Příloha č. 1 Zadávací dokumentace – Technická specifikace zadavatele

Příloha č. 1 Kupní smlouvy – Technická specifikace kupujícího

1 Technická specifikace zadavatele (kupujícího)

Obsah

Kupující požaduje dodávku jednotlivých komponent dle této technické specifikace včetně příslušenství v níže uvedené minimální specifikaci.

Musí se jednat o zařízení nová, nepoužitá, nerepasovaná a určená pro prodej v České republice, potažmo v EU.

Součástí dodávky níže uvedených technologií budou i dále uvedené služby.

Součástí dodávky bude dále dodávka dokumentace a nezbytné zaškolení administrátorů v prostředí kupujícího k běžnému provozu a ovládání dodaných technologií včetně specifik a konfigurace provedené v prostředí kupujícího.

Nabízené zboží musí být standardní, běžně dostupné a určené k produkčnímu použití.

Není dovoleno použití beta-verzí, kódu s custom úpravami či neoficiálních verzí.

Veškeré nabízené zboží musí být pokryto oficiálním supportem výrobce, přičemž požadavek na provedení bezplatného servisního zásahu musí být možné kdykoliv vznést přímo na výrobce zařízení.

Veškeré deklarované funkce a technické parametry nabízeného zboží musí být dostupné nejpozději dnem podání nabídky.

Deklarované funkce a technické parametry nabízeného zboží musí být ověřitelné prostřednictvím oficiálních datasheetů, release notes či manuálů vydaných výrobcem.

Užité pojmy níže:

- NBD – další pracovní den, tzn. například realizace opravy zařízení nejpozději další pracovní den od nahlášení
- x BD – x pracovních dnů, tzn. například realizace opravy zařízení nejpozději poslední pracovní den dané lhůty od nahlášení
- on-site – realizace například opravy zařízení v místě dodávky

Všechny firewally musí být z důvodu snadné údržby a jednotné servisní podpory od stejného výrobce. Musí být instalovány nové, nepoužité, licencované na koncového uživatele a musí na ně být poskytnuta záruka výrobce v požadované délce.

2 Určení technologií do technologických celků nemocnic holdingu

Předmět plnění této technické specifikace je určen po nasazení v následujících organizacích holdingu:

- Oblastní nemocnice Náchod a.s.
- Oblastní nemocnice Trutnov a.s.
- Oblastní nemocnice Jičín a.s.
- Městská nemocnice, a.s.

Z tohoto důvodu je potřeba odlišovat požadavek kupujícího na transparentní oddělení jednotlivých částí plnění tak, aby bylo možné jednoduché a transparentně přezkoumatelné vykázání dodávek technologií pro jednotlivé nemocnice, ale na druhou stranu samotné nemocnice a jejich zakladatel Zdravotnický holding Královéhradeckého kraje a.s. sledují klíčový cíl provozovat unifikovanou bezpečnostní a technologickou infrastrukturu, ve které si budou moci vzájemně vypomáhat, bude možné bezpečnostní technologie centrálně a jednotně řídit a její další rozvoj bude možné koordinovat společně.

Z pohledu projektu, jehož realizace je naplňována touto veřejnou zakázkou, dochází ke zvýšení kybernetické bezpečnosti v oblastech

- ID001 – Ochrana před škodlivým kódem na perimetru a uvnitř sítě
- ID003 – Nástroj pro detekci kybernetických bezpečnostních událostí (nástroj pro řešení a zpracování logů z Firewallů)

3 Místo plnění

Místem plnění jsou areály jednotlivých nemocnic na následujících adresách (lokalitách):

- **Oblastní nemocnice Náchod a.s.**
  - Purkyňova 446, 54701 Náchod
  - Bartoňova 951, 54701 Náchod
  - Jiráskova 506, 51601 Rychnov nad Kněžnou
  - Smetanova 91, 55001 Broumov – Nové Město
  - Národní 83, 55101 Jaroměř – Pražské Předměstí
  - T. G. Masaryka 367, 54901 Nové Město nad Metují, Česko
  - Pitkova 635, 517 73 Opočno
- **Oblastní nemocnice Trutnov a.s.**
  - Maxima Gorkého 77, 54101 Trutnov - Kryblice
  - Slezská 166, 54101 Trutnov – Vnitřní Město (budova finančního úřadu)
- **Oblastní nemocnice Jičín a.s.**
  - Bolzanova 512, Valdické Předměstí, 506 01 Jičín
  - Jana Maláta 493, 50401 Nový Bydžov
- **Městská nemocnice, a.s.**
  - Vrchlického 1504, 544 01 Dvůr Králové nad Labem
  - Rooseveltova 474, 54401 Dvůr Králové nad Labem

4 Počet a typ technologií

Počet a typ jednotlivých technologií, které jsou specifikovány níže, je definován v samostatné příloze zadávací dokumentace v podobě cenové tabulky.

Instalační a další související práce spojené s dodávkou a nasazením jednotlivých technologií prodávající zohlední v ceně jednotlivých zařízení.

5 Firewally

Kupující již v nemocnicích provozuje na perimetru sítě FireWall FortiGate 100F UTP (Typ A v lokalitách Rychnov n. K., Broumov, Jičín, Trutnov a Dvůr Králové n. L.). Pro zajištění vysoké dostupnosti (HA) těchto prvků bude v rámci plnění dle této specifikace stávající řešení rozšířeno o druhé, plně kompatibilní boxy.

