# *Technická specifikace*

*Na specifikaci technického řešení se podílela společnost Deloitte Advisory s.r.o., IČO 27582167, pod vedením pana Ing. Jiřího Slabého, PhD.*

## 1 Popis celkového řešení

Národní centrum kybernetické bezpečnosti (dále jen *„NCKB“*) buduje se zapojenými partnerskými organizacemi (dále také jako *„Partneři“*) Systém sledování provozu a detekce bezpečnostních událostí (dále jen *„Systém*“) s cílem **zvýšit pravděpodobnost detekce pokročilých kybernetických útoků a bezpečnostně nežádoucího chování**. Toto výběrové řízení je jen jednou z částí celkového řešení.

V rámci Systému budou Partneři s vládním pracovištěm GovCERT.CZ, které je součástí NCKB, sdílet

- nezpracované údaje o síťovém provozu z perimetru jejich sítě,
- vybrané detekované bezpečnostní události z jejich sítě.

NCKB bude výše uvedené údaje od Partnerů a z externích informačních zdrojů automaticky i manuálně zpracovávat a vzájemně korelovat, což umožní upozornit i na události, které by v rámci jedné organizace nebyly vyhodnoceny jako nežádoucí.

Partneři nebudou s NCKB sdílet ani lokální detailní aktivitu, ani obsah komunikace uživatelů ve své vnitřní síti. Všechny dodatečné prvky informační infrastruktury instalované v rámci Systému v sítích Partnerů budou v plné správě jejich pracovníků kybernetické bezpečnosti.

**NCKB následně poskytne zapojeným partnerským organizacím aktualizace, které jim pomohou lépe identifikovat hrozby v jejich sítích.** Hrozbami, proti kterým je Systém detekce namířen, jsou především:

- DoS/DDoS útoky,
- zapojení do BOTNET sítí,
- komunikace do sítí a na adresy se špatnou reputací,
- malware,
- skenování sítě,
- brute-force pokusy o prolomení autentizace u služeb nabízených sítí.

Pro zapojené partnerské organizace tak bude mít Systém dvojí význam:

- zvýší bezpečnost sítě,
- umožní splnit část požadavků kladených zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, konkrétně technická opatření *„nástroj pro detekci kybernetických bezpečnostních událostí“* a *„nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí“*.

**Systém má dvě hlavní části**, které jsou soutěženy v rámci samostatných výběrových řízení (VŘ):

- **Samostatné systémy sběru síťových dat a detekce anomálií**, nasazené v rámci zapojených partnerských organizací s integrací do centrály GovCERT.CZ. **Tato část *JE* předmětem tohoto VŘ.**
- **Analytický systém**, který bude zpracovávat bezpečnostní události a síťové toky z jednotlivých partnerských organizací. Tato část *NENÍ* součástí tohoto výběrového řízení.

# 2 Architektura systému

Nákres celkové architektury s vyznačenými komponentami je obsažen v příloze L smlouvy – Nákres celkové architektury systému. Součásti tohoto výběrového řízení znázorňuje pouze spodní část nákresu ohraničená azurovou tečkovanou čárou a nadepsaná *"Součást dodávky VŘ Technologie sledování síťového provozu"*.

Horní část ohraničená růžovou tečkovanou čárou je předmětem jiného výběrového řízení, pro lepší představu o celkové architektuře a následném zpracování dat však přikládáme celý nákres.

# 3 Popis systému pro sběr síťových dat a detekci anomálií

Systém sběru síťových dat a detekci anomálií bude nasazen ve vybraných lokalitách připojených Partnerů. Systém bude pasivně monitorovat síťový provoz, odbočený z aktivních síťových prvků (SPAN) a přímo z linek (TAP). **Systém má 5 základních funkčních celků:**

**a)** **TAP** – sloužící k odbočení síťového provozu z linek
**b)** **Sonda** – pro sběr síťového provozu a generování IPFIX/NetFlow statistik
**c)** **Kolektor** – který sbírá a ukládá IPFIX/NetFlow statistiky ze všech sond v dané lokalitě pro možnost vyhodnocování veškerého provozu v dané lokalitě
**d)** **Moduly** – určené pro běh na kolektoru a/nebo sondě, případně dodané jako samostatný HW a SW; moduly vyhodnocují NetFlow/IPFIX data, případně další informace
**e)** **Aktualizační server** – umístěný v infrastruktuře NCKB
**f)** **Zabezpečená komunikační linka/bezpečný přípojný bod** – pro propojení Partnerů a pracoviště GovCERT.CZ.

