4.1. Identifikace a analýza požadavků na bezpečnost

Identifikace požadavků na bezpečnost CMS 2.0 je předpokladem správného nastavení bezpečnosti CMS 2.0. Po identifikaci požadavků musí následovat jejich analýza s cílem určit, co jednotlivé požadavky znamenají pro návrh, realizaci a provoz CMS 2.0. Dodavatel provedl identifikaci a základní analýzu požadavků na bezpečnost CMS 2.0. V této kapitole jsou uvedeny podklady, ze kterých Dodavatel vycházel a stručný přehled hlavních požadavků uvedených v jednotlivých podkladech.

4.1.1. Zákonné a regulační požadavky

- **Zákon číslo 240/2000 Sb. a nařízení vlády číslo 462/2000 Sb.** Zákon i nařízení vlády se týkají obecně krizové připravenosti, nejsou zaměřeny pouze na informační bezpečnost. Zákon a nařízení obsahují zejména následující požadavky.
    - Vypracovat plán krizové připravenosti subjektu kritické infrastruktury do jednoho roku od rozhodnutí vlády nebo ode dne nabytí právní moci opatření obecné povahy, kterým byl prvek kritické infrastruktury určen.
    - Umožnit příslušnému ministerstvu nebo jinému správnímu úřadu vykonání kontroly plánu krizové připravenosti.
    - Oznámit příslušnému ministerstvu nebo jinému správnímu úřadu informace o změnách, které mají vliv na určení prvku kritické infrastruktury.
    - Povinnost jmenovat styčného bezpečnostního zaměstnance.
- **Usnesení vlády č. 140/2010 Sb. ČR z 22. února 2010.** Toto usnesení vlády mj. schvaluje Národní program ochrany kritické infrastruktury, který mj. požaduje vypracování programů pro ochranu kritické infrastruktury:
    - zpracování analýz ohrožení celostátně významných prvků kritické infrastruktury,
    - provedení úprav metodik pro zpracování plánů v oblasti bezpečnosti: krizové plány, plány bezpečnosti,
    - plány kontinuity činnosti subjektů kritické infrastruktury,
    - úpravy vnitřních předpisů a standardů pro příslušné oblasti kritické infrastruktury.
- **Nařízení vlády č. 432/2010 Sb. ČR z 22. prosince 2010.** Toto nařízení v příloze definuje odvětvová kritéria pro určení prvků kritické infrastruktury. Nároky na zabezpečení prvků

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

kritické infrastruktury bude definovat připravovaný Zákon o kybernetické bezpečnosti a zejména jeho prováděcí vyhlášky

- **Usnesení vlády č. 385/2012 Sb. ČR z 30. května 2012.** Toto usnesení vlády mj. požaduje předložit Koncepci rozvoje KIVS 2013-2017. MV zpracovalo v souladu s požadavkem Koncepci rozvoje KIVS na léta 2013 – 2017. V ní pro oblast bezpečnosti zejména požaduje:
    - zajištění návaznosti KIVS na kybernetickou bezpečnost státu a na ochranu kritických infrastruktur státu,
    - redundanci a vysokou dostupnost CMS2,
    - CMS 2.0 má poskytovat služby spojené s ochranou proti DDOS útokům,
    - CMS 2.0 má poskytovat služby spojené se zajištěním kybernetické bezpečnosti,
    - závazek vytvořit bezpečnostní dokumentaci, zejména bezpečnostní politiky KIVS až na úroveň katalogových listů,
    - dohled nad dodržováním bezpečnostní politiky a bezpečnostní monitoring.
- **Zákon č. 101/2000 Sb., o ochraně osobních údajů.** CMS 2.0 nebude ukládat ani zpracovávat osobní údaje. Ty se mohou vyskytovat v přenášených datech. Proto bude součástí definice katalogových listů služeb CMS 2.0 informace o bezpečnosti každé služby, aby se subjekty používající CMS 2.0 pro přenos a šíření osobních údajů mohly rozhodnout, zda jsou bezpečnostní opatření CMS 2.0 pro příslušný účel dostatečná. Provozovatel CMS 2.0 nebude správcem ani zpracovatelem osobních údajů ve smyslu Zákona, nicméně v ESB se budou při komunikaci mezi AIS a ZR přes ESB vyskytovat v nešifrovaném tvaru osobní údaje, které se bez ESB přenáší mezi AIS a ISZR šifrovaným spojením. Požadovanou součinností proto je potvrzení možnosti šíření osobních údajů prostřednictvím CMS 2.0 a možnost výskytu nešifrovaných osobních údajů v ESB.
- **Zákon č. 121/2000 Sb., o právu autorském.** Zákon o právu autorském se na CMS 2.0 vztahuje v tom smyslu, že v CMS musí být používán software v souladu s licencí a musí používat veškeré materiály (např. propagační) v souladu s uvedeným zákonem.
- **Zákon č. 227/2000 Sb., o elektronickém podpisu.** Zákon upravuje používání elektronického podpisu a elektronické značky a poskytování certifikačních služeb. Provozovatel CMS 2.0 bude poskytovat certifikační služby (pouze ale v případě, že nebude využita CA SZR), ale nebude kvalifikovaným poskytovatelem certifikačních služeb, který vydává kvalifikované

certifikáty nebo kvalifikované systémové certifikáty nebo kvalifikovaná časová razítka nebo prostředky pro bezpečné vytváření elektronických podpisů.

- **Zákon č. 365/2000 Sb., o informačních systémech veřejné správy.** Zákon stanoví práva a povinnosti, které souvisejí s vytvářením, užíváním, provozem a rozvojem informačních systémů veřejné správy. CMS 2.0 ani jeho žádná část (tedy ani ESB) nebude informačním systémem veřejné správy. Některé paragrafy se ale týkají Dodavatele jakožto budoucího provozovatele CMS 2.0. Paragraf 6g definuje, že MV může svěřit provozování CMS právnické nebo fyzické osobě. Dodavatel se tedy může stát provozovatelem CMS 2.0. Dodavatel bude jako budoucí provozovatel spolupracovat se Zadavatelem při plnění požadavků Zákona.

- **Zákon č. 441/2003 Sb., o ochranných známkách.** Zákon určuje podmínky přidělování a používání ochranných známek. Dodavatel zajistí správné označení ochranných známek v dokumentaci a software CMS 2.0 a zajistí, aby názvy používané v dokumentaci CMS 2.0, při propagaci CMS 2.0 a v komponentách CMS 2.0 nenarušovaly cizí práva týkající se ochranných známek.

- **Zákon č. 127/2005 Sb., o elektronických komunikacích.** Zákon reguluje poskytování veřejně dostupných komunikačních činností. CMS 2.0 nebude veřejně dostupný komunikační systém. Je určeno pro využívání orgány státní správy. Proto se na Dodavatele ani provozovatele CMS 2.0 uvedený zákon nevztahuje.

- **Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.** Zákon upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy. CMS 2.0 není určeno k přenosu a zpracování utajovaných informací. Proto ustanovení tohoto zákona nejsou pro CMS 2.0 ani Dodavatele a provozovatele CMS 2.0 relevantní.

- **Zákon č. 111/2009 Sb., o základních registrech.** Zákon vymezuje obsah základních registrů, informačního systému základních registrů a informačního systému územní identifikace a stanoví práva a povinnosti, které souvisejí s jejich vytvářením, užíváním a provozem a zřizuje Správu základních registrů. CMS 2.0 je mj. určeno pro zprostředkování komunikace mezi AIS a ZR. Z paragrafu 5 Zákona vyplývá, že CMS 2.0 ani jeho provozovatel nesmí referenční ani jiné údaje ze ZR a AIS nijak využívat a ani je nesmí poskytovat dalším subjektům. Komunikace mezi AIS a ZR je šifrovaná a tedy pro provozovatele CMS 2.0 nepřístupná. Výjimkou je komunikace ESB s vnějším rozhraním ISZR. Uvnitř ESB se data přenášená mezi AIS a ESB a mezi AIS a ISZR budou vyskytovat nešifrovaná. CMS 2.0 jako celek a ESB speciálně budou

navrženy tak, aby přístup k přenášeným datům byl pro provozovatele CMS 2.0 možný pouze v případě řešení problémových stavů a okruh oprávněných osob byl maximálně omezen. Zvláštní otázkou je přístup ESB k vnějšímu rozhraní ISZR. ESB není AIS. Součinností MV je nutné zajistit povolení přístupu ESB k ZR.

- **Usnesení vlády č. 727/2009 Sb., ke Zprávě o přechodu na IPv6.** Usnesení souhlasí s přechodem na IPv6, ukládá ministrům a vedoucím ostatních ústředních orgánů státní správy zajistit od 30. června 2009 při pravidelné obnově síťových prvků jejich kompatibilitu s IPv6 a zajistit do 31. prosince 2010 přístup k internetovým stránkám a veřejně dostupným službám eGovernmentu přes IPv6. Dodavatel respektuje odpovědnost MV jako Zadavatele za plnění Usnesení a CMS 2.0 bude postaveno na hardwarových i softwarových komponentách podporujících plně IPv6. To umožní subjektům používajícím CMS 2.0 využívat IPv6 bez omezení.

- **Koncepce rozvoje KIVS 2013-2017.** MV zpracovalo v souladu s požadavkem Usnesení vlády ČR číslo 385/2012 Sb. koncepci rozvoje KIVS na léta 2013 – 2017. V ní pro oblast bezpečnosti požaduje hlavně:

    - zajištění návaznosti KIVS na kybernetickou bezpečnost státu a na ochranu kritických infrastruktur státu (str. 2, Důvody ke změně koncepce KIVS),

    - požadavky na novou generaci CMS, tj. na CMS 2.0.

Všechny uvedené požadavky Dodavatel zahrnul do návrhu řešení.

Určitou neznámou zůstávají požadavky navrhovaného Zákona o kybernetické bezpečnosti, protože není k dispozici definitivní znění ani prováděcí předpisy. Nicméně návrh Zákona vychází z požadavků normy ČSN ISO/IEC 27001:2006 a je velmi pravděpodobné, že i obsah prováděcích předpisů bude odpovídat požadavkům této normy. Dodavatel postupuje v oblasti informační bezpečnosti podle této normy.

4.1.2. Požadavky Zadavatele

Dodavatel dále vychází ze všech požadavků na bezpečnost, které jsou uvedeny v zadávací dokumentaci.

Zadavatel jako jeden z hlavních nedostatků CMS 1.0 uvádí nevyhovující formu řízení informační bezpečnosti. Při řízení informační bezpečnosti CMS 2.0 Dodavatel postupuje podle mezinárodních standardů, zejména podle normy ISO/IEC 27001:2006 a doporučení NIST 800-53, což je zárukou dodržení mezinárodně doporučovaných postupů při řízení informační bezpečnosti.

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

Zadavatel klade velký důraz zajištění vysoké dostupnosti CMS 2.0 a odolnost vůči útokům typu odepření služby (DOS, DDOS). Dodavatel navrhuje vybudovat dva rovnocenné uzly CMS 2.0, každý z nich umožňuje plnou funkcionalitu CMS 2.0. A v rámci jednoho uzlu bude použita redundantní konfigurace síťových zařízení, serverů, kabeláže a elektrických rozvodů. Opatření proti útokům typu odepření služby budou navržena na všech rozhraních, na kterých CMS 2.0 komunikuje s externími prvky. Nejenom tedy na rozhraní do Internetu, ale i do sítí EU, do DC atd.

V souladu s požadavky Zadavatele bude provedeno bezpečné oddělení CMS 2.0 od externích sítí (Internet, sTESTA a dalších). CMS 2.0 bude na všech rozhraních vybaveno výkonnými a účinnými firewally a detektory pokusů o útok proti CMS 2.0.

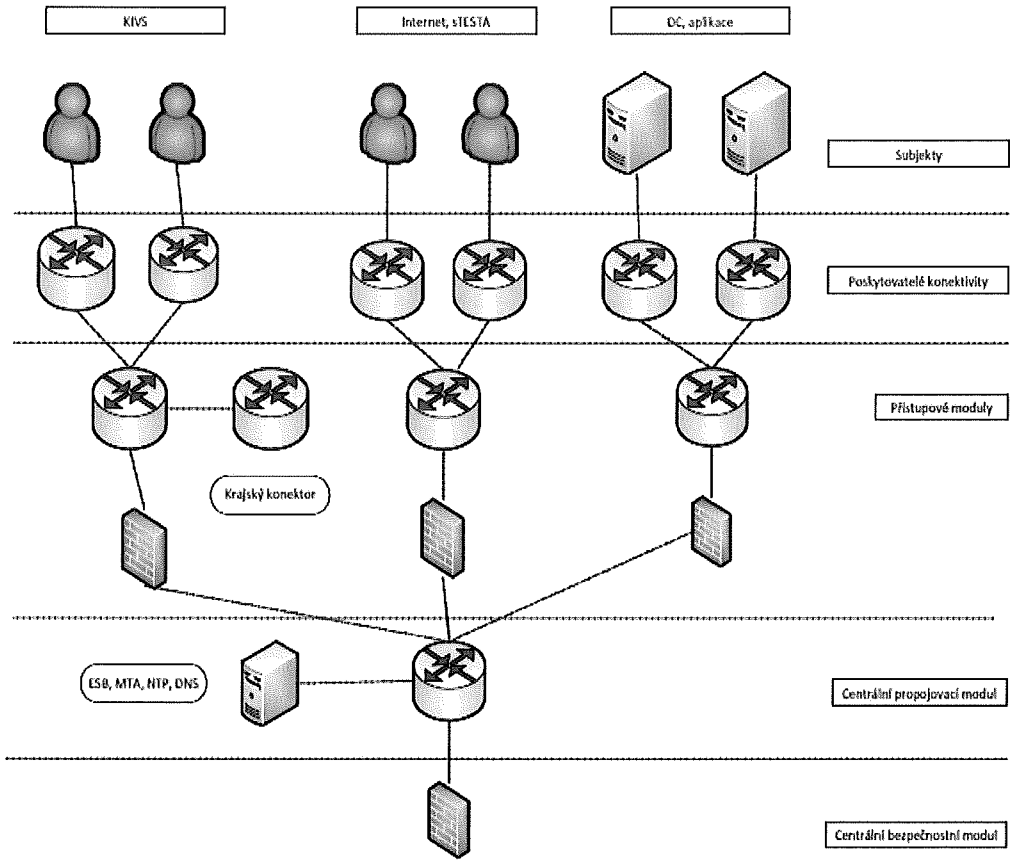
Síťový provoz jednotlivých subjektů připojených do CMS 2.0 bude oddělen technickými prostředky a vzájemná komunikace bude možná pouze na základě souhlasu komunikujících subjektů a na základě definovaných a odsouhlasených pravidel.

Podrobnější popis realizace jednotlivých opatření z této kapitoly je uveden v dalších kapitolách v tomto dokumentu. Část opatření je popsána přímo u popisu technických řešení jednotlivých komponent.

4.2. Bezpečnostní architektura

Z pohledu bezpečnosti lze identifikovat několik vrstev. V každé z nich jsou aplikovatelná rozdílná opatření a za jejich realizaci a dodržování je odpovědný jiný subjekt. Schematické znázornění je na následujícím obrázku.

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.



Obrázek 26 - Bezpečnostní architektura CMS 2.0

V horní části ve vrstvě „Subjekty" jsou uživatelé CMS 2.0. Jsou to jednak subjekty, které nabízejí služby, a za druhé subjekty, které tyto služby používají. Jedná se především o služby nabízené informačními systémy připojených subjektů. Za bezpečnost v této vrstvě bude odpovídat příslušný subjekt. Správce CMS 2.0 může jeho činnost ovlivňovat a regulovat pomocí standardů pro připojení k CMS 2.0 a pro provoz CMS 2.0.

Ve vrstvě „Poskytovatelé konektivity" jsou subjekty poskytující konektivitu pro připojení subjektů k CMS 2.0. Za bezpečnost v této vrstvě bude odpovídat příslušný poskytovatel. Správce CMS 2.0 může opět jeho činnost ovlivňovat a regulovat pomocí standardů pro připojení k CMS 2.0 a pro provoz CMS 2.0 a smluvními podmínkami. Ve sloupci „KIVS" jde technicky o MPLS sítě poskytovatelů. Ve sloupci „Internet, sTESTA" jde o infrastrukturu poskytovatelů připojení do Internetu, respektive sTESTA. Ve sloupci „DC" jde o infrastrukturu provozovatelů DC připojených k CMS 2.0. Ve sloupci „Aplikace" jde o infrastrukturu provozovatele DC, ve kterém bude umístěn modul Portál.

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

Za bezpečnost ve vrstvě „Přístupové moduly" bude odpovídat správce CMS 2.0 a provozovatel CMS 2.0. Zařízení v této vrstvě budou pod jejich přímou kontrolou. Jde o přístupová zařízení (směrovače), souhrn zařízení označovaných jako firewall a další zařízení pro kontrolu přístupu (SSL servery, VPN koncentrátory). Zařízení v této vrstvě tvoří hranici CMS 2.0 a provádějí následující bezpečnostní funkce.

- Normalizace provozu (defragmentace).
- Inspekce provozu. Detekují výskyt škodlivého software (malware) a anomálie v použitých protokolech atd.
- Ochrana proti útokům na dostupnost služeb (DOS a DDOS útoky).
- Identifikace a autentizace subjektů. Tj. kontrola, zda je možné povolit subjektu přístup do CMS 2.0. Dělá se pouze pro některé typy spojení.

Hlavním účelem vrstvy „Centrální propojovací modul" bude co nejrychleji propojovat ostatní moduly. Druhým účelem bude umožnit přístup k infrastrukturním službám a aplikačním službám CMS 2.0. Nebude mít žádné globální bezpečnostní funkce, jednotlivé služby umístěné v této vrstvě budou zabezpečeny lokálně na úrovni vlastní služby (lokální firewall apod.).

Ve vrstvě „Centrální bezpečnostní modul" bude umístěn centrální firewall, který bude provádět dvě základní funkce:

- překlad adres (pokud je potřeba),
- autorizaci propojení. Povolí pouze ta spojení, která odpovídají schváleným žádostem na služby CMS 2.0.

4.3. Hodnocení rizik

Hodnocení rizik a návrh protiopatření je klíčovou částí řízení bezpečnosti informačních a komunikačních systémů obecně a tedy i CMS 2.0.

Rozsah hodnocení rizik je vymezen hranicemi CMS 2.0:

- Subjekty CMS 2.0.
- Služby CMS 2.0.
- Data CMS 2.0.

- Software CMS 2.0.
- Hardware CMS 2.0.
- Lokality CMS 2.0.

Nejdůležitějším aktivem jsou data, tedy informační aktiva, a služby pro zpřístupnění těchto dat.

Služby CMS 2.0 jsou definovány Katalogem služeb CMS 2.0. V CMS 2.0 budou zpracovávána následující **data** (informační aktiva).