Dále je v ON Trutnov i firewall typu SOPHOS model XG210 (2 kusy v HA režimu active-pasive), u kterého je rovněž požadováno provést analýzu bezpečnostních pravidel a bezpečnostní politiky a výstup této analýzy zohlednit pro nově nasazovaná zařízení.

Do lokalit Nový Bydžov, Jaroměř, Opočno a Nové Město n. M. je požadována dodávka redundantního řešení FireWallu Typu B, tedy v počtu dvou kusů pro každou z lokalit. V rámci plnění je požadována kompatibilita s možností aplikace stejné technologie a pravidel s ostatními typy firewallů dle této technické specifikace a dále požadavek kompatibility s nástrojem na zpracování logů z firewallů v rámci plnění této specifikace. Cílem plnění podle této specifikace je sjednocení technologické úrovně a úrovně zabezpečení napříč nemocnicemi holdingu jako celku. Je požadována migrace bezpečnostních politik a pravidel ze stávajících technologií založených na zařízených typu FortiGate 60E.

Do lokalit Nová Paka a Chlumec n. C. bude dodán nový FireWall (Typ C), který nahradí stávající řešení VPN brány a bude kompatibilní s Firewally v rámci plnění této specifikace a dále s nástrojem na zpracování logů z firewallů v rámci plnění této specifikace.

Zadavatel připouští dodávku NGFW (včetně systému pro řešení a zpracování logů z FireWallů uvedené dále v této specifikaci) jiného výrobce. Nabízené řešení musí být stejných nebo lepších parametrů a musí plně nahradit stávající a nově poptávané prvky v minimální konfiguraci a funkcionalitami stanovenými v tabulce níže pro každý typ zařízení.

Každý typ firewallu (A, B, C) musí splňovat následující technickou specifikaci, která stanoví odlišné minimální požadavky na firewall typu A, B a C.

Next Generation FireWall	
Požadavek na funkcionalitu	**Minimální požadavky**
HW appliance	ANO
Podpora režimu vysoké dostupnosti minimálně jako active/active a active/passive, cluster o dvou fyzických zařízeních	ANO

Možnost nasazení v režimu L2 bridge režim (inline), L3 router/NAT režim (inline), explicitní proxy (inline/out of path), transparentní proxy (inline)	ANO
Management rozhraní - sériový konzolový port	ANO
Grafické konfigurační rozhraní (např. webový prohlížeč) a příkazový řádek bez omezení na počet administrátorů	ANO
Podpora virtualizace na daném HW, vytváření a provozování tzv. virtuálních kontextů, každý virtuální kontext musí pracovat izolovaně.	10
Podpora stavového firewallingu pro IPv4 i IPv6, podpora nat 64/46	ANO
Ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign On	ANO
Podpora funkcí VPN brány - IPSec VPN	ANO
SSL VPN pro klientský přístup s tunelovacím režimem včetně klienta pro osobní počítače i mobilní platformy a portálový režim pro bezklientský přístup	ANO
Podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3	ANO
Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 4000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií	ANO
Podpora dvoufaktorové autentizace pomocí HW nebo mobilních OTP tokenů	ANO
Funkce QoS, traffic shaping a SD-WAN minimálně v režimu vytvoření overlay a underlay virtuálních sítových rozhraní zahrnující fyzické propoje, IPSEC tunely či jiná rozhraní s možností definice pravidel pro řízení směrování, strategie využívání jednotlivých linek současně a monitorování stavu jednotlivých linek	ANO
Obousměrná integrace firewallu s nástrojem pro sběr a vyhodnocování logů požadovaného dále v této technické specifikaci	ANO
Typ A a Typ B	
Funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (tzv. mobile malware), detekce	ANO

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 běžných kancelářských dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby); podpora napojení na sandboxovací funkce včetně funkce akceptace lokálních signaturových databází generovaných sandboxem, vše bez nutnosti instalace pluginů do prohlížeče.	
Funkce kategorizace webových stránek (web filtering), výrobcem aktualizovaná a udržovaná databáze; požadované akce – povolení stránky, logování stránky, brouzdání s proklikem, nutnost autentizace uživatele pro určitou kategorii, možnost definice časových kvót pro uživatele a kategorie webu	ANO
Možnost blokovat sítový provoz na základě URL, kategorie webové stránky, IP adresy (rozsahu), GeoIP databáze, data a času	ANO
Funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, integrovaný anomální filtr a mechanismus kontroly validity vybraných protokolů	ANO
Funkce ochrany před únikem citlivých dat (data leak prevention), která umí zachytit pokus o odeslaní/upload označeného dokumentu přes internet na základě vodoznaků, popisu regulárním výrazem atp.	ANO
Technický support výrobce v režimu 24x7 včetně nároku na nejnovější firmware a subskripce	5 let
Typ A	
Formát zařízení	HW s montáží do 19‘‘ rozvaděče 1U
Počet fyzických portů	2x 10 GE SFP+, 18x GE RJ45, 8x GE SFP
Minimální propustnost firewallu pro IPv4 provoz (měřeno na UDP komunikaci o paketech s velikostí 512 B).	18 Gbps
Počet současně navázaných spojení firewallu	1 500 000
Celková propustnost IPSEC VPN při použití AES256-SHA256	11,5 Gbps

