Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Moderní datová centra

Bc. Jan Velehradský

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Jan Velehradský

Informatika

Název práce

Moderní datová centra

Název anglicky

Modern data centers

Cíle práce

Diplomová práce je zaměřena na problematiku datových center. Hlavním cílem této práce je analyzovat infrastrukturu a zabezpečení vybraného datového centra s ohledem na služby, které by mělo poskytovat. Dílčí cíle práce jsou:

- obecně představit současný stav datových center a jejich historický vývoj
- zpracovat přehled problematiky datových center, definovat jejich účel, možnosti, metody zabezpečení a související technologie
- představit design, uvést technologie a služby vybraného datového centra a analyzovat jejich kvalitu a vhodnost
- pomocí připravených scénářů zhodnotit stávající řešení vybraného datového centra a případně navrhnout řešení kvalitnější
- shrnout získané poznatky a výsledky, uvést odhad a možnosti budoucího vývoje

Metodika

Metodika řešené problematiky diplomové práce vychází ze studia a analýzy odborných informačních zdrojů. V první části práce je nejprve uveden současný stav a historický vývoj datových center. Dále je představena samotná problematika, účel a související technologie. Jsou zde také chrakterizovány metody zabezpečení a řešení designu datových center.

Po dokončení teoretických východisek následuje praktická část, která se zabývá především analýzou datového centra ve zvoleném prostředí. Zde je představena infrastruktura vybraného datového centra a jeho zabezpečení, dále také design a poskytované služby společně s používanými technologiemi a postupy. Na základě analýzy získaných poznatků je zhodnoceno stávající řešení vybraného datového centra a jsou navrženy možnosti ke zkvalitnění jeho služeb i zabezpečení. Pomocí syntézy teoretické a praktické části jsou následně formulovány závěry diplomové práce, kde jsou shrnuty výsledky a také uvedeny možnosti a odhad vývoje do budoucna.

Doporučený rozsah práce

50 – 60 stran

Klíčová slova

datové centrum, zabezpečení, počítačová síť, virtualizace, cloud computing, IaaS, PaaS, SaaS, server

---

Doporučené zdroje informací

ARREGOCES, Mauricio. a Maurizio. PORTOLANI. Data center fundamentals. Indianapolis, Ind: Cisco, 2004. ISBN 1587050234.

BUFFINGTON, Jason. Data protection for virtual data centers. Indianapolis, Ind.: Wiley, c2010. Serious skills. ISBN 9780470908242.

Datová centra – zkušenosti, rady, pomoc, tipy. BusinessIT: Informační technologie pro profesionály [online]. ©2011-2016. Dostupné z: http://www.businessit.cz/cz/rubrika-datova-centra.php

GENG, Hwaiyu. Data center handbook. Hoboken, New Jersey: John Wiley & Sons Inc., 2015. ISBN 978-1-118-93758-7.

JOSHI, Yogendra a Pramod KUMAR. Energy efficient thermal management of data centers. New York: Springer, 2012. ISBN 9781441971234.

SODOMKA, Petr a Hana KLČOVÁ. Informační systémy v podnikové praxi. 2., aktualiz. a rozš. vyd. Brno: Computer Press, 2010. ISBN 978-80-251-2878-7.

Předběžný termín obhajoby

2017/18 ZS – PEF (únor 2018)

Vedoucí práce

Ing. Jiří Vaněk, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 23. 5. 2016

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 2. 8. 2016

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 14. 08. 2017

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Moderní datová centra" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 30. 3. 2018 _____

Poděkování

Rád bych touto cestou poděkoval vedoucímu mé diplomové práce panu Ing. Jiřímu Vaňkovi, Ph.D. za podnětné připomínky a osobitý přístup. Dále také společnosti Casablanca INT s.r.o. za možnost realizace praktické části práce.

Moderní datová centra

Souhrn

Diplomová práce je zaměřena na problematiku datových center. Hlavním cílem této práce je analyzovat infrastrukturu a zabezpečení vybraného datového centra s ohledem na služby, které by mělo poskytovat. V první části práce je nejprve uveden současný stav a historický vývoj datových center. Dále je představena samotná problematika, účel a související technologie. Jsou zde také charakterizovány metody zabezpečení a řešení designu datových center. Praktická část se zabývá především analýzou datového centra ve zvoleném prostředí. Zde je představena infrastruktura vybraného datového centra a jeho zabezpečení, dále také design a poskytované služby společně s používanými technologiemi a postupy. Na základě analýzy získaných poznatků je zhodnoceno stávající řešení vybraného datového centra a jsou navrženy možnosti ke zkvalitnění jeho služeb i zabezpečení. Pomocí syntézy teoretické a praktické části jsou následně formulovány závěry diplomové práce, kde jsou shrnuty výsledky a také uvedeny možnosti a odhad vývoje do budoucna.

Klíčová slova: datové centrum, zabezpečení, počítačová síť, virtualizace, cloud computing, IaaS, PaaS, SaaS, server

Modern data centers

Summary

The thesis is focused on data center issues. The main goal of this work is to analyze infrastructure and security of the selected data center with respect to the services it should provide. In the first part of this thesis is presented current state and historical development of data centers. Furthermore, the main problematics and related technologies are described. Security methods and design solutions for data centers are also defined there. Practical part deals first and foremost with data center analysis in selected environment. The infrastructure of the selected data center and its security is presented here, as well as the design and provided services along with the technologies and procedures used. Based on the analysis of acquired knowledge, the existing solution of the selected data center is evaluated and possibilities for improvement of its services and security are proposed. The synthesis of the theoretical and practical part is followed by the conclusions of the diploma thesis, which summarizes the results and also gives possibilities and estimation of the future development.

Keywords: data center, security, computer network, virtualization, cloud computing, IaaS, PaaS, SaaS, server

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

V dnešní době již internet většina lidí chápe jako každodenní součást svého života. Vysoká spolehlivost, dostupnost a kvalita služeb založených na síťovém protokolu je v současnosti pro velkou část moderně žijící společnosti standardem. Navštěvování oblíbených webových stránek, sociálních sítí či využívání aplikací by však dnes již nebylo možné bez existence datových center provozovaných tou či onou společností. V datovém centru obvykle figuruje velké množství počítačů, síťových prvků, datových úložišť a dalších hardwarových zařízení, potřebných pro bezproblémový chod samotného datacentra. Výše zmíněný hardware tvoří počítačovou síť (či sítě), umožňuje využívání tolik potřebného software a dále také zajišťuje spojení datacentra s vnějším světem – globální sítí internet. Agentura ochrany životního prostředí USA definuje datové centrum jako souhrn převážně elektronických zařízení používaných pro zpracování dat (servery), ukládání dat (datové sklady) a komunikaci (síťová zařízení), které zpracovává, ukládá a přenáší digitální informace. Dále se stará o konverzi a zálohování energie, udržuje spolehlivý a vysoce kvalitní výkon a správnou teplotu. Zjednodušeně lze tedy říci, že datové centrum je průmyslový komplex určený k provozování informačních a telekomunikačních technologií za zvláštních podmínek. [1]

Obrázek 1 - Datové centrum společnosti Facebook ve Švédsku[17]

Valná většina společností provozujících webové stránky, online aplikace atd. umisťuje svá data na zařízení (server, úložiště), které se většinou nachází právě v nějakém datovém centru. Díky dnešnímu rozmachu cloudu tak v konečném důsledku lidé využívají služeb nějakého datacentra téměř pokaždé, když vstoupí na internet. V návaznosti na výše zmíněné informace je nutné si uvědomit rostoucí požadavky na kvalitně řešenou infrastrukturu a zabezpečení datových center, neboť každá ztráta dat či komplikace v přístupu k datům může mít v současnosti fatální důsledky. A to ať už se jedná o data celé společnosti nebo jednotlivce. Bezpečnost je potom třeba chápat z více hledisek. Nejen z pohledu potenciálních útoků z internetu (DDoS útoky, brute force útoky apod.), ale také z pohledu možných přírodních katastrof či oprávnění osob v přístupu do serverovny. Infrastruktura datového centra potom s bezpečností úzce souvisí, přičemž řeší rozvržení celé sítě a použité technologie. Dále se zabývá umístěním jak samotného datacentra, tak jednotlivých prvků a jejich efektivním provozem.

Výše uvedené problémy tvoří základní pilíře této diplomové práce a budou zkoumány u datového centra vybrané společnosti.

2 Cíl práce a metodika

2.1 Cíl práce

Diplomová práce se zabývá problematikou datových center. Hlavním cílem této práce je analýza infrastruktury a zabezpečení datového centra vybrané společnosti s ohledem na služby, které by mělo poskytovat.

Dílčí cíle jsou:

- představení současného stavu datových center a jejich historického vývoje
- zpracování přehledu problematiky datových center, definování jejich účelu, možností, metod zabezpečení a uvedení souvisejících technologií
- představení designu, technologií a služeb vybraného datového centra a analýza jejich kvality a vhodnosti
- zhodnocení stávajícího řešení vybraného datového centra pomocí připravených scénářů a případný návrh řešení kvalitnějšího
- shrnutí získaných poznatků a výsledků, uvedení odhadu a možností budoucího vývoje

2.2 Metodika

Metodika řešené problematiky diplomové práce vychází především ze studia a analýzy odborných informačních zdrojů. V úvodní části práce je nejprve představen současný stav a historický vývoj datových center. Dále je uvedena samotná problematika, účel a související technologie. Jsou zde také charakterizovány metody zabezpečení a řešení infrastruktury datových center.

Po sestavení teoretických východisek následuje praktická část, která se zabývá především analýzou datového centra ve zvoleném prostředí. Představena je zde infrastruktura datového centra vybrané společnosti a jeho zabezpečení, dále také poskytované služby společně s používanými technologiemi a postupy. Na základě analýzy získaných poznatků je zhodnoceno stávající řešení vybraného datového centra a jsou navrženy možnosti ke zkvalitnění jeho infrastruktury, služeb i zabezpečení. Pomocí syntézy teoretické a praktické části jsou následně formulovány závěry diplomové práce, kde jsou shrnuty výsledky a také uvedeny možnosti a odhad vývoje do budoucna.

3 Teoretická východiska

3.1 Vývoj a současný stav

Datacentra mají své kořeny v obrovských počítačových halách pro sálové počítače, které vznikaly v raném věku počítačového průmyslu. Kolem roku 1990 začínají počítače nacházet svá místa ve starých počítačových místnostech. Dostupnost levných síťových zařízení (spolu s novými standardy pro strukturovanou kabeláž) umožnila použití hierarchického návrhu, který specifikoval umístění serverů na konkrétní místa uvnitř firem. Používání termínu „serverovna“ ve významu „speciálně konstruovaná počítačová místnost“ začalo být stále více populární.

Během internetové horečky (1996-2001) firmy potřebovaly rychlé připojení k internetu a neustálou provozuschopnost pro nasazování systémů a zajištění dostatečné konektivity. Instalace takovýchto zařízení však nebyla únosná pro mnoho menších firem. Velké společnosti tak začaly budovat rozsáhlé prostory, tzv. internetová datová centra, která poskytovala podnikům řadu řešení pro nasazení a provoz systémů. Nové technologie a postupy byly navrženy tak, aby zvládaly velký rozsah provozních požadavků a náročných operací. Tyto praktiky nakonec vedly ke vzniku menších soukromých datových center (serveroven). [2][3]

V roce 2006 začíná Amazon Web nabízet služby IT infrastruktury podnikům ve formě webových služeb, které jsou dnes běžně známé jako cloud computing. Roku 2012 již průzkumy naznačily, že 38 procent podniků využívá cloud a 28 procent plánuje buď zahájení nebo rozšíření využití cloudu. Datová centra pro cloud computing, se nazývají cloudová datová centra. V dnešní době však toto rozdělení vymizelo, vše je tedy integrováno do pojmu „datová centra“.

Společnost Telcordia pak v roce 2013 zavádí obecné požadavky na vybavení a prostory telekomunikačních datových center. Dokument představuje minimální prostorové a environmentální požadavky na vybavení a prostory datových center. Také společnost Google investovala v roce 2013 masivní kapitálové výdaje ve výši 7,35 miliardy dolarů do své internetové infrastruktury. Výdaje byly vynaloženy na masivní expanzi globální sítě datových center společnosti Google, která představuje možná největší stavební úsilí v historii odvětví datových center.

Dnešní datová centra se přesouvají z modelu vlastnictví infrastruktury, hardwaru a softwaru na model předplatného a kapacity na vyžádání. Ve snaze podpořit požadavky aplikací, zejména prostřednictvím cloudu, musí dnešní funkce datových center odpovídat takovým schopnostem. Celý průmysl datových center se nyní mění díky konsolidaci, kontrole nákladů a podpoře cloudů. Cloud computing, který je spárován s dnešními datovými centry, umožňuje, aby se rozhodnutí o IT prováděly na základě informací, jakým způsobem jsou přístupné zdroje. Samotná datová centra však zůstávají zcela vlastní entitou.[2]

3.2 Typy datových center

Jako datacentrum se označuje objekt, kde jsou alokovány servery, úložné systémy, síťové prvky a další počítačové technologie. Datová centra zajišťují jejich napájení, nepřetržitý provoz, poskytují jim konektivitu a potřebné parametry prostředí, například chlazení a bezprašnost. Obvykle jsou také vybavena systémy eliminujícími výpadky elektrické energie a protipožárními prostředky. Důležitá je rovněž bezpečnost hardwaru i dat. Každé datacentrum však používá odlišné prvky a nabízí jiné služby. Stejně tak obchodní model nemusí být vždy stejný. [4]

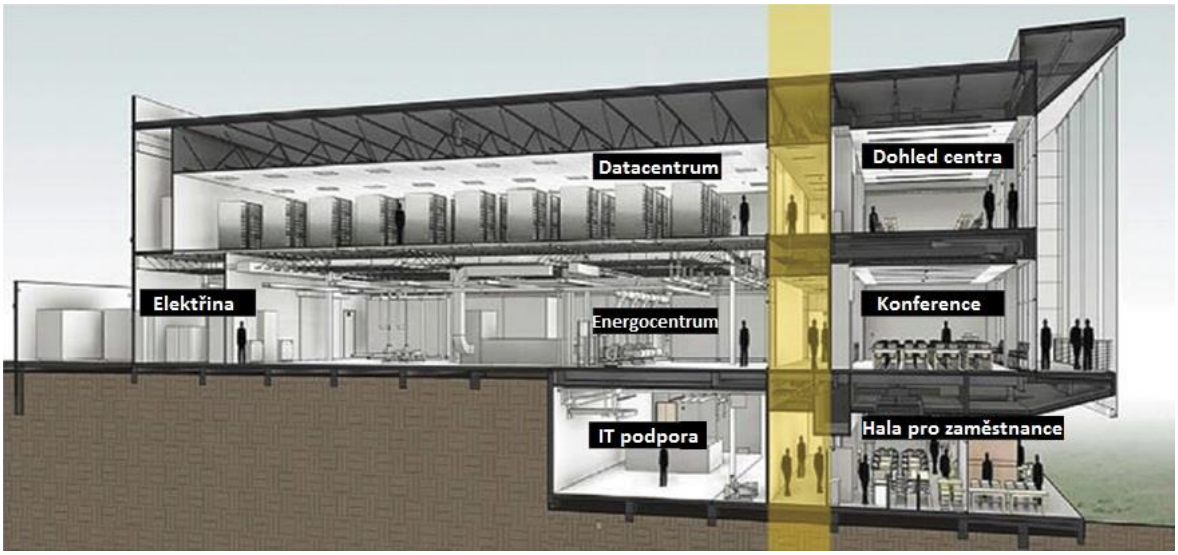
- **Privátní datová centra** – Provozovaná obvykle větší organizací, která své datové centrum sama navrhne, postaví a dále spravuje. Možnosti tohoto zařízení závisí čistě na dané firmě, která datové centrum vlastní.
- **Kolokace** – Datová centra, která jsou využívána více nájemci. Kolokační prostor tak může být prodáván jiným podnikům ve formě skříňky pro server, rackové skříně apod. Tento způsob využívá velké množství malých a středních společností. Zákazníci mají neustálou kontrolu nad svým hardwarem, ale o správu samotného datového centra a vnitřních systémů se stará poskytovatel.
- **„Wholesale“ datová centra** – Tento model datových center je obdobný jako kolokace, nicméně poskytovatel zde pronajímá větší prostor datového centra najednou a obvykle má také méně zákazníků. Datové centrum může být např. vystavěno na míru pouze pro jednoho zákazníka. Koncept lze přirovnat k pronájmu skladu či kanceláře, kde pronajímatel obstarává údržbu zařízení.