- Uživatelská data. Patří sem data přenášená a zpracovávaná CMS 2.0 z iniciativy uživatelů.
- Konfigurační data. Veškeré konfigurace zařízení a serverů, které jsou součástí CMS2.
- Identifikační, autentizační a autorizační údaje o uživatelích a správcích.
- Data pro správu CMS 2.0. Patří sem data přenášená a zpracovávaná CMS 2.0 z iniciativy správců a pro jejich potřebu.

K zajištění služeb CMS 2.0 bude potřebný určitý **software** (programová aktiva).

- Software pro provoz CMS 2.0.
- Software pro správu CMS 2.0.

Provoz CMS 2.0 bude zajišťován pomocí **technických prostředků** (fyzická aktiva).

- Zařízení pro provoz CMS 2.0.
- Zařízení pro správu CMS 2.0.
- Podpůrná zařízení CMS 2.0.

Do hodnocení rizik budou zahrnuty i **lokality**, ve kterých jsou umístěny komponenty CMS 2.0.

Dodavatel provede **hodnocení** informačních **aktiv**. Každému aktivu přiřadí hodnotu, která vyjadřuje míru důsledků, pokud nastane porušení některé složky bezpečnosti informací.

Hodnocení rizik, která ohrožují data, bude provedeno s ohledem na všechny základní složky bezpečnosti informací:

- dostupnost,

- důvěrnost,
- integrita.

Doplňující složka bezpečnosti informací je:

- nepopiratelnost.

Dostupnost je schopnost zajistit přístup oprávněným subjektům k aktivům, když je to potřeba.

Dostupnost je základní vlastností aktiv. V případě informačních aktiv má garantovat, že oprávněný subjekt dostane správnou informaci ve správný čas a na správném místě. Ve většině informačních a komunikačních systémů včetně CMS 2.0 se jedná o **kritický požadavek,** který musí být zajištěn prioritně.

Důvěrnost je schopnost zajistit přístup k aktivům pouze oprávněným subjektům. Je zapotřebí zajistit že k aktivům bude mít přístup pouze přesně definovaná skupina oprávněných subjektů (osob). V případě informačních aktiv jde o požadavek na to, aby si informace nemohl přečíst nikdo jiný než oprávněné osoby.

Integrita je schopnost zajistit správnost a úplnost aktiv. V případě informačních aktiv jde o požadavek, aby během přenosu nebo zpracování dat nedošlo k jejich neoprávněné změně (úmyslným poškozením, pozměněním, chybami přenosu atd.).

Nepopiratelnost je schopnost zjistit autorství jakékoli změny či autorství nového záznamu. Účelem zajištění nepopiratelnosti je schopnost přisoudit určitou vykonanou činnost jednoznačně subjektu, který tuto činnost provedl.

4.3.1. Hodnocení informačních aktiv

Informační aktiva bude Dodavatel hodnotit z hlediska dostupnosti, důvěrnosti, integrity a v případě některých služeb i z hlediska nepopiratelnosti.

U komunikačních systémů, jako je CMS 2.0, se při posuzování dostupnosti jedná o schopnost poskytovat příslušné služby pro přenos uživatelských dat. Při posouzení důvěrnosti jde o záruky, že se data využívající nějakou službu dostanou pouze k adresátovi a ne k neoprávněné osobě. Při posouzení integrity jde o zajištění toho, že data nebudou mezi odesílatelem a příjemcem změněna. A při posuzování nepopiratelnosti jde o zajištění průkaznosti toho, že nějaký subjekt určitou zprávu odeslal a nějaký subjekt ji přijal.

Stanovení hodnoty informačních aktiv proběhne na základě stanovení potenciálních dopadů v případě narušení jednotlivých složek bezpečnosti informací. Dodavatel pracuje s hodnotami, které mají jednotlivá aktiva pro něj. Dodavatel nezná hodnotu informačních aktiv, kterou mají pro jejich vlastníky, tj. uživatele CMS 2.0.

4.3.2. Identifikace závislostí mezi aktivy

V dalším kroku identifikuje Dodavatel závislosti mezi aktivy. Vyjde od informačních aktiv a vyhledá, která fyzická a programová aktiva jsou potřeba pro zpracování informačních aktiv pomocí jednotlivých služeb. A k jednotlivým fyzickým aktivům přiřadí lokality.

Výsledkem je znázornění závislostí formou obrázku nebo tabulky. Cílem je zjistit, která další aktiva jsou potřeba pro zpracování informačních aktiv, a bude je nutné odpovídajícím způsobem chránit.

4.3.3. Rizika a jejich hodnocení

Dodavatel uváží následující kategorie rizik. U jednotlivých kategorií jsou uvedeny příklady rizik, nejde o vyčerpávající seznam rizik.

- Fyzická.
    - Ohrožení zařízení CMS 2.0 přírodními vlivy (záplavy, bouře, sníh, zemětřesení, blesk), ohněm, průmyslovými haváriemi, nepokoji, nebo karanténami.
    - Ohrožení zařízení CMS 2.0 nevyhovujícími podmínkami pro provoz (teplota, vlhkost, prašnost).
    - Připojení neschváleného zařízení k CMS 2.0.
- Personální.
    - Chyba obsluhy: chybné konfigurace hardware nebo software, chybné příkazy administrátorů. Chyby v DNS, směrování, IP adresách.
    - Sociální inženýrství proti osobám podílejícím se na provozu nebo správě CMS 2.0.
- Informační (kybernetická).
    - Výskyt malware v CMS 2.0.
    - Kybernetický útok vedený proti CMS 2.0.
    - Útok na dostupnost CMS 2.0 (jako specifický typ kybernetického útoku).

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

- Falšování identity. Může jít o použití falešných IP adres nebo o pokus vydávat nějaké neschválené zařízení za zařízení autorizované pro připojení k CMS 2.0.

- Technická.
  - Nedostupnost konfiguračních dat aplikací.
  - Chyba software.
  - Chyba hardware.
  - Nedostupnost komunikací.

- Cílem hodnocení rizik je:
  - prokázat, že navržená bezpečnostní opatření jsou dostatečná,
  - identifikovat případnou potřebu realizace dodatečných bezpečnostních opatření.

V etapě hodnocení rizik přiřadí Dodavatel každému aktivu relevantní hrozby. Hrozba je akce, která může být podniknuta proti jednotlivým aktivům systému nebo systému jako celku.

Zranitelnosti jsou bezpečnostně slabá místa spojená s aktivy informačních a komunikačních systémů. Tato slabá místa mohou být využita jednou nebo více hrozbami. Výsledkem využití zranitelnosti hrozbou je bezpečnostní incident, tj. narušení bezpečnosti aktiva a tím celého systému. To znamená, že incident narušující bezpečnost aktiva může vzniknout pouze za předpokladu existence zranitelnosti a hrozby, která tuto zranitelnost využije.

Riziko je kombinace hrozby a zranitelnosti. Cílem hodnocení rizika je stanovení míry rizika. Míra rizika vyjadřuje jeho závažnost. Míra rizika se stanoví tak, že se zjistí priorita rizika výpočtem z hodnoty aktiva, úrovně hrozby a úrovně zranitelnosti. Čím vyšší priorita rizika, tím vyšší míra rizika.

Výsledkem etapy hodnocení rizik bude seznam rizik a hodnocení míry každého rizika. Hodnocení každého rizika vyjadřuje míru rizika, pokud budou realizována všechna navržená opatření.

Výsledkem hodnocení rizik může být zjištění, že některá rizika vykazují příliš vysokou míru rizika i při navržených opatřeních. Pokud taková situace nastane, rozhodne Dodavatel o způsobu zvládnutí rizika.

4.3.4. Zvládání rizik

Existuje několik metod pro zvládnutí rizika existujícího i po realizaci navržených opatřeni. Tato rizika se nazývají zbytková rizika. Následuje seznam metod pro zvládání rizik.

- Snížení rizika výběrem takových opatření (dosud nerealizovaných a nenavržených), aby mohlo být riziko přehodnoceno jako akceptovatelné nebo dočasně akceptovatelné.
- Vědomé přijetí (akceptace) rizika se může použít v případě, že se nejedná o vysoké riziko a není vážně ohrožena bezpečnost informačních aktiv a jsou splněny požadavky zadavatele na bezpečnost informací.
- Přenos rizika lze použít v případě, že je obtížné snížit riziko na přijatelnou úroveň vlastními zdroji. Možnými metodami je pojištění nebo outsourcing.
- Vyhnutí se riziku znamená jakoukoli akci, při které jsou podmínky provozu informačního nebo komunikačního systému změněny tak, abychom se vyhnuli výskytu rizika.

Dodavatel preferuje první metodu zvládání rizik, tj. realizaci opatření na eliminaci nebo aspoň snížení rizika. Ostatní metody použije ve výjimečných případech a za předpokladu, že nebudou znamenat porušení požadavků zadavatele na bezpečnost CMS 2.0 a legislativnívh požadavků na bezpečnost CMS 2.0.

4.4. Návrh bezpečnostních opatření

Bezpečnostní opatření jsou ekonomicky přiměřená a technicky dostupná opatření, která mohou mít následující formy:

- bezpečnostní standardy v bezpečnostní politice CMS 2.0,
- pracovní postupy používané při správě a užívání CMS 2.0,
- technická opatření,
- personální opatření,
- organizační opatření.

Cílem opatření je zajistit přiměřenou bezpečnost CMS 2.0 v následujících oblastech.

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

- Fyzická bezpečnost. Tato opatření zajišťují bezpečné umístění technických prostředků CMS 2.0 a omezení fyzického přístupu k zařízením CMS 2.0. Dodavatel realizuje za součinnosti Zadavatele s ohledem na poskytnutá datová centra.
- Bezpečnost prostředí. Tato opatření zajišťují bezpečné podmínky pro provoz technických zařízení CMS 2.0 včetně klimatizace a dostatečných montážních prostor a pravidla pro bezpečnou údržbu.
- Kybernetická bezpečnost. Tato opatření zajišťují bezpečnost dat v digitální formě při jejich zpracování, ukládání a přenosech včetně ochrany proti malware a hackerským útokům.
- Personální bezpečnost. Tato opatření zajišťují bezpečnost činnosti osob při provozu CMS 2.0. Zahrnuje definice postupů pro různé činnosti, obsazování bezpečnostních rolí důvěryhodnými osobami, povinnosti zachovávat mlčenlivost a bezpečnostní vzdělávání.
- Organizační bezpečnost. Tato opatření zajišťují jasnou definici kompetencí, práv a odpovědností.

Součástí návrhu řešení CMS 2.0 popsaného v tomto dokumentu je řada bezpečnostních opatření. Během výběru dalších opatření v technickém projektu bude důležité zvážit náklady na zavedení a provozování opatření ve vztahu k hodnotě chráněných aktiv. Bude zapotřebí identifikovat taková opatření, která splní požadavky na snížení míry rizika a budou při tom realizovatelná z hlediska existujících omezení, především finančních, časových a technických.

Pro kontrolu úplnosti navrhovaných bezpečnostních opatření použije Dodavatel seznamy opatření definované v normách ČSN ISO/IEC 27001:2006 a NIST 800-53. Vyloučena budou pouze opatření, která nemají pro CMS 2.0 smysl. Návrhy opatření uvedené v normách jsou obecné. Např. „zavést restrikce na použití software", nebo „posílení / vynucování přístupu". Proto dodavatel opatření konkretizuje pro podmínky CMS 2.0.

Skupiny opatření ČSN ISO/IEC 27001.

- Politika bezpečnosti.
- Organizace bezpečnosti informací.
- Řízení aktiv.
- Bezpečnost lidských zdrojů.
- Fyzická bezpečnost a bezpečnost prostředí.

- Řízení komunikací a provozu.
- Řízení přístupu.
- Získávání, vývoj a údržba informačních systémů.
- Zvládání bezpečnostních incidentů.
- Řízení kontinuity činností.
- Soulad s požadavky.

Skupiny opatření NIST 800–53.

- Řízení přístupu.
- Bezpečnostní informovanost a trénink.
- Audit a odpovědnost.
- Hodnocení bezpečnosti a autorizace.
- Správa konfigurací.
- Plánování kontinuity.
- Identifikace a autentizace.
- Zvládání incidentů.
- Údržba.
- Ochrana médií
- Fyzická ochrana a ochrana prostředí.
- Plánování.
- Personální bezpečnost.
- Hodnocení rizik.
- Získávání systémů a služeb.

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

- Ochrana systému a komunikací.
- Integrita systémů a informací.

4.4.1. Opatření pro zajištění fyzické bezpečnosti

Opatření na zajištění fyzické bezpečnosti zařízení CMS 2.0 tvoří základ bezpečnostních opatření. Pokud totiž útočník získá fyzický přístup k některým zařízením, stanou se bezpečnostní opatření proti určitým typům útoků neúčinná. Proto věnuje Dodavatel opatřením fyzické bezpečnosti velkou pozornost. Datová centra CMS 2.0, která v rámci součinnosti dodá Zadavatel, musí splňovat následující podmínky:

- DC s uzly CMS 2.0 budou v budovách s kontrolou vstupujících osob.
- DC a prostory s uzly CMS 2.0 budou vybaveny požární signalizací a protipožárními opatřeními.
- DC budou umístěna a vybavena tak, aby byla chráněna proti živelným katastrofám (záplavy, vítr, sníh, blesk, případně zemětřesení) a průmyslovým vlivům.
- Prostory se zařízeními CMS 2.0 budou vybaveny detektory zaplavení vodou.
- Prostory se zařízeními CMS 2.0 budou vybaveny ochranou proti elektromagnetismu a statické elektřině (antistatická podlaha).
- Zařízení CMS 2.0 budou umístěna ve skříních, aby byla zabezpečena proti neoprávněnému přístupu a také proti mírným vibracím.
- Přístup do prostor, ve kterých budou umístěna zařízení CMS 2.0, bude vybaven kontrolou a evidencí osob, které žádají o vstup.
- Ostraha DC bude mít povolen přístup do prostor se zařízeními uzlu CMS 2.0 pouze v případě mimořádných událostí a každý vstup ostrahy bude zaprotokolován.
- Datové rozvody budou až na výjimky ve vlastnictví a správě provozovatele. Výjimky budou uvedeny u jednotlivých služeb poskytovaných CMS 2.0.
- Část zařízení pro provoz CMS 2.0 bude umístěna mimo uzly CMS 2.0. Jde o Krajský konektor CMS 2.0 a případně jiná zařízení potřebná k zajištění služeb CMS 2.0. Dodavatel bude schvalovat umístění těchto zařízení u příslušného provozovatele, např. u provozovatele Krajského DC.

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

- Pracovní stanice, tiskárny a kopírky určené k zajištění provozu CMS 2.0 budou umístěny v prostředí, kde je kontrolován pohyb cizích osob.

4.4.2. Opatření pro zajištění bezpečného provozního prostředí

Běžná zařízení výpočetní techniky potřebují ke své činnosti přiměřené provozní podmínky, zejména určitou teplotu a vlhkost a omezenou prašnost. Pro spolehlivé fungování zařízení je důležité takové prostředí zajistit. Dále tato zařízení potřebují zásobování elektřinou a to opět v určité kvalitě. Kolísání proudu a napětí ovlivňuje negativně nejen životnost zařízení výpočetní techniky ale i jejich funkce. Správné funkce a prodloužení životnosti zařízení lze také zajistit pravidelnou údržbou podle pokynů výrobce.

Dodavatel proto věnuje provozním podmínkám zařízení přiměřenou pozornost a pro umístění zařízení bude požadovat splnění zejména následujících opatření.

- Fyzická zařízení uzlů CMS 2.0 umístit v prostorách, které splňují požadavky instalovaných zařízení na provozní podmínky (teplota, vlhkost, prašnost). Bude zajištěno instalací klimatizačních jednotek včetně zvlhčovačů vzduchu a filtrů prachu dostatečné kapacity a vysoké dostupnosti.
- Zajistit bezpečný přístup k jednotlivým zařízením uzlů CMS 2.0 a zajistit dostatečné servisní prostory kolem nich.
- DC s uzly CMS 2.0 vybavit elektrickými silovými rozvody dostatečné kapacity a kvality.
- Elektrické kabely vést chráněným způsobem.
- Zajistit kvalitu proudu a ochranu před kolísáním napětí.
- Zajistit bezpečné zásobování všech zařízení CMS 2.0 elektřinou.
- Vybavit DC centrálním záložním zdrojem, respektive centrálními záložními zdroji elektrické energie.
- Ve vybraných klíčových zařízeních zajistit dva napájecí zdroje.
- Všechna zařízení uzlů CMS 2.0 provozovat a udržovat v souladu s doporučením výrobce, respektive dodavatele. Veškeré servisní a opravárenské zásahy budou provádět pouze oprávněné osoby s potřebnou kvalifikací. Veškeré opravy a servisní zásahy budou prováděny pouze se souhlasem provozovatele a za dozoru jeho zástupce nebo jím pověřené osoby.

- Bude zajištěno bezpečné vymazání obsahu paměťových médií v případě jejich likvidace a v případě jejich použití pro jiný účel než pro CMS 2.0.

4.4.3. Personální zajištění a bezpečnost

Důležitým prvkem pro zajištění bezpečného provozu CMS 2.0 bude dostatek kvalifikovaného a důvěryhodného personálu. Existují osoby, které budou mít fyzický přístup k zařízením CMS 2.0, a osoby, které budou mít privilegovaný (ve smyslu vysokých oprávnění) logický přístup k zařízením CMS 2.0.

Dodavatel si je jako budoucí provozovatel CMS 2.0 vědom rizik spojených s fyzickým přístupem a logickým privilegovaným přístupem osob k zařízením CMS 2.0 a věnuje proto pozornost výběru osob na příslušné pozice. Nábor pracovníků se řídí interními pravidly dodavatele. Na všech pozicích je požadován čistý trestní rejstřík a na výše uvedené pozice je požadována odpovídající kvalifikace, provádí se kontrola životopisu a zjišťují reference. S pracovníky bude uzavírána dohoda o mlčenlivosti.

Pracovníci, kteří se budou podílet na zajištění provozu CMS 2.0, budou mít odpovídající vzdělání a praxi. Dodavatel bude organizovat interní školení zaměstnanců v informační bezpečnosti a podle potřeby vysílat pracovníky na školení a kursy.

Dodavatel definuje bezpečnostní role potřebné pro provoz a správu CMS 2.0 a zajistí jejich obsazení kvalifikovanými a důvěryhodnými osobami. Při definici rolí bude důsledně vycházet z oddělení řídících a výkonných rolí. Role se budou lišit náplní práce a oprávněními. Každé roli budou přidělena pouze minimální nezbytná práva pro výkon role.

