**Příloha č. 1 – Technická specifikace**

# Technické požadavky na zajištění služby SOC

Pojmy, které začínají velkým písmenem a nejsou zavedeny v této příloze, se vykládají podle vlastní zadávací dokumentace a podle přílohy zadávací dokumentace obsahující návrh smlouvy (dále jen „**návrh smlouvy**“ nebo „**smlouva**“).

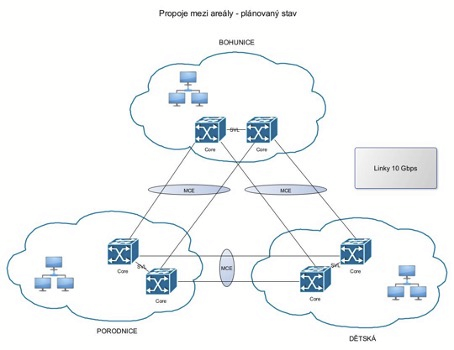
## Základní údaje o zadavateli

FN Brno tvoří tři pracoviště: Pracoviště medicíny dospělého věku s areálem v Brně-Bohunicích na Jihlavské ulici, Pracoviště dětské medicíny s areálem v Černých Polích (Dětská nemocnice) a Pracoviště reprodukční medicíny na Obilním trhu (Porodnice). V jejich rámci pracují desítky specializovaných odborných klinik, ústavů, center a laboratoří.

Prostředí FN Brno je situováno z hlediska Datové sítě do 3 lokalit v Brně:

* areál Bohunice, Jihlavská 20, Brno;
* areál Porodnice, Obilní trh 11, Brno;
* areál Dětská nemocnice, Černopolní 9, Brno;

a do jedné lokality v Třebíči - transfuzní stanice Purkyňovo náměstí 2, Třebíč.



Rámcové parametry Datové sítě:

|  |  |  |
| --- | --- | --- |
| Parametr | Hodnota parametru | Poznámka |
| Počet informačních systémů základní služby identifikovaných dle zákona č. 181/2014 Sb. | 29 |  |
| Přibližný počet IP adres | 9000 |  |
| Počet zdravotnických prostředků na síti (max. hodnota) | 700 |  |
| Počet zaměstnanců celkem | 6500 |  |
| Uživatelské PC/NB na síti | 3 500 | Z toho 1000 VDI Horizon. Nebude přímo logováno |
| Počet uživatelů v síti celkem | 8 900 | Z toho cca 240 firemních účtů dodavatelů |
| Wifi access points | 750 | Řízení přes CISCO WLC - aktuální počet 750 a do 3 let zvýšení o 450ks |

## Zdroje bezpečnostních dat

FN Brno provozuje, případně implementuje následující Zdroje bezpečnostních dat, tj. následující systémy se považují za Zdroje bezpečnostních dat:

* systém centrálního log managementu, který bude sloužit jako hlavní zdroj standardizovaných informací z celé infrastruktury FN Brno a u kterého se počítá s necelými 1300 zdroji logů pro základní fázi implementace. Tento počet bude v průběhu dalšího období rozšiřován na průmyslové, řídící prvky ve FN Brno a zdravotnické prostředky. Implementovaným systémem log managementu je Logman.io od společnosti TESKA Labs. Požadovaná Služba SOC musí být se systémem log managementu plně kompatibilní a být schopna v reálném čase využívat a analyzovat data z tohoto systému jako zdroj informací o ICT prostředí zadavatele, a to jak strojově, tak pomocí operátorů.
* systém pro správu privilegovaných účtů (PIM/PAM), jehož dodání je předmětem probíhajícího zadávacího řízení pro nadlimitní veřejnou zakázku „Zvýšení kybernetické bezpečnosti FN Brno II – systém pro správu privilegovaných účtů II“;
* systém pokročilé síťové analýzy Greycortex / Mendel;
* hlavní perimetrický Firewall Checkpoint 6900 Plus appliance;
* proxy servery Squid;
* zálohovací systémy Veeam, IBM Spectrum Protect;
* vulnerability management systém Greenbone appliance;
* nástroj pro ochranu před škodlivým kódem Bitdefender GravityZone s cloudovým Managementem.

Zadavatel požaduje, aby služba SOC byla poskytována nad údaji poskytovanými Zdroji bezpečnostních dat.

Stanovené Zdroje bezpečnostních dat pracují v režimu 24x7x365. Služba SOC musí být schopna v reálném čase využívat data ze Zdrojů bezpečnostních dat jako zdroj informací o Datové síti, jak je tento pojem definován v návrhu smlouvy, a to jak strojově, tak pomocí operátorů.