- **Dedikovaný hosting** – Poskytovatel provozuje a pronajímá server jednotlivým zákazníkům. Jinými slovy, servery nejsou sdíleny mezi více zákazníků. Žádné dodatečné služby zde nejsou poskytovány a zákazník má plnou kontrolu nad serverem, přičemž údržbu má na starosti poskytovatel. Někteří poskytovatelé však nabízejí zákazníkům dodatečné služby, jako jsou např. vzdálený restart k serveru či upgrade softwaru.
- **Managed hosting** – Neboli „řízený hosting“ je typ datacentra, kde poskytovatel provozuje servery a úložiště pro své zákazníky, ale také poskytuje další administrativní a inženýrské služby. Rozsah služeb může být různorodý a rozsáhlý. Jedná se například o správu databází, operačního systému, zabezpečení, obnovy dat či systémů monitorování a vzdáleného řízení. Hardware může být ve vlastnictví zákazníka nebo poskytovatele.
- **Sdílený hosting** - V tomto případě, zákazníci sdílejí kapacitu serveru. Poskytovatel zde vytvoří uživatelské rozhraní na fyzickém serveru. Toto rozhraní pak poskytuje aplikace, díky nimž zákazníci mohou konfigurovat své služby[5]

Existují i další modely, které však více či méně zasahují do výše uvedeného rozdělení. Stejně tak lze s určitostí nalézt jiná hlediska, dle kterých lze datová centra dělit.[5] Některé další klasifikace budou dále uvedeny v následujících kapitolách.

3.3 Infrastruktura a technologické celky datového centra

Účelem infrastruktury datového centra je zajistit vysokou škálovatelnost portů, dostupnost a zabezpečení serverů, datových úložišť a dalších potřebných prvků. Na procesu návrhu datového centra se obvykle podílí architekt budovy, konstrukční inženýři a technici řešící elektronické a mechanické stránky datacentra. Dále se řeší síťová topologie, architektura serverových či ukládacích platforem, infrastruktura síťové kabeláže a lokalita pro umístění samotné budovy. Kvalitní návrh datového centra s přínosem všech klíčových zúčastněných stran pomůže zajistit, aby datové centrum fungovalo a vykonávalo svou funkci v celém životním cyklu jednotlivých zařízení a poskytovalo provozní efektivitu po dobu mnoha technologických cyklů.[1][6]



Obrázek 2 - Průřez datovým centrem HPC[1]

3.3.1 Elektřina a zálohování napájení

Aby bylo možné dostatečně definovat základní požadavky na funkcionalitu, obchodní potřeby a požadované operace datového centra, je třeba brát v úvahu několik zásadních kritérií. Především je nutné vědět, jaká je požadovaná provozní doba zařízení. To znamená, zda bude možné tolerovat krátkodobou nedostupnost některých prvků. Dalším kritériem je rozhodnutí o použití konkrétního elektrického zařízení, které má být nasazeno. To se odvíjí od typu napájení, množství energie, kterou spotřebují jednotlivé prvky a také od celkového harmonického zkreslení napětí a proudu. Třetí krok sestává z vytvoření jednoho nebo více návrhů elektrické konstrukce. Existují tři hlavní topologie

elektrické stránky datového centra – konstrukce N, N+1 a 2N (nebo N + N). Systém N používá přesný počet zařízení nebo systémů bez vestavěné redundance. Konstrukce N+1 má zabudovaný jeden další systém jako redundanci, zatímco 2N představuje systém, který využívá dvojnásobek potřebných zařízení, což poskytuje maximální redundanci.[1]

Před výpadky elektrického proudu z rozvodné sítě jsou datacentra chráněna transformátory zálohovanými několika zdroji elektrické energie**.** Plnou zálohu zajišťují paralelně či sériově zapojené UPS (Uninterruptible Power Supply) jednotky se samostatnými bateriovými moduly. UPS jsou zdroje nepřerušeného napájení, které poskytují okamžité zásobování elektrickou energií v době mezi začátkem výpadku sítě a nastartováním záložních zdrojů napájení. Pro překlenutí delšího výpadku jsou používány dieselové motorgenerátory, které dokážou napájet datové centrum i několik desítek hodin. Diesel agregáty se zapojují do sestav z důvodu zvýšení jejich výkonu či redundance a k synchronizaci jejich provozu je obvykle používán automatický zátěžový přenosový switch (přepínač)**.**[1][24]

Obrázek 3 - Dieselový motorgenerátor[18]

3.3.2 Chlazení

Chlazení (klimatizace) slouží k odvodu technologického tepla, které ve velké míře produkují veškerá technická zařízení umístěná v datovém centru. V případě poruchy klimatizace dochází v serverovně k brzkému přehřátí všech zařízení během poměrně krátké doby (jedná se zpravidla o jednotky minut). Ventilační a klimatizační systém musí také účinně filtrovat především polétavý prach a další drobné nečistoty obsažené v ovzduší tak, aby se jakékoliv nežádoucí materiály nedostaly do serverů i do dalších technologických zařízení umístěných v datovém centru.

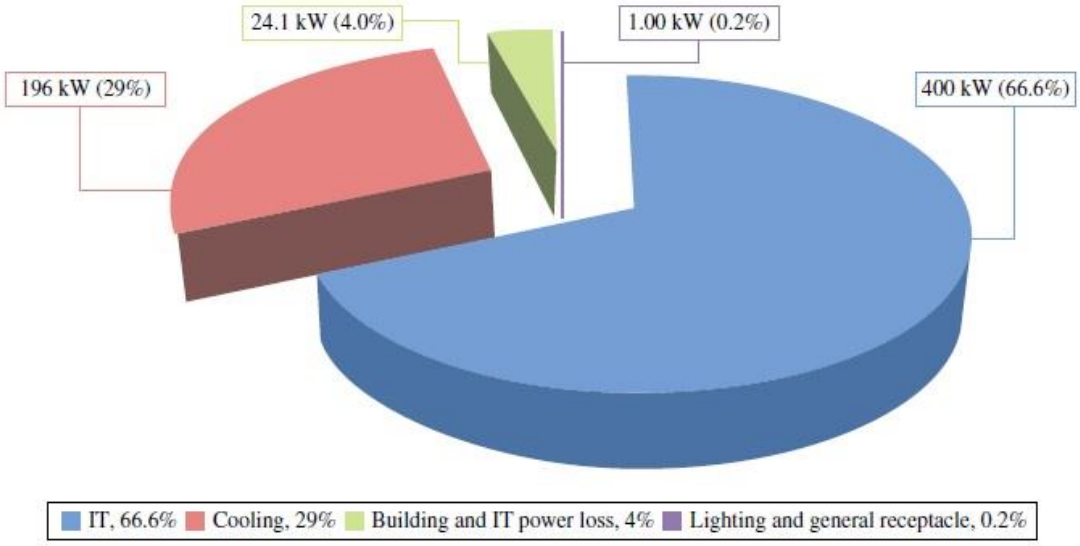
V zásadě se dá schéma chlazení v datovém centru rozdělit na tři oblasti: výrobu chladu, dopravu a rozvod. Základem správného chlazení je vodní chladicí okruh s jedním nebo více chillery v kombinaci s volným nebo suchým chlazením. Chiller je chladící jednotka, která odstraňuje teplo z kapaliny pomocí kompresního nebo absorpčního chladicího cyklu. Tato kapalina pak může cirkulovat přes výměník tepla k ochlazení zařízení nebo jiného procesního proudu (jako je vzduch nebo voda). Jako vedlejší produkt vytváří chiller odpadní teplo, které musí být odčerpáno do okolního prostředí nebo ho lze využít k vytápění. Datové centrum se chladí přiváděnou ochlazenou vodou, zatímco ohřátá voda odvádí z datového centra odpadní teplo. Voda se následně ochlazuje pomocí chillerů a výměníků volného chlazení tím, že v případě volného chlazení chladí vodu přímo venkovní vzduch (jsou-li pro to vhodné klimatické podmínky). Zařízení nakonec čerpá ochlazenou vodu zpátky do datového centra. Teplota přiváděné vody proudící výměníkem tepla v datovém centru určuje, jak studený bude přiváděný vzduch pro servery. Servery se přitom mohou podle ASHRAE (Americká společnost pro vytápění, chlazení a klimatizaci) bez problémů provozovat s přiváděným vzduchem o teplotě do 27°C. Protože je v evropských zeměpisných šířkách po většinu roku možné volné chlazení venkovním vzduchem (tzv. „free cooling“), uspoří se zároveň peníze i energie. Je umožněn také kombinovaný provoz, kde se voda nejprve předběžně ochladí volným chlazením a poté chiller upraví přiváděnou vodu na požadovanou teplotu. Jen za velmi teplých letních dnů, kdy je venkovní teplota vyšší než teplota vratného toku vody, běží chiller neustále.[1][7]

Obrázek 4 - Chillery umístěné na střeše datového centra[19]

Alternativní zdroje chladu může poskytovat např. geotermie. Chladná voda zvenčí se dá získávat pomocí čerpadel z podzemních zásob vody. V takovém případě se jedná o dva vodní okruhy od sebe striktně odděleny a propojeny jen jedním výměníkem tepla. Jestliže se při tomto způsobu volného chlazení používá jako přepravní médium voda, hovoříme o „nepřímém volném chlazení“. Při „přímém volném chlazení“ se jako přepravní médium používá chladný vzduch. Nemusí se instalovat výměníky tepla, čerpadla a potrubí, což znamená další možné zvýšení efektivity. Při teplotě vzduchu přiváděného do serveru až 27 °C lze chladný venkovní vzduch používat z větší části roku, a to bez dalších opatření pro chlazení. Při přímém volném chlazení je však nutno dodržovat některé důležité podmínky. Vzduch proudící do datového centra nesmí být příliš studený, protože jinak se může tvořit kondenzát. Vzduch proudící dovnitř se proto smíchává s teplým odpadním vzduchem tak, aby byla dosažena optimální teplota vzduchu přiváděného do serveru. Také je nutno dbát na správnou vlhkost vzduchu (eliminování kondenzátu, statického náboje) a případně používat zvlhčovač nebo odvlhčovač. Kromě toho se také musí používat filtry proti prachu a podle okolností také proti škodlivým plynům. Stoupne-li venkovní teplota nad teplotu přiváděného vzduchu, je nutno zajistit další způsob chlazení.

K tomu se používají chillery, které přimíchávají studený vzduch, nebo adiabatické chlazení, při němž se rozprašuje jemná vodní mlha. Při odpařování vody se vzduch ochlazuje na požadovanou teplotu a zároveň se zvýší vlhkost vzduchu. Dalším řešením přímého volného chlazení jsou rotační výměníky tepla, které se používají již desítky let u klimatizace budov k rekuperaci tepla.[7]

Rotační výměník tepla je konstruován jako velké rotující kolo. Jedna polovina se nachází v datovém centru, druhá polovina mimo datové centrum, přechod je utěsněn lamelami. Ve venkovní oblasti proudí chladný vzduch výměníkem tepla a ochlazuje ho. Rotující výměník tepla přepravuje chladivo do datového centra. Zde se střetává s teplým odpadním vzduchem serveru a opět ho ochlazuje. Protože mezi datovým centrem a venkovní oblastí nedochází k výměně vzduchu, nemusí být zajištěno zvlhčování nebo odvlhčování.

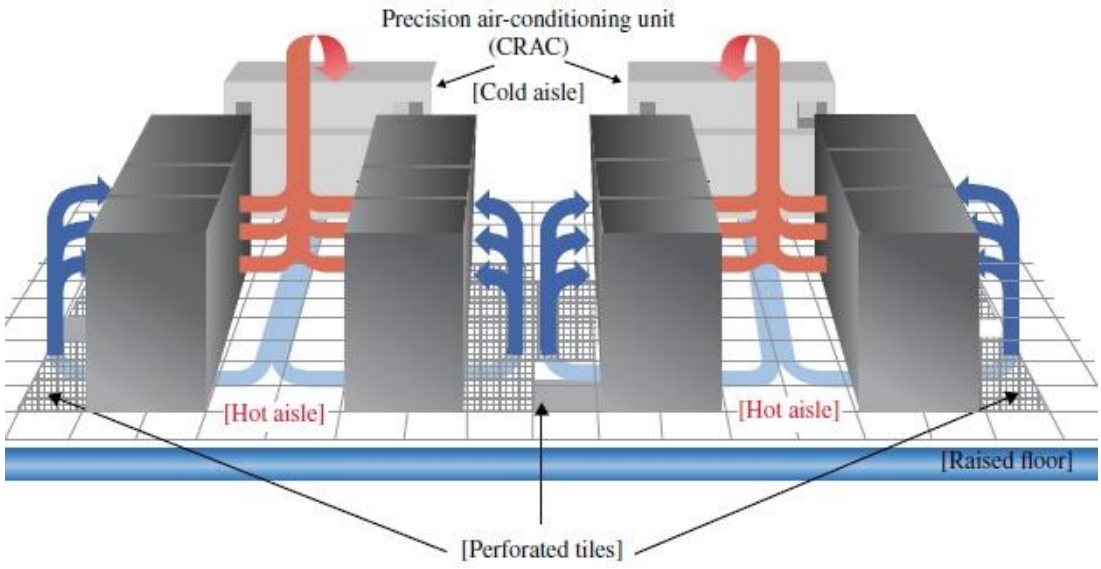


Obrázek 5 - Graf spotřeby energie v datových centrech z března roku 2012[1]

Pro efektivní chlazení datového centra je rozhodující cílené vedení vzduchu a rozvod chladiva. Klíčovou roli přitom hraje průměrné tepelné zatížení serverového rozvaděče. Pokud se tepelné zatížení rozvaděče nachází pod hodnotou 6 až 7 kW, lze přivádět studený vzduch k serverům dvojitou podlahou pod tlakem pomocí systémů CRAC (Computer Room Air Conditioning). Systémy CRAC nasávají teplý vzduch serverové místnosti, ochlazují jej ve výměníku tepla a vyfukují studený vzduch do dvojité podlahy. Perforované podlahové desky před serverovými rozvaděči zajišťují cílený přívod vzduchu. Při použití tohoto systému se instaluje uzavřená ulička, která vzájemně odděluje oblasti studeného

a teplého vzduchu, a zabraňuje tak směšování teplého a studeného vzduchu, což přináší úsporu energie. Rozvaděč se nejprve utěsní, aby se zabránilo vzduchovým zkratům mezi přední a zadní stranou, takže studený vzduch může proudit výhradně serverem. Řady rozvaděčů jsou uspořádány tak, aby přední nebo zadní strany stály proti sobě, a vytvářely tak studenou nebo teplou oblast. Nad uličky, stejně jako u přístupů do uliček, se instaluje přepážka, takže vzduch zůstane ve vymezeném prostoru.

Vzroste-li v rozvaděčích průměrný ztrátový výkon, je obtížnější přivádět chladný vzduch dvojitou podlahou. Alternativu představuje takzvané řadové chlazení, neboli systém „teplé a studené uličky“. Výměníky tepla přitom stojí se serverovými rozvaděči v jedné řadě a tvoří studenou a teplou uličku. Dvojitá podlaha pro vedení vzduchu není zapotřebí, protože řadové klimatizace produkují chladný vzduch přímo do studené uličky, kde vzduch mohou nasávat servery. Teplý odpadní vzduch serverů v teplé uličce opět nasávají řadové klimatizace, které odvádějí vzduch do výměníků tepla, kde se ochlazuje. Protože nyní je dráha vzduchu mezi klimatizací a serverem kratší, může v rozvaděčích proudit větší množství vzduchu, což umožňuje větší ztrátové výkony.