Komponenty a), b), c) a d) se nachází v síti příslušného Partnera. Komponenty e), f) se nachází v síti NCKB. Všechny komponenty jsou popsány v textu níže. **Jednotlivé funkční celky lze nabídnout jako samostatné HW nebo SW komponenty, případně jako kombinace více funkčních celků v jednom HW/SW zařízení.**

Hlavní principy, které musí být zachovány:

- Systém nasazený u jednoho Partnera bude plně ve správě tohoto Partnera a bude sloužit pro účely lokálního bezpečnostního a výkonnostního monitoringu sítě,
- systém bude předávat do GovCERT.CZ:
    - detekované bezpečnostní události a
    - surová NetFlow/IPFIX data z perimetru sítě.

Všechny komponenty s výjimkou *„TAP"* musí zaznamenávat svoji činnost (logovat) v souladu s § 21 vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti[1].

Následuje popis jednotlivých komponent.

## 3.1 Komponenta *„TAP"*

TAPy (pasivní síťové monitorovací sondy) budou nasazeny pro přímý monitoring síťových linek. Požadavky na TAPy jsou:

- zcela transparentní pro monitorovanou síť
- zcela pasivní – sonda připojená na TAP nemůže ovlivnit obsah vlastního provozu
- 4 porty pro každou linku (2x produkční linka, 2x monitorovací porty – pro každý port jeden)
- fail safe – výpadek TAPu neovlivní provoz na monitorované lince
- redundantní napájení - v případě metalických TAPů
- možnost zapojení do standartních 19" racků

[1] Plné znění předmětné vyhlášky zde: https://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/provadeci-pravni-predpisy-k-zakonu-c-1812014-sb-o-kyberneticke-bezpecnosti-a-o-zmene-souvisejicich-zakonu/.

## 3.2 Komponenta *„Sonda“*

Zadavatel explicitně požaduje dodávku systému, který pasivně sbírá síťový provoz a generuje síťové statistiky ve formátu NetFlow/IPFIX, které slouží jako zdroj dat pro bezpečnostní a provozní moduly. Požadavky na NetFlow/IPFIX jsou:

- IPFIX protokol podle IETF RFC7011
- Export doplňujících L7 informací, minimálně v rozsahu:
    - http-metoda
    - http-user-agent
    - http-hostname
    - http-url
    - DNS requests
    - detaily protokolu SMB

volitelně možné další výhodou. V celé zadávací dokumentaci jsou tedy termínem *„NetFlow/IPFIX“* míněna data obohacená o L7 data uvedená výše.

**Pro účel tohoto projektu Zadavatel považuje NetFlow/IPFIX statistiky, obohacené o L7 informace, za dostatečné pro potřeby detekce bezpečnostních událostí.** Zadavatel nepožaduje zachytávání kompletního surového síťového provozu (DPI – Deep Packet Inspection). Sondy mohou být funkcí DPI vybaveny volitelně, s možností importu komerčních, komunitních nebo vlastních filtrů typu SNORT/Suricata. Pokud tuto funkci budou obsahovat, musí být v základním nastavení deaktivována.

Zadavatel požaduje nezávislé sondy pro generování NetFlow/IPFIX statistik z důvodů jednotného formátu (IPFIX) a vysokých požadavků na kvalitu dat, nelze tedy uvažovat export síťových statistik z již existujících aktivních prvků v rámci jednotlivých partnerských organizací. Výjimkou je situace, kdy již nasazená technologie v lokalitách je stejného výrobce jako uchazečem nabízená technologie.