Min. počet site-to-site IPSEC tunelů	2 000
Propustnost SSL VPN	1 Gbps
Propustnost funkce SSL inspekce	1 Gbps
Propustnost funkce IPS (reálná hodnota, měřeno na běžném provozu – real world traffic, včetně logování)	2,6 Gbps
Propustnost funkcí next generation firewallingu (stavový firewall, IPS, analýza aplikací, reálná hodnota, měřeno na běžném provozu – real world traffic)	1,6 Gbps
Propustnost funkcí ochrany před hrozbami (stavový firewall, IPS, analýza aplikací, ochrana před škodlivým kódem, reálná hodnota, měřeno na běžném provozu – real world traffic)	1 Gbps
Udávaná latence firewallu (udp provoz)	< 5 µs
Typ B	
Formát zařízení	Desktop, nebo jako Typ A
Počet fyzických portů	10x GE RJ45,
Minimální propustnost firewallu pro IPv4 provoz (měřeno na UDP komunikaci o paketech s velikostí 512 B).	10 Gbps
Počet současně navázaných spojení firewallu	700 000
Celková propustnost IPSEC VPN při použití AES256-SHA256	6,5 Gbps
Min. počet site-to-site IPSEC tunelů	200
Propustnost SSL VPN	900 Mbps
Propustnost funkce SSL inspekce	630 Mbps
Propustnost funkce IPS (reálná hodnota, měřeno na běžném provozu – real world traffic, včetně logování)	1,4 Gbps
Propustnost funkcí next generation firewallingu (stavový firewall, IPS, analýza aplikací, reálná hodnota, měřeno na běžném provozu – real world traffic)	1 Gbps

Propustnost funkcí ochrany před hrozbami (stavový firewall, IPS, analýza aplikací, ochrana před škodlivým kódem, reálná hodnota, měřeno na běžném provozu – real world traffic)	0,7 Gbps
Udávaná latence firewallu (udp provoz)	< 5 µs
Typ C	
Formát zařízení	Desktop, nebo jako Typ A
Počet fyzických portů	4x GE RJ45,
Minimální propustnost firewallu pro IPv4 provoz (měřeno na UDP komunikaci o paketech s velikostí 512 B).	5 Gbps
Počet současně navázaných spojení firewallu	500 000
Celková propustnost IPSEC VPN při použití AES256-SHA256	4 Gbps
Min. počet site-to-site IPSEC tunelů	100
Propustnost SSL VPN	450 Mbps
Propustnost funkce SSL inspekce	300 Mbps
Udávaná latence firewallu (udp provoz)	< 4 µs
Technický support výrobce v režimu 24x7 včetně nároku na nejnovější firmware a subskripce	5 let

6 Nástroj pro řešení a zpracování logů z Firewallů

Je požadována dodávka systému pro řešení a zpracování logů z Firewallů v sítích nemocnic. Systém musí být plně kompatibilní s nabízeným řešením NGFW dle této specifikace a musí podporovat analýzu logů nad provozem. Dále musí být řešení schopné poskytovat reporty nad logy a informovat správce systému o hrozbách, které byly v síti odhaleny. Minimální technické parametry na řešení jsou uvedeny tabulce níže.

V Oblastní nemocnici Náchod je již se stávajícím řešením NGFW provozován specializovaný nástroj pro řešení a zpracování logů – FortiAnalyzer (S/N: FAZ-VMTM20000878 s kapacitou 11 GB logů/den a 5 TB úložné kapacity). Tento nástroj bude rozšířen o poptávanou kapacitu a výkon, nebo nahrazen nástrojem jiného výrobce stejných nebo lepších parametrů s dosažením minimálních požadavků na řešení dle této specifikace.

Nástroj řešení a zpracování logů	
Požadavek na funkcionalitu	**Minimální požadavky**

Virtuální appliance s podporou minimálně VMware, KVM a Hyper-V	ANO
Možnost škálovatelného navýšení kapacity úložiště na základě licence	ANO
Obousměrná integrace s nabízenými NGFW dle této specifikace, tzn. že data se přenáší jednak z firewallu na logovací a reportovací platformu, ale zároveň je možné přímo v GUI firewallu přistupovat k log údajům na logovací a reportovací platformě	ANO
Podpora pro Syslog kompatibilní zařízení	ANO
Výkon logování **pro Náchod** (cílový stav)	16 GB /den
Kapacita storage (uložení historických dat) **pro Náchod** (cílový stav)	9,5 TB
Výkon logování pro **Jičín, Trutnov**	11 GB /den
Kapacita storage (uložení historických dat) pro **Jičín, Trutnov**	6 TB
Výkon logování pro **Dvůr K. n. L.**	6 GB /den
Kapacita storage (uložení historických dat) pro **Dvůr K. n. L.**	3 TB
Real-time prohledávání logovaných dat	ANO
Vyhledávání historických dat podle typu události nebo typu provozu	ANO
Funkce zpětné kontroly logů o přístupu na web (až 7 dní) z důvodu „zero-day“ malicious websites	ANO
Korelace logů	ANO
Vyhledávání podle zařízení	ANO
Uživatelská definice reportů (vzhled, obsah apod.)	ANO
Automatické generování reportů v daném čase a periodě	ANO
Automatické odesílání reportů emailem	ANO
Technický support výrobce v režimu 24x7 včetně nároku na nejnovější firmware a subskripce	5 let

7 Emailová brána

Výše uvedené bezpečnostní řešení perimetru sítí v podobě firewallů je požadováno rozšířit v rámci plnění dle této specifikace o dedikované email brány (1ks pro každou nemocnici - počet uveden v cenové tabulce,

která je přílohou smlouvy) ve formě virtuální appliance pro stávající virtualizační platformu VMware provozovanou v prostředí nemocnic.