4.4.4. Patch management

Instalace aktualizací použitého software je prostředek ke snížení zranitelnosti software. Cílem aplikace opravných balíčků bezpečnostní kategorie je odstranit ze software známé zranitelnosti. Aplikace oprav kategorie bezpečnostní je tedy nezbytností. Na druhé straně každý zásah do software s sebou nese riziko zavlečení nové chyby, nebo riziko nekompatibility s nějakým software, který je na záplatovaném systému nainstalovaný.

Proto dodavatel v roli provozovatele CMS 2.0 nebude žádné aktualizace instalovat na serverech a zařízeních automaticky, ale půjde vždy o manuální a kontrolovaný zásah. Před instalací každého opravného balíčku do provozního prostředí bude provedeno otestování funkčnosti příslušného zařízení po instalaci balíčku v testovacím prostředí, pokud v testovacím prostředí bude k dispozici odpovídající zařízení. Rozsah testování bude záviset na konkrétním zařízení a technických možnostech otestování příslušné funkcionality.

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

Aplikace opravných balíčků na provozní zařízení bude probíhat v časech s nejnižší úrovní provozu. K dispozici bude vždy postup, jak vyřešit případnou nefunkčnost zařízení, na které byl balíček aplikován. Pro řešení problémových stavů budeme používat některý z následujících postupů, nebo jejich kombinace.

- Návrat k předcházející verzi software (tj. odstranění balíčku).
- Aktivace jiného zařízení jako náhrady.
- Omezení funkcionality zařízení, pokud se omezení nevztahuje na kritické funkce zařízení.

Při aplikaci opravných balíčků bude dodavatel dodržovat několik zásad s výjimkou situací, kdy nutnost aplikace balíčků bude kritická, např. kvůli vysokému ohrožení CMS 2.0 existující zranitelností:.

- Uzly CMS 2.0 budou umístěny ve dvou různých lokalitách. Dodavatel bude balíčky aplikovat postupně na skupiny zařízení po lokalitách, nejprve jedna lokalita a s časovým odstupem stejná zařízení ve druhé lokalitě. Odstup bude zvolen podle typu zařízení, typu opravy a míře ohrožení existující zranitelnosti.
- Většina zařízení v každém uzlu je zdvojena. Dodavatel bude balíčky aplikovat postupně vždy nejprve na jedno a potom na druhé zařízení, pokud bude tento postup technicky možný. Odstup bude zvolen podle typu zařízení, typu opravy a míře ohrožení existující zranitelnosti.
- Dodavatel bude najednou aplikovat omezenou množinu oprav, aby usnadnil analýzu případných problémů.

4.4.5. Antivirová ochrana

Antivirová ochrana bude primárně zajištěna na všech rozhraních CMS 2.0 inspekcí provozu na firewallech.

Na základě výsledků hodnocení rizik rozhodne dodavatel, zda je potřebné nasadit antivir na další systémy, konkrétně na servery poskytující infrastrukturní a aplikační (mj. MTA a eGON Service Bus) služby. Pokud se nasazení antiviru na tyto systémy ukáže jako potřebné, navrhuje dodavatel nasazení antiviru na úrovni hostitelského systému virtualizační platformy.

Navrhujeme systémy poskytující služby provozovat jako virtuální servery, pokud je to možné, a antivir implementovat takovým způsobem, aby kontroloval výskyt malware v adresovém prostoru virtuálního serveru. Znamená to, že není nutné instalovat antivir do každého systému a zajišťovat jeho aktualizace na více místech a starat se o kompatibilitu antiviru se systémovým software a všemi použitými aplikacemi.

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

V systémové bezpečnostní politice budou definovány standardy pro zabezpečení pracovních stanic, které smí být použité pro správu CMS 2.0. Pro stanice určené pro správu CMS 2.0 bude antivirová ochrana povinná.

4.4.6. Oddělení CMS 2.0 od jiných počítačových sítí

CMS 2.0 zprostředkovává komunikaci mezi informačními systémy různých subjektů umístěných v různých počítačových sítích. Díky připojení CMS 2.0 do Internetu nejde nutně pouze o komunikaci mezi informačními systémy subjektů státní správy.

Z hlediska informační bezpečnosti jde o sítě s různou úrovní zabezpečení. Z hlediska zabezpečení považuje Dodavatel CMS 2.0 za nejvíce zabezpečenou síť a ostatní sítě za různě ale méně zabezpečené. Dodavatel připouští výjimečnou možnost, že dojde k narušení bezpečnosti samotného CMS 2.0 a vybuduje proto bezpečné oddělení CMS 2.0 od externích sítí částečně symetricky. Proto Dodavatel navrhuje bezpečné oddělení všech uvedených sítí od CMS 2.0 tak, aby byla zajištěna bezpečnost CMS 2.0 před hrozbami z uvedených sítí a opačně bezpečnost uvedených sítí před hrozbami z CMS 2.0.

Oddělení CMS 2.0 od jiných počítačových sítí bude realizováno dvoustupňově.

- Na hranici CMS 2.0. Primárním cílem zabezpečení na hranici CMS 2.0 je zachytit útoky vedené z externí sítě proti CMS 2.0 a naopak z CMS 2.0 proti jiné síti, nebo aspoň významnou část těchto útoků.
- Centrálně. Primárním cílem centrálního zabezpečení je řízení a omezení komunikace mezi systémy umístěnými v různých externích sítích tak, aby byla povolená komunikace pouze podle definovaných pravidel.

Komunikace mezi systémy připojenými do CMS 2.0 bude (téměř) vždy probíhat přes CBM, který bude spojení povolovat, respektive zakazovat na základě zadaných pravidel. Speciálně nebude povolena přímá komunikace mezi systémy připojené přes různé připojovací moduly. Budou existovat výjimky, které jsou částečně popsány v tomto dokumentu (komunikace v rámci jedné VPN, přímý Internet) a budou přesně specifikovány v technickém projektu.

Dodavatel vybaví všechna komunikační rozhraní s externími sítěmi firewally s funkcí inspekce provozu (IDS/IPS). Externí sítí se v tomto kontextu míní i Management síť.

Zařízení IPS/IDS jsou určena k detekci / blokování určitých typů útoků a jsou zaměřena jak na detekci / blokování často zneužívaných protokolů a aplikací, tak (některé z nich) na ochranu proti novým

dosud neznámým útokům, tzv. zero day útokům. IDS / IPS většinou kombinují několik různých metod detekce útoků.

- Známé vzory (signatury).
- Detekce anomálií síťového provozu a odchylek od standardního chování.
- Detekce odchylek od definic použitých síťových protokolů.

IDS reagují na ohrožení bezpečnosti záznamem události a oznámením obsluze. IPS škodlivý provoz navíc v reálném čase blokují. Pro oddělení CMS 2.0 od ostatních sítí Dodavatel použije síťová IDS/IPS. To jsou systémy, které analyzují síťový provoz v určitém bodě počítačové sítě nebo v určité části sítě, případně v celé síti.

Existují také lokální IDS/IPS, které se používají na jednotlivých zařízeních. Tento typ IDS/IPS je buď určen ke kontrole síťového provozu určeného pro jedno zařízení, nebo ke kontrole útoků proti zařízení. V řadě případů představuje lokální IDS/IPS jedinou možnost, jak zjistit úspěšné napadení zařízení. Realizuje se kontrolováním změn software a vybraných souborů. Jejich možné využití bude specifikováno v technickém projektu.

Rizikem nasazení IPS jsou tzv. false positives, tj. blokování zdánlivě škodlivého provozu, který je ve skutečnosti legitimní. Proto Dodavatel věnuje velkou péči nastavení blokovacích pravidel, aby k tomuto jevu nedocházelo. Před nasazením blokujících pravidel prověříme jejich účinky na provoz.

Firewally budou splňovat následující požadavky.

- Budou zabraňovat útokům typu odepření služby (DOS, DDOS).
- Umožní detekci / blokování útoků vedených na L3 a L4 OSI modelu. Jde o detekci, respektive blokování paketů s takovými kombinacemi dat v hlavičkách L3 a L4, které neodpovídají standardům a představují možné ohrožení.
- Umožní blokování neznámých protokolů a protokolů, které nejsou založeny na IPv4 nebo IPv6.
- Umožní detekci / blokování některých typů aplikací (Peer to Peer, online hry apod.).
- Umožní bypass, tj. použití náhradní cesty v případě výpadku zařízení.

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

K řízení a filtrování provozu mezi jednotlivými sítěmi je určen centrální bezpečnostní modul. Jeho primárním úkolem bude povolit komunikaci pouze mezi určitými VPN, respektive IP adresami s použitím pouze definovaných protokolů.

4.4.7. Zabezpečení aplikačních služeb CMS 2.0

CMS 2.0 bude poskytovat řadu standardních síťových služeb klientským systémům připojeným do CMS 2.0. Jedná se zejména o standardní infrastrukturní služby typu přesného času (NTP) a jmenných služeb (DNS).

Tyto služby jsou často z hlediska klientů (uživatelů) jednoduchou samozřejmostí, nicméně na většině z nich závisí správné fungování ostatních služeb. A jejich vyřazení může mít za důsledek nedostupnost jiných služeb a jejich neoprávněná modifikace může ohrozit další aspekty bezpečnosti informací - integritu a důvěrnost.

Proto budou tyto služby provozovány na zabezpečených serverech a bezpečným způsobem.

- Logický i fyzický přístup k serverům bude omezen.
- Pro každou službu bude vyhrazen jiný server.
- Na serveru nebudou spouštěny jiné služby.
- Software poskytující služby bude nakonfigurován tak, aby poskytoval minimum informací o své konfiguraci a použitém software.
- Služby budou provozovány s minimálními systémovými právy.
- Budou odstraněny standardní komponenty dodávaného software (zejména různé příklady), pokud nejsou přímo potřebné pro poskytování služby.
- Přístup ke službám bude logován a logy budou vyhodnocovány.
- Podle technologických možností uvážíme nasazení lokálních IDS, které budou detekovat neoprávněné změny obsahu důležitých systémových komponent a konfiguračních souborů.
- Budou změněna implicitní přihlašovací hesla.

Pro jednotlivé sdílené služby realizuje Dodavatel navíc specifická bezpečnostní opatření.

4.5. Bezpečnostní monitoring

Dodavatel vybuduje komplexní bezpečnostní platformu zajišťující sběr a archivaci logů z jednotlivých komponent CMS 2.0.

Platforma bude obsahovat analytickou část pro interpretaci událostí a jiných informací v uživatelském, aplikačním a síťovém kontextu. Bude umožňovat sběr událostí ze všech prvků a úrovní CMS 2.0. To znamená ze síťových zařízení, firewallů i aplikačních serverů. A úrovněmi se myslí hardwarová vrstva, síťová a aplikační vrstva.

Řešení bude podporovat vytváření korelačních pravidel pro detekci událostí složených z jiných událostí. Korelační pravidla budou připravena a bude je možno nahradit nebo doplnit vlastními pravidly.

Bude podporována schopnost dynamického učení nových síťových a aplikačních vzorů chování. Systém tak bude schopen rozpoznat aktivitu neznámých služeb, nestandardně pracující služby, úroveň využití služby v kontextu denní doby a konkrétního uživatele, aktivitu i dosud neznámého malware apod.

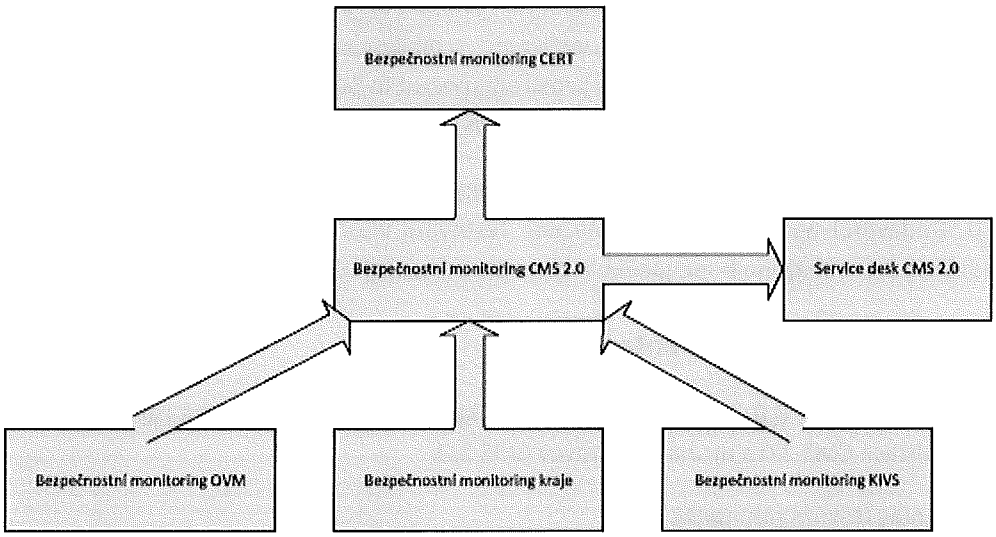
Řešení bude možno nasadit jak ve fyzickém tak také ve virtuálním prostředí.

Požadované základní funkce.

- Sběr a archivace logů a bezpečnostních událostí ze všech komponent CMS2.
- Analýza informací získaných v každém kontextu.
- Kontinuální kontrola shody s regulacemi a predikce vzniku hrozeb v závislosti na zranitelnostech, konfiguračních chybách a dalších faktorech.
- Provoz v režimu vysoké dostupnosti.
- Možnost vyhodnocování údajů o provozu CMS 2.0 od všech komponent. To znamená, že bude možné přijímat a zpracovávat data v těch formátech, ve kterých je produkují jednotlivé systémy a zařízení CMS 2.0. Současně bude podporovat sběr dat pomocí standardních protokolů, které se pro tento účel používají (zejména syslog, SNMP a WMI).
- Hlášení o výskytu bezpečnostních událostí v reálném čase. Při výskytu definovaných událostí bude informován příslušný administrátor alertem. Bude podporována možnost předávat alerty různými způsoby, např. pomocí mailu nebo SMS. Dále bude podporováno předávání alertů na Service Desk.

- Vyhodnocování bezpečnostních událostí a sledování zvolených metrik z oblasti informační bezpečnosti za zvolené období.
- Vytváření standardních a příležitostných reportů.
- Schopnost přijímat zpracovávat velké objemy dat v reálném čase bez degradace výkonu a prodlužování doby odezvy.

Řešení bude navrženo jako integrovatelné horizontálně i vertikálně. Horizontálně půjde o integraci se Servis Deskem. Vertikálně bude bezpečnostní monitoring CMS 2.0 schopen přijímat události od bezpečnostních systémů subjektů CMS 2.0 a bude schopen předávat vybrané události CMS 2.0 do nadřazených monitorovacích systémů.



Obrázek 27 - Bezpečnostní monitoring CMS 2.0

4.6. Testování bezpečnosti

Testování bezpečnosti CMS 2.0 tvoří zvláštní kategorii testů. Jejich cílem je v praxi ověřit účinnost realizovaných bezpečnostních opatření. Bezpečnostní testy CMS 2.0 dodavatel navrhne v produkčním prostředí provádět pouze před uvedením do provozu. Do té doby bude nutné provést bezpečnostní testy vybraných skupin bezpečnostních opatření.

Dodavatel vypracuje v technickém projektu scénáře, které budou zahrnovat základní aktivity používané při penetračních testech:

- Získávání informací o CMS 2.0 z pohledu různých útočníků (Internet, KIVS, interní CMS 2.0, DC, DCK): skenování portů, informace o použitém software.
- Pokusy o neoprávněný přístup ke komponentám a datům CMS 2.0.
- Pokusy o ovládnutí komponent CMS 2.0.
- Falšování identity.
- Pokusy o zahlazení stop.

Po uvedení CMS 2.0 do provozu budou obdobné testy prováděny pouze ve vývojovém a testovacím prostředí. Příslušná opatření, která vyplynou z opakovaných testů, dodavatel, respektive provozovatel CMS 2.0, ověří v testovacím prostředí (pokud to bude technicky možné) a teprve potom je standardním postupem aplikujeme i v produkčním prostředí.

Součástí Provozního řádu CMS 2.0 budou podmínky pro provádění bezpečnostních testů uživateli CMS 2.0. Dodavatel navrhne povolit omezené testování vlastních systémů uživatelů v testovacím prostředí CMS 2.0. Zakázáno bude jakékoli testování infrastruktury CMS 2.0 uživateli.

4.7. Bezpečnostní dokumentace

Součástí dodávky CMS 2.0 bude bezpečnostní dokumentace. Část dokumentů je určena pro fázi návrhu a realizace CMS 2.0 a druhá pro provoz CMS 2.0.

Do první skupiny dokumentů patří:

- analýza požadavků na CMS 2.0,
- analýza rizik CMS 2.0.

Do druhé skupiny dokumentů patří:

- Havarijní plány pro případ výpadku jednotlivých komponent CMS 2.0. Tyto plány budou rovněž popisovat, jak je zajištěna kontinuita činností CMS 2.0 v případě příslušného výpadku.
- Krizové plány pro případ výskytu mimořádných událostí. Jde o plány pro velké a silné útoky na komunikační infrastrukturu státní správy, pro rozsáhlé přírodní nebo jiné katastrofy.

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

- Plán bezpečnosti bude obsahovat návrhy na další rozvoj CMS 2.0 v oblasti bezpečnosti. Bude průběžně aktualizován, aby zohledňoval aktuální stav v oblasti informační bezpečnosti CMS 2.0.
- Systémová bezpečnostní politika CMS 2.0 bude definovat bezpečnostní standardy závazné pro CMS2.
- Postupy pro vyšetřování bezpečnostních událostí a bezpečnostních incidentů.
- Směrnice pro činnost osob zastávajících bezpečnostní role při zajištění provozu a správy CMS2.
- Informace pro uživatele CMS 2.0 o zabezpečení jednotlivých služeb CMS 2.0. Pro uživatele je to základní informace, pro jaké účely mohou jednotlivé služby použít.

Bezpečnostní podmínky pro uživatele CMS 2.0. Tyto podmínky budou součástí provozního řádu CMS 2.0 a uživatelé je budou akceptovat při podpisu smlouvy o používání CMS 2.

5. Management a monitoring

Shrnutí kapitoly	Kapitola popisuje návrh provozního a výkonnostního monitoringu. Provozní monitoring je určen k předcházení problémových situací a výkonnostní k plnění SLA a sledování dostupnosti služeb a kvality poskytování služeb. Ve zbytku kapitoly je popsána správa CMS 2.0. Ta bude prováděna s využitím oddělené, tzv. OOB sítě.
Vazba kapitoly na Výzvu Zadavatele	Požadavky na management a monitoring jsou uvedeny v kapitole 7 Přílohy 1 Výzvy Zadavatele.

5.1. Monitoring CMS 2.0

Součástí dodaného řešení bude systém monitorování CMS 2.0 a jeho komponent. Cílem je zajistit plynulý a bezpečný provoz CMS 2.0. Prostředkem k dosažení tohoto cíle je nasazení technických prostředků a nastavení procesů na straně provozovatele CMS 2.0.