Zadavatel má následující požadavky na funkční celek sond pro sběr síťového provozu a generování IPFIX/NetFlow statistik:

- Podpora IPv4 , IPv6, IEEE 802.1Q (VLAN)
- Dle typu sondy zpracování provozu:
    - na 1GbE portu bez ztráty paketu (rychlost linky)
    - minimálně 1,5 milionu paketů za sekundu na každém 10 GbE portu
- Metalické RJ-45 konektory pro 1GbE variantu sondy
- SFP+ šachty pro 10 GbE variantu sondy (SFP/SFP+ moduly jsou součástí dodávky)
- Zpracování zachycených dat bez vzorkování
- Vytvářet NetFlow/IPFIX na základě monitorovaného provozu dle požadavků výše
- Exportovat (odesílat) NetFlow / IPFIX záznamy na funkční celek kolektoru pro další zpracování
- Konfigurace pomocí SSH
- Grafické uživatelské rozhraní dostupné přes protokol HTTPS (TLS/SSL)
- Šifrování disků (FIPS 140-2 level 2)
- Zachytávat vybraný provoz do PCAP pro pozdější analýzu na základě manuálního zadání a automatického triggeru na základě události. Provoz bude odeslán a zpracován komponentně kolektoru.
- Sondy jako samostatný HW musí být ve formátu pro montáž do standartního 19“ racku
- Aktualizace a upgrades pouze přes aktualizační server v rámci GovCERT.CZ

## 3.3 Komponenta *„Kolektor“*

Zadavatel má následující požadavky na funkční celek kolektoru:

- Kolektor může být dodán jako samostatná HW appliance, případně může být dodán jako společná appliance sondy a kolektoru

- Zpracování příchozích NetFlow/IPFIX
- Konfigurace pomocí SSH
- Uložení NetFlow/IPFIX na lokální úložiště
- Grafické uživatelské rozhraní dostupné přes protokol HTTPS (TLS/SLL)
- Základní rozhraní pro práci s NetFlow/IPFIX
    - Hledání, filtrace, agregace dle zejména: IP adresy, MAC adresy, LAN segmentu, služby či portu, TCP příznaků, detekované aplikace a dalších L7 metadat
    - Grafické výstupy
    - Možnost vytvářet reporty a zasílat je šifrovaným emailem podepsaným pomocí PGP
- Kapacita úložného prostoru minimálně pro uložení NetFlow/IPFIX záznamů po dobu 6 měsíců (dle připojených linek, viz specifikace lokalit)
- Kolektory jako samostatný HW musí být ve formátu pro montáž do standartního 19“ racku
- Šifrování disků (FIPS 140-2 level 2)
- Možnost filtrovat NetFlow/IPFIX před jejich odesláním do GovCERT.CZ na základě IP adresy (možnost výběru pouze externí komunikace pro přeposlání do GovCERT.CZ)
- Přijímat NetFlow/IPFIX ze sond a z jiných kolektorů, filtrovat a směrovat ho do GovCERT.CZ (přes zabezpečenou komunikační linku)
- Přijímat syslog z jiných kolektorů a modulů a směrovat ho do GovCERT.CZ (přes zabezpečenou komunikační linku)
- Rozhraní pro konfiguraci a zpracování cílených záchytů do PCAP
- Aktualizace a upgrades pouze přes aktualizační server v rámci GovCERT.CZ

## 3.4 Komponenta *„Moduly“*

Zadavatel požaduje, aby moduly byly provozovány přímo na fyzické appliance kolektoru, případně byly dodány jako samostatný HW/SW paralelně ke kolektoru. Nicméně musí být zachováno oddělené vyhodnocování částí infrastruktury včetně možnosti odesílat bezpečnostní události popsaným bezpečným způsobem do GovCERT.CZ.