Řešení musí splňovat následující minimální požadavky na parametry a funkcionalitu:

Email brána	
Požadavek na funkcionalitu	**Minimální požadavky**
Virtuální appliance pro prostředí VMware	ANO
Podpora režimu vysoké dostupnosti. (Pokud řešení vyžaduje dodávku licence, tak musí být tato licence již součástí plnění a zohledněna v ceně)	A-A, A-P
Počet síťových rozhraní	4
Podpora diskové kapacity	min. 0,5 TB
Možnost nasazení v režimu gateway (MTA) i transparent	ANO
Podpora IPv4 i IPv6	ANO
Podpora VLAN	ANO
Podpora SMTP autentizace min. pomocí protokolů	LDAP, RADIUS, POP3, IMAP
AntiSpam funkcionalita včetně IP reputační databáze výrobce, graylisting, reputace odesílatelů, behaviorální analýza, analýza hlaviček mailů, heuristická analýza mailů, podpora systémů třetích stran (blacklisty), kontrola založená na Bayesian přístupu, white a black listing, analýza obrázků s možností detekce a selekce newsletter emailů, podpora funkce tzv. bounce verification.	ANO
Integrovaná funkce Antivirové ochrany mailového provozu s podporou real-time ochrany před outbrake škodlivého kódu. Databáze antivirových signatur musí být udržována výrobcem a automaticky aktualizovaná	ANO
Požadujeme plnou integraci s platformou typu sandbox, která je součástí plnění dle této specifikace (plnou integraci se rozumí uchování emailu ve frontě až do ukončení kontroly na sandbox platformě. Výsledná akce je volena i na základě výsledku analýzy na sandbox platformě. Zároveň požadujeme obousměrnou komunikaci mezi mailovou bránou a sandbox platformou, tj. přímo na mailové bráně musí být možné dohledat detailní informace o provedené sandbox inspekci)	ANO
Možnost limitace v rámci SMTP navázané relace (počet zpráv od jednoho klienta za určitou dobu, maximální počet spojení od jednoho klienta za	ANO

určitou dobu, podpora endpoint reputace, napojení na LDAP za účelem verifikace uživatelů; možnost omezení počtu HELO/EHLO v rámci jedné SMTP relace, možnost omezit počet emailových zpráv v rámci SMTP relace, možnost omezit počet příjemců v rámci adresátů emailu, možnost manipulace s hlavičkou mailu (odstranění Received hlavičky)	
Analýza PDF	ANO
Plnohodnotná kontrola příchozí i odchozí komunikace (stejné konfigurační možnosti pro příchozí i odchozí směr)	ANO
Granulární konfigurace pravidel (pravidla na základě IP adres a/nebo domén příjemce, možnost využití wildcard notace)	ANO
Podpora karantény s uživatelským přístupem umožňujícím běžné operace	ANO
Podpora systémové karantény	ANO
podpora TLS, S-MINE, DKIM, SPF a DMARC	ANO
Podpora funkce šifrování přenosu mailové komunikace end-to-end bez nutnosti instalovat software na pracovní stanice (např. uložení šifrované zprávy lokálně s možností vyzvednout zprávu bezpečným způsobem přes web rozhraní)	ANO
Podpora funkce ochrany před útoky typu DoS, Antispoofing, rate limiting, vyhodnocování lokálního skóre odesílatelů (na základě nedávné aktivity) s možností nastavení chování pro různé úrovně skóre	ANO
Podpora tzv. neutralizace dokumentů v příloze (odstranění potencionálně nebezpečných prvků v dokumentu (zejména makra a URL) v dokumentech MS Office a PDF při zachování původního typu dokumentu	ANO
Automatická dekrypce šifrovaných dokumentů za pomoci administrátorem předdefinovaného slovníku hesel, za účelem provedení plné AV a AS kontroly	ANO
Reakce na detekovanou hrozbu min.: přidání tagu, přidání hlavičky, přeposlání emailu na jiný SMTP server, odmítnutí (reject), zahození (discard), uložení do karantény, přepsání adresy příjemce	ANO
Podpora opakované kontroly emailu ve chvíli jeho vyzvednutí z karantény	ANO
URL click protection (vložené URL je přepsáno tak, aby byla provedena kontrola ve chvíli rozkliknutí odkazu uživatelem)	ANO
Ochrana před útoky typu BEC (Business Email Compromise)	ANO

Architektura MTA musí umožnit provést kontrolu emailu ještě před uložením do emailové fronty	ANO
Plnohodnotná správa	web gui (HTTPs), CLI (SSH)
Integrované logování a reporting, včetně monitoringu	ANO
Podpora protokolů začlenění do monitorovacího a logovacího systému	SNMP(v2c, v3), SYSLOG
Zařízení nesmí být licencováno na počet chráněných emailových schránek/uživatel. V opačném případě požadujeme licenci pro jejich neomezený počet.	ANO
Řešení nesmí být omezeno na počet chráněných domén. V opačném případě musí být součástí dodávky podpora pro minimálně 20 emailových domén	ANO
Požadovaný výkon při plné inspekci (antivirus, antispam), referenční velikost mailu 100 kB.	25000 mailů/hod.
Záruka na funkcionalitu a podpora výrobce v režimu 24x7 včetně portálu výrobce pro zadávání tiketů, web chatu pro rychlé dotazy, přístup k aktualizacím SW.	5 roků

8 Nástroj pro ochranu před škodlivým kódem (AntiX)

V rámci plnění je požadována dodávka a nasazení jednotného řešení pro ochranu koncových stanic a serverů před škodlivým kódem s centrální správou pro každou nemocnici.

