AUTOCONT

STUDIE PROVEDITELNOSTI VÝMĚNY SERVEROVÉ INFRASTRUKTURY.

vímejak

AUTOCONT

ZÁKLADNÍ INFORMACE O DOKUMENTU

Název projektu	**Studie proveditelnosti výměny serverové infrastruktury**

Pozměňovací návrhy

Datum	Verze	Popis	Autor
27.2.2018	0.9	poslední pracovní verze	Kolektiv autorů (P. Zapadlo, Tomáš Kadlčík)

AUTOCONT

OBSAH

1. ÚČEL DOKUMENTU

Tento dokument obsahuje popis stávajícího stavu ICT ve společnosti Město Hranice. Shrnuje popis aktuálního stavu používaných prostředků informačních a komunikačních technologií, především serverové části pro potřeby návrhu obměny zastaralého vybavení. Obsahuje pohled bezpečnostní a licenční tak, aby návrh odstraňoval systémové chyby vzniklé v minulosti.

1.1. MANAŽERSKÉ SHRNUTÍ

V dokumentu je nastíněn aktuální stav IT prostředí na úřadu města Hranice. Ukazuje se, že serverová infrastruktura zajišťující provoz klíčových aplikací již neodpovídá aktuálním potřebám jak po stránce potřebného výkonu, tak je její provoz značně nákladný.

Dokument rozebírá aktuální stav a navrhuje konfiguraci pro novou serverovou infrastrukturu. Dále posuzuje stav aktivních prvků LAN, jejich doplnění a výměnu přístupových prvků v další etapě konsolidace stavu IT na úřadě. Taktéž se zamýšlí nad stavem bezpečnosti a pro navrhované projekty doporučuje zapracování změn vedoucích ke zvýšení úrovně bezpečnosti.

Dalším projektem, který je potřeba řešit je výměna zálohovacího prostředí, který používá a i v budoucnu bude používat komponenty z předchozího projektu technologického centra. Tyto již přesluhují a v krátké budoucnosti bude nutné je vyměnit pro zachování bezpečnosti dat.

2. POPIS STÁVAJÍCÍHO STAVU

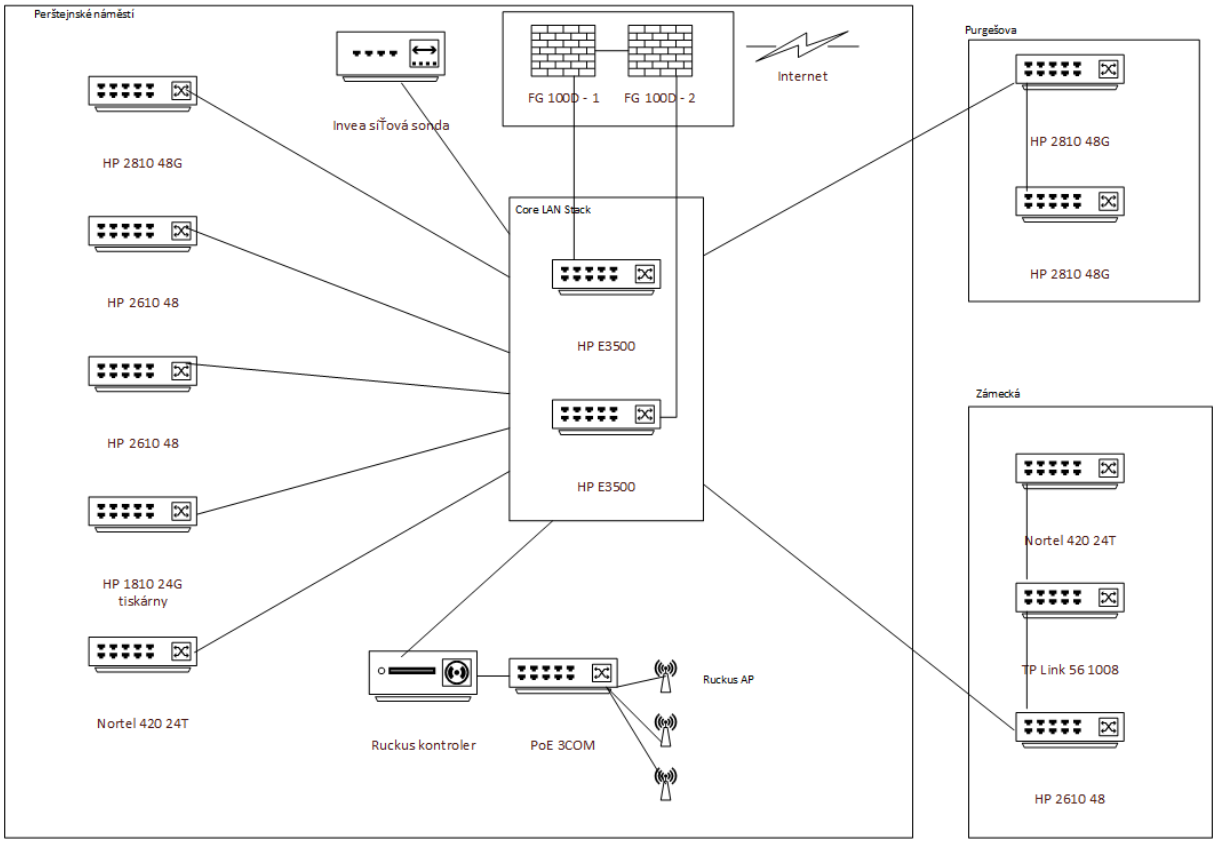
2.1. SEZNAM SÍŤOVÝCH ZAŘÍZENÍ

Typ zařízení	Počet	Vyžaduje nákup licence Windows CAL	Poznámka
Uživatelská PC	155	Ano, User CAL	
Síťové skenery	2	Ne	
Síťové tiskárny	32	Ne	
Docházkové terminály	3	Ano, Device CAL	
Platební terminály	3	Ne	
Wifi systém	7	Ne	1 kontroler, 6 AP
NAS	2	Ano, Device CAL	
Síťová sonda	1	Ne	
Firewall	2	Ne	
PC řidičské průkazy	8	Ano, Device CAL	
Vyvolávací systém	2	Ne	
Diskové pole	2	Ne	
Záložní zdroj	1	Ne	
Celkem	220	155 Windows User CAL, 13 Device CAL	

2.2. SÍŤOVÁ INFRASTRUKTURA

2.2.1. SCHÉMA TOPOLOGIE

Schéma sítě:



Ve schématu síťové topologie nejsou zahrnuty lokální malé switche, které jsou rozmístěny v kancelářích v blízkosti uživatelských stanic tam kde není dostatek kabelů.

