.
* Pokud dodavatel vyžaduje využití konkrétních softwarových produktů a jím zvolený přístup k realizaci zadání je na takových konkrétních řešeních závislý, musí jejich pořízení zahrnout ve své nabídce v potřebném rozsahu a v rámci nabídnuté ceny.
* Pokud dodavatelem nabízené řešení vyžaduje komponenty či služby neobsažené v požadavcích zadání, zahrne dodavatel do své ceny všechny náklady na jejich pořízení, instalaci, konfiguraci a další služby potřebné pro uvedení do provozu, přičemž nesmí překročit předpokládanou hodnotu zakázky.
* Zadavatel z důvodů co nejjednodušší a jednotné správy a minimalizace provozních nákladů vyžaduje využití stávajících prostředků a používaných technologií. V případě, že dodavatel vyžaduje ve svém řešení stejné nebo podobné funkce, jaké poskytují stávající prostředky a technologie, je povinen využít nebo vhodným způsobem rozšířit stávající prostředky.
* Veškeré dodávané HW a SW produkty musí být získány legálně a umožňovat využití těchto produktů zadavatelem, jako koncovým zákazníkem, v souladu s distribučními a licenčními podmínkami výrobce.
* V případě dodání HW a SW produktů zadavateli, jako koncovému zákazníkovi, nesmí být zadavatel nijak omezen ve svých nárocích vyplývajících ze záruky výrobce dodávaného zařízení a z produktové podpory, kterou tento výrobce k dodávaným HW a SW produktům poskytuje. Uvedené musí zahrnovat i nárok zadavatele na přístup k relevantním SW releases a novým verzím SW po celou dobu trvání podpory výrobce.
* Musí být umožněn online přístup Zadavatele k dokumentaci výrobce HW/SW a znalostní bázi, kterou výrobce v rámci své podpory poskytuje.
* V databázi výrobce musí být Zadavatel veden jako první uživatel zboží a licencí / subscripcí / operačních systémů.
* Dodavatel musí garantovat, že v případě dodání zboží Zadavateli, jako koncovému zákazníkovi, bude Dodavatelem poskytnuta k dodávanému zařízení záruka a produktová podpora v plném, poskytovaném rozsahu.
* Součástí všech zařízení musí být dodávka SW a firmware v aktuální verzi.
* Dodavatel může nabídnout řešení a zboží s lepšími parametry (v případě, že lze objektivně stanovit, že se jedná o parametry lepší), nikoliv s parametry horšími (či horší kvality), než požaduje zadavatel v zadávacích podmínkách. Zadavatel připouští i jiná kvalitativně a technicky obdobná řešení za podmínky, že nesmí dojít ke zhoršení požadovaných parametrů.

## Implementace

Zadavatel požaduje implementaci výše uvedeného HW a SW a to v tomto rozsahu:

* Vypracování technicko-implementačního projektu s popisem budoucího stavu a plánem migrace na novou infrastrukturu i s akceptačními testy,
* Vypracování dokumentace skutečného provedení a provozní dokumentace.
* Zajištění zkušebního provozu infrastruktury v délce minimálně 2 týdnů včetně technické podpory specialistů na dané zařízení/službu s dostupností specialisty maximálně do 2 hodin od nahlášení požadavku v pracovní den v době od 8h do 17h.
* Činnost omezující práci uživatelů musí být prováděny mimo běžnou pracovní dobu úřadu, tj. mimo pracovní dny 7 – 15 hod.

## Požadavky na testovací prostředí.

* Zadavatel nedisponuje testovacím prostředím,
* Vyžaduje-li Uchazeč pro realizaci zakázky testovací prostředí, zahrne do nabídky náklady na jeho vybudování a požadovanou součinnost Zadavatele.

## Obecné požadavky na provedení akceptačních testů a přechod do ostrého provozu

1. Uchazeč navrhne způsob a provedení akceptačních testů. Součástí akceptačních testů musí být pro každou komoditu minimálně:
2. Prokázání kompletnosti dodávky a splnění povinných parametrů a požadavků,
3. Prokázání funkčnosti migrovaných systémů,
4. Prokázání aktivací aktivačními klíči či jinými prostředky, je-li aktivace potřebná.
5. Pro každý systém či modul navrhne Uchazeč vhodné doplňující testy a kritéria, kterými bude prokázána bezproblémová funkčnost, bezpečnost a odpovídající výkon a stabilita dodaného řešení,
6. O provedení akceptace a jejím výsledku musí být vyhotoven písemný protokol,
7. Přechodem do ostrého provozu se rozumí okamžik úspěšné akceptace díla včetně vypořádání všech vad a nedodělků.

## Součásti nabídky

* Nabídka musí obsahovat následující položky:
	+ Cenu za 500 ks SW licencí pro ochranu koncových zařízení splňujících plně technické požadavky Zadavatele,
	+ Cenu takového řešení na 3 roky včetně podpory výrobce a přístupu k aktualizacím,
	+ Cenu za uvedení do provozu tzn. implementace a 1 měsíc zvýšené podpory,
	+ Cenu za 3 roky poskytování ServiceDesku a Heldesku Dodavatele v řežimu 9x5,
	+ Cenu za zaškolení administrátorů:
		- distribuce licencí uživatelům
		- dohled
		- aktualizace SW
		- řešení obvyklých poruchových stavů
		- tvorba pravidel pro všechny typy bezpečnostních funkcionalit
	+ Informaci o minimálních provozních požadavcích jak pro agenta, tak pro management