Obrázek 6 - Princip teplé a studené uličky[1]

Při velkých ztrátových výkonech se používá ještě další varianta. Tou je přídavné chlazení a klimatizování samotného rozvaděče. Výměník tepla je přitom umístěn z boku rozvaděče a produkuje studený vzduch přímo před rovinu serveru. Teplý odpadní vzduch se nasává ještě v rozvaděči a přivádí se do výměníků tepla. Vzduch tedy horizontálně

cirkuluje v malém vymezeném prostoru. Speciální variantu přitom představují pasivní zadní dveře „RDHx“ (Rear Door Heat Exchanger). Zadní dveře rozvaděče jsou v tomto případě provedeny jako výměník tepla. Tento výměník nemá vlastní ventilátory a nespotřebovává na rozdíl od výše uvedených zařízení žádnou energii. Teplý odpadní vzduch je do výměníku tepla vháněn ventilátory integrovanými v serverech. Výměník tepla ochlazuje odpadní vzduch a odvádí jej do místnosti, kde jej opět mohou nasát servery. Také jednotlivá ložiska tepla se dají dobře klimatizovat, protože RDHx cíleně odvádí teplo a připravuje v místnosti „neutrální“ klima.[1][7]

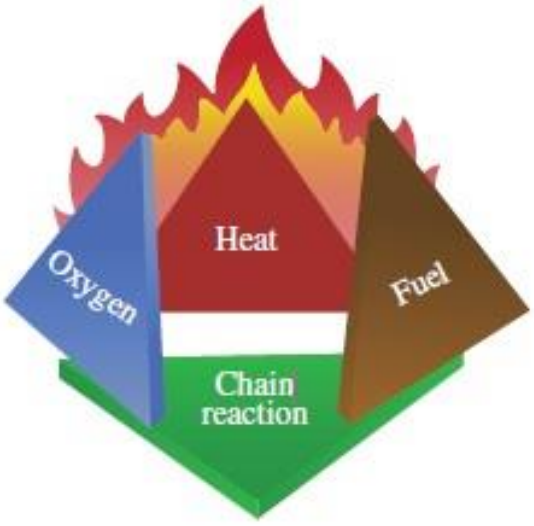
3.3.3 Požární ochrana a ochrana před přírodními katastrofami

Oheň je rizikem, s nímž se musí potýkat každý podnik. Pro datová a telekomunikační centra toto riziko zahrnuje nejen bezpečnost osob v budově, ale i kontinuitu provozu a hodnotu zařízení či dat.

Požární ochranu lze rozdělit na pasivní a aktivní. Cílem pasivní ochrany je co nejvíce zpozdit rozšíření ohně z přilehlého prostoru tak, aby se získalo co nejvíce času pro využití aktivní požární ochrany nebo pro případný zásah hasičů. Samozřejmostí je existence požárních úseků, únikových cest a východů. Dále se také zohledňuje požární odolnost stavebních prvků. Tato problematika se řeší již při výstavbě budovy datového centra a správnou konstrukcí lze vznik a šíření požáru velmi snížit.[1]

Jako aktivní požární ochrana jsou v současnosti využívány především automatické hasicí systémy – stabilní hasicí zařízení (SHZ), které je tvořeno rozvody po celé serverovně a hasicími náplněmi. V případě zjištění požáru elektrickou požární signalizací (EPS) dochází k vypuštění hasiva obvykle v horizontu 30 vteřin. Jako hasicí médium se ještě v nedávné době hojně používal plyn Halon 1301, jehož použití je však již na ústupu z důvodu jeho klasifikace, jako látky poškozující ozonovou vrstvu. V současnosti se k hašení využívá vodní mlha, hydrofluorované uhlovodíky, inertní plyny a plyn Novec 1230 či FM-200 (popřípadě obdobné plyny). Důležité je, aby hasicí prostředek nepoškozoval instalované technologie a byl také částečně dýchatelný. Jednou z možností, která je v některých zemích využívána, je zavedení hypoxického vzduchu neboli redukce kyslíku. Membránový systém udržuje v prostorách datového centra hladinu kyslíku ve vzduchu okolo 14%. Díky tomu v daném prostředí prakticky nemůže vzniknout

požár. Zdržovat se v prostorách, kde je hladina kyslíku nižší než 19% je však pro člověka škodlivé a zejména při dlouhodobé expozici životu nebezpečné. [1][9]



Obrázek 7 - Čtyřstěn vzniku a šíření ohně[1]

V tuzemských podmínkách však větší nebezpečí hrozí spíše od vody. Zásadní roli při ochraně před záplavou opět hraje výběr lokality, kde je umístěno samotné datové centrum. Budova by neměla být poblíž stoupaček vodovodních rozvodů či odpadů. Ideální je umístit serverovny mimo veškerou vodovodní instalaci. Nutné je také brát ohled na umístění datacentra mimo záplavové zóny, nejlépe v bezletových zónách. Eliminovat případné škody způsobené záplavou pak lze použitím dvojitých podlah. Pod jednotlivými racky tak vznikne prostor, kde se může voda shromáždit. V případě rizik vyplývajících z přírodních jevů, jako je povodeň, záplava, požár, zemětřesení, vichřice či zásah blesku apod. je vždy vhodné zjistit historický výskyt takových událostí a na základě těchto informací zvolit vhodné místo pro stavbu budovy datového centra.

Další rizika mohou vyplývat z událostí v blízkém okolí. Takovou událostí může být havárie, požár, výbuch, pád vzrostlého stromu apod. Jde zejména o pozemní a leteckou dopravu, rozvody elektřiny, plynu, vody, páry apod. Podstatné je zaručit minimální vzdálenosti od objektů, které mohou být zdrojem takových událostí.[9][8]

3.3.4 Bezpečnostní systémy a fyzická ochrana

Fyzické zajištění dat bývalo v minulosti velmi podceňovanou složkou kybernetické bezpečnosti, a i když se dnes situace výrazně zlepšila, ne všechna datová centra splňují

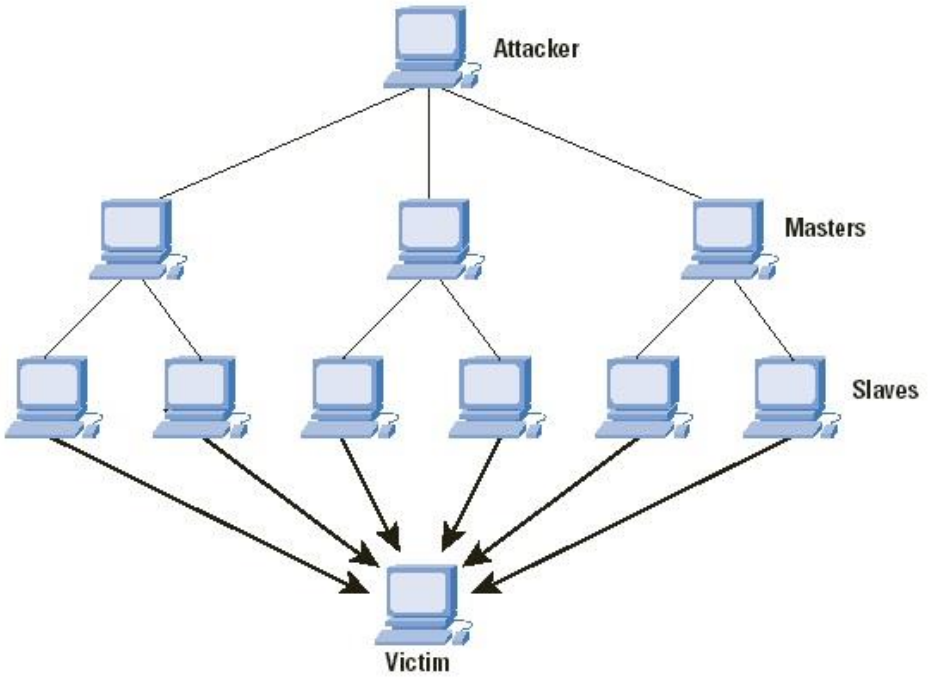
požadované parametry. Obecně můžeme charakterizovat fyzickou bezpečnost dat jako zajištění před zcizením nosičů (hardwaru) nebo neoprávněnou manipulací.

Hranicí, kde začíná snaha o fyzickou ochranu, je venkovní perimetr, tedy jasně definovaný prostor (plot, zeď, cesta, čára na mapě), ve kterém mohou pohybující se osoby představovat reálné nebezpečí. Útočník je tímto na cestě k budově nucen překonat otevřený prostor. Perimetr v tomto případě slouží především k identifikaci možných pokusů o průnik a zpomalení útočníka. V městské zástavbě je perimetrická bezpečnost ztížena a pro její správné fungování je nutné systém pečlivě plánovat a uvést do souladu s platnou legislativou. Další vrstvou fyzické ochrany je pak přítomnost ostrahy budovy a použití kamerových systémů se záznamem. Systémy pro video analýzu mohou, kromě tradiční detekce pohybu v určité oblasti, odhalit i určité vzorce chování nebo upozornit na anomálii. Kamery je vhodné umístit také uvnitř serveroven či u jejich vstupů, popřípadě na dalších kritických místech. Pro ochranu perimetru je kromě kamerového systému dostupná celá řada dalších řešení detekce průniků s různou účinností. Jde o tenzometrická nebo vibrační čidla, mikrofony, drátěné osnovy, pohybové, seizmické či tlakové senzory nebo dokonce senzory magnetických anomálií. V současnosti se používají také infračervené závory či mikrovlnné a laserové radiolokátory. Využít lze i do země ukládané optické a štěrbinové kabely.[10]

Na perimetru by dále měly figurovat prvky kontroly a řízení přístupu osob zajišťující identifikaci osob na branách nebo vstupech. Přístup osob by měl být evidován. Bezpečnostní dveře jsou nutností a naprostým standardem, autentizace je však vždy více faktorová. Dnes jsou nejvíce rozšířeny systémy pracující s čipovými a bezkontaktními kartami. Ty slouží jako primární identifikátory. Zvláště novější bezkontaktní karty lze v objektu spolehlivě sledovat a tím určit polohu držitele. K přímé autorizaci přístupu se kromě klasických zámků s číselníky prosazují stále více biometrická řešení (otisk prstu, sítnice, duhovky nebo cévního řečiště). Takto zabezpečené by neměly být pouze vstupní body objektu a samotné místnosti, ale také samotné racky nebo uličky, ve kterých jsou umístěny servery a datová úložiště. Nasadit lze také hlasovou autorizaci, ta však disponuje poměrně vysokou mírou chybných odmítnutí. S rozvojem kamerových systémů se postupně začínají nasazovat také systémy pro rozpoznávání tváře.[10][11]

3.3.5 Síťová bezpečnost

Součástí zabezpečení moderních datových center musí být kromě výše popsané fyzické bezpečnosti i síťová bezpečnost. Ta zahrnuje vše od kvalitního antiviru, přes hardwarové firewally, až po systémy prevence narušení sítě (IPS/IDS) a specifické stupně ochrany před DDoS (distributed denial of service) útoky. Nutná je také redundance všech aktivních síťových prvků a připojení z několika nezávislých přípojek s dostatečnou přenosovou kapacitou. Za redundantní síť je považována taková počítačová síť, která je odolná proti poruše některé ze svých částí. Při výpadku jedné části sítě by měla s co nejmenšími následky veškerý provoz sítě převzít její zbylá část.



Obrázek 8 - Princip DDoS útoku[20]

Základním stavebním kamenem bezpečné sítě je firewall, který je v základní verzi dostupný na úrovni operačního systému. Firewall kontroluje a filtruje síťový provoz, je schopný zachytit útoky na známé chyby, ale poskytuje i základní ochranu před útoky. Firewally nové generace (UTM - Unified threat management) v sobě kombinují i další funkce, například IPS/IDS (detekce a prevence průniku), eliminace hrozeb maskující se jako legitimní provoz, emailové filtry a další. Jako ochranu proti DDoS útokům je vhodné použít speciální zařízení, které se učí statistický profil provozu sítě a serverů.

Při odchylkách v případě útoku jsou schopna tento útok nejen automaticky rozpoznat, ale také vygenerovat dynamickou signaturu a DDoS útok zablokovat. Robustní sítě v datovém centru s příslušnou ochranou, jsou schopny řešit a pohlcovat útoky až do výše propustnosti páteřních datových linek. Čím robustnější síť s vyšší propustností, tím masívnější útok je schopna rozmělnit. To vše ovšem pouze za předpokladu, že na perimetru je instalováno zařízení podobné firewallu filtrující síťový provoz.[10][8]

Obrázek 9 - UTM zařízení pro zabezpečení sítě[21]

3.3.6 Monitoring

Jedním z klíčových aspektů moderního datového centra je centrální dohled. V datacentru jsou umístěny stovky čidel, které kontrolují, zda nedošlo k úniku vody, plynu, popřípadě vzniku ohně. Monitoring pak sestává z technických prostředků zajišťujících místní nebo vzdálený dohled infrastruktury datového centra. Jedná se zejména o jednotlivé technologie energocentra, sítě, vzduchotechniky, chlazení, přístupový systém, zhášení, parametry prostředí, úniky kapalin a plynu atd. Data z čidel jsou online zpracována a dále vyhodnocována dohledovým týmem v režimu 24/7, čímž je zajištěna připravenost na změny nebo požadavky ze strany zákazníků.[9][8]

Obrázek 10 - Ukázka dohledového systému[22]

3.4 Dostupnost a klasifikace datových center

Celosvětově uznávanou klasifikací pro porovnávání vlastností, výkonnosti a dostupnosti infrastruktury datových center jsou certifikace Tier (česky „stupeň“). Koncept vymyslelo v roce 1993 americké konsorcium společností Uptime Institute, kterému nebyla lhostejná značně kolísavá úroveň různých datových center a jejich zabezpečení. Uptime Institute vydefinoval na základě dosavadních zkušeností klasifikační čtyřstupňový systém sahající od hodnot Tier I, po Tier IV, který reprezentuje nejvyšší úroveň zabezpečení a provozní dostupnosti.[13]

Tier certifikace počítají s minimální redundancí napájecích a chladících technologií, které zajišťují garanci alespoň částečného provozu datacentra prakticky nepřetržitě. Operuje se zde s proměnou N, která označuje minimální množství nezbytných technologií ke garanci bezproblémového provozu infrastruktury (zdroje chladu, napájení serverů, přímé chlazení racků, záložní zdroje a generátory) a číslem, které označuje míru zálohy. Datacentra s označením N, nejsou zálohovaná nijak a výpadek jakékoli komponenty může vést k zastavení celého kolosu. Označení N+1 a 2N naopak představuje vzrůstající úrovně zálohy systémů, které jsou jednou z podmínek získání stupňů Tier 2-4. Redundance chlazení a napájení umožňuje vykrývat výpadky technologií takzvaně za chodu, tedy bez toho, že by došlo k výpadku běžících serverů a úložišť. V případě stupňů Tier III a Tier IV

je redundance N+1 brána jako samozřejmost (Tier IV počítá spíše s 2N+1). Stupně Tier existují čtyři:

- **Tier I** - Jsou jednoduchá datová centra bez záložních a rezervních prvků, avšak už s poměrně vysokou dostupností 99,671 procenta (průměrná doba výpadku je 28,8 hodiny na jeden rok).
- **Tier II** - Datová centra s jediným napájecím a chladícím distribučním procesem s podporou redundantních prvků, které zaručí i při neočekávaném výpadku nepřerušený provoz. Jejich dostupnost je 99,741 procenta a průměrná doba výpadku je 22,0 hodin.
- **Tier III** – Datová centra obsahující záložní bezpečnostní systém, resp. více aktivních napájecích a chladících prvků a to včetně redundantních komponent. Výměna a údržba komponent centra může probíhat za plného provozu (průměrná doba výpadku je 1,6 hodiny a dostupnost 99.982%).
- **Tier IV** - Nejlépe zabezpečená datová centra, nalezneme zde více aktivních napájecích a chladících prvků, včetně redundantních komponent a systémem prevence výpadků. Posouvají hranici dostupnosti až na 99,995 procenta a přidávají další bezpečnostní systémy. Tímto stupněm je certifikováno jen několik desítek nejextrémnějších a nejnáročnějších datových center na světě.[12][13]