Z hlediska zaměření na určitou oblast bude monitoring CMS 2.0 rozdělen na následující skupiny:

- provozní dohled;
- sledování výkonnosti a dostupnosti;
- bezpečnostní dohled. Je popsán v kapitole o bezpečnosti CMS 2.0.

5.1.1. Provozní dohled

Hlavním cílem provozního dohledu je zajistit bezchybné a efektivní fungování CMS 2.0 a jeho vysokou dostupnost včasnou detekcí možných chybových stavů a přetížení komponent CMS 2.0. Dosahuje toho sledováním stavu jednotlivých prvků a sledováním síťového provozu. Technickým prostředkem bude sledování a vyhodnocování záznamů o provozu (logů) jednotlivých komponent a záznamů o síťovém provozu (NetFlow).

Hlavní sledované metriky budou:

- zatížení procesorů;
- obsazení vnější a vnitřní paměti zařízení;
- využití kapacity komunikačních portů zařízení;
- výskyt chyb na zařízení (chyby paměti, procesorů, disků a dalších součástek);

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

- teplota zařízení, zejména procesoru;
- zastavení služeb;
- zatížení sítě;
- chyby při přenosech;
- překročení kapacity linky, respektive komunikačního kanálu.

Většina síťových zařízení a serverů je schopna poskytovat zprávy o své činnosti a posílat je na zadanou adresu v určitém standardním formátu. Nejpoužívanějším formátem a současně protokolem je syslog. Dalším standardním způsobem je poskytovat informace o svém stavu na dotaz. Nejpoužívanějším způsobem jsou SNMP a WMI. A konečně řada zařízení umožňuje generovat při dosažení určitých hodnot definovaných metrik zprávu a zaslat ji na zadanou adresu. Nejpoužívanějším způsobem je SNMP trap.

Provozní dohled umožní zpracovávat informace ze všech uvedených zdrojů. Dodavatel předpokládá nasazení systému, který umožní sběr potřebných informací ze všech komponent CMS 2.0, jejich normalizaci do standardního formátu a centralizované uložení. Nad daty bude možno provádět minimálně následující operace:

- zjištění okamžitého stavu jednotlivých zařízení, sítí a CMS 2.0 a jako celku;
- vyhodnocování stavu za zvolené období včetně zjišťování trendů.

Pro sledování provozu a anomálii v síti CMS bude nasazen NetFlow kolektor. NetFlow kolektor bude sbírat data z NetFlow sond nebo zařízení podporujících odesílání NetFlow dat. Jako výstup NetFlow kolektoru budou poskytovány reporty o datových tocích v CMS 2.0. NetFlow kolektor též umožní detailnější filtraci Flow záznamů pro identifikaci a analýzu, jak který protokol nebo služba vytěžuje síť CMS 2.0.

5.1.2. Sledování výkonnosti a dostupnosti

Cílem tohoto typu monitoringu je kontrola plnění SLA a včasné upozornění na výpadek služeb CMS 2.0.

Pro většinu služeb CMS 2.0 je ve Výzvě Zadavatele uveden požadavek na dostupnost ve formě procent času, kdy musí být služba během určitého časového intervalu dostupná. Pro sledování plnění této SLA metriky bude nasazen systém sledování dostupnosti služeb CMS 2.0, u kterých je tato

metrika uvedena a u služeb, u kterých sice není uvedena, ale je měřitelná (přístupy z Internetu nebo Extranet).

Monitoring SLA budou provádět sondy umístěné tak, aby jejich měření dávala relevantní výsledky. Tyto sondy budou provádět v pravidelných intervalech pokusy o přístup k měřené službě a výsledky budou zasílat do centrálního vyhodnocovacího systému. Tím bude buď provozní, nebo bezpečnostní dohled. Ten bude záznamy ukládat a vyhodnocovat. V případě nedostupnosti nějaké služby systém vygeneruje alert, který upozorní operátora.

Sondy budou umístěny tak, aby usnadňovaly hledání příčin výpadku. Bude tedy sledována dostupnost jednotlivých služeb CMS 2.0, ale i dostupnost komponent, ze kterých se služba může skládat, např. dostupnost KIVS přípojek operátorů, dostupnost eGON Service Bus atd.

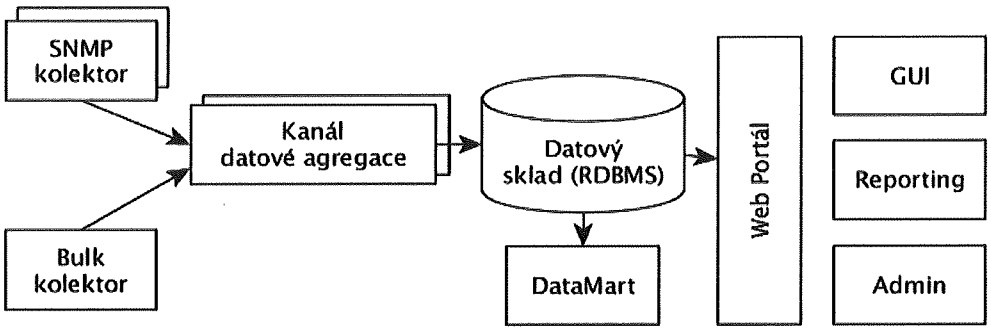
Mimo doby dostupnosti služeb budou sledovány, zaznamenávány a vyhodnocovány i časy potřebné k vyřízení požadavků na služby s využitím dedikované HW komponenty provozované v místě odběru služeb. Ze získaných dat bude prováděno vyhodnocení kvality služeb poskytovaných CMS 2.0.

Celý systém sledování výkonnosti a dostupnosti CMS 2.0 bude navržen jako konsolidační platforma, která bude podporovat komplexní heterogenní síťové struktury obsahující prvky různých dodavatelů a na rozličných technologických platformách. Systém bude sloužit ke sledování dostupnosti, spolehlivosti a efektivity využití síťových zařízení, protokolů a služeb. Zároveň bude vybaven datově-analytickými funkcemi pro statistické vyhodnocování trendů v různých časových horizontech (minuty, hodiny, dny, týdny, měsíce, roky) včetně notifikace stavu formou oznamovaných událostí při překročení stanovených prahových podmínek.

Systém bude dodáván s hotovou podporou co největšího počtu síťových technologií formou aplikační knihovny, která bude ve správě dodavatele a bude podléhat standardním podmínkám technické podpory a údržby. Tato knihovna bude obsahovat příslušné KPI parametry (typicky definované pomocí SNMP MIB) pro danou technologii a výrobce včetně agregačních formulí a předkonfigurovaných reportů, a to s maximálním možným použitím tzv. industry best-practices.

Architektura systému bude modulární, a to z důvodu rozšiřitelnosti, vysoké dostupnosti a škálovatelnosti. Doporučené blokové schéma je znázorněno na obrázku:

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.



Obrázek 28 - Schéma implementace performance managementu CMS 2.0

Sběr dat ze sítě bude probíhat pomocí distribuovaných datových kolektorů. Základní typové rozdělení kolektorů je:

- **SNMP kolektor** – sběr dat přes SNMP rozhraní
- **Bulk kolektor** – generický import datových souborů z ostatních zdrojů a rozhraní (např. XML nebo CSV)

Datová agregace (časová, sdružování zdrojů do skupin, pod.) pro definované KPI metriky bude probíhat průběžně (on-line) a společně s detekcí prahových hodnot v reálném čase. Překročení limitů bude indikováno do návazného Event management systému pomocí SNMP událostí. Základní požadované typy prahových situací jsou následující:

- **burst** – aktivuje se na základě délky časového úseku po sobě jdoucích překročení prahových hodnot
- **period** – tento typ je založen na konceptu celkové akumulované doby, po kterou je prahová hodnota překročena. Tato hodnota inkrementálně narůstá až do konce sledované SLA periody
- **risk** – proaktivní situace, při které jsou detekovány prvky s rizikem budoucího překročení prahových hodnot
- **baseline** – tento typ porovnává aktuální hodnoty s průběhem vypočteným z historických dat na základě standardní odchylky

Součástí základního systému bude i centrální administrační GUI pro konfiguraci jednotlivých modulů a jejich parametrů. Zde bude mimo jiné umožněno editovat jednotlivé sledované prvky (přidat, smazat, importovat, exportovat atd.), bude poskytován grafický náhled na sbíraná data, poskytován

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

informace o nastavení datových kolektorů, sledování stavu celého systému, podrobný přehled o využití databáze a datových struktur.

Předpokladem a zároveň požadavkem je využití jednotného webového uživatelského prostředí (GUI), které bude společné pro všechny ostatní integrované management systémy (Event management, network management, Application performance management). Toto uživatelské prostředí bude formou webového portálu zajišťovat kontextovou provázanost jednotlivých modulů a současně poskytne jednotnou správu uživatelských skupin a nastavení uživatelských profilů včetně rozvržení obrazovky a obsahu. Dále bude zajištěna plná podpora LDAP a Single-Sign On.

Zabudovaný reportingový nástroj bude umožňovat návrh a úpravu reportů podle vlastních potřeb (např. změna tabulek, loga, obrázku, atd.) a publikaci reportů v různých formátech (pdf, xls, csv, html). Editace reportů bude probíhat pomocí uživatelsky komfortního prostředí (drag-and-drop). Nástroj bude obsahovat standardní předvytvořené reporty.

5.2. Správa CMS 2.0

Ke správě CMS 2.0 bude přednostně používána management síť oddělená od provozních sítí. Popis této sítě je uveden v kapitole 2.5 Modul Management. Management síť bude využívána jednak provozovatelem CMS 2.0 a za druhé správci systémů připojených do CMS 2.0.

5.2.1. VPN koncentrátory

Pro vzdálený přístup administrátorů bude využit VPN koncentrátor modulu Remote Access. VPN koncentrátor proto bude podporovat vytváření různý autentizačních profilů, včetně přizpůsobení vzhledu přihlašovacích stránek. Propojení bude přímo z Firewallu Remote Access modulu do firewallu Management modulu.

Podrobný popis vlastností SSL a IPSec VPN viz Remote Access modul.

5.2.2. Firewall / IPS

Management modul bude samostatná Out-of-Band management síť, což bude oddělená síť určená pro správu všech aktivních prvků a serverů v CMS 2.0. Servery, které neumožňují Out-of-Band management, nebudou připojeny do modulu management. Pro bezpečnostní oddělení Management sítě bude použit firewall s IPS modulem. Firewally budou zapojeny v režimu vysoké dostupnosti.

Ze sítě CMS 2.0 do sítě Management bude přístup hlavně na AAA server pro ověřování uživatelů při přístupu ke službám a zdrojům sítě CMS. Ostatní komunikace bude ve většině případů interní v modulu Management.

5.2.3. AAA server

Součástí Management modulu bude AAA server pro ověřování uživatelů. Na AAA serveru se budou uchovávat účty správců sítě a jejich práva k jednotlivým aktivním prvkům. AAA server bude autentizovat správce sítě při přístupu k aktivním prvkům a ověřovat (autorizovat) příkazy zadávané správci.

AAA server bude nabízet Captive portál pro autentizaci uživatelů přistupujících k datům v síti CMS 2.0. Uživatel se bude moci ověřovat proti lokální databázi nebo nějaké uživatelské databázi. Proto je nutné, aby AAA server mohl ověřovat proti více a různým uživatelským databázím.

Na AAA serveru se budou ověřovat i uživatelé přistupující do sítě CMS 2.0 přes SSL a IPSec VPN koncentrátor.

Rozhraní AAA serveru musí být schopné komunikovat s aktivními prvky v síti a na základě autentizace uživatele přiřazovat uživatelské profily. Po úspěšném přihlášení uživatele jsou na bezpečnostní prvky v síti (firewall, IPS sonda) nasazena dynamická pravidla na tohoto uživatele. AAA server musí být schopen komunikovat s bezpečnostním dohledem tak, aby bezpečnostní incidenty mohly být přiřazeny konkrétnímu uživateli. V případě autentizace správce bude AAA server v návratových atributech též posílat uživatelská práva správce.

Captive portál se bude využívat především pro autentizaci uživatelů přistupujících ze sítě KIVS, kde za IPSec VPN může být více uživatelů s různými oprávněními. V případě pokusu o přístup do prostředí CMS 2.0 bude uživatel přesměrován na Webovou autentizační stránku, kde bude muset prokázat svou identitu. Na základě této autentizace bude uživateli povolen nebo odmítnut přístup k datům v CMS 2.0.

U AAA serveru je požadováno nasazení ve vysoce dostupném módu, a proto musí podporovat režim vysoké dostupnosti na více uzlech v režimu Active - StandBy, nebo v režimu Active - Active.

5.2.4. Terminálový server

Součástí management sítě bude konzolový server (terminálový server), který bude nabízet dostatečné množství sériových portů. Na sériové porty budou připojené konzolové porty aktivních prvků. To umožní vzdálený přístup na konzole aktivních prvků. Vzdálený přístup na konzolové porty umožní správcům sítě monitorovat stav aktivních prvků i v případě nedostupnosti aktivního prvku přes IP síť.

5.2.5. Dohledové centrum NOC

Služby správy a dohledu nad CMS 2.0 budou realizovány v NOC (Network Operations Center). NOC bude sledovat záznamy o provozu CMS 2.0, bude adresátem alertů o provozních událostech. Bezpečnostní události bude řešit SOC (viz dále).

Další požadavky bude NOC dostávat od Service desku.

NOC bude provádět kompletní administraci, logistiku a řízení incidentů počínaje nahlášením, přes předání technikovi, až po ukončení incidentu, včetně sledování SLA. Také se stará o průběžné informování o stavu průběhu incidentu všech zúčastněných stran a snaží se odhadnout ETTR (Expected Time to Repair). Je zde řešeno přímé řízení logistiky náhradních dílů, evidenci servisních dílů, aby nedocházelo ke zbytečným prodlevám při řešení incidentů.

5.2.6. Technická podpora (TAC)

První úroveň podpory řeší incidenty 24 hodin denně 365 dnů v roce. Povinností TAC bude udržování záznamů v elektronické provozní dokumentaci a dispečerské tabuli incidentů, která zároveň slouží i pro zpětný záznam incidentů. V případě, kdy TAC není schopen problém vyřešit v určeném časovém okamžiku, podstoupí problém certifikovanému specialistovi (ATAC).

5.2.7. Specialisti technologie (ATAC)

Druhá úroveň podpory Advanced Technical Assistance Center (ATAC) poskytuje další stupeň podpory při řešení problémů. ATAC přijímá incidenty od první úrovně podpory (TAC), kterému poskytuje servis a pokročilou intenzivní podporu řešení incidentů. ATAC primárně pracuje v pracovních dnech v době od 8:00 do 18:00. Mimo tuto dobu je zajištěn systém pohotovostí, který je vždy N+1, pro případ nenadálých událostí.

5.2.8. Security Operations Center (SOC)

Bezpečnost provozu CMS 2.0 bude zajišťovat skupina bezpečnostních správců, kteří budou v režimu 24x7 vyhodnocovat potenciální kyberhrozby a řešit bezpečnostní události. Administrátoři NOC vyhodnotí v případě bezpečnostních událostí, zda jde o bezpečnostní incident a pokud ano, předají ho k vyšetření bezpečnostnímu manažerovi CMS 2.0.

Úkolem SOC je mj. implementace doporučení vydaných vládním CERT a to na základně důkladné znalosti technologie a topologie provozovaných služeb. Jde také o programování a tvorbu signatur pro systémy IPS a následná implementace s oddělením NOC.

Dále bude SOC proaktivně vyhodnocovat potenciální rizika a upozorňovat na ně. Jde hlavně o detekci a analýzu anomálii a ohrožení. Základními pracovními nástroji SOC jsou analyzátory a korelátory logů

(SIEM), nástroje na vyhodnocení rizik (Risk Management), monitorovací nástroje toků (Flows) a nástroje na proaktivní bezpečnostní testování služeb poskytovaných v rámci eGovermentu. Část incidentů bude muset být reportována do národních, respektive vládních CERT pracovišť.

Úkolem bude i stanovování postupů, konfiguračních šablon a ověření shody všech zařízení CMS 2.0 se stanovenou bezpečnostní politikou. Jde hlavně o úzkou spolupráci s NOC, které se staré o konfiguraci infrastruktury až po koncové body KIVS.

Součástí práce SOC bude dále spolupráce a přijímání požadavků na analýzu a řešení požadavků od subjektů připojených do CMS 2.0. A to také ve spolupráci s operátory KIVS. SOC s nimi bude spolupracovat při vyhodnocování hrozeb, které jim hrozí a při vyjasňování jejich bezpečnostních událostí a vyšetřování jejich bezpečnostních incidentů. Jedním z úkolů SOC bude poskytnout subjektům využívajícím služby CMS 2.0 relevantní data, týkající se jejich bezpečnostních událostí a incidentů.

Důležité bude také publikování znalostní databáze a sdílení této databáze s dalšími subjekty a hlavně s národním, respektive vládním CERT. Znalostní databáze bude důležitým nástrojem jako pro vnitřní fungování SOC tak také pro OVM, které z ní budou čerpat a proaktivně nastavovat a zabezpečovat své systémy.

SOC bude ve spolupráci se subjekty a operátory KIVS potlačovat DoS a DDoS útoky. A to včetně pravomocí odpojení operátora, či subjektu KIVS, ze kterého by útok probíhal.

5.3. Service Desk

Chybové stavy v CMS 2.0 budou řešeny na úrovni sítě, hardware a software. Pro jejich správu bude použit centrální Service Desk.

Řešení pro Service Desk bude obsahovat též IT Asset Management a bude integrované v kombinaci procesů servisních požadavků, řešení chybových stavů, změn, uvolňování verzí, konfigurací, majetku, řízení smluvních a dodavatelských vztahů. Všechny tyto procesy budou sdílet jednotné procesní, datové, integrační a grafické prostředí.

Service Desk bude obsahovat mimo jiné CMDB (change management database), která bude naplněna záznamy o spravovaných zařízeních a službách, včetně jejich parametrů (SLA). Tímto způsobem bude též provedeno propojení s poskytovateli KIVS, respektive s jejich středisky podpory.

Chybové stavy, oznamované jako incidenty připojenými subjekty veřejné správy, budou hlášeny odpovědným pracovníkem příslušného subjektu na Service Desk CMS 2.0. Pokud incident nebude moci Service Desk CMS 2.0 vyřešit, nahlásí jej na Service Desk providera a zároveň ponechává

otevřený TT (trouble ticket) na své straně, který odkládá z důvodu předání řešení na providera. Provoz Service Desku bude v režimu 24x7.