2.2.2. AKTIVNÍ PRVKY LAN

Počet a typy aktivních prvků

Typ	Umístění	Počet	
HP 3500yl 24G	Perštejnské náměstí	2	Core
HP1810-24G	Perštejnské náměstí	1	Tiskárny
3COM Office connect POE 8	Perštejnské náměstí	1	Wifi AP
HP 2810-48G	Perštejnské náměstí	1	
HP 2610-48	Perštejnské náměstí	2	
Nortel Networks BayStack 420-24T	Perštejnské náměstí	1	
HP 2610-48	Zámecká	1	
Nortel Networks BayStack 420-24T	Zámecká	1	
TPLINK SG – 1008	Zámecká	1	
Switche	Purgešova	2	

Celkem			

2.2.3. FIREWALL

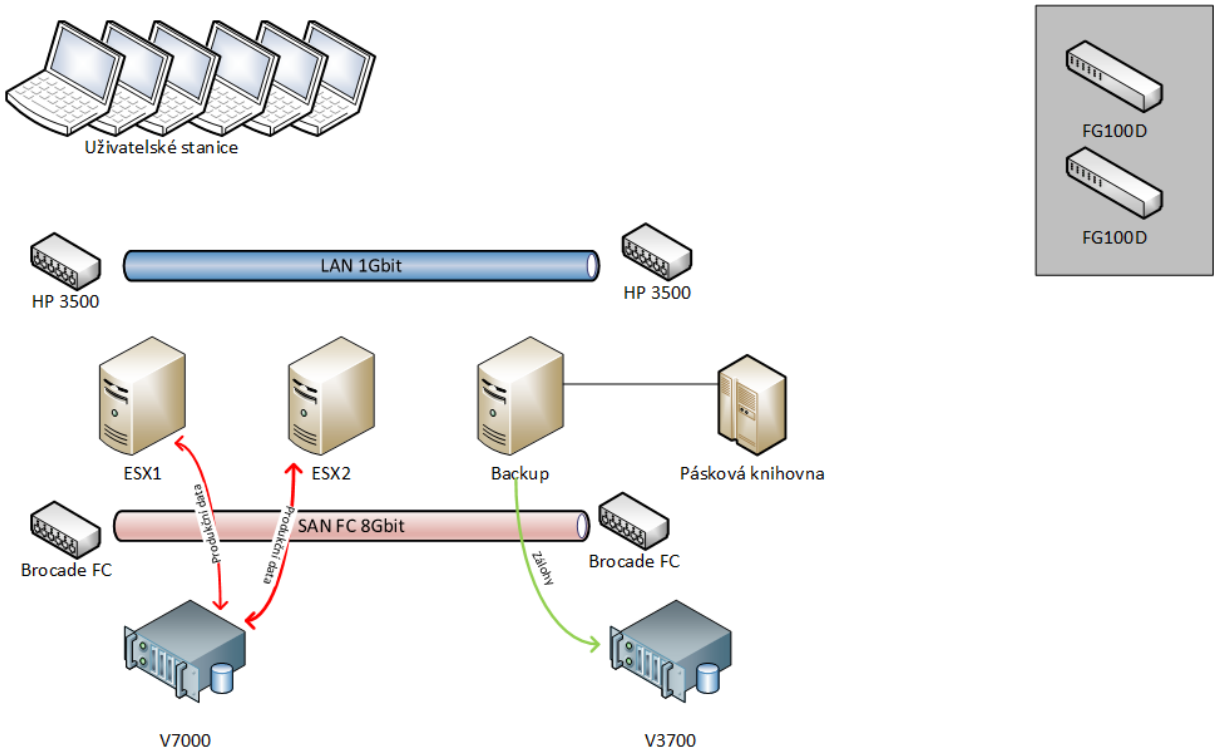
Perimetr sítě je chráněn dvojicí Fortigate FG100D zapojené ve vysoce dostupném clusteru. Tyto FW jsou zakoupeny včetně bezpečnostního balíku UTM a běží platná podpora do července roku 2018. (rok pořízení 2015).

2.3. SERVEROVÁ INFRASTRUKTURA

2.3.1. TOPOLOGIE

Současná infrastruktura byla pořízena na konci roku 2011 v rámci projektu TC ORP.

Schéma:



Základem je virtualizační prostředí existující na dvou serverech IBM x3690X5, které sdílí diskové pole IBM Storwize V7000. Pole je se servery propojeno pomocí dvou FC switchů Brocade redundantním způsobem. FC switche a propoje jsou na rychlosti 8Gbit/s. Na druhou stranu směrem do LAN a ke klientům komunikují servery pomocí 4portů 1Gbit ethernet, které jsou zapojeny do dvojice core switchů HP ProCurve 3500.

Servery x3690X5 a switche brocade jsou již mimo podporu výrobce a tento již neumožňuje její prodloužení.

Na diskové pole V7000 je podpora výrobce dokoupena a bude platná do konce roku 2018. Nicméně další prodlužování podpory se zdá být neekonomické a je vysoce nákladné.

Virtualizace je založena na technologii Vmware a momentálně je instalována verze 6.0. Město Hranice si platí podporu, která umožňuje využívání aktuálních verzí. Použitý HW však přestává být v nových verzích podporovaný a hrozí riziko nutnosti setrvání na instalované staré verzi.

2.3.2. ACTIVE DIRECTORY A OS VM

Město Hranice používá licence Microsoft Windows Server 2008 R2 Datacenter. Doménové kontrolery jsou 2 (Meu01 a MeuDC02), level AD je 2008.

Konec podpory této verze Windows Serveru je oznámen na 14.1.2020. Od tohoto data nebudou pro tuto verzi serverového operačního systému dostupné žádné bezpečnostní opravy a jeho použití v produkčním prostředí bude krajně nevhodné a nebezpečné.

2.3.3. ZÁLOHOVÁNÍ DAT

V roce 2015 zakoupilo Město Hranice licenci zálohovacího systému Veeam Backup&Replication essentials Standard pro celkem 4 CPU, která pokryla virtualizační platformu, na které je provozováno produkční prostředí úřadu. Primární záloha na disk je ukládána na diskové pole Storwize V3700 zakoupené v rámci projektu v roce 2015. Toto pole je umístěno v jiné budově. Sekundární záloha je směrována na páskovou knihovnu osazenou LTO5 mechanikou. Zálohování je realizovováno ze samostatného HW backup serveru, který společně s knihovnou je již mimo podporu výrobce a tudíž na něj nejsou dostupné náhradní díly. Na backup serveru je instalovaný OS Windows Server Standard 2008 R2. Na SW Veem B&R Essentials Standard je placena podpora, takže úřad má právo používat poslední dostupné verze a licence je tak využitelná i v novém prostředí.

