

## Cenová nabídka - vypracování studie proveditelnosti pro umístění technologického zařízení - mobilního datového kontejneru

na základě požadavků Fakultní nemocnice v Brně - Bohunice, Jihlavská 20 a dle zákona o kybernetické bezpečnosti v souladu se směrnicí NIS2 EU

Datové centrum FN Brno, konkrétně jednotky DC\_T a DC\_15, jsou stěžejní pro poskytování IT infrastruktury, vyžadující konstantní dostupnost (24/7) pro nezbytné IT operace. Tento studie bude v dokumentu zkoumat současné umístění a potenciální alternativy pro novou modulární serverovnu, která by nahradila nedostačující DC\_T a udržela nezbytnou úroveň dostupnosti.

Pro informované rozhodování je potřebná detailní studie umístění nové kontejnerové serverovny, zahrnující stavební, hygienické, požární a infrastrukturní aspekty, stejně jako zajištění energetické efektivity a dostupnosti klíčových služeb.

Pro možnosti umístění mobilního datového kontejneru je nezbytné vytvořit stabilní základnu pro modulární serverovnu a zabezpečit propojení s nezbytnými síťovými infrastrukturami. Detailní technické a finanční hodnocení provede IOd/HTS. Na základě podkladů této studie.

### Zadání:

Z hlediska umístění IT pracovníků, vedení FNB rozhodlo o přemístění administrativních a projektových pracovníků do rekonstruovaného prostoru OBJ.9, zatímco technický personál zůstane v budově T.

Pro každé centrum je nezbytné zajištění samostatného fungování i integrace do celkového systému, aby byla zajištěna redundance a vysoká dostupnost. DC musí odpovídat prostorovým a technickým specifikacím DC\_15, ačkoli redukce do kontejnerové formy je vnímána jako úsporné opatření vzhledem k finanční situaci FN Brno.

V obou centrech jsou implementovány moderní technologie a zařízení pro zajištění nepřetržité dostupnosti služeb. Propojení datových center zahrnuje použití páteřních optických tras a redundantních síťových prvků pro minimalizaci rizika výpadků.

Klíčovým bodem je zajištění energetické nezávislosti prostřednictvím centrálních UPS systémů, a zvážit umístění blízko klíčové infrastruktury pro rychlé zásahy a údržbu. V případě havárií nebo pravidelných údržeb je preferováno blízké umístění DC, aby se minimalizoval čas nutný pro servisní zásahy.

Detailní studie a technické posouzení jsou nezbytné pro informované rozhodnutí ohledně umístění nové kontejnerové serverovny, s ohledem na energetickou efektivitu, dostupnost infrastruktury a personální rozložení.

## Podstatná kritéria pro umístění mobilního datového kontejneru

1. Stavební úřad:
  - Ohlášení/Stavební povolení: Zjistěte, zda je pro umístění kontejneru potřebné ohlášení u stavebního úřadu nebo stavební povolení. Předpisy se mohou lišit v závislosti na lokalitě a účelu kontejneru.
2. Hygiena:
  - Měření hluku: Prověřte, zda jsou potřebné studie měření hluku, zejména pokud se kontejner nachází v blízkosti obytných oblastí nebo má obsahovat hlučnější zařízení.
3. Požární bezpečnost a PBŘ (požární bezpečnostní řešení):
  - Zajištění požární bezpečnosti kontejneru v souladu s příslušnými předpisy a normami. Zahrnout může požární odolnost materiálů, dostupnost hasicích přístrojů a evakuační cesty.
4. Umístění kontejneru:
  - Zhutnění podloží: Ujistěte se, že místo, kde bude kontejner stát, má odpovídající zhutněné a stabilní podloží. Podloží by mělo být schopné nést hmotnost kontejneru a jeho obsahu bez rizika sesedání.
5. Ostatní problematika:
  - Přístupové cesty: Zajistěte, že jsou přístupové cesty ke kontejneru dostatečně široké a pevné pro manipulaci s kontejnerem a pro případnou údržbu.
  - Elektrické a síťové připojení: Zvažte potřeby pro elektrické a síťové připojení a zajistěte, že budou splněny všechny technické a bezpečnostní požadavky.
  - Klimatizace a ventilace: Pokud kontejner obsahuje technické zařízení, zajištění adekvátní klimatizace a ventilace je klíčové pro jeho správnou funkčnost a životnost.

Při plánování umístění mobilního datového kontejneru je důležité zohlednit všechny tyto aspekty a řídit se místními předpisy a normami.

### Alternativy umístění zahrnují:

- Umístění vedle stávající serverovny u budovy T.
- Lokalita u OBJ.9, protilehlá čerpací stanici.
- Kanceláře CI v budově bývalého CanoCar.