Vlastnosti nabízeného řešení:

- unifikace Service Desku, změnových řízení a správy majetku
- správa licencí
- kompletní správa IT majetku
- grafické rozhraní, přizpůsobující se roli uživatele
- podpora mobilních zařízení

Service Desk bude mít grafické prostředí na bázi tenkého klienta s využitím webového prohlížeče. Uživatelské prostředí bude přizpůsobitelné koncovým uživatelem. Na administrační úrovni je umožněno konfigurovat příslušné obrazovky/formuláře. Uživatelské prostředí bude vícejazyčné s možností přepínání za běhu aplikace na úrovni obrazovky/formuláře.

Koncoví uživatelé budou mít možnost v uživatelském rozhraní zadávat nové požadavky, sledovat jejich stav, komunikovat s řešiteli a vyhledávat ve znalostní databázi. K zadávání požadavků mohou využít katalog servisních požadavků.

Součástí řešení bude rovněž nástroj, který umožní přímo z používaného rozhraní připojení ke vzdálené ploše počítače a komunikaci se zadavatelem incidentu v reálném čase. Tuto komunikaci lze přikládat k danému incidentu.

Součástí řešení bude též reporting, který je plně integrován. Integrační nástroje systému budou umožňovat komunikaci s okolními systémy pomocí webových služeb, výměny XML či flat souborů, DB komunikace a zasílání JMS zpráv. Data je možno též importovat a exportovat z CSV a XLS souborů. Integrační nástroje budou přímo ovládány a integrovány v grafickém rozhraní systému.

Řešení poskytne znalostní databázi, která bude plně provázána se Service Deskem. Její obsah bude postupně naplňován řešiteli jednotlivých požadavků a incidentů. Každý záznam může být zpřístupněn i koncovým uživatelům, kteří v této znalostní databázi budou vyhledávat.

5.4. Konfigurační management síťových zařízení

Systém pro správu konfigurací síťových zařízení bude poskytovat automatizované řešení pro heterogenní prostředí. Bude provádět správu konfigurací zařízení, změny na síti, upgrade operačního

systému a dohled nad dodržováním bezpečnostních politik (podnikových standardů) na síťových zařízeních (směrovač, přepínač, firewall, atd.). Systém pokryje správu celého životního cyklu síťového zařízení včetně:

- „discovery" sítě;
- automatické zálohy konfigurace;
- obnovy konfigurace bez nutnosti restartu zařízení;
- možnosti provádět hromadné změny na síti;
- automatické detekce a synchronizace změn na zařízení;
- odfiltrování přímého přístupu na zařízení s omezením zakázaných příkazů (nastavitelný filtr na úrovni systému) včetně kompletního zaznamenávání pohybu na zařízení;
- OS upgrade;
- validace konfigurace vůči bezpečnostním standardům;
- provisioning nových zařízení na základě vytvořené šablony konfigurace.

Celé řešení bude splňovat požadavky na vysokou spolehlivost a dostupnost, rozšiřitelnost a přímou integraci s ostatními funkčními moduly. Dále bude mít celé řešení jednotné grafické rozhraní ve webovém portálu tak, aby byl přístupný z prohlížečů jakéhokoli operačního systému (Linux, Windows). Současně také poskytne jednotnou správu uživatelských skupin a nastavení uživatelských profilů včetně rozvržení obrazovky a obsahu.

5.5. Konfigurační management serverů

Konfigurační management HW serverů bude zajišťovat:

- poskytnutí infrastruktury jako služby,
- efektivní provisioning s minimálními nároky na administraci,
- vysokou dostupnost a automatickou obnovou služby při výpadku,
- odolnost proti chybám na všech vrstvách (hardware, hypervisor, management virtualizace),
- balancování výkonu mezi více systémy,

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

- podporu více typů hypervisorů: ESX, Hyper-V, řešení konfiguračního managementu bude nezávislé na použitém hardware spravovaných strojů,
- samoobslužný přístup uživatelů pro správu jejich prostředí - virtuálních počítačů, sítí a úložišť,
- poskytnutí infrastruktury jako služby v plně distribuovaném prostředí,
- plnohodnotnou správu životního cyklu virtuálních strojů,
- optimalizaci, konfiguraci a automatizaci vytváření nových obrazů virtuálních strojů,
- analýzu virtuálních obrazů v celé infrastruktuře.

Řešení bude disponovat schopností samosprávy – to znamená, že dokáže zajistit běžící služby i během hardwarových a softwarových výpadků. Konfigurační management bude disponovat schopností správy životního cyklu virtuálních strojů. Z hlediska obsluhy a přístupu k administraci bude poskytovat přehledné webové rozhraní i přístup prostřednictvím příkazové řádky.

Řešení konfiguračního managementu bude poskytovat nástroj pro vytváření obrazů virtuálních strojů. Tento nástroj umožní skládat nové obrazy pomocí standardizovaných komponent (operační systém, softwarové balíky a uživatelské konfigurace a skripty) v grafickém rozhraní.

Pro zachování přehledu v již nasazených obrazech nástroj poskytne možnost detailně sledovat změny, které na nich byly provedeny, porovnávat je mezi sebou a vyhledávat nainstalovaný software. Na základě těchto informací bude provádět distribuci opravných balíčků a další nutné akce.

Nástroj bude podporovat rychlou obnovu po výpadku (rychlé spuštění virtuálního obrazu na jiném hardware) a rychlé přidání nového hardware do infrastruktury pomocí PXE protokolu.

5.6. Provisioning

Řešení pro provisioning virtuálních počítačů bude zajišťovat:

- poskytnutí infrastruktury jako služby,
- vysokorychlostní paralelní provisioning s minimálními nároky na administraci,
- vysokou dostupnost a automatickou obnovou služby při výpadku,
- odolnost proti chybám na všech vrstvách (hardware, hypervisor, management virtualizace),
- balancování výkonu mezi více systémy,

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

- podporu více hypervisorů: ESX, Hyper-V, řešení je zcela nezávislé na hardware,
- samoobslužný přístup uživatelů pro správu jejich prostředí - virtuálních počítačů, sítí a úložišť,
- poskytnutí infrastruktury jako služby na plně distribuovaném prostředí,
- plnohodnotnou správu životního cyklu virtuálních počítačů pro optimalizaci vytváření jejich obrazů, konfigurací a automatizaci vytváření virtuálních strojů,
- analýzu virtuálních obrazů v celé infrastruktuře.

Řešení dokáže zajistit běžící služby i během hardwarových a softwarových výpadků. Řešení bude disponovat schopností správy životního cyklu virtuálních strojů. Z hlediska obsluhy a přístupu k administraci bude poskytovat přehledné webové rozhraní i přístup prostřednictvím příkazové řádky a API.

Řešení bude poskytovat nástroj pro vytváření obrazů virtuálních strojů. Tento nástroj umožní skládat nové obrazy pomocí standardizovaných komponent (operační systém, softwarové balíky a uživatelské konfigurace a skripty) v grafickém rozhraní.

Pro zachování přehledu v již nasazených obrazech virtuálních strojů bude nástroj poskytovat možnost detailně sledovat změny, které na nich byly provedeny, porovnávat je mezi sebou a vyhledávat nainstalovaný software. Na základě těchto informací bude provádět distribuci opravných balíčků a další nutné akce.

Pro provisioning obrazů virtuálních strojů je preferováno využívání datových proudů proti klonování. Dále je požadována podpora rychlé obnovy po výpadku (rychlé spuštění virtuálního obrazu na jiném hardware) a rychlé přidání nového hardware do infrastruktury pomocí PXE protokolu.

5.7. Billing

Pro účtování služeb bude CMS 2.0 disponovat funkcionalitou pro evidenci, účtování, export podkladů jednotlivých služeb a jejich nákladů.

Účtovací systém bude splňovat přísná kritéria v bezpečnosti uložených dat, rychlosti zpracovávání účtovaných operací, spolehlivosti přístupu k datům, robustnosti s ohledem na serverovou platformu, použité databáze. V neposlední řadě bude používání Billingu nezávislé na uživatelské platformě, tzn. Web 2.0 aplikace pracující z běžných internetových prohlížečů a operačních systémů.

Řešení Billingu bude splňovat následující požadavky:

- Modulární řešení integrovatelné se Service Deskem, Network Inventory a účetním systémem.
- Umožní průběžný i zpětný náhled na prováděné operace, tvorbu uzávěrek, atd.
- Umožní vyúčtovávat a předepisovat platby jak periodické tak i dynamické (na základě vyúčtování služby). A to i jednorázově, za zřizovací náklady nebo jednorázové náklady.
- Bude schopen na základě okamžité informace o stavu klientského salda (pohledávka po splatnosti, přeplatek, došlá platba, atd.) zaslat informaci do Service Desku.
- Bude splňovat požadavek na běh v režimu vysoké dostupnosti.
- Bude připraven na datové nebo databázové úrovni komunikovat s jinými systémy.
- Bude škálovatelný od několika klientů po stovky tisíc a nebude závislý na počtu současně pracujících uživatelů, dále bude připraven zpracovávat neomezené množství a typy služeb.

Typy účtovaných služeb:

- **Periodické platby** - modul musí u každého koncového uživatele kontrolovat pravidelně opakující se služby a předepisuje mu platby k jednotlivým pravidelným vyúčtováním.
- **Jednorázové platby** - modul přiřadí k pravidelným vyúčtováním jednorázové platby za služby, které byly v průběhu ukončeného účetního období objednány.
- **Dynamické platby** - modul musí načítat externí data z různých předem definovaných systémů a přiřazovat je klientům, vést o nich podrobné záznamy a přiřazovat je k pravidelným vyúčtováním.

Dále bude řešení Billingu splňovat tyto požadavky.

- Billing bude podporovat fixní účetní nebo plovoucí období. To znamená, že při zakládání služby se zvolí účtované období měsíc, čtvrtletí, rok a účtovat bude vždy od prvního dne v měsíci po poslední den v období, nebo plovoucí období, které začíná vždy běžet od data připojení, aktivace služby, atd. (například vždy od 15tého do 14tého dne dalšího měsíce).
- Billing bude také sledovat náklady na jednotlivé klienty, nebo poskytované služby. Proto v systému bude možné zadat dodavatele a jejich dodávané služby a definované SLA, atd. Ve spolupráci s monitorovacími nástroji pak umožní importovat SLA pro jednotlivé služby.

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

- Billing bude podporovat dělení poměru nákladů na více klientů nebo služeb a bude definovatelná poměrná část nákladu na jednu službu, klienta, síť.
- Systém bude schopen komunikace s bankovním rozhraním vybraných českých bank a bude schopen provádět párování došlých i odchozích plateb. Billing bude notifikovat zákazníky prostřednictvím mailu popř. jiným rozhraním na nespárované platby nebo na pohledávky po splatnosti, export pohledávek na uživatelský portál CMS 2.0.
- Součástí Billingu bude deník změn, tedy evidence přesných záznamů „kdo, kdy a co" změnil u jednotlivého klienta, služby, atd. Zpětně bude možnost definovat každou změnu v systému a získat informace, kdo tuto změnu provedl.

5.8. Zálohování

Zálohovací systém bude v CMS implementován s cílem ochránit virtuální stroje, souborové servery, databáze, centrální servery a vyexportované konfigurace síťových prvků před ztrátou. Zálohování dat slouží k rychlé obnově dat po haváriích nebo v případě jejich nechtěného smazání. Pravidelné zálohování dat je základním předpokladem pro provedení řady scénářů obnovy po haváriích. Zálohy budou uchovávány po omezenou dobu, zpravidla několik dnů až týdnů.

Archivací rozumíme dlouhodobé uložení dat pro potřeby auditů, řešení sporů a vykazování. Pro efektivní práci s archivovanými daty je nezbytné rychlé vyhledávání a třídění výsledků. Pro práci s archivem pak bude nejdůležitější jeho uspořádání a dlouhodobá spolehlivost.

Zálohování bude sloužit pouze pro potřeby zálohování a obnovy komponent CMS 2.0, ne pro systémy uživatelů CMS 2.0. Stejně tak archivace bude určena pouze k dlouhodobému uložení dat o provozu CMS 2.0, ne pro archivaci dat, která jsou uložena v systémech uživatelů CMS 2.0.

Není vyloučeno, že v rámci CMS 2.0 bude služba zálohování a archivace dat uživatelů v budoucnu nabízena, ale není to v rozsahu aktuální nabídky realizace CMS 2.0.

Zálohovací systém bude umožňovat následující funkce.

- Zálohování a obnovu.
- Archivaci a vyhledávání.
- Snapshoty online databází a ochranu aplikací.
- Obnovy dat v případě jejich nečekané ztráty i v případě selhání celého systému.

- Prevenci duplikace dat, plných záloh a optimální využití zálohovaného prostoru.
- Efektivní správu záloh z více lokalit.
- Automatizaci migrace dat mezi třídami úložiště a správu archivů.

Jedním z hlavních nároků na správu úložných systémů je administrace velkého počtu řešení pro ochranu dat, zvláště pak požadavky na obnovu dat, které vyžadují více nástrojů. V rámci jednotného uživatelského rozhraní je požadována správa:

- Různých typů systémů a aplikací — virtuálních serverů, databází, atd.
- Různých lokalit — datových center po haváriích.
- Požadavků na různé úrovně poskytovaných služeb (čas poslední zálohy a délka obnovy RPO/RTO).
- Různých typů poruch — ztráta souborů/zpráv, poškození dat, chyby hardwaru, přírodní katastrofy.

Řešení bude čelit nárůstu vytvářených a ukládaných dat prostřednictvím funkcí pro snížení objemů dat včetně:

- Progresivní inkrementální zálohy, která odstraní nutnost redundantních opakovaných plných záloh.
- Zabudované deduplikace dat, která odstraní redundantní soubory a podsoubory jak na straně zdrojových dat, tak na straně dat cílových ve vlastní záloze.
- Bezproblémové integrace se souvisejícími zálohovacími knihovnami apod.
- Migrace dat podle nastavených pravidel na pomalejší a méně nákladná záložní media a automatické expirace.

Požadované funkční parametry:

- Zálohování na disky a pásky s možností definice trvanlivosti dat (expiračních pravidel) separátně pro zálohy na discích a na páskách.
- Zálohovací SW umožní kontinuální zálohování (automatické a okamžité zálohování změněných dat) při každé změně v bloku na filesystému (funkce CDP - Continuous data protection).

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

- Zálohovací SW umožní vytváření inkrementálních snapshotů, které respektují běžící databáze a umožní jejich zprovoznění z tohoto snapshotu.
- Instant recovery pro okamžité (<1min) zprovoznění provozu kritických aplikací v případě poškození datového disku ze snapshotu v záloze. Dokončení zpětné fyzické replikace dat ze snapshotu nebude vyžadovat restart serveru nebo způsobit výpadek.
- Připojení zálohy k libovolnému serveru jako virtuální disk s možností Read-Write přístupu, aby bylo možné spustit aplikace/databáze na historických datech pro účely testování nebo vyhledání/vykopírování potřebných dat z databází.
- Ovládání zálohování a obnovy virtuálních serverů prostřednictvím grafického klientského rozhraní.
- Transparentní šifrování zálohovaných dat.

U zálohování virtuálních serverů bude mít zálohovací systém následující funkce:

- Okamžitou obnovu jednotlivých souborů.
- Obnovu celého disku - obnova na pozadí.
- Obnovu celého virtuálního stroje i na nový HW.
- Zálohování nebude vyžadovat cyklický Full Backup při zálohování databází.
- Zálohování souborových systémů čistě pomocí inkrementálních záloh bez nutnosti vytváření pravidelných plných záloh.
- Automatickou duplikaci všech zálohovaných objektů na dvě fyzicky oddělená media ve dvou fyzicky oddělených lokalitách.
- Replikování dat do záložní lokality následně umožní transparentní obnovu z těchto replikovaných médií.
- Duplikace dat bude probíhat současně se zálohováním.
- Automatická archivace dat do hierarchického úložiště (HSM), data takto automaticky archivovaná budou uživateli dostupná transparentně v původních adresářích na diskovém systému.

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

- Systém zálohování bude integrován s HSM systémem, aby byl schopen data zálohovat v době během nebo před migrací na páskové medium, aby nedocházelo k nutnosti zpětné obnovy archivovaných dat z pásek během zálohování.
- Deduplikace zálohovaných/archivovaných dat na úrovni klienta i serveru bez dodatečných nákladů.
- Zálohovaná/archivovaná data mohou být šifrována.
- Možnost šifrování záloh za běhu.
- Podpora diskového zálohovacího úložiště bez omezení kapacity.

Pro volbu a používání záložních médií bude Dodavatel v roli provozovatele CMS 2.0 dodržovat následující pravidla:

- Jako záložní médium bude používat pouze takové nosiče, které odpovídají současným standardům pro zálohování a u nichž výrobce garantuje minimálně dva roky čitelnosti zapsaných údajů.
- U záložních médií bude respektovat životnost doporučenou výrobcem.
- Po vyřazení záložní médium fyzicky zničí.
- Při manipulaci s médiem během zálohování i později zajistí, že k němu mají přístup pouze oprávněné osoby.
- Zálohy uložené na médiu zkopíruje na jiné médium před koncem životnosti média.
- Zajistí uložení záloh na bezpečném místě:
    - v prostorách zabezpečených proti požáru, krádeži, neoprávněnému přístupu a živelní pohromě.
    - v prostorách splňujících parametry prostředí podle doporučení výrobce záložního média (teplota, vlhkost).

Systém bude odděleně (na logické úrovni) zálohovat následující kategorie dat:

- Software, konfigurační data a data pro správu: relativně malé objemy a relativně málo časté změny.

- Auditní záznamy a protokoly o činnosti CMS 2.0: relativně velké objemy a kontinuální vznik nových dat.

Existuje několik situací, ve kterých může být potřeba relativně snadný přístup k historickým údajům o provozu CMS 2.0:

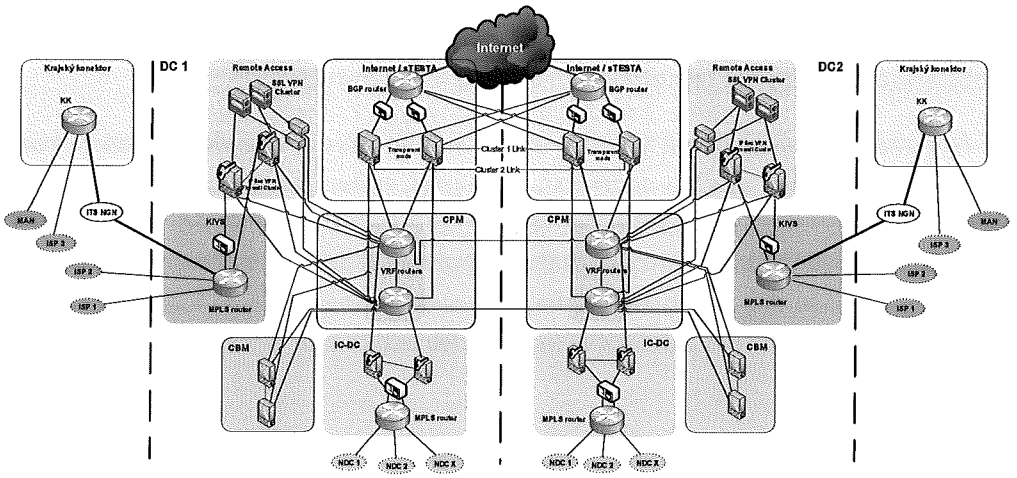
- Důkazy o dodržování SLA pro jednotlivé služby a důkazy o dodržování smluvních podmínek.
- Vyšetřování bezpečnostních událostí a incidentů v CMS 2.0.
- Podpora uživatelů CMS 2.0 při řešení jejich problémů. V první řadě jde o podporu při obstarávání důkazů pro řešení problémů, které mají sami uživatelé.