2.3.4. VÝKONOVÝ AUDIT STÁVAJÍCÍHO STAVU

Seznam virtuálních serverů (VM):

Guest VM Name	Hypervi-sor	OS	Used Me-mory	Provisi-oned Me-mory	Virtual CPU	Virtual Disk Size	Is Running
MeuIT	esxi2	WS 2008 R2 (64-bit)	1.00 GB	4.00 GB	2	60.00 GB	Yes
Meu01	esxi2	WS 2008 R2 (64-bit)	204.00 MB	4.00 GB	2	180.00 GB	Yes
MeuIntraDoc	esxi2	WS 2008 R2 (64-bit)	450.00 MB	4.00 GB	2	60.00 GB	Yes
MeuDC02	esxi2	WS 2008 R2 (64-bit)	163.00 MB	4.00 GB	2	75.00 GB	Yes
MeuSQL	esxi1	WS 2008 R2 (64-bit)	2.56 GB	8.00 GB	4	1.03 TB	Yes
MeuGinis	esxi1	WS 2008 R2 (64-bit)	245.00 MB	4.00 GB	2	130.00 GB	Yes
vCenter Server	esxi1	SUSE Linux 11 (64-bit)	3.28 GB	8.00 GB	2	114.39 GB	Yes
Monitoring	esxi2	SUSE Linux 10 (32-bit)	204.00 MB	4.00 GB	2	320.00 GB	Yes
MeuWorkspace	esxi2	WS 2008 R2 (64-bit)	614.00 MB	4.00 GB	2	360.00 GB	Yes
MeuApl	esxi1	WS 2008 R2 (64-bit)	409.00 MB	4.00 GB	2	70.00 GB	Yes
MailKerio	esxi1	WS 2008 R2 (64-bit)	1.20 GB	4.00 GB	2	510.00 GB	Yes
MeuMP	esxi2	WS 2008 R2 (64-bit)	307.00 MB	6.00 GB	2	60.00 GB	Yes

Tem-plate_W2008R2_Data-center_EN	esxi1	WS 2008 R2 (64-bit)	4.00 GB	4.00 GB	2	60.00 GB	No
MeuGinisExt	esxi1	WS 2008 R2 (64-bit)	204.00 MB	4.00 GB	2	60.00 GB	Yes
MeuSSL (MeuTFAM)	esxi2	WS 2008 R2 (64-bit)	163.00 MB	4.00 GB	2	160.00 GB	Yes
MeuFS	esxi1	WS 2008 (32-bit) (32-bit)	430.00 MB	3.00 GB	2	110.00 GB	Yes
MeuTAM	esxi2	WS 2008 (32-bit) (32-bit)	163.00 MB	4.00 GB	4	100.00 GB	Yes
Fenix	esxi2	WS 2008 R2 (64-bit)	450.00 MB	4.00 GB	2	60.00 GB	Yes
off MeuFTP	esxi1	WS 2008 R2 (64-bit)	4.00 GB	4.00 GB	4	60.00 GB	No
MeuDC01	esxi1	WS 2008 R2 (64-bit)	245.00 MB	4.00 GB	2	75.00 GB	Yes
tmapy-ext	esxi2	CentOS 4/5/6/7 (64-bit)	40.00 MB	4.00 GB	2	200.00 GB	Yes
T-WIST	esxi1	RHEL 6 (64-bit)	81.00 MB	4.00 GB	2	350.00 GB	Yes
MeuRadar	esxi1	WS 2008 R2 (64-bit)	245.00 MB	4.00 GB	2	310.00 GB	Yes

Operační paměť:

Oba virtualizační servery mají instalovano 48GB RAM, tj v součtu je dostupné 96GB operační paměti. Virtuální servery mají alokováno 91,26GB Ram – tj zbývá velmi málo volné paměti. Navíc je alokován plný rozsah paměti, tj při výpadku jednoho z fyzických virtualizačních serverů není možné havarované VM spustit na přeživším esxi serveru. Tj, prakticky není vysoká dostupnost funkční.

CPU:
Stávající server x3650 jsou osazeny 2x E6540 (6Core, 2GHz) každý, tj k dispozici je 48 NetCPU cyklů (GHz), špička za sledované období je 32,5% (14,8GHz). Přiděleno je celkem 52vCPU, tj virtualizační poměr je 2,17:1 (vCPU: Core).

Storage:
Sdílený storage V7000 disponuje celkovou kapacitou 6,5TB dat a z toho je 17,9% volného místa (1,16TB). Výkonové špičky se objevují především v okamžicích zálohy a v těchto okamžicích překračují hodnotu 3400 IOPs. V běžném provozu je průměrná zátěž 661IOPs, při poměru 60% čtení, 40% zápis.

Průměrná čtecí latence je cca 2,85ms a zápisová 0,36ms. Tyto hodnoty systém překračuje především při zálohách, kdy se latence šplhají k 50ms pro zápis i čtení.

Průměrný datový tok v produkční dobu je do 50MB/s, výše se šplhá především v zálohovacích špičkách, kdy dosahuje cca 150MB/s. Při vytváření a zapracovávání snapshotu se datový tok pohybuje kolem 450Mb/s.

LAN:

Servery jsou připojeny každý 4x 1Gbit ke core switchům, přičemž celková datová propustnost se v zálohovacích špičkách pohybuje kolem 1Gb/s, běžném provozu se špičky propustnosti LAN šplhají max ke 100Mbit/s.

2.4. BEZPEČNOSTNÍ ZHODNOCENÍ SOUČASNÉHO STAVU

LOGICKÁ STRUKTURA SÍTĚ

Základní rozdělení síťové infrastruktury počítá s možností dalšího členění podle potřeby, která v budoucnu vyvstane. Prozatím je struktura dělena na VLANy podle využití provozu, tedy na

bezdrátovou síť, tiskové úlohy, serverovou VLAN a zbytek je ponechán v jedné velké uživatelské VLAN. Zde by bylo možné a vhodné provést rozdělení uživatelské VLANy jednak podle lokalit a jednak podle logických celků nebo odborů.

Účelem tohoto opatření je usnadnění správy, monitoringu a troubleshootingu. Dále pak omezením přístupu a rozbitím tak velké kolizní domény dojde ke snížení dopadu udeřivších kybernetických hrozeb (omezení rozsahu botnetu, omezení šíření nákazy ze zavirovaného zařízení).

Bezdrátová síť je z pohledu členění dostatečně strukturovaná a z pohledu dalšího rozvoje ji nepovažujeme za prioritu, řešení kontroleru Ruckus je postačující pro současnou potřebu.

OCHRANA PERIMETRU SÍTĚ

Internetová konektivita je zajištěna jednou linkou bez zálohy. Linka je terminovaná na výkonném firewallu Fortinet FG100D, který je zdvojen pro zajištění vysoké dostupnosti. Toto řešení není v současnosti aktivováno a přepínání je nastaveno v manuálním režimu, který vyžaduje přítomnost obsluhy na místě. Pro tento případ doporučuji provést update firmware na obou zařízeních na stejnou verzi a nastavit automatické přepínání.

Další používanou funkcí na firewallu je IPS inspekce provozu na vnějším rozhraní, kterou lze podle potřeby rozšířit i na jednotlivé segmenty vnitřní sítě. Stejné rozšíření pak bude možné aplikovat i pro rozsah analyzovaného síťového provozu pomocí služby cloudového Analyzeru Fortinetu, který je v současné době aplikován a funkční.

Z dalších služeb FG100D lze zmínit sandboxing a spamfilter, které jsou využívané.

Jediným doporučením je tak rozšíření logování a jeho centralizace do společného úložiště pro využití při šetření bezpečnostních incidentů a forenzní analýzu chování sítě.

MONITORING SÍŤOVÉHO PROVOZU

Infrastruktura je osazena FlowMon sondou pro sledování datového toku. Sonda je využívána příležitostně při řešení jednotlivých případů, její potenciál tak není plně využit při předcházení kolizí nebo zvýšených zátěží sítě.