Zadavatel požaduje plnou integraci Služby SOC se systémem HelpDesk zadavatele, kterým je systém ALVAO. Zadavatel požaduje, aby dodavatel vedl v tomto systému HelpDesk Provozní deník. Zadavatel umožní on-line integraci systému HelpDesk s obdobným systémem dodavatele pomocí REST API. **Pro plnění smlouvy bude rozhodné to, co je uvedeno v systému HelpDesk Objednatele.**

## Požadavky na komunikační vazby

Všechna data ze Zdrojů bezpečnostních dat, jak je tento pojem definován ve smlouvě, budou dodavatelem přenášena do SOC v zabezpečené a zašifrované podobě, přičemž použité šifrovací algoritmy musí splňovat minimální požadavky na kryptografické algoritmy uvedené v doporučení NÚKIB v oblasti kryptografické bezpečnosti ve verzi 4.0 platné ke dni 5. 2. 2025[[1]](#footnote-2).

Veškerá přenášená i zpracovávaná data musí být chráněna proti neoprávněným změnám (zásahům) a proti neoprávněnému přístupu, a to alespoň na úrovni minimálních požadavků na kryptografické algoritmy uvedených v doporučení NÚKIB v oblasti kryptografické bezpečnosti ve verzi 4.0 platné ke dni 5. 2. 2025.

Internetové připojení Služby SOC k Datové síti si na své náklady zajišťuje dodavatel, tj. dodavatel je povinen toto internetové připojení Služby SOC k Datové síti zajistit a provozovat na vysoké úrovni kybernetické bezpečnosti a tak, aby mohl bez omezení plnit své povinnosti ze smlouvy. Zadavatel proto, zejména s ohledem na nastavení úrovní Služby SOC ve smlouvě a Zadávací dokumentaci, doporučuje zajistit toto internetové připojení na odpovídající úrovni dostupnosti. Toto internetové připojení Služby SOC k ICT infrastruktuře musí být realizováno prostřednictvím Site-to-Site VPN, které bude po celou doby poskytování služby splňovat aktuální doporučení v oblasti kryptografické bezpečnosti NÚKIB aktuálně obsažené v dokumentu „Minimální požadavky na kryptografické algoritmy“ ve verzi 4.0 platné ke dni 5.2.2025, přičemž veškerá doporučení v něm obsažená se považují pro účely této veřejné zakázky za povinné.

Dodavateli bude umožněno nad rámec Povinných systémů instalování a připojení dalších systémů (hardware i software) pro sběr a přenos informací potřebných pro provoz dohledového centra z Datové sítě, tj. pro poskytování Služby SOC, po dohodě se zadavatelem a za podmínky, že takové instalování a připojení nepovede ke snížení úrovně kybernetické bezpečnosti zadavatele (tyto další systémy jsou dle smlouvy Zařízení Poskytovatele). Veškeré náklady na instalaci a řádný provoz Zařízení Poskytovatele musí být součástí nabídkové ceny.

# Požadavky na obsah služby SOC

Zadavatel požaduje externě provozovanou službu bezpečnostního dohledu nad Datovou sítí, a to v režimu 7 dní v týdnu, 24 hodin denně a 365 dní v roce (dále a výše jen „**24x7x365**“).

SOC bude centralizovat kontrolní činnosti, správu událostí a incidentů a koordinovat analýzy anomálií a aktivně spolupracovat při řízení krizových úkonů při zvládání následků incidentů se zadavatelem.

Služba SOC bude poskytována jako externí outsourcovaná služba a musí, vedle ostatních požadavků, splňovat tyto požadavky zadavatele:

* služba musí pracovat s bezpečnostními nástroji zadavatele i dodavatele, tj. vždy s Povinnými systémy a se Zdroji bezpečnostních dat;
* musí dávat podnět k analýze v případě, že dojde k jakékoliv nestandardní situaci;
* musí zajišťovat analytické činnosti pro včasné identifikace KBU díky vyhodnocování výstupů z připojených bezpečnostních detekčních nástrojů (Zdroje bezpečnostních dat a Povinné systémy a případná Zařízení Poskytovatele);
* musí provádět analýzu bezpečnostních anomálií ve veškerém sledovaném síťovém provozu zadavatele, tj. v Datové síti;
* sledování a analýzy toků na perimetru infrastruktury FN Brno, tj. Datové sítě;
* sledování a analýzy toků v rámci Datové sítě;
* odhalování zero-day zranitelností a vektorů útoků;
* v případě detekce KBU iniciuje Služba SOC odpovídající reakci dle návrhu smlouvy.