Všechny tyto situace mají společné to, že je nemožné dát přesné návody pro jejich řešení. Není možné dopředu odhadnout všechny možné situace, které mohou nastat, a určit data, která budou potřeba. Proto Dodavatel zajistí archivaci dat takovým způsobem, aby umožňoval správcům CMS 2.0 zpřístupnit relativně jednoduchým způsobem data o provozu CMS 2.0 a využívání služeb jednotlivými uživateli po definovanou dobu zpět. Tato doba bude stanovena na základě legislativních požadavků (ty určí minimální časové období) a praktické realizovatelnosti (maximální časové období).

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

6. Seznam komponent CMS 2.0

Shrnutí kapitoly	V kapitole je uveden seznam základních komponent, ze kterých se bude CMS 2.0 skládat.
Vazba kapitoly na Výzvu Zadavatele	Obsah kapitoly nemá přímou vazbu na žádnou kapitolu Výzvy Zadavatele.



Obrázek 29 - Blokové schéma komunikační infrastruktury CMS 2.0

6.1. Připojovací modul Internet/sTESTA

6.1.1. ASBR směrovače

Pro propojení s Internetem a sítěmi EU budou použity směrovače ASBR (Autonomous System Boundary Router). Tyto ASBR směrovače pomocí dynamických směrovacích protokolů komunikují se směrovači ostatních poskytovatelů služeb. Toto propojení se nazývá Peering/InterConnect. Do těchto směrovačů se také často připojují přímá propojení pomocí dynamických směrovacích protokolů, které nejsou realizovány přes přepínanou propojovací infrastrukturu, které se nazývají tzv. Direct Peering, kde se dva poskytovatele přímo domluví a navážou tzv. InterConnect (Direct Peering).

Základním požadavkem na ASBR směrovače je vysoká škálovatelnost počtu dynamických směrovacích protokolů tzv. "Neighbors". Dále také škálovatelnost v počtu směrovacích záznamů. Tyto směrovače budou mít minimálně dvě cesty do všech sítí Internetu, tzv. "FullBGP" směrovací tabulky od dvou

poskytovatelů konektivity. Dále také směrovací záznamy z propojení s partnery v rámci tzv. Internet Exchange Point. V Čechách je největším propojovacím uzlem NIX.CZ.

Tyto směrovací záznamy se ukládají do části paměti, které se nazývá RIB (Route Information Base), kde by měly existovat směrovací záznamy na všechny internetové sítě. Z těchto záznamů se poté spočítá tabulka nejlepších cest, která se ukládá v moderních směrovačích s distribuovanou architekturou do linkových karet. Proto budou mít ASBR směrovače distribuovanou architekturu.

Pro zvýšení kapacity linek, které se dostávají na hranici možností fyzického média, bude možné zátěž rozložit pomocí rozkládání na L3 vrstvě.

Při výběru směrovačů je jeden z důležitých parametrů počet VRF, které je možné konfigurovat. VRF je technologie, která umožňuje mít v jednom zařízení vice instancí směrovacích tabulek. V případě CMS 2.0 bude nutné velké množství směrovacích záznamů jak na IPv4 tak na IPv6 v rámci těchto VRF bez dopadu na výkonnost, tzv. směrovaní v hardware.

V každém uzlu CMS 2.0 bude umístěn cluster směrovačů, umožňující sdílet společnou konfiguraci a zajišťující redundanci směrovačů.

Každý směrovač bude mít možnost osazení 1GE, 10GE, 40GE, 100GE rozhraními na modulárních linkových kartách, které umožňují různé varianty portu v rámci jedné karty.

Každý směrovač bude mít lokální ochranu proti DoS útokům, tzv. CPP (Control Plane Policing). CPP umožňuje konfiguraci tzv. QoS pro jednotlivé typy provozu a tím směrovač chrání před nadměrným zatížením.

Směrovače budou mít možnost definovat minimálně šesti tříd provozu:

- směrovací protokoly (OSPF, IS-IS, BGP);
- správa směrovače (telnet, ssh, dns, radius, tacacs+ atd);
- testování dostupnosti – ICMP;
- monitoring zařízení (SNMP);
- vyhrazeno pro budoucí použití;
- zahozený provoz.

Na všech těchto třídách provozu bude možné zapnout logování provozu při překročení povolené šířky pásma zahazování paketů (rate limit).

Pro zabezpečení přístupu na směrovače budou použity tzv. AAA protokoly TACACS+ a RADIUS a to včetně možnosti použití jiných forem přihlašování než jenom uživatelským jménem a heslem, např. certifikátem.

V případě výpadku přihlašovacích autorit (AAA) budemožnost přihlášení pomocí SSH klíče administrátora.

6.1.1.1.Rychlá konvergence směrovačů

Pro rychlou konvergenci směrovačů bude směrovač podporovat BFD protokol pro směrovací protokoly dle (RFC 5581). Směrovače budou vybaveny redundantní řídící logikou, kde v případě výpadku jedné okamžitě převezme funkce druhá, tzv. "nonstop routing".

6.1.1.2.Management směrovačů

Směrovače budou vybaveny porty pro management a to jak po ethernetu, tak rozhraní sériové komunikace (RS-232) na každé řídící logice zvlášť. Jde o použití vyhrazených ethernet portů pro management směrovačů mimo provozní sít, tzv. OOB Management.

6.1.1.3.Propojení směrovačů

Směrovače budou propojeny do čtverce, kdy každý směrovač bude mít linku na dva jiné směrovače a vždy z jiné linkové karty.

6.1.1.4.Software směrovačů

Software směrovače bude mít modulární architekturu. Bude mít možnost ukládání, porovnávání a verzování konfigurace směrovače. Dále bude software směrovače vybaven funkcí následného potvrzení konfigurace v čase, kdy v případě, že nedojde k dalšímu potvrzení konfigurace, tak směrovač vrátí v zadaný čas zpět původní konfigurace. Jde o ochranu před chybou administrátora.

6.1.1.5.Požadované funkce směrovačů

Směrovače budou splňovat následující požadavky:

- Neblokující architektura směrování, tzv. wire-speed portu.
- Možnost výměnu klíčových komponent za běhu bez degradace výkonu zařízení po dobu výměny.
- Distribuovaná architektura směrování (oddělený Control Plane a Data Plane).
- Směrování IPv4 tak IPv6 v hardware a to jak směrových tak vícesměrových vysílání.

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

- Možnost výměny software za běhu služeb bez přerušení těchto služeb.
- Redundance klíčových komponent.
- Shaping, Policing bez snížení propustnosti směrovače.
- Replikace více směrových paketů v hardware.
- Plná podpora MPLS (VPLS [BGP, LDP], L2VPN [LDP, RSVP], L3VPN, Inter AS VPN).
- Celkový výkon směrovače bude pro L2, L3 IPv4 i IPv6 minimálně 2,6 Mil. Pps.
- Podpora monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v (pseudo)reálném čase minimálně: zdrojová/cílová IP, zdrojový/cílový TCP/UDP port/protokol – ve formátu NetFlow/IPFix nebo ekvivalent. Funkce monitorování bude implementována bez negativních vlivů na zátěž a výkon řídících procesorů, nebo bude realizována pomocí externích zařízení.
- Kontrola zdrojové IPv4, IPv6 adresy na fyzických i logických L3 rozhraních podle aktuální směrovací tabulky - antispoofingová kontrola ekvivalentní funkci uRPF (Unicast Reverse Path Forwarding).
- Podpora bezstavových filtrů na rozhraních v hardware bez vlivu na výkon směrování i přepínání.
- Podpora Jumbo Frame s playloadem (obsahem) minimálně 9KByte.
- Podpora Ethernet 802.3ah OAM (minimálně Neighbor Discovery, Link Monitoring, Remote Fault Indication).
- Podpora Ethernet 802.1ag CFM.
- Možnost výměny komponent (hot-swap) bez ovlivnění funkce zařízení.
- Hardwarová podpora zajištění kvality služby (QoS) podle L2/L3/L4 atributů umožňující implementaci QoS podle modelu rozlišovaných služeb (DiffServ dle RFC 2474, 2475, 2597, 2598, 2697, 3270):
    - Klasifikace a reklasifikace rámců/paketů na vstupu i výstupu (IEEE 802.1p, IP DSCP, IP Precedence, EXP MPLS).

- Omezování provozu (policing) na vstupu i výstupu (kompatibilita s RFC 2697 a/nebo RFC 2698), alespoň 8 výstupních front (jedna s absolutní prioritou) na každém rozhraní, konfigurovatelné mechanismy preventivní ochrany proti zahlcení.

- Podpora ECMP (Equal-cost multi-path routing), minimálně 16.
- Tx and Rx optical power monitoring (DOM) na optických portech.

6.1.2. Hraniční firewall

Modul bude mít vlastní hraniční firewally. Pro další bezpečnostní funkce bude využívat zařízení z modulu Remote Access.

Hraniční firewally budou poskytovat základní ochranu CMS 2.0 proti útokům z Internetu a sítí EU. Termínem firewall se zde myslí jedno nebo vice zařízení, která poskytují ochranu proti DOS útokům, umožňují inspekci běžných síťových protokolů a detekci anomálií v těchto protokolech a poskytují služby ochrany proti kybernetickým útokům (IPS/IDS). Budou umožňovat stejnou funkcionalitu pro IPv4 i IPv6.

Hraniční firewally budou provozovány v L2 transparentním režimu. V tomto režimu je možné se na firewall připojit pouze přes management IP adresu, která bude dostupná z Management modulu. Tímto se zvýší ochrana firewall proti přímým útokům.

Firewally budou nabízet dostatečnou propustnost, aby nedocházelo ke ztrátám v komunikaci.

Firewally budou podporovat správu konfigurací a to minimálně 50 konfigurací zpět. Budou umožňovat kontrolu správnosti konfigurace před nasazením, automatické obnovení předchozí konfigurace v případě nepotvrzení změn a porovnávání konfigurací. Konfigurace firewallu bude čitelný textový nebo XML soubor.

Autentizace správců hlásících se na firewall se bude provádět proti AAA serveru modulu Management. Mimoto bude firewall podporovat lokální autentizaci. V případě lokální autentizace bude možné se přihlásit uživatelským jménem a heslem, nebo certifikátem.

6.2. Modul Remote Access

Modul Remote Acces bude obsahovat více zařízení, jejichž služby budou využívat ostatní připojovací moduly. Konkrétně půjde o následující typy zařízení:

- SSL VPN koncentrátory.

- IPSec VPN koncentrátory.
- Stavové firewally.
- Aplikační firewally.
- Load balancery.

Fyzicky může jít o více zařízení, nebo jedno zařízení, obsahující funkční moduly. Některé z těchto typů zařízení jsou popsána podrobněji dále v této kapitole.

6.2.1. SSL VPN koncentrátory

SSL VPN koncentrátory modulu Remote Access budou poskytovat možnost vzdáleného připojení do sítě CMS 2.0. Budou použity dva SSL VPN koncentrátory v režimu vysoké dostupnosti. Pro poskytnutí SSL VPN jako služby pro organizace bude možné spustit SSL VPN jako virtuální službu a v případě požadavku delegovat administraci virtuální SSL VPN na správce organizace.

SSL VPN koncentrátor bude nabízet přístup jak přes L3 VPN klienta, tak přístup bez klienta z Internetového prohlížeče. V případě využívání L3 VPN klienta bude možné data přenášet jak protokolem ESP, tak přes SSL/TCP spojení, dle preference uživatele. Přístup z Internetového prohlížeče musí nabízet Reverzní Proxy s podporou web aplikací, port forwarding, sdílení souborů, klienta pro Microsoft Terminal Services a SSH/Telnet klienta.

SSL VPN koncentrátor musí být schopen autentizovat uživatele proti uživatelským databázím a to minimálně RADIUS, LDAP, AD, RSA SecurID, Local Database a seznamu certifikátů. Pro komunikaci s LDAP nebo AD serverem musí být použit zabezpečený kanál např. LDAPS.

VPN koncentrátor musí nabízet autentizaci minimálně uživatelským jménem a heslem a uživatelským certifikátem. Současně bude umožňovat dvou faktorovou autentizaci uživatele (např. uživatelským certifikátem a následně ještě uživatelským jménem a heslem).

Přiřazení přístupových práv uživateli bude možné na základě informací z AAA serveru (členství v LDAP skupinách, RADIUS atributy) nebo též na základě atributů v uživatelském certifikátu

Autentizace proti uživatelské databázi bude umožňovat Single sign-on, aby se uživatel nemusel opakovaně autentizovat při přístupu k různým zdrojům CMS 2.0. V případě vypršení uživatelského hesla bude možné přes rozhraní SSL VPN nastavit v uživatelské databázi nové heslo. Pro větší bezpečnost bude VPN koncentrátor umět vynucovat komplexnost uživatelského hesla.

VPN koncentrátor bude schopen komunikovat s bezpečnostními prvky v síti a případě bezpečnostního incidentu vyvolaného uživatelem připojeného přes VPN, problematického uživatele odpojit nebo mu omezit přístup.

SSL VPN koncentrátor bude podporovat zprávy typu syslog pro odesílání zpráv o stavu zařízeni. Součástí musí být ladící nástroje pro identifikaci případných problémů, jako například podrobné sledování stavu autentizace uživatele, uživatelských práv, která mu byla přiřazena a na základě čeho mu byla práva přiřazena. Protože se předpokládá využívání SSL VPN různými subjekty a skupinami uživatelů, musí být možné provozovat SSL VPN na více veřejných IP adresách současně a každé IP adrese mít možnost přiřadit jiný certifikát.

6.2.2. IPSec VPN koncentrátory

IPSec VPN koncentrátory budou zakončovat IPSec VPN spojení z Internetu, z sTESTA, z KIVS a případně i z dalších připojovacích modulů CMS 2.0.

Všechny IPSec VPN budou v tzv. směrovacím módu, aby skrz IPSec VPN spojení bylo možné provozovat dynamické směrovací protokoly. IPSec VPN bude vždy navázána dvakrát, do každého Datového centra jedna IPSec VPN. Pomocí dynamického směrovacího protokolu bude zajištěna vysoká dostupnost IPSec VPN spojení. Spojení bude řídit firewall modulu Remote Access. Firewall tedy musí podporovat dynamické směrovací protokoly. Případně rozdělení IPSec VPN KIVS a IPSec VPN Internet do různých směrovacích tabulek, s možností komunikace mezi směrovacími tabulkami uvnitř firewallu a možností definování bezpečnostních politik mezi směrovacími tabulkami.

Pro zabezpečení IPSec VPN bude použit protokol ESP s šifrovacím algoritmem AES a délkou klíče minimálně 128 bitů, hash algoritmus SHA1 nebo SHA2 a PFS group 2 nebo group 6. Preferovaný způsob autentizace IPSec VPN bude pomoci certifikátu.

IPSec VPN koncentrátor bude podporovat zprávy typu syslog pro odesílání zpráv o stavu zařízeni. Součástí musí být ladící nástroje pro identifikaci případných problémů, jako například podrobné sledování stavu autentizace uživatele, uživatelských práv, která mu byla přiřazena a na základě čeho mu byla práva přiřazena.

6.2.3. Stavové firewally

Stavový firewall bude oddělovat modul Remote Access od ostatních částí CMS 2.0 a bude vynucovat bezpečnostní pravidla uživatelů přihlášených přes SSL VPN nebo IPSec VPN. Firewally budou v L3 směrovacím módu a zapojené v režimu vysoké dostupnosti.

Firewall umožní rozdělení sítí do bezpečnostních zón a bude monitorovat a logovat komunikaci jak mezi bezpečnostními zónami, tak uvnitř bezpečnostními zóny. Bezpečnostní politiky mezi zónami bude možné definovat jak pro protokol IPv4, tak pro IPv6. Pro bezpečnostní politiky bude možné specifikovat čas jejich platnosti. Logovaní událostí bude možné zapnout na úrovni jednotlivých bezpečnostních politik.

Firewall bude podporovat Route/NAT mód. Součástí firewallu bude podpora NAT pro překlad adres Source NAT, Destination NAT, Static NAT. Bude možné definovat QoS a policing pro omezování rychlosti. Firewall bude podporovat minimálně protokol NetFlow verze 9 pro monitorování a analýzu průtoků přes Firewall.

Další vlastnost, kterou firewall bude splňovat, je směrování jak pro protokol IPv4, tak pro protokol IPv6. Firewall bude podporovat statické směrování i dynamické směrovací protokoly. Pro oddělení překryvných IP rozsahů a bezpečnostní rozdělení IP provozu je nutná podpora vytváření Virtuálních směrovacích tabulek VRF.

Autentizace správců hlásících se na firewall se bude provádět proti AAA serveru modulu Management. Mimoto bude firewall podporovat lokální autentizaci. V případě lokální autentizace bude možné se přihlásit uživatelským jménem a heslem, nebo certifikátem.

6.2.4. Aplikační firewally

Na aplikačním firewallu bude možné specifikovat povolené aplikace na základě jejich rozpoznání firewallem, místo specifikování TCP/UDP portu. Firewall umožní definovat pro jednotlivé aplikace specifické bezpečnostní politiky. Současně bude možné definovat pro jednotlivé aplikace QoS a pro omezování nebo upřednostňování aplikací a bude možné o jednotlivých aplikacích vytvářet statistiky. Firewall bude schopen rozpoznávat minimálně 300 aplikací.

Autentizace správců hlásících se na firewall se bude provádět proti AAA serveru modulu Management. Mimoto bude firewall podporovat lokální autentizaci. V případě lokální autentizace bude možné se přihlásit uživatelským jménem a heslem, nebo certifikátem.

6.2.5. Load balancery

Pro garanci dostupnosti, zajištění škálovatelnosti a optimalizace služeb bude použito zařízení pro vyvažování zátěže tzv. Load Balancery. Množině serverů nebo jiných zařízení s vlastní IP adresou je přidělena jedna virtuální IP adresa (VIP) a např. serverová farma tak vystupuje vůči uživateli jako jeden logický server. Z toho plyne prakticky neomezená škálovatelnost, vysoká dostupnost a optimalizace provozu. Každé takové řešení umožňuje dynamické a hlavně, z pohledu uživatele,

transparentní přidání a odebrání zdrojů. Rovněž výpadek jednoho nebo i více serverů zůstane před uživatelem skryt.