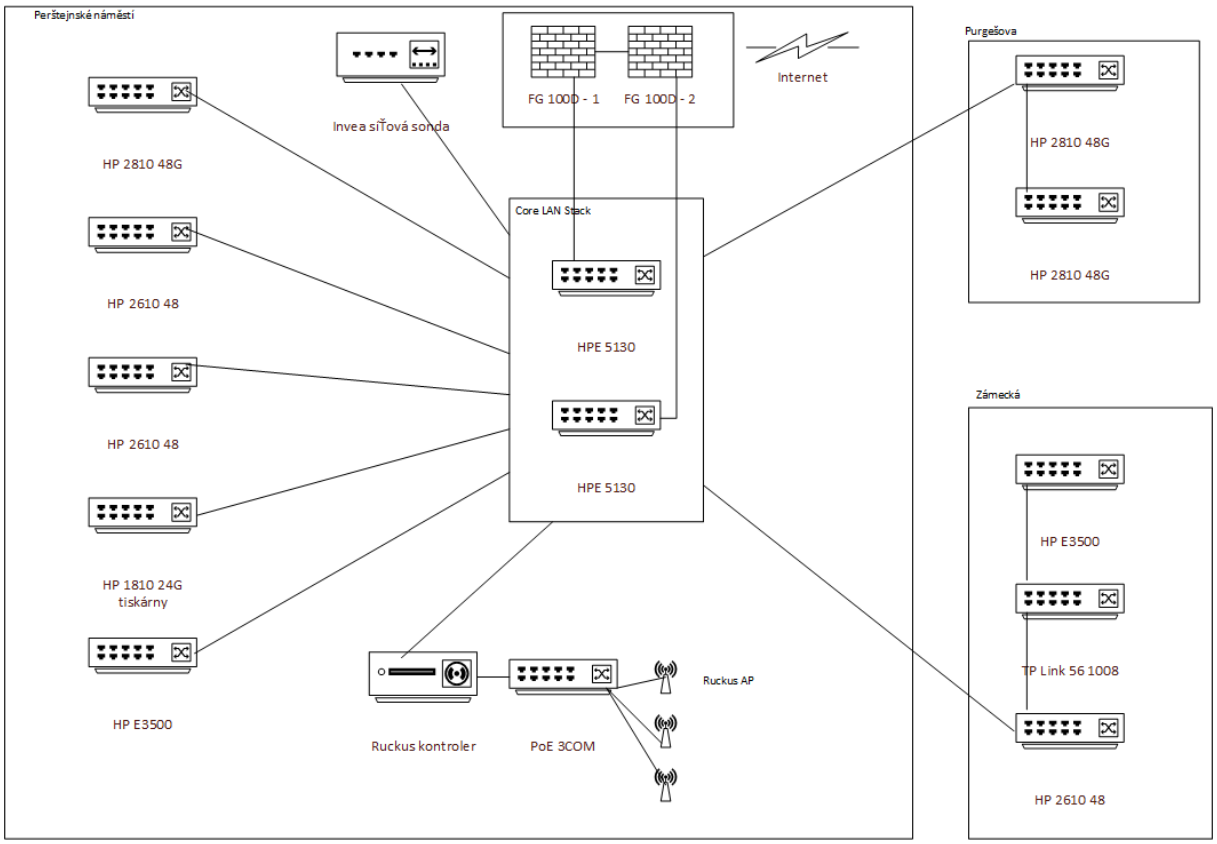
Povaha provozu Městského úřadu je relativně stabilní zátěž bez náhlých špiček provozu.

Občasné použití FlowMon sondy je možné, avšak nedá se říci, že efektivní.

3. NÁVRH CÍLOVÉHO STAVU

3.1. SÍŤOVÁ INFRASTRUKTURA

3.1.1. SCHÉMA TOPOLOGIE



V topologii je změna na úrovni core, kde proběhne výměna zastaralých E3500 za switche HPE 5130, které jsou vybaveny i 10Gbit porty potřebnými pro propojení serverů. Stávajícími E3500 lze nahradit nejstarší Nortel switche.

3.1.2. AKTIVNÍ PRVKY LAN

Stávající switche jsou generačně poměrně zastaralé, poslední větší obměna proběhla v roce 2009, kdy úřad zakoupil základ stávajícího systému. Většina aktivních prvků je sice pod podporou výrobce (doživotní HP), tohle se však netýká nejstarších switchů Nortel. Použité aktivní prvky jsou však zastaralé a nezvládají moderní technologie. Nadpoloviční většina portů je pouze 100Mbit což má dopady i do produktivity práce koncových uživatelů. Vzhledem ke stáří provozovaných aktivních prvků je jejich další použití v core LAN prakticky vyloučené. Pro potřeby nové infrastruktury je nutné v rámci projektu pořídit dvojici nových core prvků, které poskytnou dostatečný výkon pro budoucí období (10Gbit porty), ale také budou poskytovat základ na kterém lze stavět provozní a bezpečnostní technologie.

V souvislosti s výměnou core LAN je třeba zvážit realizaci projektu, který posoudí aktuální stav topologie a segmentace sítě a navrhne úpravy interní LAN úřadu, aby tato mohla plnit požadované funkce. Změny jsou nezbytné nejen z provozního hlediska, kdy se řeší mimo jiné problémy s nedostatkem adres, portů a přípojných míst, ale také z bezpečnostního hlediska, kdy stávající topologie je příliš otevřená a neodděluje jednotlivé skupiny zařízení a uživatelů což má za následek výrazně větší riziko při bezpečnostních incidentech. (například při nákaze ransomware)

Taktéž stávající aktivní prvky neumožňují nasazení technologií, které zajišťují bezpečnost a auditovatelnost dat a přístupů k nim, přičemž je jasné, že tyto technologie budou povinné. Výskyt drobných nekonfigurovatelných switchů „pod stoly“ u uživatelů v sobě nese riziko nejen neoprávněného přístupu do sítě, ale především funkčních poruch – omylem propojený kabel do smyčky způsobí úplné a náhlé selhání kompletní LAN úřadu. Přičemž této poruše nejde na switchi bez možnosti managementu jakkoliv předejít.

3.1.3. FIREWALL

Vzhledem ke končícímu předplatnému na bezpečnostní funkce (a záruky HW) doporučujeme prodloužit toto předplatné na další období. Pro bezpečný provoz a maximální účinnost je nutné dbát aktualizace obou firewallových boxů v co nejčastějších intervalech.

Dále doporučujeme provést detailní analýzu nastavených pravidel a reimplementaci bezpečnostního modelu v souvislosti s novou situací a pro odstranění zapomenutých a již nevyužívaných prostupů přes fw.

Následným doporučením je rozšíření logování a jeho centralizace do společného úložiště pro využití při šetření bezpečnostních incidentů a forenzní analýzu chování sítě.

3.2. SERVEROVÁ INFRASTRUKTURA

Aktuální spotřebu základních serverových zdrojů ukazuje následující tabulka:

Zdroj	Spotřeba
RAM	91GB
CPU	48GHz
Kapacita storage	6,5TB
Propustnost storage	3400 IOPs
Propustnost LAN	1Gb

Pro návrh nové infrastruktury je třeba tyto parametry modifikovat s ohledem na nasazení nových verzí OS, aplikací, SQL … Dále je třeba dimenzování provést s ohledem na budoucí růst, odhadnout budoucí potřeby.