Řešení musí splňovat následující minimální požadavky na parametry a funkcionalitu:

Nástroj pro ochranu před škodlivým kódem (AntiX)	
Požadavek na funkcionalitu	**Minimální požadavky**
SW řešení (agent) pro zajištění zabezpečení pracovních stanic a serverů.	ANO
Centrální on-premise konzole pro správu ve formě SW instalovaného na obecný server s OS Windows Server 2019 a vyšší	ANO
Jednoduché lokalizované uživatelské rozhraní, možnost uzamknutí privilegovaných operací a úkonů před běžným uživatelem na straně pracovní stanice	ANO

Odesílání telemetrických informací (informace o pracovní stanici a jejím stavu, přihlášeném uživateli) na konzoli centrální správy	ANO
Podpora funkce Zero Trust Network Access (dynamicky vytvářený přístup k publikovaným službám a aplikacím bezpečným přístupem v režimu on-net i off-net bez nutnosti navazování VPN spojení), kontrola provozu per session	ANO
Podpora napojení na sandboxing applianci za účelem rozboru zkoumaných souborů na přítomnost škodlivého kódu	ANO
Integrovaný firewall založený na analýze sítových aplikací (aplikační firewall)	ANO
Podpora detekce zranitelností na pracovní stanici s funkcí aplikace automatického patchingu či jiné administrátorské akce	ANO
Podpora funkce kategorizace webových stránek založené na principu výrobcem udržované databáze s min. 60 kategoriemi	ANO
Podpora funkce definování politiky pro přístup k USB periferiím	ANO
Podpora funkce antivirové inspekce s pokročilým nástrojem pro odhalování neznámých či podezřelých hrozeb pomocí strojového učení a umělé inteligence	ANO
Funkce automatické karantény pracovní stanice v případě detekce bezpečnostní hrozby	ANO
Sběr informací o instalovaném SW na pracovní stanici	ANO
Integrovaná ochrana proti škodlivému kódu typu Ransomware	ANO
Podporované operační systémy: MS Windows 10, 11 (32/64 bit), MS Windows Server 2012 a novější, MacOS 10.14, 10.15 a 11+, mobilní platformy iOS (od verze 9) a Android (od verze 5)	ANO
Podpora vzdálené instalace agenta na pracovní stanice uživatelů skrze prostředí domény	ANO
Integrace s Microsoft Active Directory	ANO
Podpora práce s uživatelskými skupinami, možnost definovat různé politiky a pravidla pro různé skupiny uživatelů	ANO

Plná podpora multitenancy centrálního managementu s oddělenými kontexty (pokud tato funkce vyžaduje dodatečnou licenci, tak musí být součástí plnění dle této specifikace)	ANO
Je požadována licence v délce trvání 3 let, včetně nároku na aktualizační balíčky zranitelností a software. Dále je požadována podpora v podobě nových verzí software a aktualizační balíčky zranitelností po dobu dalších 2 let, tedy do celkových požadovaných 5 let podpory.	ANO

9 Sandbox - Nástroj pro ochranu před „Zero Day“ útoky

Do prostředí Oblastní nemocnice Náchod a.s. je požadována dodávka a implementace výkonného SandBox systému jako ochrana před neznámým škodlivým kódem a útoky „nultého dne“. Tento systém bude integrován dle této specifikace s dalšími bezpečnostními komponentami a bude sdílen jako bezpečnostní infrastruktura z Náchodu do všech zbývajících nemocnic uvedených v této specifikaci pro užití ve spolupráci s bezpečnostními technologiemi dodávanými v rámci plnění dle této specifikace. Tato konfigurace a nastavení sdílení sandboxové platformy je součástí plnění dle této specifikace.

Řešení musí splňovat následující minimální požadavky na parametry a funkcionalitu:

Nástroj pro ochranu před „Zero Day“ útoky (sandbox)	
Požadavek na funkcionalitu	**Minimální požadavky**
Specializovaná HW appliance pro řešení ochrany před zero-day škodlivým kódem, plně a obousměrně integrovatelná s emailovou bránou dodávanou v rámci této specifikace.	ANO
Montáž do standardního datového rozvaděče 19‘‘	ANO
Redundantní „hot swap“ napájecí zdroj	ANO
Počet síťových rozhraní 1GE UTP (RJ45)	2
Počet síťových rozhraní 10GE SFP+	2
Počet paralelně běžících instancí pro sandboxing OS Windows včetně licencí Microsoft	40
Možnost rozšíření až na 70 paralelně běžících instancí pro sandboxing OS Windows včetně licencí Microsoft	ANO
Počet instancí pro sandboxing souborů pro MS Office prostředí	4