Požadavky na Load balancer:

- Monitorování stavu a zátěže zdrojů/serverů.
    - Kontinuální monitorování nejen serverů, ale i celé cesty.
    - Možnost kombinace (AND/OR) více metod (ARP, ICMP, DNS, HTTP, TCP port, SSL Hello, SMTP, RADIUS, LDAP atd.).
    - Možnost definování intervalu pro monitorování.
- Rozdělování zátěže a přesměrování provozu.
    - Load balancing na L4 i L7.
    - Podle obsahu na L7 (cookies, parametry HTTP – řeč, typ prohlížeče atd.).
    - Podle aktuálního provozu.
    - Podle počtu spojení.
    - Podle počtu uživatelů.
    - Podle doby odezvy.
    - Podle váhy serveru.
    - Cyklické.
    - Podle hash funkce.
- Podpora až 1024 serverů na virtuální IP (VIP).
- Možnost definovat periodu pro postupnou zátěž pro servery po restartu.
- Rozdělování zátěže mezi více lokalitami (tzv. GSLB – Global server load balancing).
    - Na základě DNS (load balancer si „drží" DNS A záznam pro danou službu).
    - Možnost odpovídat vice DNS A záznamy.

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

- Na základě vlastnosti aplikací, HTTP přesměrování (HTTP hlavička 302 - Moved Permanently).
- Pomocí proxy (klient NAT).
- Možnost určit, která lokalita je schopna obsloužit požadavek nejrychleji (tzv. proximity).

- Směrování zátěže na stejný server (tzv. perzistence).
  - Na základě L3/L4 parametrů (např. zdrojová IP).
  - Hash funkce na základě IP.
  - Na základě L7 parametrů (statické i dynamické cookies, HTTP hlavička).
  - RADIUS.
  - ID SSL spojení.
- Modifikace provozu.
  - Vložení/přepsání cookie.
  - Modifikace URL.
  - Možnost vložit zdrojovou IP do L7 hlavičky.
  - Modifikace HTTP obsahu.
- Možnosti nasazení.
  - Podpora směrování (RIP, OSPF, BGP).
  - Podpora VLAN (802.1Q).
  - Podpora sdružování portů (LAG/LACP).
  - Podpora vysoké dostupnosti (VRRP) pro load balancery .
  - Možnost nasadit load balancer jako dedikovaný hardware, jako virtuální instanci na vlastním hardware, jako virtuální appliance s podporou různých hypervizorů.

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

- Podpora různých topologií – připojení na router/L3 přepínač (tzv. one leg), implementace „v cestě" (in-line), možnost posílat odpovědi serverů přímo klientovi (tzv. local triangulation).

- Musí poskytovat stejnou funkcionalitu pro IPv4 a IPv6 provoz.
- Podpora 1GE i 10GE portů.
- Garantovaný výkon.
- Optimalizace provozu.
  - Ukončování SSL spojení (tzv. SSL offloading) což výrazně snižuje zátěž serverů a mimo jiné usnadňuje management certifikátů.
  - SSL offloading na dedikovaném hardwarovém modulu.
  - Možnost znovu navázat SSL spojení pro ukončená spojení (tzv. backend encryption). Se serverem je navázano jedno spojení a může být šifrováno slabším klíčem. Provoz je pak šifrován od klienta až po server a zároveň server je výrazně méně zatížen.
  - TCP multiplexing, kdy jedno TCP spojení mezi serverem a load balancerem obsluhuje více spojení mezi klientem a load balancerem.
  - Transparentní komprese http.
  - Caching.
- Podpora vizualizace.
  - Datové centrum bude obsluhovat různé typy aplikaci i aplikace různých subjektů. Proto je kritické, aby load balancer podporoval na jednom hardware více virtuálních instancí. To umožní efektivní správu, automatizaci a konsolidaci. V neposlední řadě virtualizace přináší úspory z pohledu spotřeby energie, chlazení datového centra, prostoru atd.
  - Virtuální instance musí být plně oddělené (od ARP tabulky, směrovací tabulky až po management) a jakákoliv změna včetně případné chyby na jedné instanci load balanceru nemá vliv na chod jiných instancí.

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

- Konfigurace a vlastnosti (mimo výkonnost a L2 parametry) musí být shodné pro dedikovaný hardware, virtuální instance na vlastním hardware i virtuální appliance pro hypervisory.
- Podpora až 256 virtuálních instancí na jednom hardware.
- Možnost převodu konfigurací mezi jednotlivými formami load balancem.

- Podpora API (XML) a šablon pro automatizaci zprovoznění služeb (provisioning).
- Možnost definovat nezávislé správce a uživatele pro jednotlivé instance load balancerů včetně jejich práv a rolí (např. jen pro monitorování), tzv. RBAC (Role based Access Control).
- Podpora automatizace.
  - Podpora API a SDK (XML / Web Services).
  - Podpora integrace s různými hypervizory.
  - Podpora šablon pro automatizaci.
- Možnost definovat metody přístupu (SSH, Telnet, HTTP/HTTPS, SNMP atd.).
- Podpora NTP.
- Podpora logování událostí, jak lokálně tak i přes SYSLOG.
- Podpora autentizace přístupu (RADIUS, TACACS+).
- Možnost pracovat s konfigurací v textovém formátu.
- Centrální management a monitoring s možností granulární definice rolí a práv uživatelů (tzv. RBAC) na úrovni jednotlivých instancí load balanceru.

6.3. Připojovací modul KIVS

Připojovací modul KIVS bude obsahovat MPLS směrovače v konfiguraci vysoké dostupnost, hraniční firewally a koncová zařízení na straně subjektů připojených do CMS 2.0 přes operátory KIVS, tzv. CPE zařízení.

Modul KIVS bude mít vlastní hraniční firewally. Pro další bezpečnostní funkce bude využívat zařízení z modulu Remote Access.

6.3.1. Směrovače

Pro propojení s operátory KIVS budou použity směrovače MPLS. Tyto směrovače budou komunikovat s MPLS směrovači jednotlivých operátorů KIVS.

MPLS směrovače budou podporovat následující funkce:

- MPLS forwarding;
- MPLS load balancing;
- MPLS Fast Reroute;
- MPLS Traffic Engineering;
- VPLS.

Část MPLS směrovačů modulu KIVS bude umístěna jako Krajský konektor CMS 2.0 mimo uzly (DC) CMS 2.0.

6.3.2. Hraniční firewally

Hraniční firewally budou poskytovat základní ochranu CMS 2.0 proti útokům z prostředí KIVS.

Tyto firewally budou mít stejné vlastnosti jako firewally modulu Internet/sTESTA.

6.3.3. Koncová zařízení u uživatelů CMS

Přes linky poskytovatelů připojené do modulu KIVS se do CMS 2.0 budou připojovat kraje, města, obce atd. Pro monitorování kvality služeb a zajištění bezpečnosti koncového místa CMS 2.0 - KIVS, je nutné na konec služby poskytovatele umístit zařízení ve správě CMS 2.0, tzv. CPE zařízení.

Pro bezpečný přístup bude použita IPSec VPN, která nabízí nejen šifrování dat, ale i autentizaci a ověření integrity přenášených zpráv. Každé CPE (koncové zařízení na druhé straně VPN tunelu) bude navazovat vždy dva IPSec VPN tunely, primární a záložní. Pro zabezpečení vysoké dostupnosti přes dva IPSec VPN tunely bude využitý dynamický směrovací protokol.

Jako CPE zařízení je možné použít stávající aktivní prvky, pokud budou splňovat požadované parametry nutné pro komunikaci s CMS 2.0.

CPE musí být bezpečnostním zařízením nabízející zónový firewall, překlad IP adres (NAT), IPSec VPN, IKEv1, IKEv2. Pro VPN musí umět autentizaci pomocí Pre-shared klíče nebo Certifikátu. Požadovaná je podpora Route Base IPSec VPN. IPSec tunely musí podporovat minimálně tuto sadu bezpečnostních

funkcí, pro šifrování AES, AES192, AES256, 3DES, protokoly ESP a AH, hash funkce SHA1 a SHA256, Diffie Hellmann Group 1, Group 2 a Group 5. Ze směrovacích protokolů je požadován minimálně protokol OSPFv3, IS-IS s podporou pro IPv6, RIPv2, RIPng.

Výkonnost prvku bude dle typu služby KIVS.

6.4. Připojovací modul IC-DC

Připojovací modul IC-DC bude obsahovat MPLS směrovače v konfiguraci vysoké dostupnost a hraniční firewally.

Modul bude mít vlastní hraniční firewally. Pro další bezpečnostní funkce bude využívat zařízení z modulu Remote Access.

6.4.1. Směrovače

Pro propojení s operátory KIVS budou použity směrovače MPLS. Tyto směrovače budou komunikovat s MPLS směrovači jednotlivých operátorů KIVS.

MPLS směrovače budou podporovat následující funkce:

- MPLS forwarding;
- MPLS load balancing;
- MPLS Fast Reroute;
- MPLS Traffic Engineering;
- VPLS.

6.4.2. Hraniční firewally

Hraniční firewally budou poskytovat základní ochranu CMS 2.0 proti útokům z prostředí DC.

Tyto firewally budou mít stejné vlastnosti jako firewally modulu Internet/sTESTA.

6.4.3. IPSec VPN koncentrátory

IPSec VPN koncentrátory budou zakončovat IPSec VPN spojení z DC, pro která bude požadováno transparentní šifrování provozu.

6.5. Centrální propojovací modul

CPM bude obsahovat výkonné směrovače v konfiguraci vysoké dostupnosti a několik aplikačních modulů pro předávání zpráv: MTA a ESB.

6.6. Centrální bezpečnostní modul

CBM bude obsahovat výkonné firewally v konfiguraci vysoké dostupnosti. Tyto firewall budou pracovat na L3 a budou provádět překlad adres (pokud bude nutný) a povolovat spojení mezi VPN různých subjektů.

Firewall bude podporovat správu konfigurací a to minimálně 50 konfigurací zpět. Bude umožňovat kontrolu správnosti konfigurace před nasazením, automatické obnovení předchozí konfigurace v případě nepotvrzení změn a porovnávání konfigurací. Konfigurace firewallu bude čitelný textový nebo XML soubor.

Firewall bude podporovat Route/NAT móde a transparentní mód. Součástí firewallu bude podpora NAT pro překlad adres Source NAT, Destination NAT, Static NAT. Firewall musí být možné definovat a nasadit QoS a policing na omezování rychlosti. Firewall bude podporovat minimálně protokol NetFlow verze 9 pro monitorování a analýzu průtoků přes Firewall.

Další vlastnost, kterou firewall musí splňovat je směrování jak pro protokol IPv4, tak pro protokol IPv6. Firewall musí podporovat statické směrování i dynamické směrovací protokoly. Z dynamických směrovacích protokolů musí být podporovány OSPF, RIP, BGP, IS-IS. Současně musí být podporováno směrování multicast provozu protokolem PIM a podpora protokolu IGMPv2, IGMPv3. Pro případné oddělení překryvných IP rozsahu, nebo bezpečnostní rozdělení IP provozu, je nutná podpora vytváření Virtuálních směrovacích tabulek VRF. Pro zvýšení propustnosti musí firewall podporovat protokol LACP pro sdružení více linek.

Autentizace správců hlásících se na firewall se bude provádět proti AAA serveru modulu Management. Mimoto bude firewall podporovat lokální autentizaci. V případě lokální autentizace bude možné se přihlásit uživatelským jménem a heslem, nebo certifikátem.

6.7. Prostředí Management

6.7.1. Hraniční firewally

Hraniční firewally budou poskytovat ochranu CMS 2.0 proti útokům na Management prostředí.

Tyto firewally budou mít stejné vlastnosti jako firewally modulu Internet/sTESTA.

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

6.7.2. AAA server

AAA server bude součástí Management modulu a bude použit pro ověřování uživatelů. AAA server musí podporovat všechny standardní autentizační metody PAP, CHAP, EAP, EAP MS-CHAP, EAP MD5-challenge, EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTP a ověřování Certifikáty. Současně musí být možné navázat AAA server na uživatelskou databázi pro ověření uživatelských identit. Podporované uživatelské databáze jsou LDAP, nativní AD, RADIUS, RSA ACE, Trust SiteMinder, NIS, Lokální databáze uživatelů. AAA server bude umožňovat vytvářet více Lokálních uživatelských databází. V případě autentizace proti uživatelské databázi (např. AD) musí být možné tzv. Single Sign-On.

Rozhraní AAA serveru musí být schopné komunikovat s aktivními prvky v síti a na základě autentizace uživatele přiřazovat uživatelské profily. Uživatelským profilem je bezpečnostní politika, která se přiřazuje uživateli na základě autentizace. Po úspěšném přihlášení uživatele jsou na bezpečnostní prvky v síti (firewall, IPS sonda) nasazena dynamická pravidla na konkrétního uživatele dle přiřazeného profilu. AAA server musí být schopen komunikovat s bezpečnostním dohledem tak, aby bezpečnostní incidenty mohly být přiřazeny konkrétnímu uživateli. V případě autentizace správce bude AAA server v návratových atributech též posílat uživatelská práva správce.

U AAA serveru je požadováno nasazení ve vysoce dostupném módu, a proto musí podporovat zapojení do Clusteru a to jak v režimu Active/StandBy, tak v režimu Active/Active.

Součástí AAA serveru bude i Captive portál (Webový autentizační portál) pro autentizaci uživatelů při přístupu ke konkrétním zdrojům CMS 2.0. Captive portál se bude využívat především pro autentizaci uživatelů přistupujících ze sítě KIVS, kde za jedním IPSec VPN může být více uživatelů s různými oprávněními.

6.7.3. Terminálový server

Součástí management sítě bude konzolový server (terminálový server), který bude nabízet dostatečné množství sériových portů. Na sériové porty budou připojené konzolové porty aktivních prvků. To umožní vzdálený přístup na konzole aktivních prvků. Vzdálený přístup na konzolové porty umožní správcům sítě monitorovat stav aktivních prvků i v případě nedostupnosti aktivního prvku přes IP síť.

6.7.4. VPN koncentrátory

VPN koncentrátory budou zakončovat management VPN spojení z Internetu a CMS 2.0 do management sítě CMS 2.0.

7. Testování prostředí CMS 2.0

Shrnutí kapitoly	V kapitole jsou definovány kategorie testů, které dodavatel provede, a jejich stručný popis.
Vazba kapitoly na Výzvu Zadavatele	Obsah kapitoly nemá přímou vazbu na žádnou kapitolu Výzvy Zadavatele.

Testování vybudovaného řešení CMS 2.0 je základním nástrojem pro ověření funkčností nejen jednotlivých služeb CMS 2.0, ale také celého prostředí a jeho geografické redundance.

Vzhledem k migračnímu postupu bude prostředí CMS 2.0 před uvedením do provozu testováno v rámci jedné lokality, kde bude vybudována redundantní topologie. Toto testování prokáže požadované vlastnosti prostředí CMS 2.0 a bude podkladem pro akceptaci projektu Zadavatelem.

Postupy technické, procesní a organizační přípravy testování CMS 2.0 zapracuje dodavatel do harmonogramu projektu a načasování bude spojeno s průběhem migrace služeb z prostředí CMS 1.0 do prostředí CMS 2.0. Migrace služeb může proběhnout až po provedení funkčních a zátěžových testů prostředí CMS 2.0.

7.1. Funkční testy CMS 2.0

Účelem funkčních testů bude ověřit, zda jednotlivé funkce služeb CMS 2.0 plní svoji roli a zda odpovídají své funkční specifikaci. Cílem funkčních testů pak bude odhalení a eliminace případných chybných funkčností jednotlivých služeb CMS 2.0.

7.1.1. Integrační testy modulů CMS 2.0

Integrační testování modulů CMS 2.0 proběhne za účelem ověření integrace všech modulů prostředí a jejich plné vzájemné funkčnosti. Jedná se především o spolupráci podpůrných systémů jako Service Desk, Konfigurační management, Performance management, Provisioning a ostatních.

7.1.2. Integrační testování eGON Service Bus

Integrační testování eGON Service Bus proběhne za účelem ověření integrace systému eGON Service Bus a Informačního systému základních registrů (ISZR). Dále potom za účelem integrace systému eGON Service Bus a agendovými informačními systémy AISEO, ISDS, AISC a ISUI/ISKN.

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

7.2. Zátěžové testy CMS 2.0

Zátěžové testy je možné realizovat po provedení funkčních testů a případném odstranění závad zjištěných při funkčním testování. Účelem zátěžového testování prostředí CMS 2.0 bude ověřit, zda výkon a průchodnost prostředí CMS 2.0 odpovídá nastaveným mezním hodnotám u jednotlivých služeb CMS 2.0.

7.3. Bezpečnostní testy CMS 2.0

Bezpečnostní testy CMS 2.0 jsou popsány v kapitole 6.6 „Testování bezpečnosti CMS 2.0" tohoto dokumentu.

7.4. Analýza testování a testovací scénáře

Vytvoření analýzy testování prostředí CMS 2.0 a specifikace testovacích scénářů a procesů testování prostředí CMS 2.0 dodavatel popíše v technickém projektu.

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

8. Inženýring CMS 1.0

Shrnutí kapitoly	Kapitola popisuje cíle a výstupy etapy projektu Inženýring CMS 1.0. Kapitola vymezuje povinnosti Dodavatele a požadované součinnosti Zadavatele při vyhodnocování výstupů Inženýringu CMS 1.0.
Vazba kapitoly na Výzvu Zadavatele	Cíle etapy Inženýring CMS 1.0 a požadované výstupy této etapy projektu jsou popsány v kapitole 9. Přílohy Výzvy Zadavatele.

8.1. Cíle inženýringu

V rámci této fáze realizace projektu CMS 2.0 budou prověřeny následujících oblasti a budou dodány podklady jejich skutečného provedení:

- Prověření přesného HW osazení všech částí stávajících bloků CMS a jeho soupis.
- Identifikace všech prvků a částí bloků využitelných pro vlastní realizaci povýšení na CMS 2.0 s přihlédnutím ke zde definovaným požadavkům na vlastnosti HW, topologii a charakter služby.
- Jednoznačné a maximální využití stávajícího HW, pokud samozřejmě plně vyhovuje daným specifikům a nebude nijak omezujícím faktorem pro budoucí požadovanou architekturu a funkci.
- Prověření všech skutečností, které nemusí být známy zadavateli a jenž by mohly zefektivnit navrhované řešení či jeho formu.
- Prověření stavu a dostupnosti datových center pro umístění prostředí CMS 2.0

8.2. Výstupy inženýringu CMS 1.0

Dodavatel jako výstup inženýringu předá Zadavateli dokument „Inženýring CMS 1.0", který bude obsahovat všechny požadované skutečnosti dané kapitolou 9.2 Přílohy 1 Výzvy.