CPU:

Návrh CPU musí zohledňovat nejen potřebný procesorový výkon, ale i také licenční pohled – především klíčové licence produktů firmy Microsoft jsou vázány na počty jader. Proto doporučujeme maximálně 8 jádrové CPU tak aby v každém serveru bylo max 16 core. (pod tento počet cena licence již neklesá). Pro maximální CPU výkon dvojici Intel Gold 6144 do každého serveru (8 core, 3,5GHz základní takt). V případě cenové optimalizace využít do každého serveru 1x Gold 6132 (14core, 2,6Ghz základní takt)

Výkon:

4x Gold 6144 bude 112 NetCPU GHz (2,33 násobek stávajícího prostředí)

2x Gold 6132 bude 72,8 NetCPU Ghz (1,51 násobek stávajícího prostředí)

RAM:

Současná RAM je nejužším místem, dostupné je 2x 48GB, tj 96GB, přičemž je přiděleno více než 90GB. Tohle zásadním způsobem omezuje vysokou dostupnost jinak korektně navrženého prostředí. Navíc při pohledu do tabulky VM je zřejmé, že je přiděleno jednotlivým VM paměť na dolní hranici doporučované hodnoty. V případě aktualizace OS na současné verze (WS 2016) se zvedne bazální spotřeba paměti asi na dvojnásobek, s ohledem na budoucí potřeby je vhodné dimenzovat na cca 3x stávající spotřeby. Aby nebylo porušeno pravidlo vysoké dostupnosti, je nutné tuto paměť mít dostupnou na obou virtualizačních serverech, tj každý server by měl mít minimálně 300GB RAM. Navržené CPU disponují 6 kanály, tj každý server musí být osazen 12x 32GB RAM moduly, výsledná kapacita bude tedy 384GB RAM na každém serveru.

Storage:

Aktuální spotřeba diskového prostoru je 6,5TB, stejně jako v případě pamětí, pouhou změnou verze serverového OS ve VM dojde k navýšení spotřeby diskového prostoru. Tuto zvýšenou potřebu odhadujeme na cca 1,3násobek stávajícího prostoru, tj cca 8,45TB. Při výhledu zvýšení kapacity dat o 15% ročně vychází potřebná kapacita na konci 5letého období takto:

Období	Potřebná kapacita
2018	9,71TB
2019	11,16TB
2020	12,83TB
2021	14,75TB
2022	16,96TB
2023	19,50TB

Diskový prostor na konci období by tedy měl mít kapacitu cca 19TB. Vzhledem k vývoji kapacit disků a především SSD může být výhodné zakoupit kapacity na polovinu období udržitelnosti a kolem roku 2021 tuto rozšířit. V té době budou ještě nakoupené servery plně podporované a nové větší disky budou pro ně dostupné a zároveň tyto budou cenově výhodné.

Na současné infrastruktuře diskový subsystém není úzkým místem – i z důvodu tieringu na SSD vrstvu. Tato je však velmi malá vůči celkové kapacitě (200GB versus 6,6TB). Doporučujeme tento poměr posunout na minimálně 0,3:1 lépe 0,5:1. Dále využít koncepci, která umožňuje využití NVMe disků, které mají výrazně menší latence ve srovnání s klasickou topologií SAS/SATA.

LAN:

Současné core prvky LAN a servery jsou propojeny linkami 1Gbit a i když se zdá, že i při maximální zátěži je tato rychlost dostatečná - zvlášť v situaci, kdy každý server je připojen 4 linkami, přesto s ohledem na technologický rozvoj, cenu 10Gbit komponent a snížení síťových latencí doporučujeme výměnu core switchů za současné moderní s možností alespoň 4x 10Gbit linků na switch a to s možností stohování. Pokud realizují switche stohováním přes porty, doporučujeme aby každý switch měl minimálně 6 portů 10Gbit.

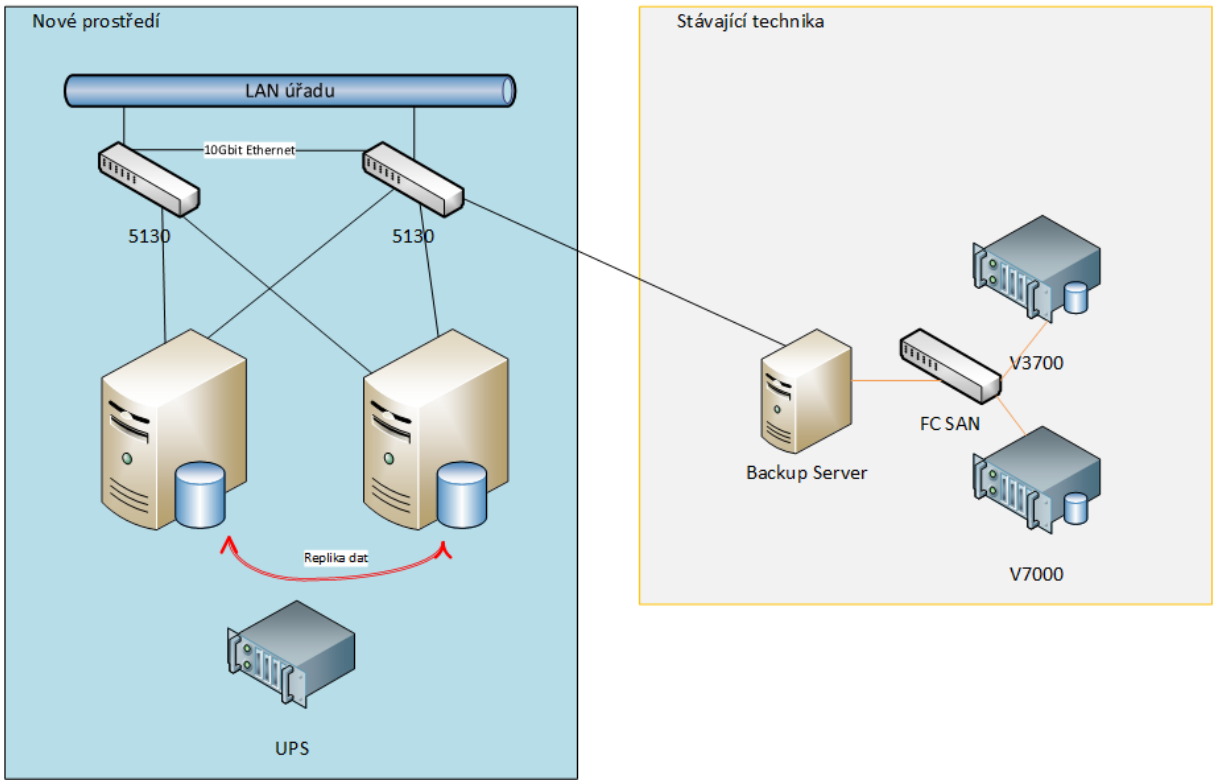
3.2.1. TOPOLOGIE

Trendy současného rozvoje IT infrastruktury jdou cestou hyperkonvergovaných řešení, které integrací storage části a virtualizační části dosahují zajímavých ekonomických nákladů nejen na pořízení ale i na provoz a následné udržování takovéto technologie.