3.5 Související technologie

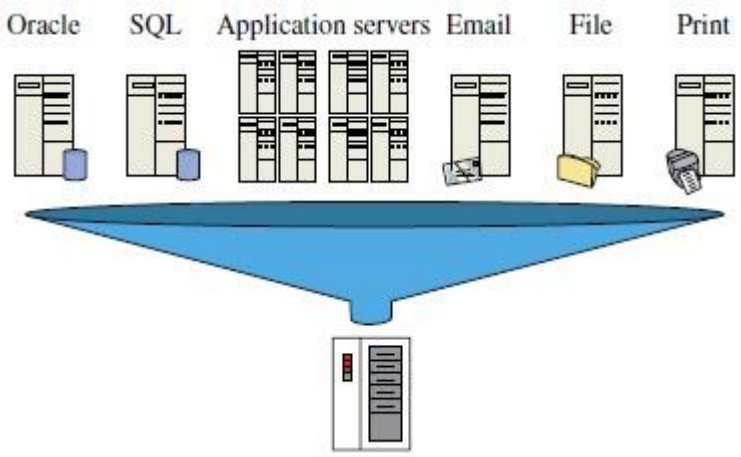
Vzhledem k účelu datových center je samozřejmé, že je při jejich provozu využíván nespočet technologií. V síťové infrastruktuře obvykle figuruje celá řada prvků (routery, switche, firewally, souborové servery, optické či metalické kabely…), které používají (případně poskytují) velké množství protokolů, aplikací a služeb jako jsou např. TCP/IP, UDP, DNS, DHCP, NAT, IPSec, FTP, hlasové služby VoIP a mnoho dalších. Některé protokoly, služby či aplikace jsou nezbytné pro správnou funkcionalitu páteřní sítě a interní infrastruktury. U jiných jejich nasazení záleží čistě na firmě provozující datacentrum. Jedněmi z nejdůležitějších technologií, kterých v současné době moderní datová centra využívají, jsou virtualizace a cloud computing.[6]

3.5.1 Virtualizace

Virtualizaci lze zjednodušeně popsat jako vytvoření virtuálního, zdánlivého počítače uvnitř počítače skutečného (fyzického) pomocí vhodného softwaru. Poprvé s touto koncepcí přišla již v šedesátých letech dvacátého století firma IBM u svých sálových počítačů. V dnešních dnech, kdy virtualizační technologie značně pokročily, však již nemusí jít pouze o virtualizaci celých počítačů. Virtualizovat lze i konkrétní hardwarové komponenty (paměť, disk…) či jednotlivé aplikace. Virtualizované prostředí může být mnohem lépe přizpůsobeno potřebám uživatelů, snáze se používat, případně před uživateli zakrývat pro ně nepodstatné detaily.[14]

Aktuálně existuje hned několik metod jak virtualizovat, z nichž každá má své klady i zápory. Hlavní otázkou, kterou je třeba zodpovědět, je však proč je dnes virtualizace pro datová centra tak důležitá a užitečná. V první řadě jde o lepší využití existujícího hardwaru a jeho potenciálu. Díky možnosti provozovat mnoho virtuálních počítačů na jednom fyzickém stroji je možno vystačit s menším počtem fyzických serverů, což znamená menší spotřebu elektřiny, méně místa, méně tepla a méně nároků na chlazení. Zároveň díky stále se zvyšujícímu výkonu současného hardwaru, je možné tento výkon lépe využít provozem hned několika serverů v různých rolích na jediném fyzickém stroji. Vývojáři aplikací také mohou pomocí virtuálních počítačů snadno testovat kompatibilitu svých programů ve všech myslitelných operačních systémech – to vše na jediném fyzickém stroji.

Další velkou výhodou virtualizace je možnost rychlé implementace nových serverů. Virtuální stroj je reálně tvořen pouze několika soubory. Jakmile je tedy v jednom virtuálním stroji nainstalován a připraven operační systém se všemi potřebnými aplikacemi a aktualizacemi, produkce dalších podobných strojů je pak pouze otázkou vytvoření kopie těchto souborů a případných drobných úprav. Vytvoření nového serveru se tak z několika hodin na fyzickém hardwaru zredukuje na minuty ve virtuálním prostředí.



Obrázek 11 – Virtualizace[1]

Jak již bylo zmíněno výše, virtuální počítač je zpravidla tvořen pouze několika soubory (konfigurační soubory, virtuální disky). Virtualizovaný hardware, který virtuální počítač vidí, je vždy stejný, ať je hostitelský systém postaven na čemkoliv. Přenos na jiný fyzický stroj tedy většinou znamená jen zkopírování těchto souborů, přičemž následně lze prakticky ihned virtuální stroj opět zprovoznit. Totéž platí pro zálohování. Odpadá zde tedy komplikovaná reinstalace aplikací, obnova dat či shánění kompatibilního hardwaru, jako v případě havárie fyzického systému. Navíc je možné zálohovat i běžící virtuální počítač bez jakéhokoli výpadku provozu.

Díky možnosti virtualizovat jednotlivé aplikace odpadají problémy s kompatibilitou na různých operačních systémech. Všechny potřebné aplikace mohou být uloženy na centrálním aplikačním serveru a odsud spouštěny. Není třeba instalovat aplikace na koncové stanice, aplikace lze centrálně aktualizovat a také lze řídit přístupová práva pro jednotlivé uživatele. Uživatel navíc nemusí být vázán na konkrétní pracovní stanici.

Samozřejmě že virtualizace má i svá úskalí. Paradoxně vyplývají z výhod tohoto řešení. V případě, že jsou všechny servery či aplikace konsolidovány na jediný fyzický hardware a dojde k poruše tohoto hardwaru, bude tato porucha znamenat okamžitý výpadek celé infrastruktury. Tomu však lze předcházet provozováním virtuálních serverů v tzv. clusteru, kdy při poruše jednoho hardwarového uzlu jsou zrcadlené virtuální servery okamžitě spuštěny na druhém uzlu. Takové řešení si však žádá další investice.[14]

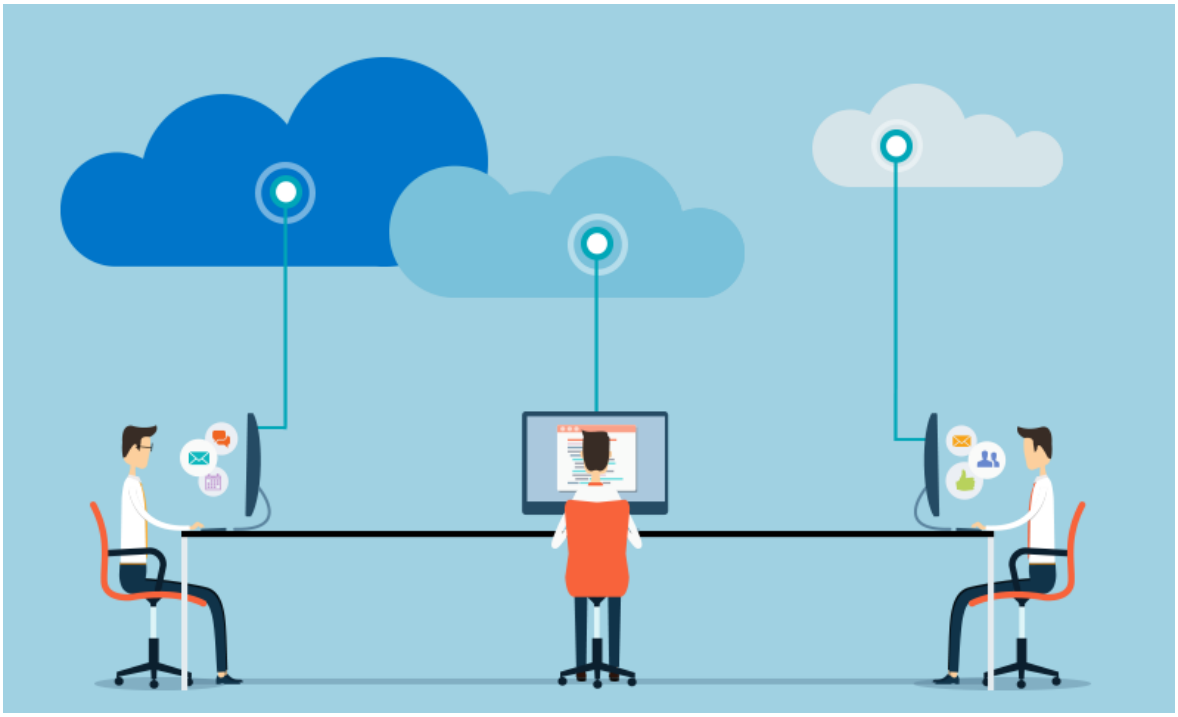
3.5.2 Cloud computing

Ve spojitosti s virtualizací je často využíván cloud computing. Jedná se o metodu přístupu k využití výpočetní techniky, která je založena na poskytování sdílených výpočetních prostředků a jejich využívání formou služby. Existují nejrůznější modely služeb a možnosti jejich poskytování, ale všechny typy cloud computingu disponují společnou schopností poskytovat prostředky na vyžádání, elasticky, samoobslužně a prostřednictvím přístupu z rozsáhlé sítě a také schopností měřit spotřebované služby v rámci sdíleného fondu prostředků. Při provozu cloudových služeb se často využívá tzv. „federace“. Jedná se o propojení několika samostatných prostředků takovým způsobem, že vystupují jako jediný větší prostředek nebo je s nimi možné interagovat jako s jediným prostředkem. Takovýto větší prostředek umožňuje vytvořit a distribuovat uživatelům (nájemníkům) jako službu balíčky, které se navzájem liší kvantitou nebo kvalitou obsaženého prostředku. Většina služeb cloud computingu spadá do tří hlavních kategorií: infrastruktura jako služba (IaaS), platforma jako služba (PaaS) a software jako služba (SaaS).[15][16]

- **Infrastruktura jako služba (IaaS)** - Úplná IT infrastruktura, která je formou služby nabízena uživatelům, vlastníkům aplikací, organizačním jednotkám apod. Každý z uživatelů neboli nájemníků má přístup k části konsolidovaného fondu federovaných prostředků, z nichž si může podle potřeby kdykoli a jakkoli vytvořit vlastní výpočetní infrastrukturu. Konsolidovaný fond prostředků je navržen tak, aby zajišťoval sdílené výpočetní prostředí s charakteristikou multi-tenancy a aby každý nájemník mohl rozhodovat o typu a vlastnostech požadované infrastrukturní služby. Takovéto sdílené prostředí typu multi-tenancy (česky „více nájemníků“) může zcela vlastnit a řídit daná organizace (tj. private cloud), nebo může jít o propojení a federaci firemních prostředků s doplňujícími externími prostředky (tj. hybridní cloud), anebo může být zcela poskytováno jinou organizací (tj. veřejný cloud).
- **Platforma jako služba (PaaS)** - Sdílené výpočetní prostředí jiného poskytovatele, ke kterému může uživatel získat vzdálený přístup za účelem vývoje a spouštění softwarové aplikace (nebo úprav softwaru nabízeného jako služba). Každý uživatel je nájemníkem ve sdíleném prostředí poskytovatele, které má charakteristiku

multi-tenancy. Přímo z definice plyne, že každý uživatel může vytvářet libovolné funkce a aplikační služby. Nebývá však obvyklé, aby samotné výpočetní prostředí nabízelo uživateli významné možnosti volit úroveň poskytovaných infrastrukturních služeb.

- **Software jako služba (SaaS)** - Softwarová aplikace, kterou lze použít pouze prostřednictvím přístupu k danému softwaru a jeho předdefinovanému výpočetnímu prostředí ze sítě, a nikoli stažením softwaru a jeho instalací do místního počítače či výpočetního prostředí. Každý uživatel je nájemníkem ve sdíleném prostředí poskytovatele, které má charakteristiku multi-tenancy. Uživatel však obvykle nemívá mnoho možností volit poskytované služby a jejich úroveň.[15][16]



Obrázek 12 - Cloud computing[23]

Součástí infrastruktury cloudu jsou obvykle funkce pro virtualizaci a federaci prostředků, standardizaci a automatizaci provozních operací, přístup uživatelů k výpočetní službě a možnost zvolit si kvalitu i kvantitu spotřebované služby. V neposlední řadě pak způsob měření a vyúčtování poskytnutých služeb. Ne všechny cloudy jsou stejné. Existuje několik způsobů nasazení prostředků cloud computingu:

- **Veřejný cloud** - Cloud computing, který poskytovatel nabízí z vlastních sdílených prostředků jako službu zákazníkům z řad veřejnosti. Podobá se outsourcingu, ale musí splňovat všechny charakteristiky cloud computingu: schopnost poskytovat prostředky na vyžádání, elasticky a samoobslužně, síťový přístup a také měřitelnost spotřebované služby v rámci sdíleného fondu prostředků. Záleží jen na rozhodnutí daného poskytovatele, které prostředky zpřístupní kterému zákazníkovi, a proto může být služba zabezpečená i nezabezpečená a prostředky mohou, ale nemusí být federovány s jinými (privátními) prostředky.
- **Privátní cloud** - Prostředí pro cloud computing, které si soukromé organizace vytvářejí pro vlastní interní využití. Prostředky, které daná organizace vlastní či přímo kontroluje, jsou konsolidovány a seskupeny jako federované prostředky. Ty jsou pak zpětně formou služby poskytovány uživatelům v rámci organizace.
- **Hybridní cloud** - Prostředí pro cloud computing, které je vytvořeno federací a sdružením prostředků z privátního cloudu určité organizace s prostředky od jiného poskytovatele. Vzhledem k tomu, že před poskytnutím výpočetní služby organizaci dochází k federování a sdružení prostředků, vystupuje hybridní cloud vůči uživatelům, vlastníkům aplikací a organizačním jednotkám přesně stejně jako privátní cloud.
- **Komunitní cloud** - Jedná se o model, kdy je infrastruktura cloudu sdílena mezi několika organizacemi, tedy skupinou lidí, kteří ji využívají. Tyto organizace může spojovat bezpečnostní politika, stejný obor zájmu apod.[16]

4 Vlastní práce

V praktické části této práce je analyzováno datové centrum české společnosti Casablanca INT s.r.o. Tato ICT firma působí na trhu již od roku 1996 a nabízí především housingové, kolokační a IP služby datacentra. Poskytuje ale také připojení k internetu, cloud, či hlasové služby (VoIP). Casablanca INT provozuje vlastní datové centrum o rozloze více než 1600 m^2. Během existence firmy docházelo k postupnému rozšiřování portfolia služeb, stejně tak jako samotného datového centra. V roce 2012 firma spustila první veřejný cloud v ČR. V tomto období také začala společnost využívat možností virtuálních serverů. V závislosti na postupu IT technologií své služby nadále rozvíjí a modernizuje.