Výrobcem udávaná propustnost souborů při plném sandboxingu a využití plné kapacity sandboxu	1500 / hod.
Výrobcem udávaná efektivní propustnost souborů při aplikaci pre-filteringu, před samotným sandboxingem a využití plné kapacity sandboxu (poměr 80% dokumentů a 20% spustitelných souborů)	60000 / hod.
Podpora operačních systémů pro sandboxing - výrobce udržuje a aktualizuje skenovací sandboxing OS	Windows 10 a 11, MacOS, Linux, Android
Možnost integrace s interními systémy pomocí dokumentovaného API, podpora funkce API musí být součástí plnění dle této specifikace	ANO
Odchozí komunikace ze sandboxovacích image musí do internetu odcházet přes dedikované síťové rozhraní	ANO
Podpora režimu clusterování s cílem dosažení vysoké dostupnosti a možnosti navyšování výkonosti v budoucnu s očekávaným navýšením provozu	ANO
Inspekce vzorků založená na vícevrstvé ochraně před škodlivým kódem: - kombinace antivirové kontroly za pomoci signatur - emulace kódu - plnohodnotný sandboxing (spuštění v reálném operačním systému) - umělá inteligence (AI)/strojové učení (ML) Všechny tyto úrovně musí být integrovány do jednoho zařízení a vzájemně spolupracovat.	ANO
Ochrana proti zjištění běhu v sandbox prostředí (anti evasion techniky)	ANO
Všechny prvky ochrany musí být poskytovány lokálně, nikoliv jako cloud služba (s výjimkou těch, u kterých to nedovoluje legislativa)	ANO
Detekce komunikace s C&C centry	ANO
Podpora detekce přístupu na kompromitované URL	ANO
Funkce reportingu nalezených problémů (Součástí výsledné informace nesmí být pouze status čistý/škodlivý kód, ale kompletní informací včetně detailního popisu chování, packet capture a v případě projevu malware v GUI také screenshoty či video záznam Podpora reportingu v MITRE ATT&CK formátu.	ANO

Podpora kontroly minimálně následujících typů souborů a aplikací: MS Office, Adobe Acrobat Reader, Adobe Flash Player, Mozilla Firefox, Google Chrome, Java, MS .NET Framework, Visual C++, Python, spustitelné soubory, JAVA, PDF, MS Office dokumenty, běžné multimediální formáty jako např. .7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm, .dotx, .eml, .elf, .exe, .gz, .htm, html, .iqy, .iso, .jar, .js, .kgb, .lnk, .lzh, .Mach, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, .rl, .vbs, WEBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip	ANO
Podpora sandboxingu průmyslových řídících protokolů a aplikací: tftp, modbus, s7comm, http, snmp, bacnet, ipmi	ANO
Podpora reportování ve standardních formátech (zejména HTML, CSV, PDF, XML)	ANO
Podpora logování na externí nástroje a SIEM	ANO
Záruka a podpora výrobce v režimu 24x7 včetně portálu výrobce pro zadávání tiketů, web chatu pro rychlé dotazy, přístup k aktualizacím SW, RMA službu s odesláním ten samý den.	5 roků

10 Požadované implementační služby

10.1 Základní instalační služby

V rámci dodávky předmětu plnění kupující požaduje následující systémové práce:

- pro firewally a software pro práci s logy
  - Fyzická montáž HW
  - Aktualizace firmware
  - Propojení NGFW do režimu HA
  - Instalace virtuální appliance pro bezpečnostní analýzu logů
  - Propojení na cluster NGFW
  - Vytvoření vzorových reportů
  - Akceptační testy
- pro další technologie dle této specifikace
  - Instalace email brány
  - Fyzická montáž HW SandBox appliance
  - Aktualizace FW a OS
  - Otestování a přesměrování email komunikace
  - Konfigurace pravidel
  - Instalace a konfigurace centrální konzole pro ochranu před škodlivým kódem
  - Pilotní konfigurace pro 10 pracovních stanic v každé nemocnici

  - Otestování vzdálené instalace agenta
  - Napojení email brány a AntiX řešení na SandBox
  - Otestování napojení na SandBox a otestování obousměrné komunikace s email bránou
  - Akceptační testy
- Společné zaškolení administrátorů technologií nemocnic (za každou nemocnici min. 1 administrátor) na dodané technologie a jejich vzájemné vazby v rozsahu min. 6 hodin (může proběhnout v jednom termínu pro všechny technologie nebo může být rozděleno na dva termíny s celkovou časovou alokací min. 6 hodin).
- Unifikací bezpečnostního řešení, ke které dojde plněním dle této specifikace, vzájemnou komunikací nově dodaných a rekonfigurovaných bezpečnostních prvků a sdílením informací dojde ke kvalitativnímu zvýšení bezpečnostní úrovně v nemocnicích kupujícího.

10.2 Sjednocení bezpečnostních pravidel na perimetru sítě a společná konfigurace bezpečnostních pravidel

V rámci realizace plnění kupující požaduje **zpracování analýzy bezpečnostních politik** v nemocnicích, jejich zdokumentování a sestavení nového návrhu, který bude nasazen společně s novými technologiemi v rámci plnění této technické specifikace.

Bude se jednat o analýzu pravidel ze stávajících firewallů a AntiX řešení. Pravidla ze stávající platformy AntiX předá prodávajícímu pro analýzu v podobě oproštěné od stávající platformy (technologie) kupující na výzvu do 5 pracovních dnů v rámci realizace plnění dle této technické specifikace.