Výhody hyperkonvergované infrastruktury:

- Množství HW je minimalizováno a je běžný komoditní
- Rozšiřování řešení v budoucnu je levné a dostupné
- Prodloužení podpory výrobce je levné, protože nezahrnuje specializované technologie
- Možnost použití NVMe disků pro velmi vysoký výkon
- Měnit nezávisle HW a SW
- Vyšší bezpečnost dat, protože tyto leží na 2 různých skupinách disků
- Možnost umístit servery do různých lokalit a mít tak i geografické oddělení dat.

Schéma takto postavené topologie s využitím stávajícího vybavení:



Základem jsou nové dva servery, které sdružují jak virtualizační výkon, tak i diskový prostor. Na těchto serverech je využita stávající licence hypervizoru VMware Sphere Esseintals Plus. Na úrovni hypervizoru je instalována vrstva diskové virtualizace, která zajišťuje replikaci dat mezi servery – odolnost storage proti výpadku jednoho ze serverů. Doporučujeme využít technologii, která umožňuje geoclustering – rozdělení serverů do různých serveren a zajištění provozu i v případě odstávky jedné ze serveroven. Jednou z možných technologií je HPE VSA software.

3.2.2. ACTIVE DIRECTORY

Stávající AD je provozována na úrovni 2008 a to na dvou doménových kontrolerech. Vzhledem blížícímu se konci podpory OS Windows Server 2008 je nutné doménové řadiče nainstalovat na novější verzi operačního systému a taktéž povýšit verzi AD na 2016. Dalším důvodem hovořící pro povýšení verze AD je neúplná podpora pro řízení současných verzí desktopových OS – Windows 10. Povýšení verze AD tedy bude nejen technologickým krokem, ale přinese i rozšířené možnosti ve správě koncových stanic.

Stávající podobu - pár doménových řadičů, z nichž každý využívá jiný virtualizační server doporučujeme zachovat.

3.2.3. ZÁLOHOVÁNÍ DAT

Zálohování jako klíčovou komponentu ochrany dat je třeba řešit komplexně a s ohledem robustnost a spolehlivost. Stávající topologii s dedikovaným backup serverem doporučujeme zachovat, protože umožňuje v případě velkých havárií výrazně zrychlit obnovu do provozního stavu. Vzhledem k finančním limitům bude nutné výměny dílčích částí serverové infrastruktury etapizovat. V prvním kroku je nutné vyměnit serverovou infrastrukturu a zachovat stávající backup server a datový prostor pro zálohy (Storwize V3700). Stávající pásková knihovna není již udržitelná v provozu a doporučujeme ji bez náhrady odstavit. Po přechodnou dobu bude tedy nutné provozovat stávající backup server, byť je už mimo podporu výrobce, takže využít náhradních dílů ze stávajících virtualizačních serverů.

Jelikož pásková knihovna je již prakticky nefunkční, je třeba vyřešit zálohování do vzdálené lokality pomocí protokolu, který je odolný proti zakryptování dat viry. Jednou z možností je využít partnerů provozujících Veeam Gateway a zálohovat do jejich cloudového prostoru. Zálohovaná data budou tedy mimo fyzické prostory úřadu, ale i mimo LAN se zabezpečeným přístupem. Cenu takto vytvořené off-site zálohy je třeba porovnat s nákupem páskové knihovny a vyhodnotit ekonomickou výhodnost toho kterého řešení.

Zálohy doporučujeme tedy realizovat tímto způsobem:

1. Primární záloha L1 na diskový prostor V3700 (serverovna zámecká)
2. Sekundární zálohu L2 směrovat na některý ze stávajících NAS
3. Terciální zálohu směrovat do cloudu.

Porovnání zálohování do cloudu versus pásková knihovna:

Cena zálohování do cloudu se stanovuje počtem VM a celkovým objemem dat. V cloudu se obvykle udržuje 2- 3 dny zpět. Při aktuálním množství VM a dat (20 VM, 8,45TB) bude průměrná měsíční cena cca 7490Kč bez DPH, zdroj www.accloud.cz).

Pásková mechanika bude mít pořizovací cenu cca 350 000Kč bez DPH (knihovna 24 pozic, 1x LTO7, 24pásek, 1x čistící, 5 let podpora).

Z uvedeného je zřejmé, že ceny obou přístupů se vyrovnají po 46 měsících. V ceně páskové knihovny nebyly zahrnuty náklady na obměnu pásek po určitém čase. (Doporučená výměna nejpozději po 2 letech).

Stávající SW Veeam lze výhodou využít i v dalším období. Za zvážení stojí povýšení licence z edice Standard na Enterprise. Toto povýšení umožní kvalitní průběžné zálohování SQL serverů bez dopadu na výkon a zachová velmi snadnou obnovu ke kterémukoliv průběžně odzálohovanému bodu. (Zálohu lze provádět i s periodou 15 minut). To umožní výrazně snížit ztrátu dat v případě havárie provozních technologií.

3.2.4. POPIS MIGRAČNÍCH PRACÍ

Výměna serverové infrastruktury je zásadní zásah do fungování interních (případně i externích) systémů úřadu. Velká část prací má kolizní charakter – po dobu práce na daném systému je tento nedostupný uživatelům, což přináší omezení pro plánování harmonogramu. Jelikož úřad využívá v produkci OS Windows 2008R2 jehož bezpečnostní podpora se blíží k závěru, je nutno v rámci výměny provést i povýšení OS v aplikačních serverech. Prakticky to bude znamenat postavit kompletně znova aplikační prostředí úřadu. Vzhledem k tomu, že většina aplikací používá a bude používat MS SQL jako svůj datový backend, je třeba implementaci provést s ohledem na maximální výkon a bezpečnost SQL dat. Nedílnou součástí implementačního projektu bude analýza zatížení SQL, nalezení úzkých míst, realizace opatření pro odstranění úzkých míst a doporučení aplikačním partnerům.

Práce lze rozdělit do několika oblastí:

- Základní infrastruktura, tato oblast připraví vlastní nové virtualizační prostředí a předpokládáme tyto činnosti:
    - Fyzickou montáž nového HW do rozvaděčů, propojení datové a napájecí
    - Instalace nových FW do dodávaných zařízení
    - Konfigurace CoreLAN switchů
    - Instalace a konfigurace virtualizačního prostředí
    - Instalace a konfigurace softwarově definované storage, návrh a příprava datových prostorů
    - Integrace s UPS a ověření korektního cyklu shutdown-start
    - Ověření vlastností infrastruktury – trhací testy (server/switch/LAN …)
- Příprava a realizace migrace aplikačního prostředí na novou verzi OS:
    - Příprava šablony OS s nově dodanou licencí W2016
    - Ověření stavu AD, instalace nových AD DC, připojení do domény Active Directory, odstranění původních AD DC, povýšení schématu domény na poslední verzi.
    - Příprava VM pro budoucí SQL server, instalace SQL
    - Příprava VM pro aplikační servery, součinnost s dodavateli aplikací pro přenos aplikací na nové VM.
- Práce související se zvýšením bezpečnosti a spolehlivosti prostředí:
    - Reinstalace stávajícího backup serveru, instalace prostředí Veeam, konfigurace zálohování, nastavení zálohování do cloud prostředí
    - Upgrade firmware ve firewallech FG100D
- Obecné práce související s projektem:
    - Dokumentace skutečného stavu díla
- Práce spojené s vyladěním výkonu klíčového SQL serveru:
    - Analýza zátěže nově instalovaného SQL server po převodu všech aplikací třetích stran na tento server
    - Realizace opatření a doporučení 3 stranám pro úpravu zátěže SQL.
- Zaškolení:

- Zaškolení pracovníků zadavatele na používání a monitoring nově dodaných technologií v předpokládaném rozsahu 8 hodin.

