Příloha č. 2 zadávací dokumentace
Technická specifikace

1 Technická specifikace

Tato kapitola podrobně popisuje technické požadavky zadavatele na dodávky dílčích služeb.

1.1 Popis současného stavu

V současné době je na straně zadavatele úroveň zajištění kybernetické bezpečnosti velice nízká a jsou plněny legislativní požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „**ZoKB**“), pouze u vybraných jihočeských nemocnic. Zadavatel má z hlediska kybernetické bezpečnosti zájem poskytnout všem jihočeským nemocnicím stejný standard, který zohlední požadavky jak současného ZoKB, tak jeho novelizované požadavky po transpozici NIS2.

Níže je uveden základní přehled o jednotlivých jihočeských nemocnicích z hlediska již používaných bezpečnostních technologiích, velikosti, počtu serverů, objemu ukládaných logů a počtu EPS.

1.1.1 České Budějovice

Základní údaje o nemocnici

Velikost nemocnice	3300 zaměstnanců
Počet serverů	160
Počet síťových prvků	500
Počet EPS	2100
Objem ukládaných logů	13 GB / den

Přehled již implementovaných bezpečnostních technologií

Technologie
Log management (IBM QRadar)
SIEM (IBM QRadar)
EDR (Sophos Intercept X)
NDR (Flowmon ADS)

Identity management (AD)
EPP (ESET Endpoint Security)
IDS/IPS (Fortinet FortiGate)
Firewall (Fortinet FortiGate)

1.1.2 Dačice

Základní údaje o nemocnici

Velikost nemocnice	100 zaměstnanců
Počet serverů	4
Počet síťových prvků	9
Počet EPS	Max 100 EPS
Objem ukládaných logů	10 GB/den (hrubý odhad)

Přehled bezpečnostních technologií

Technologie
EDR (Bitdefender)
Identity management (AD)
EPP (Bitdefender)
Log management (nemocnice má již aktuálně v řešení nákup této technologie)
IDS/IPS (nemocnice má již aktuálně v řešení nákup této technologie)
Firewall (Linux Debian 12)

1.1.3 Jindřichův Hradec

Základní údaje o nemocnici

Velikost nemocnice	1200 zaměstnanců
Počet serverů	40
Počet síťových prvků	40
Počet EPS	650 (hrubý odhad)
Objem ukládaných logů	Do 40 GB/den (hrubý odhad)

Přehled bezpečnostních technologií

Technologie
EDR (Sophos)
Identity management (AD)
EPP (Sophos)
IDS/IPS (Kerio Control – aktuálně v řešení projektu IROP Kybez pořízení jiné technologie)
Firewall (Kerio Control – aktuálně v řešení projektu IROP Kybez pořízení jiné technologie)
Log management (nemocnice má již aktuálně v řešení nákup této technologie)
NDR (nemocnice má již aktuálně v řešení nákup této technologie)

1.1.4 Český Krumlov

Základní údaje o nemocnici

Velikost nemocnice	470 zaměstnanců
Počet serverů	31
Počet síťových prvků	30

Počet EPS	500 (hrubý odhad)
Objem ukládaných logů	35 GB/den (hrubý odhad)

Přehled bezpečnostních technologií

Technologie
EDR (Sophos)
NDR (nemocnice má již aktuálně v řešení nákup této technologie – Sophos)
Identity management (AD)
EPP (Sophos Endpoint + Intercept X)
IDS/IPS (Sophos)
Firewall (Sophos)

1.1.5 Písek

Základní údaje o nemocnici

Velikost nemocnice	900 zaměstnanců
Počet serverů	56
Počet síťových prvků	70
Počet EPS	1500 (hrubý odhad)
Objem ukládaných logů	100 GB/den (hrubý odhad)

Přehled bezpečnostních technologií

Technologie
Log management (LogManager)

EDR (FortiClient)
NDR (Flowmon)
Identity management (AD)
EPP (Fortinet)
IDS/IPS (Fortinet)
Firewall (Fortinet)

1.1.6 Prachatice

Základní údaje o nemocnici

Velikost nemocnice	560 zaměstnanců
Počet serverů	45
Počet síťových prvků	75
Počet EPS	450 (hrubý odhad
Objem ukládaných logů	20 GB/ den

Přehled bezpečnostních technologií

Technologie
Log management
SIEM (IBM QRadar)
EDR (Sophos)
Identity management (AD, AC Identita)
EPP (Sophos)
IDS/IPS (Sophos)
Firewall (Sophos)

1.1.7 Tábor

Základní údaje o nemocnici

Velikost nemocnice	1200 zaměstnanců
Počet serverů	46
Počet síťových prvků	62
Počet EPS	1200 (hrubý odhad)
Objem ukládaných logů	43 GB/den (hrubý odhad)

Přehled bezpečnostních technologií

Technologie
Log management (LogManager)
EDR (Sophos InterceptX)
NDR (FlowMon)
Identity management (AD)
EPP (ESET Nod)
IDS/IPS (Fortigate)
Firewall (Fortigate)

1.1.8 Strakonice

Základní údaje o nemocnici

Velikost nemocnice	700 zaměstnanců
Počet serverů	39
Počet síťových prvků	46

Počet EPS	500 (hrubý odhad)
Objem ukládaných logů	35 GB/den (hrubý odhad)

Přehled bezpečnostních technologií

Technologie
Identity management (AD)
Firewall (Fortigate)
EDR (ESET)
NDR (FlowMon)
EPP (Fortinet)
IDS/IPS (Fortinet)

1.2 Detailní specifikace předmětu zakázky

V této kapitole jsou podrobněji popsány požadavky na plnění k jednotlivým dílčím službám.