Analýza umístění pro datová centra:

### Lokalita objektu 9:

1. Geolokační aspekty:

Zvýšená geolokační vzdálenost prezentuje výzvy v mobilitě a přístupnosti.
2. Infrastrukturní požadavky:

Existuje imperativní potřeba kompletní páteřní infrastruktury a základové podpory.

3. Dostupnost:  
Prezentuje se suboptimální přístupnost, specificky v kontextu administrativních, nikoli technických, služeb.
4. Kontingenční plánování:  
Absence rekonstrukce může vést k nevhodnosti vybrané lokality.

#### **Lokalita budovy T:**

1. Přístupová kapacita:  
Lokalita nabízí rychlý přístup pro intervenční činnosti, včetně skladištních a personálních zdrojů.
2. Infrastrukturní dostupnost:  
Přítomnost a dostupnost páteřní infrastruktury jsou zajištěny.
3. Mobilita:  
Vysoká úroveň mobility je zajištěna s minimální geografické izolací datových center.

#### **Lokalita objektu kanceláře CI v budově bývalého CanoCar:**

1. Geolokační aspekty:  
Zvýšená geolokační vzdálenost prezentuje výzvy v mobilitě a přístupnosti.
2. Infrastrukturní požadavky:  
Existuje imperativní potřeba kompletace páteřní infrastruktury a základové podpory.
3. Dostupnost:  
Prezentuje se suboptimální přístupnost, specificky v kontextu administrativních, nikoli technických, služeb.
4. Kontingenční plánování:  
Rekonstrukce objektu může vést k vhodnosti vybrané lokality.

Hodnocení silových přívodů:

Předložte preference pro lokalitu u DC T z důvodu kompatibilní technologické náročnosti a infrastrukturální podobnosti s existující technologií. Možná extenze kabeláže by neměla překročit 50 m. Specifické výzvy nastávají při umístění blíže benzinové stanici, kde je nezbytné zajistit diverzifikaci napájecích zdrojů.

Integrační a finanční zhodnocení:

Vyžaduje se důkladné zhodnocení nákladů a investiční analýza pro obě navrhované lokality. Je zásadní zvážit technologické a energetické aspekty, včetně kontingentních plánů pro zajištění nepřetržitého provozu.

Pro zpracování studie umístění mobilního datového centra na základě popisu kontejnerové serverovny z textu je třeba zohlednit několik klíčových bodů:

Analýza stávajících podmínek: Je důležité pochopit současný stav a technické požadavky datových center FN Brno DC\_T a DC\_15, které jsou klíčové pro poskytování IT služeb.

Možnosti umístění: Je nutné posoudit dvě navrhované lokace pro umístění nové kontejnerové serverovny - vedle stávající serverovny u budovy T a u OBJ.9 (naproti benzinové pumpě). Je třeba zvážit dostupnost, potřebu výstavby pevného podkladu a připojení k nezbytným sítím.

Technická řešení a nákladovost: Zpráva by měla obsahovat analýzu technického řešení, jeho nákladovost a časovou náročnost realizace. Zohlednit je třeba i potřebu zachování stejných parametrů u přípojných sítí.

Umístění personálu: Změna umístění datového centra ovlivní rozmístění personálu. Vedení by mělo rozhodnout o optimálním rozdělení zaměstnanců mezi OBJ.9 a stávající budovu T.

Nezávislý provoz a integrace: Datové centrum by mělo být navrženo tak, aby mohlo fungovat samostatně a zároveň bylo integrováno do systému pro zajištění redundance a vysoké dostupnosti služeb.

Fyzická a síťová infrastruktura: Je klíčové zvážit redundanci napájecích a síťových prvků, fyzickou redundanci tras a propojení datových center pomocí optických tras.

Energetická infrastruktura: Zajištění redundance napájení z různých trafostanic je nezbytné pro obě navrhované lokace.

Odpověď na havárie: Lokace by měla umožňovat rychlou reakci technického personálu v případě havárií nebo potřeby servisu.

Dostupnost komponentů: Blízkost skladů s potřebnými komponenty je důležitá pro rychlou reakci na potřeby servisu nebo havárie.

Technické zhodnocení pro oblast HTS: Zpráva by měla obsahovat technické zhodnocení, včetně silových přívodů a možného rozšíření infrastruktury.

Finanční zhodnocení a porovnání variant: Je potřeba provést finanční analýzu a porovnat náklady spojené s oběma možnostmi umístění datového centra.

Zpracováním těchto bodů získáte komplexní přehled nutný pro informované rozhodování o umístění nové kontejnerové serverovny.