### 3.4.1 Modul detekce anomálií (NBA)

Modul NBA slouží k vyhodnocování NetFlow/IPFIX statistik s cílem detekovat v provozu útoky a anomálie. Modul NBA musí splňovat:

- Výkon alespoň 2500 flow/s pro každou instanci
- Detekce port scan (horizontální, vertikální, TCP, UDP, ICMP, …)
- Detekce hádání hesel (nezávisle na čísle portu) pro administrační služby Telnet, HTTP/S, SSH, RDP, VNC, SMB, SMTP/S, POP/S, IMAP/S, VPN, a další.
- Detekce potencionálních úniků dat (anomální přenosy dat), datové tunely (např. HTTP uvnitř DNS)
- Detekce anomálií v datových protokolech (DNS, DHCP, HTTP, SMTP, FTP,…)
- Detekce nestandartní komunikace (P2P sítě, botnety, malware,…)
- Detekce aplikací (Skype, Tor, ICQ,…)
- Detekce na IP spoofing
- Detekce přenosu velkého objemu dat
- Detekce neočekávaného počtu spojení
- Detekce komunikace na blacklistované IP, podpora externích databází (blacklisty, SPAMlisty, DNS, geolokace, …)
- Podpora externích databází (blacklisty, SPAMlisty, DNS, geolokace, …),
- Podpora pro integraci s interní ThreatDB
- Podpora propagace signatury útoku nebo pravidla z NCKB do modulu NBA přes aktualizační server v rámci GovCERT.CZ.
- Zpracování a vyhodnocování obousměrných toků ve vzájemném kontextu

- Export bezpečnostních událostí pomocí protokolu syslog a možnost jejich odesílání do GovCERT.CZ přes bezpečný přípojný bod na kolektoru
- Aktualizace a upgrades pouze přes aktualizační server v rámci GovCERT.CZ
- Možnost označit libovolnou událost za false-positive a vytvořit z ní přesné pravidlo, aby se daná událost označovala jako false-positive i v budoucnu.
- Pravidla pro automatické označování jako false-positive musí být možno specifikovat na základě jednotlivých položek události, kterými jsou např. IP adresy, porty, počty toků, počty paketů, přenesený objem dat a další položky uvedené u události.
- Události označené jako false-positive jsou ve výpisu událostí skryty nebo jsou označeny nejnižší úrovní kritičnosti.

### 3.4.2 Modul detekce a mitigace DDOS

Modul detekce a mitigace DDOS má návaznost na další bezpečnostní projekty GovCERT.CZ a je proto integrální součástí poptávaného řešení. Modul bude využívat NetFlow/IPFIX záznamy ze sond v rámci dané partnerské organizace pro detekci DDOS útoku a vytvoření jeho signatury. Modul musí splňovat:

- Detekovat útok a vytvořit signaturu útoků (TCP/UDP/ICMP flood) a různé kombinace TCP příznaků: RST, FIN, SYN, ACK,…) způsobujících odepření služby.
- Detekce probíhajícího útoku do 1 minuty
- Reportování průběhu útoků pomocí syslog (generování bezpečnostních událostí a dále přeposlání do GovCERT.CZ
- Umožňovat konfiguraci automatizovaného zásahu v případě detekce probíhajícího útoku tak, že zařízení vyšle pokyn nejbližšímu nadřazenému routeru, aby provedl přesměrování škodlivého provozu do dedikovaného systému pro mitigaci DDOS či scrubbing centra pomocí protokolů:
  - PBR (Policy Based Routing),
  - RTBH (Remotelly Triggered Black Hole),
  - BGP (iBGP, eBGP, BGP Flowspec).
- Možnost spustit libovolný skript jako trigger na probíhající útok
- Aktualizace a upgrades pouze přes aktualizační server v rámci GovCERT.CZ

### 3.4.3 Volitelně: Modul aplikačního monitoringu

Z důvodů konsolidace nasazených technologií a tím i úspory finančních prostředků Zadavatel preferuje doplnění systému o modul aplikačního monitoringu. Modul bude poskytovat data pro interní potřeby Partnerů monitoring výkonosti a kvality komunikace nasazených aplikací. Modul je tak určen k primárnímu monitoringu interní sítě. Celý systém tak kromě primárně bezpečnostního využití bude mít i využití provozní a přispěje k efektivnějšímu využívání IT prostředků v partnerských organizacích.