Analýza bezpečnostních politik bude provedena nejen na úrovni každé nemocnice, ale bude zohledňovat požadavky na strukturu a způsob fungování síťového prostředí Zdravotnického holdingu Královéhradeckého kraje a.s., který je zakladatelem nemocnic. To znamená, že prodávající provede analýzu ve všech nemocnicích, do kterých v rámci plnění této technické specifikace bude dodávat technologie, tuto analýzu písemně sestaví, určí v ní průsečíky a dobrou praxi v jednotlivých nemocnicích a provede vyhodnocení stávajícího stavu.

Na základě takového vyhodnocení, provede prodávající **návrh bezpečnostních politik na perimetru sítě a v oblasti AntiX napříč nemocnicemi Zdravotnického holdingu Královéhradeckého kraje a.s.**, a takový návrh v podobě rozdělení na jednotlivé nemocnice a dopady do jejich konfigurací a bezpečnostních služeb na perimetru sítě a v oblasti AntiX předloží k projednání kupujícímu.

Při návrhu musí maximálně prodávající respektovat potřeby nemocnic a dále zohlednit skutečnosti, na kterých se takové potřeby zakládají, tedy zejména návaznost provozovaných informačních systémů a technologií na stávající konfiguraci a s tím související potřeby nemocnic, provést případný přechod na nové konfigurace postupně, či navrhnout i přechodná a náhradní řešení.

Součástí návrhu musí být i následující:

- požadavky na rekonfiguraci stávajících bezpečnostních prvků nemocnic v oblasti firewallů a dalších dodávaných technologií v rámci tohoto plnění a další prvky mimo plnění dle této technické specifikace, na které takové řešení bude mít dopad a bude potřeba je rekonfigurovat
- přesný instalační plán, včetně závazného **harmonogramu realizace plnění**

Termín - Zpracování analýzy a návrhu bezpečnostních politik provede prodávající nejpozději do 4 týdnů od nabytí účinnosti této smlouvy.

Kupující prodávajícímu sdělí své připomínky k výstupu analýzy do 2 týdnů.

Prodávající se zavazuje všechny připomínky kupujícího zohlednit a finalizovat návrh bezpečnostních politik do jednoho týdne.

Zahájení implementačních a instalačních prací bude předcházet odsouhlasení výstupů analýzy a návrhu realizačních prací ze strany kupujícího. Bez výslovného souhlasu kupujícího nebude možné zahájit uvedené práce a jejich zahájení v rozporu s tímto ustanovením ze strany prodávajícího bude považováno za podstatné porušení smlouvy.

Výsledný dokument analýzy bezpečnostních politik, včetně návrhu a instalačního plánu (harmonogramu) bude po zapracování připomínek kupujícího ze strany prodávajícího protokolárně předán kupujícímu a bude závazný.

Po realizaci instalační služeb prodávající aktualizuje dokument návrhu bezpečnostních politik podle skutečného provedení a dále **jej doplní o architektonickou vizualizaci výsledného řešení a vazeb mezi technologiemi**, včetně popisu jednotlivých prvků a jejich určení a výsledný dokument předá kupujícímu.

10.3 Harmonogram a časový rámec pro realizaci instalačních služeb

Do dvou týdnů od nabytí účinnosti smlouvy na předmět plnění dle této technické specifikace předloží prodávající návrh závazného harmonogramu jednotlivých dodávek a prací, včetně požadavků na součinnost osob kupujícího. Kupující do 1 týdne návrh harmonogramu odsouhlasí, nebo k němu poskytne konkrétní závazné připomínky. Následně bude harmonogram považován za závazný, včetně smluvních pokut plynoucích za jeho nedodržení zanesených v kupní smlouvě.

S ohledem na skutečnost, že nemocnice nemohou přerušit svůj provoz, a dále na skutečnost, že v prostředí nemocnic je potřeba zachovávat zvýšenou míru čistoty a klidu, mohou fyzické instalační práce probíhat v pracovních dnech pouze v časech 15:00 až 05:00 hodin a o víkendech v časech 12:00 až 05:00 hodin, nebude-li v konkrétních případech dohodnuto jinak.

Konfigurační služby a služby realizované formou vzdáleného přístupu mohou být realizovány i mimo výše uvedenou dobu, za předpokladu, že budou založeny na schváleném harmonogramu.

Přípravné práce, které nebudou zasahovat do aktivního propojení sítě bude možné ze strany prodávajícího realizovat i mimo tyto časy na základě dohody s kupujícím.

S ohledem na povahu organizace kupujícího musí prodávající při realizaci konfiguračních pracích vzít v úvahu potřebu řádného provozu informačních systémů závislých na službách zajišťovaných prostřednictvím dodávaných technologií, které budou v rámci realizace tohoto plnění nasazovány nebo rekonfigurovány a v návrhu harmonogramu a při realizaci prací toto musí prodávající zohlednit.

Tedy zejména aby prodávající svojí činností nepůsobil překážky v dostupnosti služeb prostřednictvím sítě i v jiných časech, než kdy budou dle harmonogramu odsouhlaseny práce na síťové infrastruktuře, které mohou vést k nedostupnosti prostřednictvím sítě poskytovaných nebo zprostředkovávaných služeb, které jsou součástí poskytování zdravotních služeb.

10.4 Zkušební provoz

V rámci realizovaného plnění je požadován zkušební provoz nově nasazených technologií jako celku.

Zkušební provoz je součástí plnění dle této technické specifikace a je i součástí plnění tak, že je potřeba jej zohlednit do harmonogramu prací ze strany prodávajícího.