3.3. INFRASTRUKTURNÍ LICENCE

Neodmyslitelnou částí jakékoliv ICT infrastruktury jsou i patřičné licence. Pro případ Města Hranice se jedná o licence na těchto vrstvách:

1. Licence virtualizačního hypervizoru.
2. Licence pro serverové OS
3. Přístupové licence pro serverové OS
4. Licence zálohovacího software
5. Middlewarové licence (SQL server …)

1) Licence virtualizačního hypervizoru jsou klíčové pro výkon a spolehlivost infrastruktury. Město Hranice aktuálně používá VMware vSphere Essentials plus a platí si podporu, takže má nárok na nové verze. Proto doporučujeme využít stávající licenci (která je v rozsahu 3servery po 2 CPU a management server) a tuto přenést na nové prostředí.
2) Stávající licence jsou Windows Server 2008 Datacenter. Vzhledem k velmi blízkému konci podpory těchto licencí není prakticky možné využívat tyto licence i nadále. Vzhledem k počtu virtuálních serverů s Windows OS - 19ks je ekonomické využít na pokrytí edice Windows Server licence Datacenter. Tato licence umožňuje provozovat licenčně neomezený počet VM s OS Windows Server. Tyto licence jsou vázány na počet core použitých CPU, nicméně minimální počet je 16 core. Proto je HW konfigurace navrhována tak, aby HW nepřekračoval tento počet core na server a zbytečně tak neprodražoval použité licence.

   Tj. pro pokrytí navržené infrastruktury bude třeba celkem 32core Windows Server 2016 Datacenter. Tyto licence je možno zakoupit minimálně ve 2 režimech:

   - OEM – licence je vázána na zakoupené servery
   - OLP, případně Select – licence je přenosná.

   Serverová infrastruktura se obvykle pořizuje na 5 – 7 let a stejnou dobu má praktická použitelnost i sw pro operační systémy. Proto pořízení těchto licencí ve variantě OEM může být zajímavou ekonomickou variantou.
3) Problematika přístupových licencí serverového OS je poměrně komplikovaná, některé případy a situace jsou popsány zde:

   https://blogs.technet.microsoft.com/volume-licensing/2014/03/10/licensing-how-to-when-do-i-need-a-client-access-license-cal/

   V zásadě platí, že licenci potřebuje každý uživatel a zařízení, který využívá služby serverového OS. Nicméně, pokud je uživatel pokryt licencí, potom není nutné mít ještě (duplicitně) licenci na zařízení. Jestliže například na tiskárnu tisknou jen uživatelé pokrytí licencí, pak není třeba

pořizovat Device CAL na tiskárnu byť využívá serverový OS například pro získání adresy z DHCP. Vzhledem k charakteru uživatelů uvnitř úřadu lze říci, že licenčně nepokrytý uživatel se nebude vyskytovat a tudíž není potřeba tiskárny pokrývat samostatnými Device licencemi. S využitím této logiky byla vyplněna tabulka v kapitole 2.1 – tam kde dané síťové zařízení nemá interakci se serverem, nepředpokládáme nákup Device licence. Tam, kde zařízení má interakci se serverem, ale zároveň tuto zprostředkovávají uživatelé (nositelé user licence) rovněž nepředpokládáme nákup Device licence neboť ji pokryje uživatelská licence.

4) Aktuálně je využíván zálohovací SW Veeam B&R v licenční edici Standard a prodejním balíku Essentials. Celkem má městský úřad zakoupeny licence na 4 CPU včetně supportu, tj včetně práva na aktuální verze. Doporučujeme licence zachovat a přenést na novou infrastrukturu. V rámci projektu výměny technologického centra má smysl zvážit upgrade těchto licencí ze Standard -> Enterprise. Toto rozšíření licencí umožní výrazně kvalitnější práci se zálohami ukládanými na pásky a taktéž lepší aplikační zálohy a obnovy (například zálohy dat SQL serverů).
5) Pro mnohé aplikace, které městský úřad Hranice využívá, je třeba další pomocný SW. Například se jedná o SQL server, jež je úložištěm pro většinu agendových dat, které městský úřad zpracovává. Stávající verze je: SQL 2008 R2. Podpora této verze výrobcem končí 9.7.2019. Předpokládáme, že agendové aplikace budou tuto verzi podporovat kratší dobu, tj nejpozději letos bude nutné připravit novou verzi SQL pro klíčové aplikace. Zde je třeba respektovat politiku výrobce SQL serveru a licencovat SQL server s ohledem na provoz v HA prostředí.

3.4. BEZPEČNOSTNÍ OPATŘENÍ

LOGICKÁ STRUKTURA SÍTĚ

Doporučujeme logicky rozdělit síť na menší celky (nejlépe po odděleních), tyto menší celky dát do samostatných VLAN. Komunikaci potom omezit jen na VLAN-Servery a zakázat komunikaci mezi VLAN navzájem pro snížení možnosti šíření incidentů z jednoho počítače na druhý. Účelem tohoto opatření je usnadnění správy, monitoringu a troubleshootingu. Dále pak omezením přístupu a rozbitím tak velké kolizní domény dojde ke snížení dopadu udeřivších kybernetických hrozeb (omezení rozsahu botnetu, omezení šíření nákazy ze zavirovaného zařízení).
Tento přístup taktéž pomůže vyřešit problém s aktuálním nedostatkem IP adres ve vnitřní síti.

AKTIVNÍ SÍŤOVÉ PRVKY

Plánovaná výměna aktivních prvků sítě plně odpovídá požadavkům, které je potřeba plnit právě z důvodu zvýšení bezpečnosti celé infrastruktury.
Při postupné výměně doporučujeme zavést konfigurační bázi s informacemi o konfiguraci jednotlivých prvků, která v budoucnu usnadní a zjednoduší správu sítě. Dále pak nastavit systém zálohování konfigurací pro potřebu správy a výměny zařízení.

MONITORING INFRASTRUKTURY

Jako zásadní nevýhodu vidíme absenci stálého monitoringu sítě a dohledu nad jednotlivými prvky nebo segmenty. Příležitostné využití FlowMon sondy nebo FortiAnalyzeru je sice užitečné v případě řešení oddělených problémů, ale avšak nesystémové využití prostředků. Proto doporučujeme zřízení stálého dozoru nad IT prvky včetně dozoru nad úložišti a servery. Takto komplexně pojaté řešení umožní zvýšit

efektivitu celé infrastruktury, sníží zatížení lidí z oddělení IT a umožní jejich smysluplné využití. V současnosti se kapacita pracovníků soustřeďuje na následné řešení problémů a pokrytí provozních potřeb tzv. ex post, tedy až po projevení se následků. Smysluplným využitím monitorovacích nástrojů lze předcházet výpadkům a potížím s komunikací už v době, kdy se objevují první příznaky, že dochází ke zvýšení zátěže na jednotlivých portech switchů, k nestandardnímu provozu na celých větvích sítě apod.
Z pohledu kapacity lidí na oddělení IT, nasazením plného monitoringu celé infrastruktury a profylaktické aplikace výsledků by znamenala vyčlenění jednoho člověka na minimálně šest dnů v měsíci výhradně pro zpracování výsledků a přípravu opatření. Je tedy vhodné uvažovat, zda podobného výsledku nebude dosaženo využitím služby SOC, kde by monitoring byl jednou ze služeb celého komplexu bezpečnostních opatření.