Modul aplikačního monitoringu bude využívat data sbíraná sondami (NetFlow/IPFIX a případně další data ze síťového provozu pomocí komponenty sonda) a bude umožňovat minimálně následující:

- Měření doby odezvy aplikací (https/https) a databází
- Měření z pohledu SLA (dle definovaných hodnot)
- Monitoring DB protokolů následujících databází:
  - MS SQL,
  - Oracle,
  - MySQL
  - PostgreSQL
- Pro monitoring http/https aplikace je požadováno ukládání a měření následujících metrik:
  - URL adresa
  - čas zahájení transakce[2]

[2] Pojmem *„transakce“* je myšleno jednotlivé volání aplikace – v případě http/https se jedná o URL volání, v případě DB o DB

    - čas ukončení transakce
    - doba odezvy
    - transportní čas dotazu a odpovědi
    - cookie
    - uživatel (možnost získat jeho IP, URL parametr, URL cestu, cookie, basic-auth, X-Forwarded-For) s cílem jednoznačně určit daného uživatele
- Pro monitoring DB je požadováno ukládání a měření následujících metrik:
    - DB dotaz (včetně SQL),
    - čas zahájení transakce
    - čas ukončení transakce
    - doba odezvy
    - transportní čas dotazu a odpovědi
    - uživatel
    - velikost
    - error code
- Aktualizace a upgrades pouze přes aktualizační server v rámci GovCERT.CZ

## 3.5 Komponenta *„Aktualizační server“*

Tato komponenta slouží jako centrální aktualizační server pro všechny komponenty a moduly nasazené v rámci partnerských organizací. Kromě samotných systémových a aplikačních aktualizací bude také poskytovat možnost distribuovat

- signatury útoků
- blacklisty IP / domén
- aktualizace firmwaru pro kolektory a sondy rozmístěné v partnerských organizacích

pro využití detekčními systémy rozmístěnými u partnerských organizací. Požadavky na server jsou:

- HTTPs server poskytující NBA signatury sdílené ze strany GovCERT.CZ
- HTTPs server poskytující blacklisty IP adres a domén sdílené ze strany GovCERT.CZ
- HTTPs server poskytující systémové a aplikační aktualizace pro všechny komponenty a moduly
- Virtuální appliance do prostředí KVM
- Komunikace server x klient (komponenty, moduly) pomocí protokolu https po síti internet nebo KIVS
- Konfigurace prostřednictvím příkazové řádky a/nebo jednoduchého GUI.

Zadavatel nad rámec výše uvedených funkcí požaduje 50 člověkodní (mandays – MD) pro implementaci bezešvého napojení na centrální analytický systém GovCERT.CZ běžící v infrastruktuře NBÚ, který je předmětem jiného výběrového řízení.

## 3.6 Komponenta *„Zabezpečená komunikační linka“*

Touto komponentou se rozumí veškeré vybavení potřebné pro přenos

- dat NetFlow/IPFIX
- kybernetických bezpečnostních událostí ve formátu syslog

z partnerských organizací do GovCERT.CZ.

V primární a sekundární lokalitě GovCERT.CZ bude instalován bezpečný přípojný bod, na který budou přímo kolektory (či jiné dedikované prvky z jednotlivých lokalit) odesílat data. Z tohoto konektoru pak bude možné data dále směrovat v rámci infrastruktury GovCERT.CZ. Přípojný bod bude mít více IP adres, viditelných v rámci sítě internet a v rámci sítě KIVS. Zadavatel požaduje dodávku 2 komponent (hlavní a záložní lokalita).

---

dotaz.