4.1 Historie Casablanca INT v datech

- 1996 – založení společnosti se specializací na pevná připojení k Internetu
- 1998 – poskytování serverů a vlastních routerů na bázi OS Linux RedHat
- 2000 – představení produktu Server Housing, oficiální přijetí Casablanca INT do sdružení NIX.CZ
- 2001 – založení pobočky Casablanca na Slovensku
- 2002 – rozšíření portfolia o služby: VoIP, IP VPN, WiFi
- 2004 – vysokorychlostní připojení k Internetu FastConnect
- 2006 – 10. výročí založení společnosti Casablanca INT
- 2007 – zásadní změna corporate identity - komiksový styl, investice přes 30 mil. Kč (Datacentrum, ServerHousing)
- 2008 – certifikace ISO 9001:2000, investice přes 15 mil. Kč (rozšíření Datacentra-zprovozněn datasál HC7), podpora bezpečnosti domén (DNSSEC)
- 2010 – koupě společnosti NETWAY.CZ, otevřen nový datový sál HC8, certifikace IPv6
- 2011 – investice přes 10 mil. Kč (modernizace celé sítě a infrastruktury; nástup virtualizace - začátek poskytování služeb virtuálních serverů), 15. výročí založení společnosti Casablanca INT
- 2012 – spuštění prvního veřejného cloudu v ČR - Big Blue One (technologie HP CS Matrix)

- 2013 – představení cloudových řešení: One Solution, BackUp One, Index One, změna corporate identity, virtualizace a modernizace společnosti, nové prostory, nový web
- 2014 – připojení k projektu FENIX (ochrana před DoS a DDoS útoky), rozšíření technologie cloudového řešení BBO o druhé primární datové pole - BBO rozložen do 3 nezávislých lokalit
- 2016 – 20. výročí založení společnosti Casablanca INT
- 2018 – investice přes 2,5 mil. Kč (modernizace celé sítě a infrastruktury pro cloudová řešení)

4.2 Analýza zkoumaného datového centra

Technické oddělení Casablanca INT se nachází v Praze na Vinohradské ulici v budově Stimbuilding. Zde je umístěno také datové centrum a technologie zajišťující konektivitu pro zákazníky. Budova disponuje šestnácti podlažími, přičemž technické oddělení a dohledové centrum se nachází ve druhém patře. Jednotlivé serverovny a další technologické místnosti jsou potom umístěny následovně:

- Suterén S2 – serverovny HC8, HC7 a HC5
- Suterén S1 – serverovna HC6, strojovna, UPS místnost pro HC6
- Přízemí – serverovny HC2, HC3
- 16. patro – serverovna HC16
- Střecha – antény pro bezdrátový přenos

U budovy Stimbuilding je přistavena restaurace Želivárna, jejíž střecha dosahuje úrovně druhého podlaží. Na této střeše se nachází chillery, ke kterým lze přistupovat přímo z technického oddělení.

Obrázek 13 - Budova Stimbuilding[25]

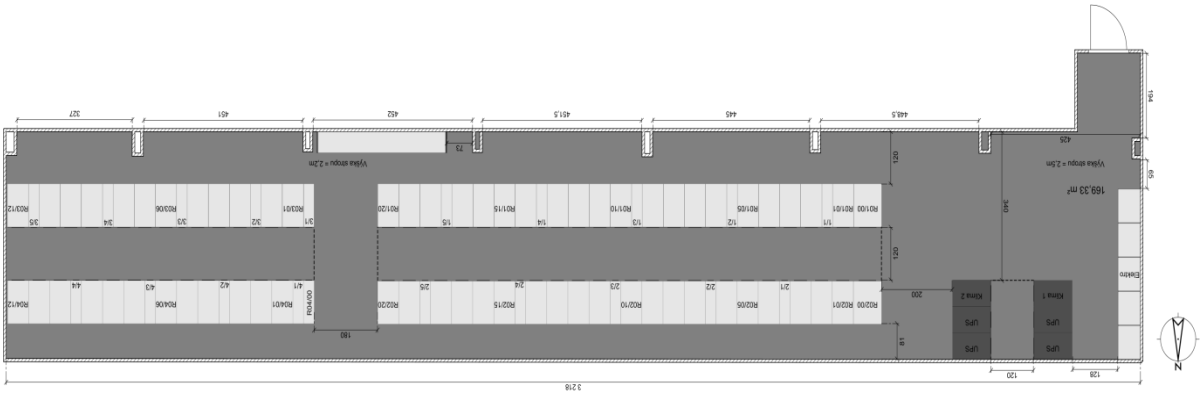
Hlavní vstup do budovy je přímo z ulice Vinohradská. Pro přístup lze také využít zadní vchod, který disponuje rampou a umožňuje tedy snadný přístup například s vozíkem. Tento vchod je na úrovni suterénu S1 a serverovny HC6.

4.2.1 Představení serveroven, design

Casablanca INT provozuje k roku 2018 celkem sedm serveroven, přičemž všechny jsou umístěny v prostorách budovy Stimbuilding. Jsou označeny zkratkou HC (housing centrum) a příslušným číslem. Pro celé datové centrum je potom používána zkratka THC (tele house centrum). Dále je uveden stručný popis jednotlivých serveroven společně s půdorysy.

HC8

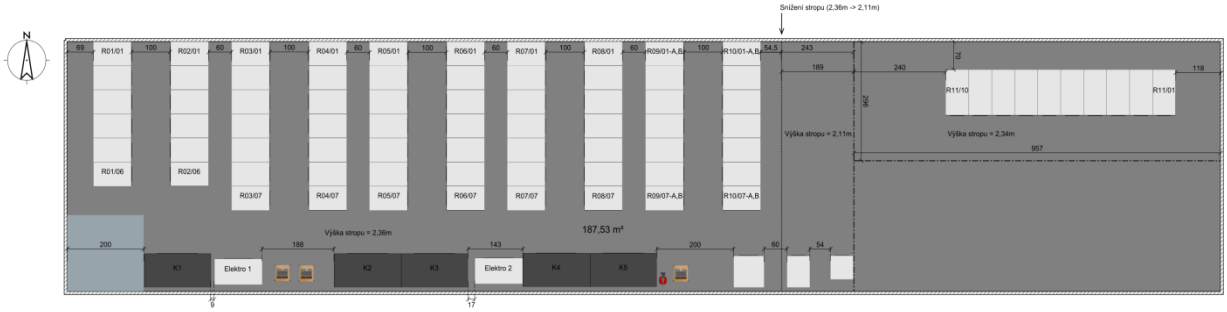
Jedná se o nejmodernější datový sál celého THC, který byl otevřen dodatečně v roce 2010. Je umístěn v suterénu S2 a disponuje systémem chlazení typu studená - teplá ulička a automatickým stabilním hasicím zařízením (SHZ).



Obrázek 14 - Půdorys HC8, ZDROJ: firemní dokumentace

HC7

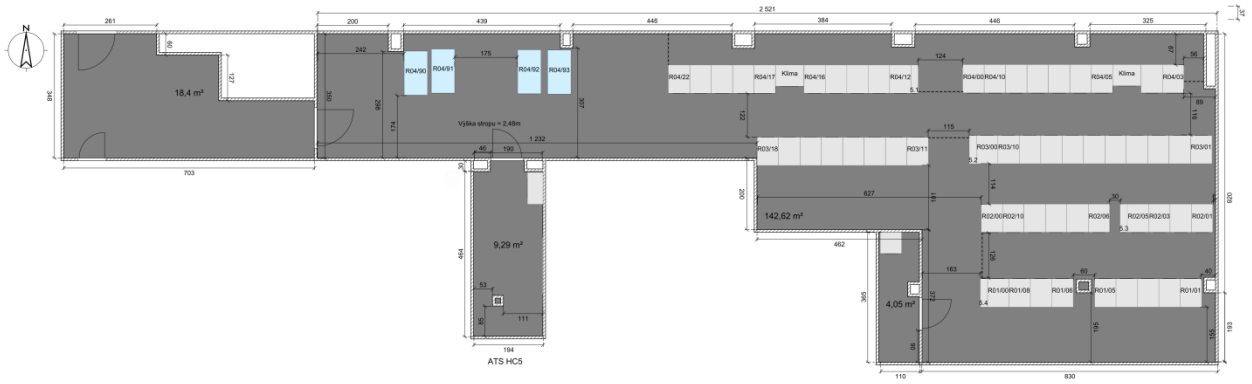
Datový sál, který byl zprovozněn v roce 2008 a je umístěn v suterénu S2 mezi vchody do serveroven HC8 a HC5. Chlazení je zde řešeno odvodem tepla pod podlahou. V této serverovně jsou také umístěny vysoko zátěžové racky, které mají přídavné pasivní i aktivní chladící prvky.



Obrázek 15 - Půdorys HC7, ZDROJ: firemní dokumentace

HC5

Serverovna, která se nachází opět v suterénu S2. Chladí se zde také systémem studené a teplé uličky, nicméně automatický SHZ jako v serverovně HC8 zde není zaveden.



Obrázek 16 - Půdorys HC5, ZDROJ: firemní dokumentace

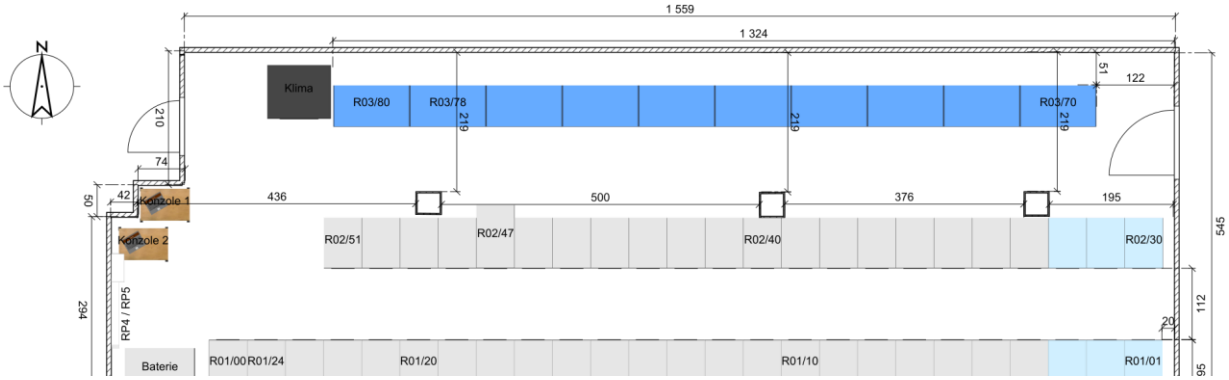
HC6

Tento datový sál je umístěn v suterénu S1 blízko zadního vchodu do budovy. Z tohoto pohledu je lokalizace serverovny velmi výhodná. Přístup a případný transport zařízení je zde ulehčen, neboť u zadního vstupu je rampa umožňující snadný vjezd např. s vozíkem. Chlazení je zde řešeno odvodem tepla podlahou. UPS zařízení pro tento datový sál se nachází v samostatné místnosti přímo naproti serverovně.

Obrázek 17 - Půdorys HC6, ZDROJ: firemní dokumentace

HC2

V přízemí budovy jsou provozovány dva datové sály. Jedním z nich je HC2, kde je chlazení řešeno opět systémem studené a teplé uličky. Kromě rackových stojanů je



Obrázek 18 - Půdorys HC2, ZDROJ: firemní dokumentace

zde také řada boxů, do kterých lze umístit jednotlivé servery. Každý z těchto boxů má potom samostatné chlazení – ventilátor v zadní části boxu.

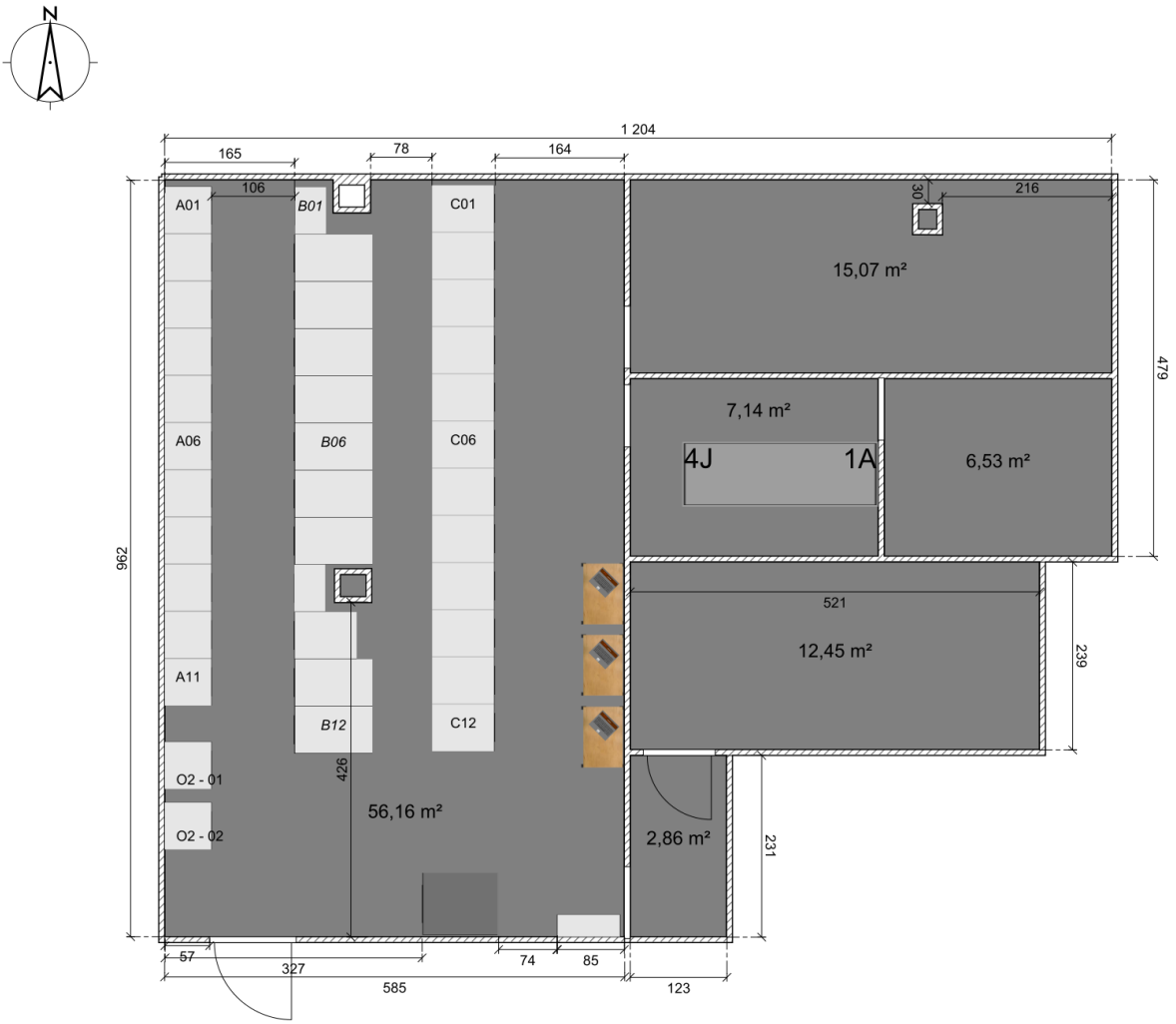
HC3

Druhým sálem v přízemí je HC3, kde jsou umístěny převážně firemní technologie. Jedná se o core switche a další klíčové prvky infrastruktury zajišťující správný chod THC a dále také technologie potřebné pro monitoring a zabezpečení. Tato serverovna je nejmenší z celého THC.

Obrázek 19 - Půdorys HC3, ZDROJ: firemní dokumentace

HC16

Nachází se v 16. patře a kromě klasických rackových stojanů jsou zde také v uzavřené sekci umístěny samostatné tower servery. Chlazení zajišťují tři velké ventilátory vhánějící studený vzduch do serverovny ze stropu.



Obrázek 20 - Půdorys HC16, ZDROJ: firemní dokumentace

Současné řešení datového centra Casablanca INT vychází především z výhodné lokality jakou budova na Vinohradské ulici určitě je. Velmi dobrá dostupnost tohoto místa je nespornou výhodou. Dále je také nutné si uvědomit, že Casablanca INT provozuje toto datové centrum již více než 15 let a inovace samotné budovy není v kompetenci firmy. Pokud se zaměříme na stavbu a řešení samotných datových sálů, pak nejnovější serverovna HC8 je bezesporu nejkvalitnějším sálem celého THC. Dále následuje HC6, kde je velikou výhodou možnost přístupu z rampy přímo od zadního vchodu budovy. Oba tyto datové sály reflektují v nejlepším světle stav a řešení zbylých serveroven THC.