Dokument tak bude obsahovat následující kapitoly:

A. Seznam použitého hardwarového vybavení CMS 1.0

B. Seznam použitého programového vybavení CMS 1.0

C. Obecný návrh náhrady nevyužitelných technologických prvků CMS 1.0

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

D. Obecný návrh implementace navrhovaného řešení prostředí CMS 2.0

E. Další návrhy oproti seznamu požadavků definovaných Přílohou 1. Výzvy.

F. Místní šetření DC Olšanská 4 .

8.3. Provedení inženýringu HW a SW

Při provádění inženýringu CMS 1.0 bude Dodavatel vycházet z požadavků zadaných v kapitole 9.2 Přílohy 1 Výzvy. Dodavatel zpracuje seznam využitého HW a SW v prostředí CMS 1.0. V tomto seznamu vyznačí použitelnost stávajících zařízení a programového vybavení. Uvede, zda zařízení již nejsou mimo podporu výrobce.

Dodavatel předpokládá, že prostředí CMS 2.0 vznikne paralelně s prostředím CMS 1.0 a tak za obecný návrh technologií pro náhradu nevyužitelných technologií a programového vybavení CMS 1.0 považuje technickou část nabídky řešení prostředí CMS 2.0.

U technologií a programového vybavení, které označí Dodavatel jako nevyužitelné, uvede Dodavatel přesný důvod nevyužitelnosti. Vyřazení technologií a programového vybavení z prostředí CMS podléhá schválení Zadavatele, který tak učiní na základě předloženého seznamu technologií a programového vybavení a důvodů nevyužitelnosti.

U technologií, které označí Dodavatel jako využitelné i v prostředí CMS 2.0, provede Dodavatel postupnou migraci do prostředí CMS 2.0. Tato migrace bude provedena v době před migrací služeb CMS 1.0 do prostředí CMS 2.0 a její termín bude úzce navázán na termíny migrace služeb tak, aby nedošlo k přerušení funkcionality migrovaných služeb.

8.4. Provedení inženýringu DC Olšanská 4

Dodavatel jako provozovatel stávajícího řešení CMS 1.0 má přístup do technologického prostoru CMS 1.0 a provede zde místní šetření, které zhodnotí možnost výstavby jednoho uzlu CMS 2.0 v lokalitě Olšanská 4 a to z pohledu prostorového řešení, kapacit napájecího a chladícího zařízení datového centra.

V případě, že umístění uzlu CMS 2.0, bude vyžadovat stavební úpravy v objektu Olšanská 4, navrhne Dodavatel jejich rozsah a provede kalkulaci tržních cen takových prací.

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

9. Přechod z CMS 1.0 na CMS 2.0

Shrnutí kapitoly	V kapitole jsou uvedeny některé aspekty přechodu z CMS 1.0 na CMS 2.0, které ovlivňují návrh, implementaci a náběh provozu CMS 2.0.
Vazba kapitoly na Výzvu Zadavatele	Obsah kapitoly má vazbu na kapitoly 2 a 4 Přílohy 1 Výzvy Zadavatele.

Migrace zákazníků a služeb z CMS 1.0 do CMS 2.0 není součástí projektu ani nabídky. Proto má tato kapitola pouze informativní charakter. Dodavatel ale počítá s tím, že bude provádět veškeré potřebné činnosti zajišťující provoz jak CMS 1.0 tak CMS 2.0 a nabídne potřebnou podporu při migraci služeb a zákazníků z CMS 1.0 do CMS 2.0.

Způsob migrace bude mít vliv i na CMS 2.0 a jeho implementaci. Na straně dodavatele může mít výběr metody migrace služeb vliv minimálně na následující oblasti řešení.

- Může být omezena možnost využití zařízení CMS 1.0 pro CMS 2.0. Dokud budou zařízení používána v CMS 1.0, není možné je použít pro CMS 2.0, nebo je možné je využít pouze v omezené míře.
- Možnost použít pro konsolidované IP adresy stejné rozsahy pro jeden subjekt v CMS 1.0 a CMS 2.0 nebo naopak nutnost použít různé rozsahy.
- Návrh některých funkcí a služeb. Jde zejména o způsob zajištění interoperability mezi CMS 1.0 a CMS 2.0.
- Dobu výstavby CMS 2.0 a průběh výstavby.
- Způsob akceptace CMS 2.0.

Dalšími aspekty, které je nutné uvážit, jsou následující.

- Nároky na subjekty, které využívají CMS 1.0. Jedná se o požadavky na změny IP adres, na změny v interních systémech subjektů (zapojení do různých VPN, respektive do různých DMZ), o požadavky na administrativní akce (vyplňování formulářů). Tyto nároky by měly být minimalizovány.
- Možnosti interoperability mezi CMS 1.0 a CMS 2.0. Jde o možnosti komunikace mezi systémy subjektů připojenými do CMS 1.0 a systémy připojenými do CMS 2.0. A o způsob zajištění interoperability.

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

- Délka migrace.

Dodavatel uvážil několik metod migrace.

- Najednou. Bude postaven jeden uzel CMS 2.0 a všechny stávající služby CMS 1.0 budou připraveny v CMS 2.0. Potom se CMS 1.0 vypne, aktivuje se CMS 2.0 a subjekty začnou používat služby CMS 2.0. Potom bude postaven druhý uzel CMS 2.0. Hlavní nevýhodou tohoto postupu je nutnost synchronizace všech subjektů CMS 1.0 a velké riziko dočasné nefunkčnosti některých služeb, protože všechny subjekty využívající CMS 1.0 musí přejít na CMS 2.0 najednou.

- Po částech. Bude postaven jeden uzel CMS 2.0 a stávající služby CMS 1.0 budou postupně (po službách nebo subjektech) migrovány do CMS 2.0. Po dokončení migrace bude postaven druhý uzel CMS 2.0. Rizikem je těžko odhadnutelná doba migrace. Po celou dobu migrace nebude CMS 2.0 splňovat požadavek na geografickou redundanci.

- Kompletní výstavba obou uzlů CMS 2.0 a zajištění interoperability mezi CMS 1.0 a CMS 2.0. Následná postupná migrace z CMS 1.0 na CMS 2.0.

Dodavatel navrhuje použít poslední uvedenou metodu. Ve zbytku kapitoly je uvedena základní představa dodavatele o doporučené metodě migrace.

- Dodavatel vybuduje oba uzly CMS 2.0. Buď ve dvou různých lokalitách, nebo oba v jedné lokalitě. V jedné lokalitě v případě, že díky obsazení Olšanské 4 uzlem CMS 1.0 nebude k dispozici lokalita, do které by bylo možné druhý uzel CMS 2.0 umístit.

- Propojí se InterConnecty CMS 1.0 (interconnet-I) a CMS 2.0 (Přístupové moduly). CMS 1.0 a CMS 2.0 budou sdílet jeden konsolidovaný adresní prostor IP adres. Bude zajištěna komunikace mezi VPN CMS 1.0 a CMS 2.0 pomocí směrování.

- Bude zastavena možnost zřizovat v CMS 1.0 některé služby, zejména vytváření nových VPN CMS 1.0. Nové subjekty se připojují do CMS 2.0. Nové VPN vznikají pouze v CMS 2.0.

- Služby CMS 1.0 se migrují do CMS 2.0 jedna po druhé. Bude nutné vypracovat rámcové plány pro migraci jednotlivých typů služeb CMS 1.0. A pro každou konkrétní využívanou službu připravit migrační plán. Rámcové (typové) plány je účelné připravit centrálně. Plány migrace konkrétních služeb používaných určitým subjektem musí být připravovány ve spolupráci se subjektem.

- Po migraci všech služeb CMS 1.0 do CMS 2.0 se CMS 1.0 vypne. Pokud jeden uzel CMS 2.0 používal lokalitu CMS 1.0, dojde k přemístění uzlu do uvolněné lokality.

Dodavatel zohlední navrhovanou metodu migrace při návrhu konkrétních řešení v technickém projektu CMS 2.0.

Migrace se bude týkat přibližně 120 subjektů, 350 VPN a 2000 používaných služeb v CMS 1.0.

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

10. Seznam pojmů a zkratek

AAA	Authentication, Authorization, Accounting. Autentizace, autorizace, účtování.
AES	Advanced Encryption Standard. Symetrická šifra.
Agregace linek	Spojení několika komunikačních linek do jednoho komunikačního kanálu za účelem získání kanálu s vysokou kapacitou.
AIFO	Agendový identifikátor fyzické osoby. Tento údaj je jednoznačně přiřazen fyzické osobě a slouží pro její identifikaci pro účely jedné agendy.
AIS	Agendový informační systém, viz Zákon 111/2009 Sb.
AISEO	AIS evidence obyvatel.
AISCIS	Ais cizinců.
alert	Upozornění na určitou událost.
API	Application Programming Interface. Programové aplikační rozhraní.
ASBR	Autonomous System Boundary Router. Hraniční směrovač.
ATAC	Advanced Technical Assistance Center
Autentizace	Ověření identity určitého subjektu - osoby nebo zařízení.
Autorizace	Udělení oprávnění k vykonání nějaké operace nebo akce.
Backup	Zálohování, záloha.
Bezpečnostní událost	Výskyt takových příznaků, které mohou znamenat ohrožení bezpečnosti aktiv informačních nebo komunikačních systémů.
Bezpečnostní incident	Událost, která skutečně znamená ohrožení bezpečnosti aktiv informačních nebo komunikačních systémů. Jde o narušení bezpečnostní politiky nebo bezpečnostních opatření.
BGP	Border Gateway Protocol. Směrovací protokol.
Billing	Evidence nákladů na provoz CMS 2.0 a jeho částí.
CA	Certifikační autorita. Subjekt určený k vydávání certifikátů veřejných klíčů.
Captive portal	Portál (webová stránka) pro identifikaci a autentizaci uživatele.
CERT	Computer Emergency Response Team. Skupina osob určená pro řešení bezpečnostních incidentů.
Certifikační politika	Dokument definující podmínky, za kterých CA vydává certifikáty.
Certifikát	Digitální struktura obsahující veřejný klíč podepsaný certifikační autoritou.

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

CMS	Centrální místo služeb. CMS 2.0 je druhá generace. Základní prvek komunikační infrastruktury veřejné správy.
CRL	Certificate Revocation List. Seznam odvolaných certifikátů.
CzechPoint	Český podací ověřovací informační národní terminál.
ČR	Česká republika
ČSN	Česká státní norma
DB	Databáze
DC	Datové centrum
DDOS	Distributed Denial of Service. Distribuovaný útok na odmítnutí služby.
diffserv	Systém klasifikace síťového provozu.
DMZ	Demilitarizovaná zóna. Vyčleněný segment sitě s určitou úrovní bezpečnosti.
DNS	Domain Name System. Systém překladu jmen na IP adresy a naopak.
Dodavatel	Česká pošta s.p., odštěpný závod ICT služby
DOS	Denial of Service. Útok na odmítnutí služby.
DWDM	Dense Wavelength Division Multiplexing. Technika multiplexování na optickém vlákně, umožňující sdílet vlákno vice komunikačními kanály.
EDNS	Protokol pro přenos DNS informací. Jde o rozšíření protokolu DNS.
eGON	Elektronizace veřejné správy sledující zefektivnění fungování státní správy a místní samosprávy a zjednodušení výkonu služeb veřejné správy.
ESX	VMware ESX je operační systém firmy VMware umožňující virtualizaci serverů.
EU	Evropská unie
ESB	eGON Service Bus.
Filtrace provozu	Prověřování odesilatele a příjemce komunikace a povolení komunikace pouze mezi povolenými subjekty.
Firewall	Zařízení určené k řízení a filtraci provozu.
Gbps	Gigabits per second. Rychlost přenosu v gigabitech za sekundu.
geocluster	Geografický cluster. Tj. geograficky rozprostřená skupina spolupracujících a vzájemně se zálohujících počítačů.
hosting	Poskytnutí fyzických prostor, počítačů pro aplikace apod.
HTTP, HTTPS	Hypertext Transfer Protocol / Secured. Internetový protokol určený původně pro výměnu hypertextových dokumentů ve formátu HTML a dalších. HTTPS je bezpečnější verzí HTTP, která umožňuje přenášená data šifrovat.

HW	Hardware. Technické vybavení.
Hyper-V	Hyper-V je operační systém firmy Microsoft umožňující virtualizaci serverů
Identifikace	Zadání identity určitého subjektu - osoby nebo zařízení.
IDS	Intrusion Detection System. Systém pro detekci narušení bezpečnosti.
IEC	International Electrotechnical Commission. Mezinárodní organizace vydávající standardy.
IKE	Internet Key Exchange. Protokol používaný v IPSec pro ustavení šifrovaného spojení.
Inspekce provozu	Prověřování obsahu datové komunikace.
ISDS	Informační systém datových schránek.
IPS	Intrusion Prevention System. Systém pro prevenci narušení bezpečnosti.
IPSec	Bezpečnostní rozšíření protokolu IP, umožňující šifrování a autentizaci každého paketu.
IPv4	Internetový protokol verze 4
IPv6	Internetový protokol verze 6
IS	Informační systém
ISO	International Organization for Standardization. Mezinárodní organizace pro standardizaci.
ISP	Internet Service Provider. Poskytovatel připojení do Internetu.
ISVS	Informační systém(y) veřejné správy
ISZR	Informační systém základních registrů
ITS NGN	Integrovaná telekomunikační síť. NGN je nová generace ITS.
IZS	Integrovaný záchranný systém
JIP	Jednotný identitiní prostor. Adresář uživatelů z veřejné správy.
KAAS	Katalog autentizačních a autorizačních služeb. Služby pro přístup k JIP.
KIVS	Komunikační infrastruktura veřejné správy
KS	Komunikační systém
LAN	Local Area Network. Lokální počítačová síť.
LDAP	Lightweight Directory Access Protocol. Protokol pro přístup k distribuovaným adresářovým službám.
Load Balancer	Zařízení pro vyvažování a rozdělování zátěže mezi několika propojenými výpočetními systémy.

malware	Počítačový program určený k narušení informační bezpečnosti systému nebo počítače.
MAN	Metropolitan Area Network. Rozlehlá počítačová síť v rámci města.
Metadata	Data popisující nějaká jiná data.
MPLS	Multiprotocol Label Switching. Protokol pro vytváření VPN.
MTA	Message Transfer Agent. Systém pro přenos elektronické pošty.
MV	Ministerstvo vnitra
NAT	Network Address Translation. Překlad adres. Pro IPv4 se používá jako bezpečnostní prostředek a prostředek snižující počet potřebných adres.
NetFlow	Protokol určený k monitorování síťového provozu na L3 OSI modelu.
NBÚ	Národní bezpečnostní úřad
NOC	Network Operation Center. Středisko pro řízení sítě (CMS).
NTP	Network Time Protocol. Protokol pro synchronizaci času zařízení přes počítačovou síť.
OOB	Out of Band (management). Nezávislý (vyhrazený) kanál pro správu.
OS	Operační systém.
OSI	Open Systems Interconnection. Model vrstev pro propojování počítačových sítí.
OSPF	Open Shortest Path First. Směrovací protocol.
OVS	Orgán veřejné správy je orgán vykonávající správu veřejných služeb a řídící veřejné záležitosti.
OVM	Orgán veřejné moci reprezentuje veřejnou moc a je oprávněn rozhodovat o právech a povinnostech fyzických a právnických osob.
Paket	Blok informací přenášených počítačovou sítí založenou na přenosech dat po blocích.
PKI	Public Key Infrastructure. Infrastruktura veřejného klíče.
Provisioning	Příprava a zřizování služeb.
PXE	Preboot Execution Environment. Technologie pro bootování počítačů z počítačové sítě.
Qos	Quality of Service. Kvalita služby.
RA	Registrační autorita. Subjekt určený k ověřování žádostí o certifikáty.
RADIUS	Protokol pro autentizaci, autorizaci a účtování.
Referenční údaj	Údaj vedený v základním registru, který zákon upravující vedení příslušného základního registru jako referenční údaj označuje.

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

Reverse proxy	Proxy server předávající požadavky na jiný server, který zastupuje.
SLA	Service Level Agreement. Dohoda o úrovni poskytování služeb
směrovač	Síťové zařízení provádějící směrování paketů na L3 OSI modelu.
SMTP	Simple Mail Transfer Protocol
snapshot	Snímek/stav systému/serveru v určitém okamžiku.
SNMP	Simple Network Management Protocol. Síťový protokol pro přenos a sběr dat pro potřebu správy sítě a jejích prvků.
SNMP trap	Zpráva oznamující protokolem SNMP, že ve sledovaném systému došlo k určité události.
SOAP	Simple Object Access Protocol. Protokol pro výměnu zpráv ve formátu XML.
SOC	Security Operation Center. Středisko pro řízení bezpečnosti.
SSO	Single Sign On. Jednotné přihlášení pro více systémů.
SSH	Secure shell. Program a protokol pro zabezpečenou komunikaci.
SSL	Secure Socket Layer. Protokol pro zabezpečení komunikace šifrováním a digitálním podpisem.
sTESTA	Počítačová síť EU.
SW	Software. Programové vybavení.
syslog	Protokol pro zasílání krátkých textových zpráv. Využívá se pro správu systému a bezpečnostní auditing.
SZR	Správa základních registrů
TACACS	Protokol pro komunikaci s autentizačním serverem.
TCP	Transmission Control Protocol. Protokol zajišťující přenos dat (transportní vrstva).
TT	Trouble ticket.
UDDI	Universal Description Discovery and Integration. Univerzální adresář obsahující seznam a popis dostupných webových služeb.
UDP	User Datagram Protocol. protokol zajišťující přenos dat (transportní vrstva).
ÚOOÚ	Úřad pro ochranu osobních údajů
VLAN	Virtual Local Area Network. Virtuální lokání síť.
VPN	Virtual Private Network. Virtuální privátní síť.
VRF	Virtuální směrovací instance
WAN	Wide Area Network. Počítačová síť pokrývající rozlehlé území.

WMI	Windows Management Instrumentation. Rozhraní pro správu systémů Microsoft Windows.
WS	Web Service. Webová služba.
WSDL	Web Services Description Language. Jazyk určený k popisu webových služeb
XML	Extensible Markup Language. Rozšiřitelný značkovací jazyk
Zadavatel	Ministerstvo vnitra České republiky
ZIFO	Zdrojový identifikátor fyzické osoby. Jde o neveřejný identifikátor, který jednoznačně identifikuje fyzickou osobu v ZR.
Zónový přenos	Přenos všech DNS záznamů určité domény.
ZR	Základní registr(y)

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" Registrační číslo projektu: CZ.1.06/1.1.00/03.05995 je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.