Základní požadavky na přípojný bod na straně GovCERT.CZ jsou:

- Podpora pro sestavení tunelu SSH, TLS či L2TP/IPSEC pro syslog data a Neflow/IPFIX z jednotlivých lokalit
- Podpora pro více externích IP adres: internet, KIVS
- Možnost konfigurace přesměrování příchozích paketů na cílové IP adresy v rámci sítě GovCERT.CZ (routing, port forwarding)
- Dodání jako virtuální appliance pro technologii KVM nebo jako samostatný HW
- Vzdálená konfigurace pomocí SSH
- Rozhraní pro monitorování stavu běhu a funkce tunelu. Cílem je mít možnost zjistit, zda komponenta běží (provozní informace) a zda je tunel funkční (sestaven a lze odesílat data). Podpora vyčítání informací přes SNMP a logování stavu pomocí syslog.
- Autentizace proběhne pomocí x509 (autentizace klienta i serveru). Certifikát bude platný, vydaný CA ve správě NBÚ (mezilehlá CA). V případě SSH bude probíhat autentizace pouze klíčem a server bude mít SSHFP (DNSSEC).
- Data bude zasílat vždy klient, server může přijetí jen potvrdit (ACK). Komponenta nebude přes tento tunel zasílat kromě uvedených potvrzování žádná data zpět a půjde tedy o jednosměrnou komunikaci.
- Komunikace bude povolena jen pro vybrané IP adresy (ACL).

Součástí kolektoru nebo jako samostatná komponenta musí být i odesílací část *„zabezpečené komunikační linky“* do prostředí GovCERT.CZ. Konektor musí umožnit směrování a odesílání NetFlow/IPFIX a syslog protokolů do prostředí GovCERT.CZ.

Požadavky na odesílací část jsou:

- Možnost konfigurace 2 a více přípojných bodů (IP adres) GovCERT.CZ – primární a záložní. Pokud se nepovede sestavit tunel, či vypadne spojení na primární bod, bude automaticky sestaveno spojení na sekundární (a další) přípojný bod.
- Automatické sestavení tunelu SSH, TLS či IPSEC pro syslog data a Neflow/IPFIX. Možné jeden společný tunel či zvlášť pro události a NetFlow/IPFIX.
- SSH: Autentizace pouze klíčem (4096b). Přijímací část bude používat SSHFP (DNSSEC).
- TLS: ověření klienta i serveru, zapnuté HSTS na straně serveru (přijímací části)
- IPSEC: Autentizace pouze klíčem (4096b)
- Klíče budou distribuovány ze strany Zadavatele v rámci implementace řešení.

# 4 Organizace, lokality a počty jednotlivých funkčních celků

Tabulka níže shrnuje počty jednotlivých komponent za jednotlivé organizace a lokality. Zadavatel požaduje dodávku následujících komponent:

- Metalických a optických TAPů
- Sond s minimálním počtem a druhem portů dle tabulky
- Potřebných SFP/SFP+ modulů dle tabulky
- Kolektorů (kolektor může být spojen se sondou, pokud je to technologicky možné a vhodné a výkonově to nelimituje běh modulů pro daný počet uživatelů v rámci lokality)
- Modulů NBA, aplikačního monitoringu a detekce a mitigace DDOS na každý kolektor (či paralelně ke každému kolektoru)
- Komponent zabezpečené komunikační linky: na každý kolektor odesílací část (či paralelně k němu) a dále přijmací část do prostředí GovCERT.CZ

| Organizace | Komponenta | Počet |
|---|---|---|
| GovCERT.CZ | Komponenta přijímající části zabezpečené komunikační linky - přípojný bod. | 2 |