1.2.1 Požadavky na zajištění služeb bezpečnostního dohledového centra (SOC)

Dodavatel provede návrh cílového řešení systému jednotného dohledu a postup implementace včetně harmonogramu implementačních aktivit.

Níže jsou uvedeny požadavky zadavatele na konkrétní služby bezpečnostního dohledového centra, které budou zajišťovány pro jednotlivé jihočeské nemocnice. Sloupec poznámka doplňuje informaci k dané službě, případně stanovuje hrubý odhad součtu požadovaných parametrů pro danou službu pro všechny nemocnice (je-li to pro danou službu relevantní).

Hlavní služby:

Oblast	Služba	Poznámka
Log Management	Sběr a ukládání logů	
	Agregace, normalizace (parsing), kategorizace, enrichments	
	Retence logů	Min. 18 měsíců/nem.
	Sběr a archivace logů v raw formátu	
	Certifikované úložiště	
	Pravidelná hlášení o provozu technologií	Report 1x měsíčně
	Provozní monitoring	Report
	Exit služby bezpečnostního sběru a předání logů	
SIEM	Analytická činnost	
	Koordinace řešení bezpečnostního incidentu	
	Návrh technických opatření na základě identifikovaných kybernetických incidentů	
	Sledování trendů v oblasti kybernetické bezpečnosti	

	Reporting	1x měsíčně
	AddHoc Reporting	
	Auditní záznam bezpečnostních událostí	
	Trendy	
	Threat inteligence	
	Real time monitoring	
	Nonreal time monitoring	
	Incident Management	
	Detekce anomálií	
	Detekce Ransomware	
	Detekce Spam, Mallware	
	IP reputace	
	Úprava a nasazování korelačních pravidel	
	Vyhodnocování bezpečnostních událostí	
	Exit služby bezpečnostního dohledu	

Vedlejší dílčí služby

Oblast	Služba	Poznámka
Tým L1 - služba	Prvotní filtr při řešení události	24x7
	Sledování dashboardů a info kanálů	24x7
	Zakládání ticketů pro bezpečnostní události	24x7
	Příprava podkladů pro analýzu bezpečnostních událostí	
	Identifikace false-positive	
	Režim aktivního monitoringu	24x7
Tým L2 - služba	Bezpečnostní dohled/monitoring v rámci NDR/EDR/XDR platforem	24x7
	Prošetřování incidentů	24x7
	Threat hunting	24x7
	Návrh a implementace protiopatření, nových use cases	
	Návrh, úprava a nasazení korelačních pravidel	
	Reporting (pravidelný, jednorázový)	1x měsíc
	Komunikace se zákazníkem	
Expertní podpora	Bezpečnostní architektura	1MD/nemocnice =8 MD/měsíc
	Bezpečnostní konzultace	
	Architektura technického řešení - nástrojů	
	Tvorba a úprava korelačních pravidel	
	Design, návrh a testování automatizovaných procesů response	
	Integrace a nasazení dalších bezpečnostních nástrojů	
EDR	Endpoint detection and response	
	Threat inteligence	

	Real+time monitoring	
	Incident Management	
	Detekce anomálií	
	Detekce Ransomware	
	Prevenční možnosti	
	Automatický update signatur a bezpečnostních hrozeb	
	podpory vyšetřování a systémového managementu	
	IOC a YARA indikátory pro operační systémy Windows, Linux a MacOS	
NDR	Network detection and response	
EPP	Endpoint protection	
	Detekce Spam, Mallware	
IDS/IPS (Vyhl. 181/2018 Sb., §18)	Monitoring síťového provozu, reakce a zabránění na základě hrozeb	
Firewall	Perimetrická ochrana	
Offensive security center - Kybernetické testování	Kontrola přítomnosti přihlašovacích účtů zákazníka v databázích úniků	
	Testování účinnosti hesel	
	Zranitelnostní skenování infrastruktury, vybraných IS a aplikací zákazníka	1x rok / nem.
	Penetrační testování infrastruktury, vybraných IS a aplikací zákazníka	1x rok / nem.
	Testování IS, infrastruktury a aplikací před nasazením do provozu	1MD / rok / nem.
Offensive security center -	Phishingové kampaně	2x rok / nem.
	Vishing a smshing	2x rok / nem.

Sociální inženýrství	Využívání sociálních sítí a alternativních webů pro získání informací, přístupů a dat	2x rok / nem.
	Využívání ostatních technik sociálního inženýrství pro získání informací, přístupů a dat	2x rok / nem.
DDoS	Denial-of-service (služby serverů)	Počet chráněných adres 85
Digital Forensics	Zajištění vyšetření a důkazního materiálu v součinnosti se Zadavatelem	