3.5. NÁVAZNÉ PROJEKTY

Výměna serverové infrastruktury je prakticky úvodní částí konsolidace IT prostředí a je vhodné ji zařadit do dalších a návazných projektů:

- Výměna serverové infrastruktury – klíčový projekt, který připraví IT prostředí úřadu pro další období a umožní provoz a rozvoj služeb.
- Realizace bezpečnostních opatření – nasazením bezpečnostních technologií a služeb pro zvýšení odolnosti před riziky
- Konsolidace LAN infrastruktury – obnova HW a zvýšení bezpečnostní úrovně LAN prostředí úřadu.
- Výměna zastaralého zálohovacího prostředí – technologická obnova a zvýšení bezpečnosti dat uvnitř úřadu.

4. POUŽITÉ POJMY A ZKRATKY

Pojem / Zkratka	Popis
AC	AutoCont je česká soukromá společnost, která přes 25 let na českém a slovenském trhu úspěšně zavádí a provozuje užitečné informační technologie.
AD	Active Directory je implementace adresářových služeb firmou Microsoft pro použití v prostředí systému Microsoft Windows. Active Directory umožňuje administrátorům nastavovat politiku, instalovat programy na mnoho počítačů nebo aplikovat kritické aktualizace v celé organizační struktuře. Active Directory ukládá své informace a nastavení v centrální organizované databázi.
AD DC	Active Directory Domain Controler – server poskytující adresářové služby. Jeho funkce je klíčová pro přihlášení uživatelů a v síti jich může (mělo by být) více. Minimálně 2 běžící na různém HW.
AP	Access Point, přístupový bod (zařízení, ke kterému se klienti připojují v bezdrátové Wi-Fi síti)
broadcast	Broadcast je v informatice zpráva, kterou v počítačové síti přijmou všechna připojená síťová rozhraní. Pokud nDení síť vhodným způsobem rozdělena (na podsítě) nebo chráněna (firewallem), mohou broadcasty způsobit zahlcení sítě.
DHCP	Dynamic Host Configuration Protocol, dynamický konfigurační protokol (je v informatice název protokolu z rodiny TCP/IP nebo označení odpovídajícího DHCP serveru či klienta. Používá se pro automatickou konfiguraci počítačů připojených do počítačové sítě. DHCP server přiděluje počítačům pomocí DHCP protokolu zejména IP adresu, masku sítě, implicitní bránu a adresu DNS serveru.)
DNS	Domain Name Systém, doménový jmenný systém (hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace. Jeho hlavním úkolem a příčinou vzniku jsou vzájemné převody doménových jmen a IP adres uzlů sítě.)
HPE	Hewlett Packard Enterprise (nadnárodní společnost zabývající se informačními technologiemi, sídlící v Palo Alto v Kalifornii) – divize Enterprise se zabývá serverovou a storage technologií.
HW	Hardware, označuje veškeré fyzicky existující technické vybavení počítače na rozdíl od dat a programů (označovaných jako software)
vmware	virtualizační platforma firmy vmware, pro x86-64 (32 a 64 bit) systémy
iSCSI	Internet Small Computer System Interface je v informatice síťový protokol, který umožňuje připojovat úložný prostor (např. diskové pole) pomocí počítačové sítě
LAN	Local Area Network, lokální síť (označuje počítačovou síť, která pokrývá malé geografické území)
ICT	Information and Communication Technologies, Informační a komunikační technologie
ISP	Internet Service Provider, poskytovatel internetového připojení
IP	Internet Protocol, internetový protokol (IP adresa je v informatice číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti)
IPv4	Internet Protocol version 4, čtvrtá revize IP (Internet Protocol), spolu s IPv6 vytvářejí základ pro komunikaci v rámci sítě Internet
IT	Information Technologies, Informační technologie
JTS	jednotná telefonní síť
Patch panel	Panel do rozvaděče se zásuvksami RJ45 (panel s řadou konektorů, obvykle stejného nebo podobného typu, pro přehledné a flexibilní propojení různých prvků)
PoE	Power over Ethernet, napájení po datovém síťovém kabelu (bez nutnosti přivést napájecí napětí k přístroji dalším samostatným kabelem)

Pojem / Zkratka	Popis
proxy	Proxy server funguje jako prostředník mezi klientem a cílovým počítačem (serverem), překládá klientské požadavky a vůči cílovému počítači vystupuje sám jako klient.
rack	rozvaděč (standardizovaný systém umožňující přehlednou montáž a propojování různých elektrických a elektronických zařízení spolu s vyústěním kabelových rozvodů do sloupců nad sebe v ocelovém rámu)
RAID1	Redundant Array of Independent Disks, vícenásobné diskové pole nezávislých disků (v informatice metoda zabezpečení dat proti selhání pevného disku, která je realizována specifickým ukládáním dat na více nezávislých disků, kdy jsou uložená data zachována i při selhání některého z nich)
RJ45	koncovka pro UTP kabely (dnes nejčastěji používaný typ zapojení síťových kabelů UTP)
storage	ukládací prostor
SW	Software (též programové vybavení) je v informatice sada všech počítačových programů používaných v počítači, které provádějí nějakou činnost. Software lze rozdělit na systémový software, který zajišťuje chod samotného počítače a jeho styk s okolím a na aplikační software, se kterým pracuje uživatel počítače.
switch	přepínač (v informatice aktivní prvek v počítačové síti, který propojuje jednotlivé prvky do hvězdicové topologie)
UPS	Uninterruptible Power Supply/Source, zdroj nepřerušovaného napájení
UTP	Unshielded Twisted Pair, nestíněná kroucená dvojlinka (druh kabelu, který je používán v telekomunikacích a počítačových sítích)
VM	Virtual Machine, virtualizované serverové prostředí
WAN	Wide Area Network, rozsáhlá počítačová síť (v informatice počítačová síť, která pokrývá rozlehlé geografické území)
WiFi	wireless fidelity, bezdrátová komunikace (v informatice označení pro několik standardů popisujících bezdrátovou komunikaci v počítačových sítích)
SOC	Security Operations Center, bezpečnostní dohled

5. ZÁVĚR

Tento dokument byl zpracován v únoru roku a březnu roku 2018. Obsahuje všechny dostupné podklady a zjištěné informace platné v tomto období. Naplánování rozvoje IT prostředí, které hraje naprosto nezastupitelnou roli ve fungování státní správy a samosprávy umožní efektivní využití veřejných prostředků a zároveň spolehlivý provoz všech aplikací a služeb úřadu.