| Organizace | Komponenta | Počet |
|---|---|---|
| GovCERT.CZ | Aktualizační server (virtuální appliance) | 1 |
| | | |
| MSp | 6 x 1 Gbps sonda (6 metalických portů) | 2 |
| MSp | 1 x 1 Gbps sonda (1 metalický port) | 11 |
| MSp | Kolektor (včetně modulů) | 1 |
| MSp | TAP (1 Gbps, metalika) | 4 |
| | | |
| MPSV | 2 x 10 Gbps sonda (2 SFP+ klece) | 4 |
| MPSV | SFP+ optický transciever (MM) | 8 |
| MPSV | SFP metalický transciever | 4 |
| MPSV | 3 x 1 Gbps sonda (3 metalické porty) | 1 |
| MPSV | Kolektor (včetně modulů) | 3 |
| MPSV | TAP (10 Gbps, optika) | 2 |
| | | |
| MF | 4 x 1 Gbps sonda (4 metalické porty) | 7 |
| MF | 6 x 1 Gbps sonda (6 metalických portů) | 1 |
| MF | 4 x 10 Gbps sonda (4 SFP+ klece) | 2 |
| MF | SFP+ optický transciever (SC) | 8 |
| MF | Kolektor (včetně modulů) | 4 |
| MF | TAP (1 Gbps, metalika) | 17 |
| MF | TAP (10 Gbps, optika) | 4 |

V tabulce níže je uveden počet uživatelů za jednotlivé lokality[3] (umístění komponenty kolektoru), dalším zdrojem informací o podobě cílových sítí jsou nákresy těchto sítí a odhady datových objemů, které jsou součástí přílohy, která bude žadatelům poskytnuta na vyžádání.

| Organizace | Lokalita | Počet uživatelů |
|---|---|---|
| MPSV | ČSSZ | 8600 |
| MPSV | Datové centrum (síť MPSV) | 12 500 |
| MPSV | Úřad pro mezinárodně právní ochranu dětí | 40 |
| | | |
| MF | Generální ředitelství cel | 5 800 |
| MF | Síť ministerstva | 17 300 |
| MF | Úřad pro zastupování státu ve věcech majetkových | 1 768[4] |
| MF | SCPSS | Nerelevantní[5] |
| | | |
| MSP | Vše | 22 446 |

Nákresy sítí jednotlivých organizací s uvedením přesných lokalit a předpokládaného zapojení jsou uvedeny v příloze X Nákresy sítí, která je vzhledem k citlivosti uváděných informací k dispozici na vyžádání u zadavatele. Žádosti o vydání přílohy prosím zašlete datovou schránkou na adresu NBÚ.

[3] Není-li uvedeno jinak, jsou počty zaměstnanců převzaty z přehledových tabulek skutečného počtu zaměstnanců státních institucí za rok 2015 z materiálu Ministerstva financí Návrh státního závěrečného účtu České republiky za rok 2015, sněmovní tisk 800/0: http://www.psp.cz/sqw/text/tiskt.sqw?O=7&CT=800&CT1=0

4 Výroční zpráva 2015 – Úřad pro zastupování státu ve věcech majetkových: http://www.uzsvm.cz/Soubor.ashx?docsouborID=1066497

5 Jedná se o datové centrum a odhad je nutné provádět čistě na základě druhu a počtu linek s ohledem na odhadovaný provoz.

# 5 Seznam některých zkratek

| Zkratka | Vysvětlení |
|---|---|
| GovCERT.CZ | Infrastruktura NBU |
| MSp | Ministerstvo spravedlnosti |
| MPSV | Ministerstvo práce a sociálních věcí |
| MF | Ministerstvo financí |
| DNSSEC | Specifikace pro zabezpečenou komunikaci DNS protokolem |
| NetFlow | Síťový protokol od společnosti Cisco pro monitorování provozu na IP sítích |
| IPFIX | Protokol pro export informací o tocích v IP sítích |
| SSH | Secure shell. Protokol pro vzdálený přístup na konzoly |
| KVM | Virtualizační technologie pro platformu Linux |
| KIVS | Linky v rámci projektu „Komunikační infrastruktura veřejné správy“ |
| TLS | Protokol pro zabezpečení přenosu informací na http vrstvě |
| L2TP | Tunelovací protokol na OSI L2 vrstvě |