Součástí studie je posouzení bezpečnostní situace, umístění a přístup do mobilního datového kontejneru dle Zákona č. 205/2017 Sb., o kybernetické bezpečnosti ze dne 1. srpna 2017 (dále jen ZoKB) , který stanovuje v §3 toto:

Orgány a osobami, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti, jsou:

- a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací, pokud není orgánem nebo osobou podle písmene b),
- b) orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem nebo provozovatelem komunikačního systému podle písmene d),
- c) správce a provozovatel informačního systému kritické informační infrastruktury,
- d) správce a provozovatel komunikačního systému kritické informační infrastruktury,
- e) správce a provozovatel významného informačního systému,
- f) správce a provozovatel informačního systému základní služby, pokud nejsou správcem nebo provozovatelem podle písmene c) nebo d),
- g) provozovatel základní služby, pokud není správcem nebo provozovatelem podle písmene f),
- h) poskytovatel digitální služby

#### **Audit bezpečnostních opatření - prověření zejména těchto oblastí:**

- Zajištění identifikace osob vstupujících do objektu
- Zajištění perimetru vstupů do objektu
- Návrh systému PZTS, monitoring DPPC, centrální dispečink pro bezpečnostní dohled.
- Možnosti využití stávajících identifikačních karet zaměstnanců na povolení vstupu do objektu (stávající karty).
- Ochrana areálu (budovy, parkoviště, navazující přilehlé komunikace, vjezdy do areálu, vchod na pozemek)
- Ochrana cenného a důležitého zařízení a majetku
- Ochrana vnějších objektů.
- Ochrana vnitřních objektů.
- Ochrana lidských zdrojů.
- Popis a posouzení stávajícího stavu ochrany osob a majetku v rozsahu opatření fyzické ochrany.
- Fyzická ostraha (místní výkon, dálkový dohled aj.).
- Režimová a organizační opatření (zejména režim vstupu osob, režim vjezdu vozidel, klíčový režim aj.).

- Systémy technické ochrany (zejména mechanické zábranné prostředky, kamerový systém, poplachový zabezpečovací a tísňový systém, systém kontroly vstupu aj.
- Ochrana osobních údajů v souvislosti se subsystémy fyzické ochrany.
- Popis všech relevantních objektů, chráněných aktiv a procesů.
- Doporučení pro optimalizaci ochrany osob a majetku v rozsahu opatření fyzické ochrany a instalace technických bezpečnostních systémů (s důrazem na efektivitu, včetně vyčíslení možných úspor).
- Doporučený harmonogram implementace opatření.
- Střednědobý výhled další racionalizace ochrany osob a majetku.
- Právní podmínky pro uchování záznamu z CCTV a DVS.
- Problematika systému vnitřních procesů.
- Identifikace možných hrozeb.
- Analýza hrozeb a rizik z pohledu ochrany osob a majetku.

Problematiku vnitřních procesů provedenou až po dekompozici jednotlivých aktiv (primární aktiva, podpurná aktiva). V rámci této dekompozice popsat jednotlivé procesy, stanovit jejich význam (kritické procesy, základní procesy apod.) a vzájemné vazby. Analýza hrozeb a rizik z pohledu ochrany osob a majetku.

Pro identifikaci možných hrozeb budeme vycházet z katalogu BSI

Risk analysis with the new threat catalogue T 0 “Elementary Threats”

[https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/threats\\_catalogue.pdf?\\_\\_blob=publicationFile&v=1](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/threats_catalogue.pdf?__blob=publicationFile&v=1)

a směrnice NIS2 EU:

<https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32022L2555>

## 1. Navrhovaný postup při zjišťování výchozí situace a technických opatření v objektech

### 1.1 Místo realizace

Místem realizace projektu je sídlo žadatele: Působnost projektu v objektu Fakultní nemocnice Brno, Jihlavská 20.

### 1.2 Popis cílových skupin projektu

Hlavním přínosem pro cílovou skupinu je zvýšení bezpečnosti informací tj. dostupnosti, důvěrnosti a integrity dat zpracovávaných v objektu Fakultní nemocnice Brno, Jihlavská 20.

Cílová skupina bude mít prospěch z realizovaného projektu tím, že se především sníží riziko porušení důvěrnosti a integrity včetně ochrany osobních údajů.

### 1.3 Popis cílů a výsledků analýzy a jejich vztahu k naplňování podporovaných aktivit

Cílem bezpečnostní analýzy je posouzení realizace technických opatření v objektu Fakultní nemocnice Brno, Jihlavská 20, v souladu se standardy kybernetické bezpečnosti podle zákona č. 181/2014. Sb., o kybernetické bezpečnosti, ve znění pozdějších a doprovodných předpisů, specifikovanými vyhláškou č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) a to v Hlavě II – Technická opatření.