HC8 využívá k chlazení systému teplé a studené uličky. Kabeláž a chladící kapalina jsou zde vedeny kvalitní zdvojenou podlahou a provedení rackových stojanů nabízí možnost pronájmu jak celých racků, tak i ½ či ¼ racků. Jednotlivé chladící jednotky jsou v rackových uličkách umístěny vždy v pravidelných intervalech a zajišťují správnou cirkulaci vzduchu. Nezbytností je však kontrola „zaslepení“ neobsazených míst v jednotlivých stojanech. Prázdný prostor ve stojanu totiž proudění vzduchu naruší a následně pak dochází k energetickým ztrátám. Automatický hasicí systém zajišťuje vysoké protipožární zabezpečení. Pomineme-li hasicí systém, jsou obdobně řešeny i serverovny HC5, HC2, HC3 a HC16, avšak jejich provedení není tak elegantní, neboť kabeláž je zde vedena stropními rastry a rackové stojany, které jsou staršího typu, mají v mnoha případech neuzavřený zadní kryt. Stejně tak nejsou plně utěsněny samotné rackové uličky. Tyto serverovny by tedy rozhodně bylo vhodné modernizovat, neboť vzhledem k jejich současnému řešení není chlazení tak efektivní jako v HC8, což lze vysledovat i z konkrétních hodnot teplotních grafů.

V případě datového sálu HC6 jsou servery chlazeny odvodem tepla skrze zdvojenou podlahu. Tudy je také vedena kabeláž a chladící rozvody. Rackové stojany mají jednotnou podobu a datový sál působí homogenně. Stejným způsobem je řešena také serverovna HC7.

4.2.2 Poskytované služby a jejich řešení

Datové centrum je primárně provozováno pro zákazníky, kteří hledají prostor k pronajmutí pro svůj server (server housing) a případně také požadují vysokorychlostní datové linky. Veškeré služby, které Casablanca INT poskytuje, jsou následující:

- Server housing - umístění serverů zákazníka v libovolném počtu, typ provedeni RM/tower, servery jsou umístěny do samostatných BOXů/stojanů, port 100Mbit/s - 1Gbit/s, počet IP není neomezen (jsou přidělovány na základě adresního plánu dle standardu RIPE NCC), datové měsíční limity pro zahraniční přenosy od 100GB.
- Zálohování dat - služba poskytující prostor pro zálohu dat do neomezené výše objemu; určená nejen pro stávající zákazníky služby ServerHousing.
- Web hosting - zajištění provozu národních/mezinárodních/ostatních domén dle požadavků zákazníka, provoz DNS, MAIL, databázových serverů
- Internet - služby zajišťující připojení účastníků do sítě Internet.
- IP VPN - virtuální privátní síť na bázi IP protokolu; určená pro firmy vyžadující vyhrazené pásmo a zejména rychlé, kvalitní a bezpečné propojení sítí jednotlivých poboček.
- Správa LAN - správa a dohled nad lokální sítí zákazníka.
- Hlasové služby – hlasové služby poskytované prostřednictvím vlastní přístupové sítě nebo veřejné sítě internet.
- Virtuální server, cloud – pronájem virtuálního hardwaru na infrastruktuře poskytovatele
- Správa serveru – administrace serverů na platformách Linux/Microsoft

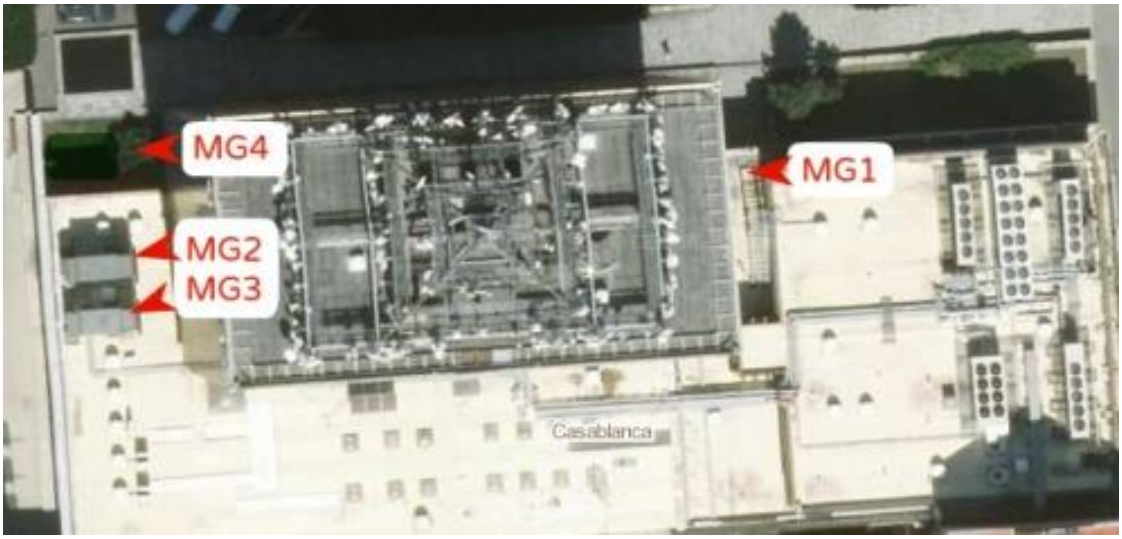
Z výše uvedeného seznamu je jasné, že ne všechny služby jsou provozovány přímo v datovém centru, nicméně na většině se provoz datového centra více či méně podílí. Primárními zákaznickými službami, které jsou provozovány přímo v datových sálech, jsou server housing, zálohování dat, pronájem virtuálního serveru (cloud) a případná správa serveru. Je možné pronajmout si prostor pro jediný server, případně celý rack (více racků, kolokační prostor), ½ rack či ¼ rack. Zákazník má možnost využít přípojek v libovolné kombinaci 10M/100M/1G/10G. V případě pronájmu virtuálního serveru jsou možnosti prakticky neomezené a záleží vždy pouze na požadavcích zákazníka. K virtualizaci je využívána platforma VMware. V případě zálohy dat či správy serveru je potom řešení individuální. Využíván je například zálohovací open source software Bacula.

Zákazníci mají možnost využít několik nadstandardních služeb pro vzdálenou správu svého serveru. Jedná se o vzdálený restart a připojení KVM konzole pro vzdálený přístup.

V obou případech stačí zavolat na podporu Casablanca INT. V případě, že má zákazník dostatečná oprávnění a autorizuje se, lze mu vyhovět. Návštěvníci také mohou využívat konzole přímo v serverovnách. V každém datovém sálu jsou 2-3 zařízení, která lze využít pro připojení k danému serveru. Sestava se skládá standardně z monitoru, myši, klávesnice a napájecího kabelu, přičemž ji lze přesouvat na pojízdném stolku. Pro přístup do vyšších míst rackových stojanů jsou v serverovnách umístěny stoličky.

4.2.3 Rozvodná síť a záložní zdroje

Přísun elektřiny do celého datového centra zajišťuje automatický zátěžový přenosový switch (ATS – automatic transfer switch). Jedná se o rozvaděč, který za standardních okolností distribuuje elektřinu přímo z elektrické sítě dále do systémů serveroven. V případě výpadku proudu potom automaticky nastartuje záložní motorgenerátory a zátěž postupně přesune na ně. Obdobně po obnovení dodávky proudu dojde k přepnutí zátěže zpět na napájení ze sítě a vypnutí agregátů. V datovém centru Casablanca INT jsou celkem 3 ATS systémy, jejich stavy indikované v monitorovacím systému jsou patrné v kapitole 4.2.9 na obrázku Obrázek 27 - Monitoring datového centra, ZDROJ: . Záložní napájení zajišťují celkem čtyři motorgenerátory o celkovém výkonu 2 MW. V případě nutnosti jsou



Obrázek 21 - Umístění motorgenerátorů u budovy, ZDROJ: firemní dokumentace

schopny napájet datové centrum až 20 hodin. Toto omezení je způsobeno zásobou paliva, kterou však lze během výpadku primárního napájení doplňovat.

Krátké či velmi krátké výpadky dodávky elektřiny potom překlenou nepřerušitelné zdroje napájení (UPS), které jsou napájeny pomocí samostatných akumulátorů. UPS jsou v každé serverovně, přičemž je používán redundantní systém N + N. Tento systém zajišťuje, že v případě použití určitého počtu UPS je využíván stejný počet záložních UPS, které jsou připraveny zastoupit původní v případě poruchy. Aktuální řešení rozvodné sítě a záložních zdrojů je pro datové centrum v současné době plně dostačující.

4.2.4 Chlazení THC

Většina serveroven je chlazena pomocí společného vodního okruhu, který je ochlazován výrobníky chladu umístěnými na střeše na úrovni druhého patra vedle kanceláří technického oddělení. Nacházejí se zde 4 chillery (výrobníky chladu) a suchý chladič (zařízení schopno ochlazovat vodu okolním vzduchem). Výjimku tvoří datový sál HC16, kde je chlazení řešeno přídavnými ventilátory umístěnými na stropě. V tomto

Obrázek 22 - Chillery a suchý chladič, ZDROJ: firemní dokumentace

případě by byl totiž rozvod ochlazené vody z úrovně druhého podlaží až do 16. patra velmi problematický a energeticky náročný.

Čerpadla zajišťující cirkulaci studené vody datovým centrem jsou umístěna ve strojovně v suterénu S1. Chiller musí běžet alespoň na jedno čerpadlo (celkem jich je 6)

aby chladil, pokud zrovna není vypnutý, přičemž sledovaná teplota studené vody je teplota, kterou se následně chladí vzduch v jednotlivých sálech. Suchý chladič pomáhá šetřit energii tím, že v případě nízkých venkovních teplot ochlazuje vodu okolním vzduchem. Samotné chladící jednotky, které chladí vzduch přímo v serverovnách, se nachází v jednotlivých uličkách s racky a podle schématu chlazení daného sálu ochlazují servery skrze podlahu či systémem studené a teplé uličky.

Dohledový systém sleduje teplotu výstupní (studené) a vstupní (teplé) vody u chillerů, teplotu vzduchu, stav čerpadel, tlak v chladících okruzích, stav kompresorů a zapnutí freecoolingu (chlazení okolním vzduchem).

Teploty v rackových skříních by se v ideálním případě měly pohybovat do 25 °C, což se ve většině případů daří splnit. V horkých měsících se teploty přibližují 27 °C, nicméně nikdy nepřesáhnou 30 °C. Jak již bylo uvedeno v teoretické části v kapitole 3.3.2, servery se mohou podle ASHRAE (Americká společnost pro vytápění, chlazení a klimatizaci) bez problémů provozovat s přiváděným vzduchem o teplotě do 27°C. Výrobníky chladu tedy v tomto případě zvládají uchladit všechny serverovny bez větších potíží a zabezpečení serverů proti přehřátí je zde dostatečné. Vzhledem k členitosti a umístění jednotlivých serveroven je však tento způsob chlazení poměrně náročný na energii. Spotřebu nicméně pomáhá kompenzovat suchý chladič, bez kterého by výdaje za energii na ochlazování byly několikrát vyšší, neboť chillery by musely běžet neustále.

4.2.5 Požární a záplavová ochrana

V každé ze serveroven jsou na klíčových místech umístěny sněhové (CO_2) hasicí přístroje. Vznik požáru a změnu teplot monitorují teplotní a optická kouřová čidla, jejichž stav je sledován v dohledovém systému. Kritický stav čidla zaznamená pracovník dohledového centra jako odpovídající alarm či zvýšenou hodnotu v grafu. Čidla jsou umístěna u stropu, případně u chladících jednotek.

Datové sály jsou vybaveny EPS (elektronickou požární signalizací) a nejnovější datový sál HC8 navíc disponuje SHZ (stabilním hasicím zařízením). Jako hasicí médium je zde použita vysokotlaká vodní mlha, která je demineralizovaná a tedy nevodivá. Hašení jakýmkoliv plynovým prostředkem v tomto případě nepřichází v úvahu, neboť serverovna se nachází v suterénu S2 a následné rozptýlení plynu mimo sál a budovu by bylo problematické. V případě zjištění požáru dojde k vypuštění vodní mlhy do 2 minut

od zapnutí alarmu EPS. Pokud pracovník dohledového centra zaznamená alarm požáru v HC8, má tedy 120 sekund na zhodnocení situace a případné vypnutí SHZ. Serverovna disponuje celkem třemi uzavřenými uličkami – dvě z nich jsou uličky s klasickými rackovými stojany, třetí sestává z UPS jednotek. Trysky pro rozptyl mlhy jsou umístěny u stropu jednotlivých uliček. V případě vzniku požáru je spuštěno SHZ a hašen pouze úsek, kde byl požár zaznamenán a veškerý obsah náplní s hasicím médiem je vyprázdněn. Vodní mlha pak musí být znovu doplněna. Na začátku jednotlivých rackový uliček jsou

Obrázek 23 - Ovládání SHZ v serverovně HC8, ZDROJ: vlastní

umístěna tlačítka, kterými lze SHZ manuálně zapnout či blokovat. Ovládání SHZ pro úsek s UPS se nachází u východu ze serverovny (UPS ulička je přímo naproti dveřím).

Budova datového centra se nenachází v záplavové zóně. Nebezpečí však hrozí v případě úniku chladící kapaliny z klimatizačních jednotek. Dále pak také během horkých dnů, kdy se na rozvodech chladících jednotek kondenzuje voda, která může následně unikat do prostor datového sálu. Z tohoto důvodu jsou chladící rozvody ve většině datových sálů vedeny zdvojenou podlahou. Serverovna HC16 se potýká ještě s jedním rizikem záplavy, vzhledem k jejímu umístění v 16. patře. Během extrémního deště zde

existuje hrozba, že voda pronikne stropem přímo do sálu. Zde je tedy nutné dbát na velmi důkladnou stropní izolaci. Záplavová čidla se nachází v každé serverovně podél všech rackových uliček a u všech chladících jednotek. V některých místech jsou čidla polohována i u stropu či pod podlahou. V případě detekce vody čidlo sepne a okamžitě indikuje alarm v dohledovém systému. Pracovník dohledového centra pak ihned fyzicky zkontroluje místo a adekvátně reaguje.

Provozování datového centra v 16. patrové budově není z hlediska požární a záplavové bezpečnosti již ze své podstaty právě ideálním řešením. Problém zde představují kanceláře, které jsou nad datovým centrem umístěny. Budovu prostupuje množství vodovodních a odpadových rozvodů a pozice serveroven vzhledem k riziku záplavy není tudíž příliš vhodná. V případě datových sálů v suterénu S2 je tato nevhodnost umístění ještě více posílena, neboť serverovny jsou provozovány přímo pod restaurací Želivárna. Důsledkem této problémové lokalizace byla například situace v roce 2014, kdy došlo k havárii vodovodního potrubí v jednom z vyšších pater budovy a voda zasáhla datový sál HC8.

Riziko vzniku požáru zvyšuje již samotná lokalita, kde je budova postavena a stejně tak množství dalších zaměstnanců, kteří v budově pracují. Pomineme-li však samotnou budovu a její umístění, je zabezpečení datového centra dostačující. Nicméně bezpečnost by bylo vhodné ještě zvýšit zavedením SHZ do všech serveroven. V současné době je SHZ instalován pouze v datovém sálu HC8. V případě vzniku požáru v některé ze zbylých serveroven je tak nutné po zaznamenání alarmu požár zlikvidovat klasickými hasicími přístroji, což může vést k vyšším škodám.