Požadovaná minimální délka zkušebního provozu je jeden kalendářní měsíc.

Předmětem zkušebního provozu je ověření provedených dodávek a služeb, tedy zejména funkčnosti dodaných zařízení a správnosti provedené konfigurace.

Zahájení zkušebního provozu proto musí předcházet nasazení všech technologií a provedení všech souvisejících dodávek a služeb (zejména konfigurací).

Zahájení zkušebního provozu podléhá předložení potvrzení o instalaci a konfiguraci technologií ze strany prodávajícího a potvrzení možnosti zahájení zkušebního provozu ze strany kupujícího.

Délka zkušebního provozu je nastavena v takové délce, aby umožnila kupujícímu ověřit správnost provedené konfigurace a dále schopnosti dodaných zařízení plnit požadavky na ně stanovené. Délka zkušebního provozu byla stanovena tak, aby kupujícímu umožnila ověřit většinu procesů a situací v rámci uvažovaného užití předmětu plnění. Jedná se zejména o nepravidelné činnosti v prostředí nemocnice a dále o pravidelné činnosti nicméně s časovým horizontem, které mají zvýšené nároky na prostředí a jeho konfiguraci, tedy předmět plnění dle této technické specifikace. Jedná se o komplexní přenosy zdravotnických dat a specifické synchronizační služby mimo prostředí nemocnic a další typické činnosti v zařízení typu nemocnice a jejího IT prostředí.

10.5 Kybernetická bezpečnost

Předmět plnění dle této technické specifikace vstupuje do informačního prostředí jednotlivých nemocnic, které podléhá na rozličné úrovni dopadům následujících právních předpisů:

- zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
- vyhláška 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)

- Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)

Prodávající musí jednat řádně a v kontextu výše uvedených právních předpisů v oblasti kybernetické bezpečnosti a v případě potřeby si v rámci realizace plnění vyžádat od kupujícího doplňující informace tak, aby byl připraven reflektovat své jednání a proces realizace plnění v souladu s výše uvedenými předpisy a jejich případnou formou implementace v jednotlivých nemocnicích.

Mezi nemocnicemi je provozovatelem informačního systému základní služby Oblastní nemocnice Náchod a.s.

V rámci realizovaného plnění a dopadu výše uvedené legislativy bude prodávající zařazen mezi tzv. významné dodavatele.

Pro všechny nemocnice je však ze strany prodávajícího nezbytné dodržet výše uvedenou národní legislativu a dále v kontextu realizovaného plnění zohlednit směrnici NIS 2, jako závazný právní předpis EU určený k implementaci jednotlivými státy EU v rozsahu, který umožňuje přímou interpretaci a vztahuje se k realizovanému plnění.

10.6 Projektové řízení

S ohledem na rozsah projektu a dopad jeho zavedení do produkčního provozu na výkon činnosti kupujícího je v rámci dodávky předmětu plnění kupujícím požadováno aplikování základních principů projektového řízení ze strany prodávajícího.

Jedná se zejména řízení projektových prací v souladu s uzavřenou smlouvu s ohledem na věcné plnění dané smlouvou – rozsah, posloupnost a hloubku projektových prací, (tj. harmonogramu) – řízení postupu prací s ohledem na závazný harmonogram projektu – dodržování termínů harmonogramu, podchycení případných kolizí, zpoždění nebo vznikajících rizik a jejich reportování směrem ke kupujícímu, aktivní řešení výše uvedených nestandardních situací

Zápisy - Zpracování pravdivých, úplných a věcně jasných a vypovídajících zápisů z konzultačních schůzek a pracovních jednání (s cílem zaznamenání klíčových rozhodnutí, ujednání, navržených nebo dohodnutých termínů a způsobů řešení dílčích částí projektu atd.)

Kontrolní dny - Prezenční účast odpovědné osoby prodávajícího na kontrolních dnech v pravidelných min. měsíčních intervalech v sídle kupujícího, případně se souhlasem obou smluvních stran formou videokonference nebo telekonference. Termíny kontrolních dnů budou součástí harmonogramu.

U kontrolních dnů kupující požaduje, aby byly organizovány společně pro všechny nemocnice Zdravotnického holdingu Královéhradeckého kraje, a.s., ve kterých dochází k realizaci plnění prodávajícím dle této technické specifikace.

Reporting - Reporting plnění na úrovni pravidelných dvoutýdenních písemných zpráv směrem k odpovědné osobě kupujícího (seznam prací, které byly vykonány pro danou část projektu, stav těchto prací (ukončeno, odloženo, v realizaci); popis vzniklých problémů a způsob jejich řešení. Kupující si vyhrazuje

právo vyžádat reporting projektu i mimo dvoutýdenní interval, na takovou žádost bude prodávající povinen reagovat vždy nejpozději písemnou zprávou do 4 pracovních dnů.

Řízení rizik plnění, hodnocení pravděpodobnosti jejich výskytu a míry dopadu, návrh řešení k jejich eliminaci.

Řízení změn na plnění, v případě požadavků na změnu v plnění provedení konzultací k ověření nutnosti změny plnění; zjištění dopadu požadovaných změn směrem ke koncepci celkového řešení, harmonogramu, dotačnímu titulu, vytížení lidských zdrojů atd. V případě odsouhlasení změn spolupráce při implementaci změn do plnění, komunikace s dalšími zapojenými osobami a specialisty za dotčené technologie a informační systémy.