## Komunikační jazyky

Veškerá ústní komunikace v rámci plnění smlouvy musí probíhat v českém jazyce nebo slovenském jazyce. Veškerá písemná komunikace v rámci plnění smlouvy musí probíhat v českém jazyce. Automatické výstupy generované systémy využívanými pro poskytování SOC, tj. Povinnými systémy, Zdroji bezpečnostních dat a případnými Zařízeními Poskytovatele, mohou být v anglickém jazyce.

## Minimální rozsah Katalogu Detekčních scénářů a Katalogu Scénářů reakce

Minimální rozsah Katalogu Detekčních scénářů a Katalogu Scénářů reakce:

* phishing (lákání citlivých údajů, apod.),
* spear-phishing (cílený a informovaný útok e-mailem),
* podvodný e-mail (lákání finančních obnosů, vydírání),
* denial of service (DoS, DDoS),
* scanning (scan rozsahu vnější sítě),
* sniffing (scan ve vnitřní síti, zachytávání komunikace),
* pokus o zneužití zranitelnosti (známých CVE nebo zranitelností nultého dne),
* drive-by download,
* útok skrze dodavatele služeb,
* spam (nevyžádaná pošta),
* útoky skrze webové aplikace (buffer overflow, SQL injection, cross-site scripting),
* ransomware,
* škodlivý obsah (virus, červ, trojský kůň, apod.),
* nelegální těžba kryptoměn (Coinminer),
* malicious Insider;

## Doba poskytování služby

Zadavatel požaduje poskytování služby SOC 7 dní v týdnu, 24 hodin denně, 365 dnů v roce (24x7x365). Plnění předmětu veřejné zakázky se bude v čase členit na dvě fáze (dále též jen „**První fáze plnění**“ a „**Druhá fáze plnění**“), přičemž **v první fázi plnění dodavatel SOC zavede a po akceptaci zavedení SOC ve zkušebním provozu převede SOC do druhé fáze plnění této smlouvy, ve které jej do konce trvání této smlouvy pro zadavatele bude řádně provozovat**, a to s odbornou péčí profesionála, na vysoké úrovni kybernetické bezpečnosti, v plném souladu s právními předpisy a dle zásad best practice, přičemž je dodavatel vždy povinen šetřit oprávněných zájmů zadavatele a usilovat o předcházení KBU a KBI v ICT infrastruktuře zadavatele. Během Druhé fáze plnění dodavatel zejména řádně provozuje SOC a poskytuje zadavateli služby sjednané smlouvou.

### První fáze plnění – Implementace a Zkušební provoz

Požadavky na Implementaci SOC jsou uvedeny v návrhu smlouvy.

Poskytovatel v rámci Zkušebního provozu provede:

* prvotní analýzu bezpečnostních hrozeb relevantních pro aplikace a služby provozované zadavatelem a návrh implementačního postupu pro aplikaci požadavků zadavatele;
* analýzu informací z centrálního implementace log managementu pro případné doplnění nebo rozšíření Logovacích schémat, včetně případně zdrojů logů (stávající seznam zdrojů logů je v příloze níže), jejichž provozně bezpečnostní informace bude vhodné také sbírat, korelovat a analyzovat. Počet monitorovaných systémů, resp. jejich kategorizace se bude po dobu poskytování služby měnit, a to jak z podnětu dodavatele, tak zadavatele v případě rozvoje ICT infrastruktury;
* návrh modifikace nastavení Zdrojů bezpečnostních dat, včetně atributů a parametrů potřebných pro řádné a efektivní provozování Služby SOC, zahrnující mj.
  + doporučení nastavení logování pro jednotlivé zdroje,
  + provedení zadavatelem odsouhlaseného nastavení logování jednotlivých zdrojů,
  + kontrolu a doporučení nastavení korelačních pravidel, reportů, parametrů,
  + provedení zadavatelem odsouhlaseného nastavení korelačních pravidel, reportů, parametrů,
  + výběr událostí a parametry jejich záznamů a metody sběru z jednotlivých zdrojů,
  + návrh doplňování logovaných informací z dalších zdrojů pro zlepšení jejich relevantnosti či srozumitelnosti;
* návrh relevantních procesů, potřebných pro řádné a efektivní provozování Služby SOC, zahrnující mj. činnosti při zjištění bezpečnostního incidentu, výpadku či omezení dostupnosti bezpečnostních technologií, způsoby notifikace kompetentních osob objednatele podle schváleného eskalačního schématu;
* vytvoření návrhu vzorového reportu (struktura) o událostech a incidentech.