Organizace Fakultní nemocnice Brno - Bohunice, Jihlavská 20, se nachází v postavení povinného subjektu podle zákona o kybernetické bezpečnosti č. 205/2017 Sb. (novelizovaný zákon č. 181/2014 Sb.) podle § 3. Svým zaměřením a charakterem současně s rozsahem organizace se jedná o subjekt, který principiálně musí řešit kybernetickou bezpečnost a to nejen z důvodů vlastní ochrany, ale také z důvodů svého zaměření.

### 1.4 Doporučení investiční varianty

Hlavním přínosem analýzy fyzické bezpečnosti objektu mobilního datového kontejneru FN Brno je zhodnocení možnosti investiční varianty a její reálné plnění požadavků na kybernetickou bezpečnost v organizaci podle aktuálních standardů a doporučení i ze strany Národního úřadu pro kybernetickou a informační bezpečnost.

Právě Fyzická bezpečnost všech zařízení musí být v FN Brno analyticky vyhodnocena a měla by definovat nejmarkantnější slabá místa v rámci technických opatření dle VyKB. Bezpečnostní analýza má pojmenovat dostatečné zajištění zařízení, zajistit kontrolu pohybu osob v celém areálu všech objektů a zajistit řízení a kontrolu přístupu oprávněných osob do neveřejných prostor FN Brno.

### 1.5 Technická opatření – Analýza současného stavu

Bude provedena rámcová analýza stavu technických bezpečnostních opatření podle standardů kybernetické bezpečnosti v souladu s požadavky vyhlášky 316/2014 Sb. Výsledky analýzy dílčích částí technických opatření jsou v následující tabulce.

Nedílnou součástí auditu bude posouzení dostupných technologických a designových možností, jak tyto požadavky naplnit, a stanovení nejvhodnějšího postupu pro dílčí technologicky zaměřené projekty.

## Cenová nabídka pro vypracování studie proveditelnosti pro umístění technologického zařízení - mobilního datového kontejneru

1MD= 9 600,-Kč  
Celkem 9MD

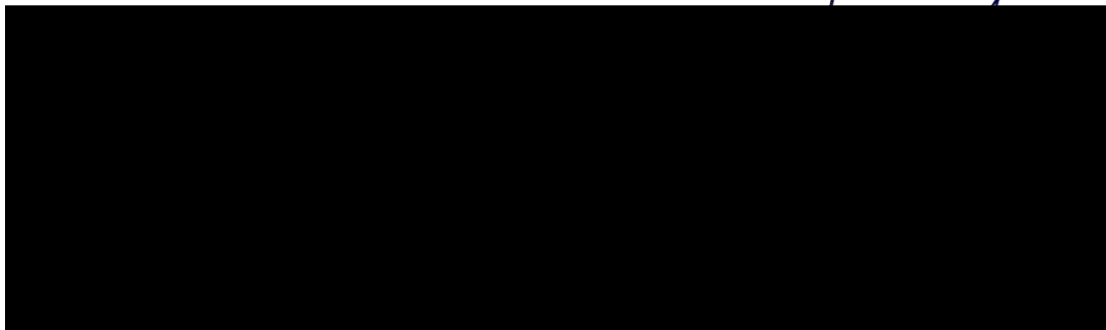
Celková cena za vypracování studie pro umístění mobilního datového kontejneru včetně posouzení z hlediska oblasti kybernetické bezpečnosti dle Zákona č. 205/2017 Sb., a na základě požadavků FN Brno – Bohunice, Jihlavská 20 činí:

**86 400,-Kč bez DPH**

Textová zpráva studie proveditelnosti a veškerá dokumentace bude na základě předávacího protokolu předána v 1 paré tisku a v elektronické verzi na datovém nosiči a bude ctít zásadu zvanou „platform, vendor and architecture independent“.

Studie proveditelnosti bude předána do 29.7.2024.

V Brně 7. 5. 2024



Společnost BRENDSON s.r.o. je specialistou pro oblast bezpečnosti IS a IT systémů, je mezinárodně certifikovaným auditorem kybernetické bezpečnosti dle zákona o kybernetické bezpečnosti (ZoKB) způsobilý k právním úkonům 6 odst. (2) Systému informační bezpečnosti – ISMS (Information Security Management Systems). Mezinárodně akreditovaný certifikační orgán pro kybernetickou bezpečnost dle standardů ISO/IEC 27001. Společnost TAYLLORCOX udělila akreditovaný titul bezpečnostní role podle - zákona č. 181/2014 o kybernetické bezpečnosti a prováděcích právních předpisů.

- Cyber Security Auditor - Certificate (ISMS) – series No: PCE ATO 2018051103
- PRINCE2 - Foundation Certificate in Project Management – TAYLLORCOX – series No: P2FO1911030
- Management – PeopleCert, AXELOS certificate No: GR633127395RM
- Certified EU GDPR DPO ISO/IEC 17024 - Data Protection Officer – Certificate (e-CF) – series No: PCE ATO 2018022301