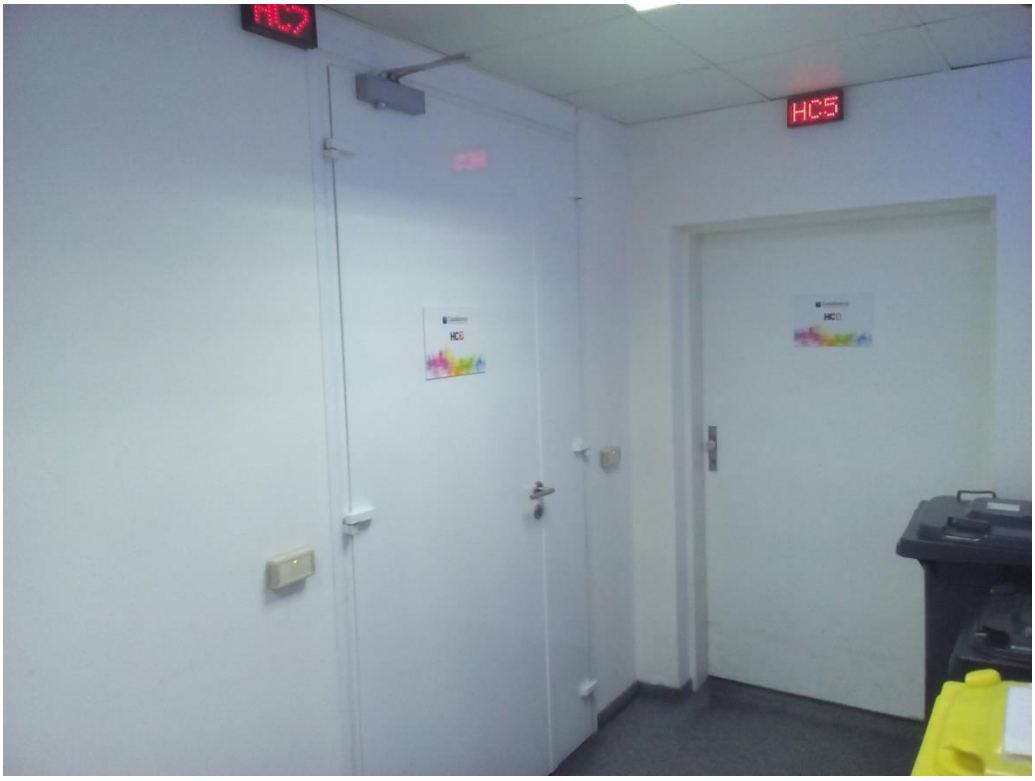
Záplavová i požární čidla jsou umístěna v dostatečném počtu a na odpovídajících místech. Umístění datových sálů zejména v suterénu S2 je však rizikové vzhledem k dalším prostorám nad sály a vodovodním (a odpadním) rozvodům v budově. V ideálním případě by datové centrum mělo být vystavěno v samostatném zařízení bez rozvodů a jednoúčelově.

4.2.6 Přístupový systém a fyzická ochrana

Vzhledem k lokalizaci datového centra je zajištění bezpečného perimetru poměrně složité. V okolí stavby jsou nicméně rozmístěny městské kamery. Vchody monitorují kamerové systémy sledované ochrankou budovy. Další kamery jsou umístěny

v serverovnách vždy u každé z rackových uliček a dále také u vstupů do jednotlivých datových sálů. Kamerový systém je provozován v souladu s příslušnými ustanoveními zákona č. 101/2000 Sb. o ochraně osobních údajů v platném znění a kamerový záznam je ukládán. Datové centrum je přístupné po celý rok 24 hodin denně, 7 dní v týdnu. Hlavní vchod je v pracovní dny mimo noční hodiny otevřen. Během víkendů či svátků a v nočních hodinách se vchod uzavírá a návštěvníkovi musí po zazvonění odemknout pracovník vrátnice. Zadním vchodem lze vejít do budovy pouze po zadání přístupového kódu.

Při první návštěvě THC získá zákazník bezdotykovou čipovou kartu pro přístup do datového centra. Tuto kartu získává zdarma proti předloženému občanskému průkazu (u cizinců cestovnímu pasu) a podpisu „Potvrzení o převzetí čipové karty“. Kontrola oprávnění přístupu do THC probíhá přiložením karty ke čtečce spolu s předložením průkazu totožnosti (občanský průkaz, u cizinců pas) pracovníkovi vrátnice/ochranky. Pro bezproblémovou autorizaci je zákazník povinen nahlásit změnu dokladu totožnosti pracovníkům firmy Casablanca INT. Pakliže evidované číslo dokladu při návštěvě datového centra nesouhlasí s dokladem předloženým, nelze zákazníkovi přístup do THC povolit. Po potvrzení již může osoba pokračovat do konkrétního datového sálu. Vstup do každé místnosti THC je vybaven další čtečkou karet/čipů, elektrickým zámkem a řízen přístupovým systémem. Po přiložení karty ke čtečce zazní zvukový signál a zákazník již může vstoupit do sálu. Uživatel kartu používá nejen k autorizaci při vstupu, ale také k evidenci odchodu. Při odchodu z budovy je návštěvník datového centra povinen elektronicky zaznamenat svůj odchod na terminálu vrátnice. V případě výskytu jakéhokoliv problému v datovém sálu (např. porucha čtečky), jsou v serverovnách k dispozici telefony s telefonním číslem přímo na technickou podporu Casablanca INT.



Obrázek 24 - Přístup do sálů HC7 a HC5, ZDROJ: vlastní

Zákazníci, kteří mají v datovém sálu pronajatý vlastní rack, dostávají k přístupu do stojanu také vlastní klíče. V případě, že chce zákazník vzít s sebou do datového sálu další osobu, musí oba vyplnit a podepsat dokument o jednorázovém přístupu, který potvrdí a podepíše zaměstnanec podpory Casablanca INT. Zákazník je v tomto případě autorizovanou osobou a přebírá veškerou odpovědnost za činnost návštěvníka.

4.2.7 Síťová infrastruktura

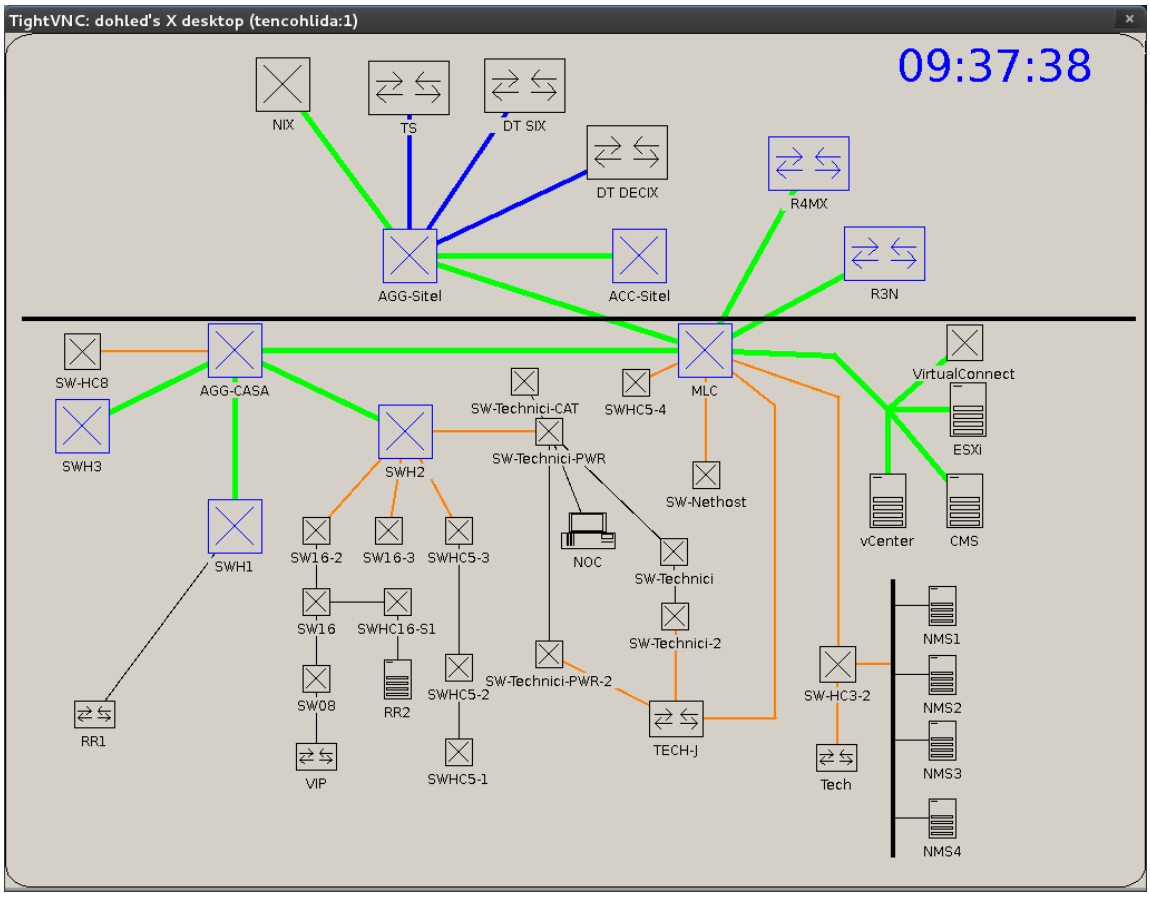
Používané síťové prvky ve zkoumaném datovém centru, lze rozdělit dle vrstev ISO/OSI modelu:

- **L1** - kabely, patch panely, optické vany
- **L2** - switche
- **L3** - routery, specializovaný hardware
- **L4 až L7** - aplikační servery, specializovaný hardware, telefony

Mimo toto rozdělení potom stojí firewally, které zajišťují síťovou bezpečnost.

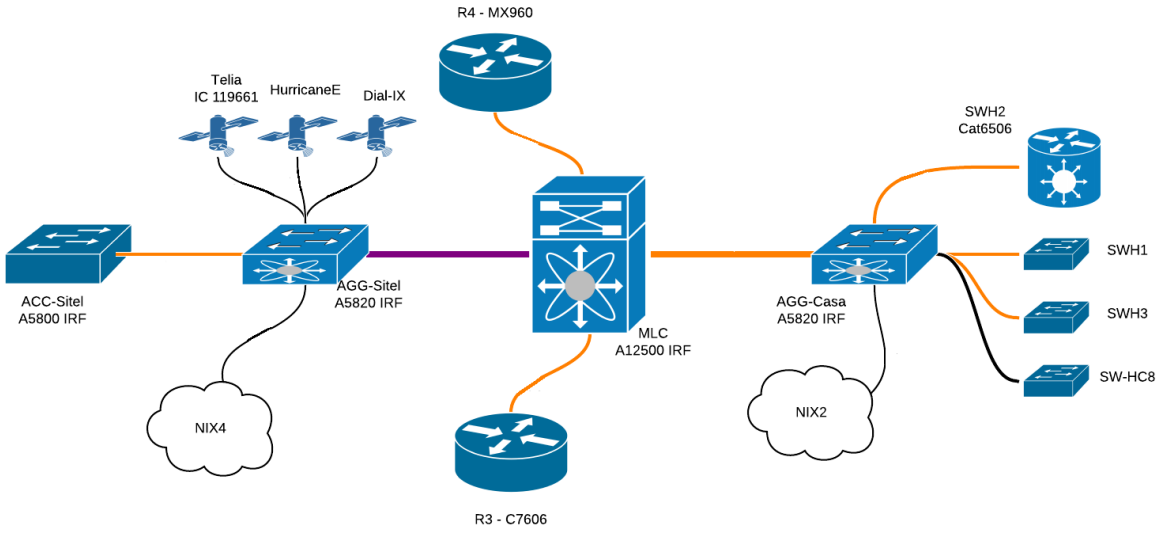
Casablanca INT má pronajaté prostory u společnosti Ce Colo (budova Sitel), kde provozuje část své páteřní síťové infrastruktury. Většina klíčových prvků sítě se nachází v datovém sálu HC3 a také právě v datovém sálu Ce Colo. Skutečné zapojení páteřní sítě vystihuje následující diagram, který slouží zároveň k dohledu sítě a bude znovu zmíněn v kapitole 4.2.9. Na diagramu je patrná dělící linie, která rozděluje infrastrukturu na dvě základní části. Horní segment diagramu představuje prvky, jež se nacházejí v serverovně

Sitelu. Ve spodní části potom figurují zařízení, která jsou umístěna v datovém centru Casablanca INT.



Obrázek 25 - Zobrazení síťové infrastruktury, ZDROJ: firemní dokumentace

Spojení agregačních prvků s okolním světem a partnerskými společnostmi je potom zobrazeno na dalším diagramu. Připojení jsou vesměs realizována optickým přenosem.



Obrázek 26 - Klíčové prvky páteřní sítě, ZDROJ: firemní dokumentace

MLC (multi-level-core) a AGG-Casa jsou agregační switche umístěné v HC3. Z nich jsou potom připojené další přepínače a routery, které rozvádí konektivitu dále po datovém centru. AGG-Sitel a ACC-Sitel jsou agregační switche umístěné v serverovně budovy Sitel. Zajišťují především spojení s vnějším internetem (trasy do společností Telia, Hurricane Electric, Dial Telecom). Výrobci jednotlivých zařízení jsou převážně společnosti Cisco, Juniper, Huawei, či Hewlett-Packard.

Připojení ke konkrétním stojanům či serverům je řešeno kroucenou dvoulinkou případně optickými kabely. Vzhledem k velkému množství kabelů je využíváno vedení pod zdvojenou podlahou nebo stropními rastry.

4.2.8 Síťové zabezpečení

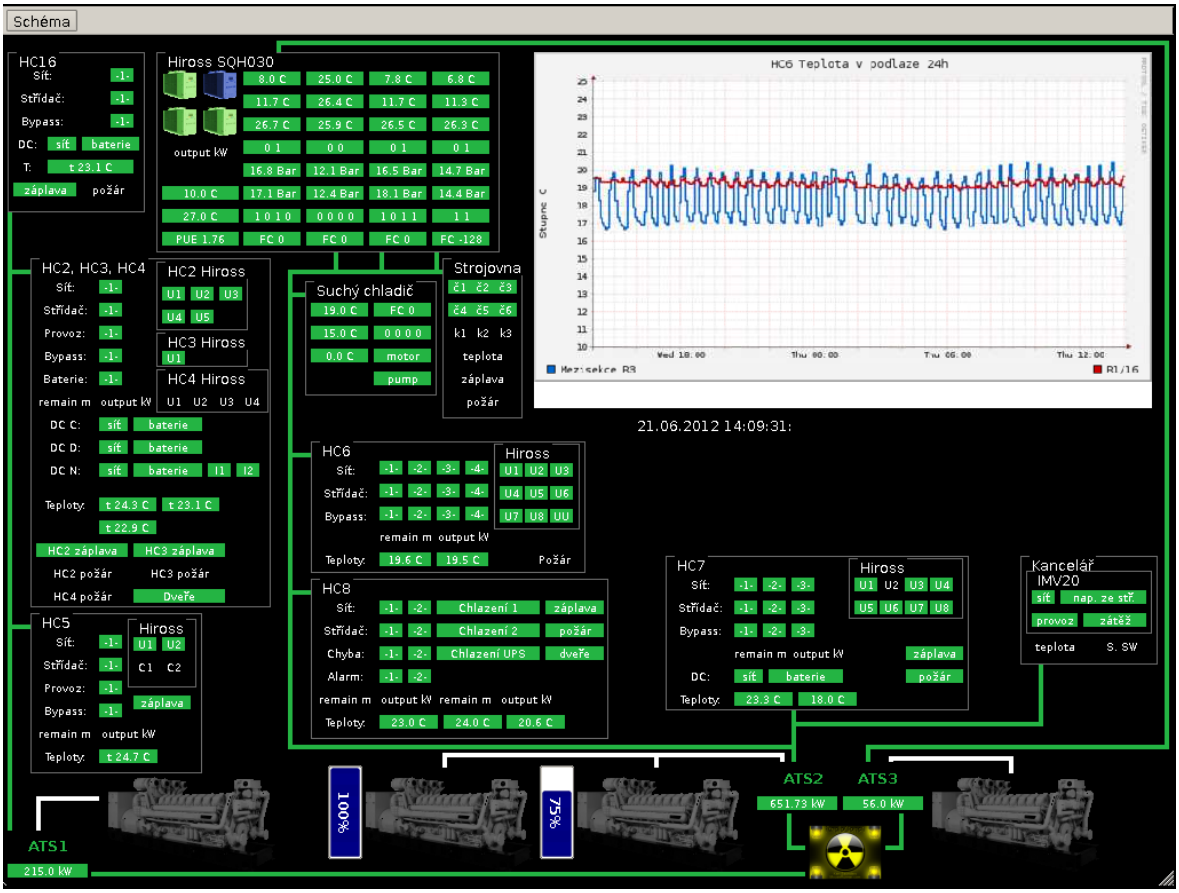
Zabezpečení sítě zajišťují firewally, jenž jsou umístěny na klíčových místech sítě – především před firemními servery. Pravidla pro komunikaci v síti lze však také adekvátně nastavit přímo na stěžejních síťových zařízeních (router, switch). Zákaznické servery a jimi využívané porty nejsou žádným způsobem blokovány, pokud ovšem zásadním způsobem nenarušují síťovou bezpečnost (DDoS, spam, apod.). V případě DDoS útoku je zde dohledový systém, který reaguje na příliš velký přenos dat a tento přenos okamžitě reportuje jako kritický. Administrátor na základě alarmu reaguje adekvátním způsobem tak, aby útok zastavil. Řešením bývá z valné většiny blokace zdrojové či cílové IP adresy (tzv. „black hole“) a její následné přidání do ACL (acces control list).