Výstupem fáze Zkušebního provozu bude:

* vytvoření technických podmínek nezbytných pro řádné poskytování SOC ve Druhé fázi plnění,
* definice Logovacích schémat, která určí, z jakých dalších zdrojů vedle Zdrojů bezpečnostních dat, Povinných systémů a Zařízení Poskytovatele, jakým způsobem a pomocí jakých senzorů (agent, sonda, apod.) budou data sbírána, případně obohacována a korelována;
* návrh optimalizace nastavení relevantních procesů a jejich integrace s bezpečnostními procesy zadavatele;
* aplikace Detekčních scénářů;
* vyhodnocení a optimalizace konfigurace stávajících Zdrojů bezpečnostních dat,
* jedno cvičení dle specifikace Služby CONS-3 (jeho specifikace bude součástí Realizačního projektu), přičemž **náklady na toto první cvičení budou součástí Ceny plnění, tj. dodavatel je nebude účtovat jako poskytnutí Ad-hoc Služby**;
* vytvoření a předání vzorového reportu dle Služby REP-1 o událostech a incidentech;
* prezentace nastavení služby SOC a výstupů Zkušebního provozu vybraným pracovníkům zadavatele.

**Seznam Zdrojů logů z projektu Logmanagement**

|  |  |  |
| --- | --- | --- |
| Specifikace Zdroje | Minimální počet zdrojů z log managementu pro připojení do SOC | Upřesnění specifikace Zdroje |
| Windows Active Directory servery | 5 | Windows 2019 servery |
| Windows IIS and Exchange servery | 30 |  |
| Windows OS servery | 230 |  |
| Linux servery | 200 |  |
| DNS / DHCP servery | 7 | DNS (4x na AD DC) a DHCP (2x samostatně) |
| Antivirus centrální management | 1 | Bitdefender Antimalware Cloud management |
| Databasové servery | 21 | MS SQL, Informix, PostgreSQL, MySQL, Oracle, Interbase |
| Proxy servery | 5 | Squid 4x farma + 1x Kiosek) |
| File servery | 4 | File server primárně MS Windows, Linux CentOS 7 (bude upgradováno) |
| Hlavní firewally | 2 | Firewall Checkpoint 6900 Plus appliance with NGTP (2x v HA), externí FW Fortigate pro pacietskou síť (u poskytovatele internetu Faster) |
| VPN koncetrátory | 5 | VPN Gateway (3x CISCO), OpenVPN |
| Routery a Switche | 310 | Routery 10ks |
| Aplikační servery | 150 |  |
| RADIUS / LDAP | 8 |  |
| Load Balancers | 0 |  |
| Email Content/Spam Filtering | 0 | Součást M365 |
| Azure Active Directory | 1 | Počet uživatelů v AAD stejný jako v Interním AD |
| MS M365 | 1 | Společně s AAD aplikace Exchange, Sharepoint, OneDrive, Teams, pro bezpěčnost MDM - inTune |
| NBA | 1 | kolektor NBA systému GreyCortex - GreyCortex Mendel ( 50Gbps průtok, zpracování 80000 toků za sekundu) |
| Network Access Control | 3 | Cisco ISE - 2ks (CISCO Large Secure Network Server for ISE Applications ) 802.1.X , 1xISE pro Wifi Pacient |
| Řízení virtualizace VMWare | 3 | VMWare NSX - vCenter pro servery 12 srv a pro PC (Horison) 12srv + 8 VMWare srv pro PACS - vCenter pro 1x Servery, 1x pro Horison, 1x PACS |
| Zálohovací řešení | 2 | Veeam, Tivoli TSM |
| Provozního monitoringu | 4 | Zabbix (Linux servery), Microsoft SCCM, Libre NMS monitoring - (monitoruje i UPS), Cisco Prime virtuální appliance pro Switche |
| Klíčová PC | 200 |  |
| Management diskových polí | 3 | HP Primera, NetApp, |
| UPS monitoring přímo zařízení | 100 | APC, Socomec, Eaton |
| Multifunkční tiskárny | 25 |  |
| Remote Access pro zdravotnícké prostředky | 5 | B.Braun, Siemens, Philips, apod. |
| Zdravotnické prostředky prioritní | 50 | V rozsahu projektu Logmanagementu |

1. <https://nukib.gov.cz/download/uredni_deska/Minimalni_pozadavky_v4_FINAL.pdf> [↑](#footnote-ref-2)