Hlavním bezpečnostním prvkem v datovém centru z hlediska cloudových služeb je IPS – systém prevence narušení, který je umístěn v HC3. Jedná se o zařízení TrendMicro TippingPoint pro softwarové zabezpečení, které chrání data před viry, exploity, útoky na webové aplikace a provádí kompletní inspekci paketů až po sedmou aplikační vrstvu ISO/OSI modelu. TippingPoint obsahuje rozsáhlou databázi potenciálních bezpečnostních rizik, která se neustále aktualizuje a chrání data na více úrovních. Ukládaná data jsou duplikována pomocí virtualizační technologie VMware a uchovávána na dvou geograficky oddělených místech - jsou tak zároveň pro všechny případy rovnou zálohována a minimalizuje se riziko jejich ztráty. Jednotlivé filtry, na základě kterých se zařízení rozhoduje, zda pakety propustí, se aktualizují 3x týdně. K dispozici jsou také reporty a logy jednotlivých operací. Tímto systémem je chráněn především cloud a některé z firemních serverů.

4.2.9 Dohledové systémy a monitoring

Jedním ze zásadních bodů zabezpečení a bezproblémového provozu datového centra je kvalitní monitoring a dohledové systémy. Dohledové centrum je provozováno v druhém patře budovy v zázemí technického oddělení. Casablanca INT používá k dohledu několik systémů či nástrojů, z nichž každý sleduje konkrétní stránky datového centra. V první řadě v dohledovém centru figurují dva projektory, z nichž každý zprostředkovává monitoring různých aspektů datového centra.

První projektor je určen pro dohled energetiky, chlazení a dalších zařízení, která monitorují stav serveroven. Dohledová plocha se skládá z textových podbarvených panelů, jednoho slotu pro graf (zde se střídají různé teplotní grafy), logu s posledními událostmi, informačních ikon a čar značících vedení energetické větve.



Obrázek 27 - Monitoring datového centra, ZDROJ: firemní monitoring

Dohledový software má 4 druhy možných notifikací událostí:

- změna podbarvení textového panelu nebo změna ikony
- záznam v logu na obrazovce
- změna pozadí do modré barvy
- přehrání zvuku

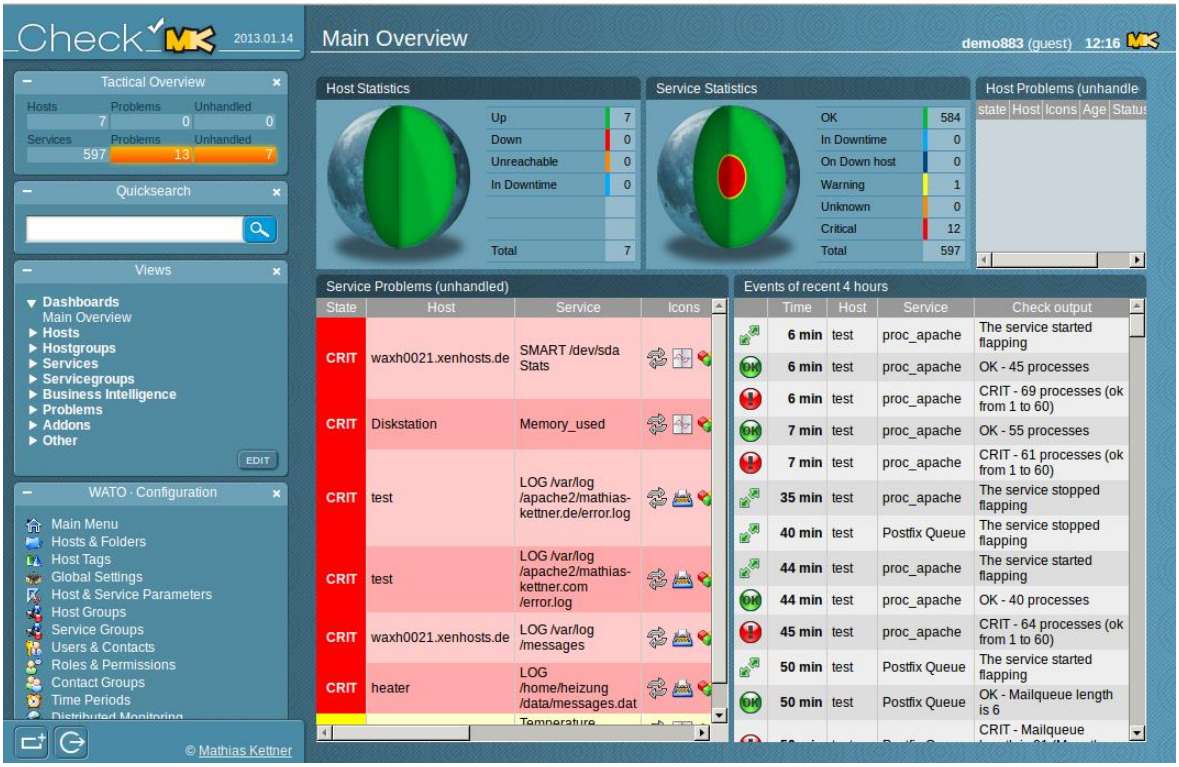
Pro různé události lze notifikace libovolně kombinovat. Některé tedy jen mění podbarvení a přehrají zvuk, jiné mění i pozadí a podobně. Textové panely mohou nabývat třech barev:

- zelená - stav, kdy je hodnota v pořádku
- červená - zjištěna chyba - hodnota je mimo rozsah apod.
- oranžová - nelze zjistit stav, protistrana neodpovídá

Druhý projektor je zaměřen na dohled samotné infrastruktury páteřní sítě (diagram druhého projektoru je zobrazen v kapitole 4.2.7). Zde jsou zobrazeny hlavní prvky datového centra – agregační switche, routery, cloud a podobně. V případě částečné nedostupnosti začne konkrétní prvek blikat oranžovou barvou a u objektu se zobrazí doprovodný text s IP adresami, kterých se problém týká. V případě úplné nedostupnosti

začne prvek blikat červeně. Kontroly dostupnosti jednotlivých objektů jsou prováděny na principu příkazu „ping“.

Dalším dohledovým nástrojem je webový portál Check_MK (Mathias Kettner), který sleduje celou řadu prvků a hodnot. Dalo by se říci, že v něm lze nastavit sledování téměř čehokoliv. Monitoruje kritické či téměř kritické hodnoty komponent konkrétních serverů (od vytížení procesoru až po zaplnění disku), provoz na páteřní síti, stav energetiky, chlazení, fyzické přístupy (např. otevření dveří datového sálu), dostupnost zákaznických linek či cloudu atd.



Obrázek 28 - Ukázka dohledového systému Check_MK[26]

Pro sledování teplotních grafů a stavu energetiky slouží další dohledový portál, stejně tak jako pro sledování provozu na jednotlivých linkách.

5 Výsledky a diskuse

Je důležité si uvědomit, že problematika datových center sestává z mnoha vrstev a technologických celků. Každou z těchto vrstev lze potom považovat za samostatné téma, které je mnohdy velmi obsáhlé. Zkoumané datové centrum bylo analyzováno za pomoci teoretických východisek a také praktických zkušeností z provozu daného centra.

5.1 Zhodnocení řešení zkoumaného datového centra

Datové centrum společnosti Casablanca INT, které se nachází v Praze na Vinohradské ulici je provozováno již více než 15 let. Od svého spuštění již prošlo několika rekonstrukcemi a vylepšeními. Lokalita, kde je datové centrum umístěno, je velmi výhodná především z pohledu dostupnosti. Ve své době se jednalo vlastně o první zařízení svého druhu, jenž bylo poblíž centra Prahy vystavěno a uvedeno do provozu a dodnes se jedná o jedno z největších datových center v ČR. Na druhou stranu je umístění některých datových sálů rizikové z hlediska bezpečnosti. Serverovny provozované v přízemí či, suterénu výškové budovy se nachází pod kancelářemi a restaurací, přičemž se nad nimi nachází i vodovodní a odpadní rozvody. Hrozí zde tedy riziko neočekávané události zaviněné třetí stranou. Toto riziko dokazuje i nehoda, která se stala roku 2014, kdy v jednom z vyšších pater došlo k havárii potrubí, voda se dostala až do serverovny HC8 a došlo k poškození zákaznických serverů a části cloudu Big Blue One. Data se však podařilo obnovit ze záloh beze ztrát. Z tohoto důvodu bylo jako dodatečné opatření pro ochranu dat zprovozněno další zálohovací pole, které je umístěno na geograficky odlišném místě (serverovna společnosti Ce Colo). Je jasné, že uvedené riziko lze v tomto případě eliminovat pouze přesunem serveroven na jiné místo, případně zapouzdřením celého datového sálu. V obou případech by to znamenalo velmi vysoké ekonomické výdaje. V případě přesunu serveroven na jiné místo, je však toto řešení prakticky nemožné, vzhledem k již existujícím datovým uzlům a přípojkám. V ideálním případě by však datové centrum mělo být vystavěno na odlehlém místě v samostatné budově bez vodovodních rozvodů.

Z hlediska energetické soustavy a zálohování přísunu elektrické energie je řešení v datovém centru dostačující. Přísun energie zajišťují celkem 3 ATS systémy, které také v případě výpadku sítě zajišťují přepnutí na napájení z motorgenerátorů. Ty jsou v datovém centru celkem čtyři a jsou schopny zásobovat THC energií 20 hodin, při

doplnění paliva i déle. Krátký výpadek (např. pokud nestihnou agregáty naběhnout ihned) pomáhají překlenout UPS systémy zapojené v redundanci N + N (či 2N). Je zde tedy počítáno i s možností poruchy aktuálně běžících UPS – v takovém případě je v provozu ihned nahradí stejný počet UPS připravených jako záloha.

Chladící soustava využívá primárně 4 výrobníků chladu, které ochlazují vodu a pomocí šesti čerpadel umístěných ve strojovně (S1) a sítě rozvodů, ji rozvádí po celém datovém centru do chladících jednotek (klimatizací). Ty následně v serverovnách vzduch ochlazují a zajišťují jeho cirkulaci. Chladící rozvody jsou v datových sálech vedeny primárně zdvojenými podlahami, případně stropními rastry (HC5, HC2). Chillery se nacházejí na střeše na úrovni druhého patra společně se suchým chladičem, který pomáhá šetřit energii v chladných měsících tím, že vodu ochlazuje okolním vzduchem. Jeden či více chillerů mohou být v takovémto případě vypnuty. Vzhledem k členitosti datového centra je rozvod vody poměrně náročný na energii. V případě umístění datových sálů na společném patře by rozvodná síť mohla být méně složitá a kratší. V serverovnách se v zásadě používají dva základní typy chlazení a cirkulace vzduchu. Prvním způsobem je systém studené a teplé uličky, druhým potom chlazení skrze zdvojenou podlahu datového sálu. Teploty ve studených uličkách během roku nepřekračují 25 °C, což je podle ASHRAE dostatečně nízká teplota pro provoz serverů a souvisejících technologií. Nicméně je třeba si uvědomit, že teplota přiváděného vzduchu je obvykle ještě mnohem nižší. Dále je nutno zmínit, že teploty v datových sálech se odvíjejí od zatížení jednotlivých serveroven a hodnoty v teplých uličkách jsou podstatně vyšší (při plném zatížení v HC8 např. až 35 °C).

Obrázek 29 - Datový sál HC8, ZDROJ: vlastní

Základním kamenem požární ochrany jsou v datovém centru optická čidla pro detekci kouře a dále také teplotní čidla, která sledují jakékoliv podezřelé zvýšení teplot. V každé ze serveroven je několik sněhových (CO_2) hasicích přístrojů, pomocí kterých lze případný vzniklý požár rychle eliminovat. Do budoucna by však bylo vhodné v datových sálech použít SHZ tak, jako je tomu v serverovně HC8. EPS v tomto případě spustí při vzniku požáru alarm a během 2 minut SHZ zajistí automatické hašení konkrétního úseku stlačenou demineralizovanou vodní mlhou. U vstupu do serverovny a do rackových uliček jsou potom také tlačítka pro manuální spuštění či blokaci SHZ. Jako dodatečná ochrana jsou v datovém sálu HC8 umístěny i klasické hasicí přístroje.

Záplavová čidla se nachází podél všech rackových uliček v podobě „modrých kabelů“. Další čidla jsou potom u chladících jednotek a pod chladícími rozvody, kde je vyšší riziko záplavy. V horkých měsících se zde může kondenzovat voda a docházet k úniku chladící kapaliny. V případě jakéhokoliv styku s vodou zaznamená dohledový systém alarm. Budova se nenachází v záplavové zóně, takže z tohoto pohledu je umístění datového centra v pořádku. Pokud by přeci jen došlo k záplavě vyššího rozsahu, je důležité, že jsou v datových sálech použity zdvojené podlahy. Zde se pak může voda hromadit a nezůstává v rackových stojanech. Serverovna HC16 je navíc riziková, pokud by došlo k extrémnímu dešti. V 16. patře zde může voda prosakovat stropem

a je tedy důležité dbát na kvalitní izolaci. Izolování stropu serverovny bylo v posledních letech posíleno a je dostatečné.

Datové centrum je přístupné celoročně 24 hodin 7 dní v týdnu. Vnější perimetr lze vzhledem k lokalitě budovy zajistit složitě. Nicméně v okolí figurují městské kamery, což by měla být dostatečná ochrana. Přístup do budovy hlídá pracovník bezpečnostní služby na vrátnici. Každý, kdo vstupuje do datového centra je povinen prokázat se pracovníkovi platným občanským průkazem (cizinci pasem) zaznamenaným v přístupovém systému Casablanca INT. Čipovou kartu následně přiloží na terminál recepce. Zde se zaznamená skutečný příchod návštěvníka do datového centra. Pro přístup do konkrétního datového sálu je potom nutné přiložit přístupovou kartu na čtečku u vstupu do dané serverovny. Jakýkoliv požadavek na zpřístupnění serveru (odemknutí racku), vzdálený restart serveru, připojení konzole KVM, výnos hardware, či jednorázový přístup třetí osoby, musí být potvrzen pracovníkem Casablanca INT. Opět je zde kontrolován platný doklad zákazníka a všechny strany podepisují protokol ohledně dané operace. Zákazník také musí mít oprávnění k dané operaci. Záznamy o zákaznících, čísla osobních dokladů a práva k operacím jednotlivých osob jsou vedeny ve firemním zákaznickém systému CRM. Zde jsou také zaznamenány veškeré operace související s přístupy do datového centra. Datové sály i kamerové systémy jsou pravidelně kontrolovány pracovníky Casablanca INT a bezpečnostní služba fyzicky prochází v daných intervalech zbylé prostory budovy. Kamery jsou umístěny ve všech datových sálech a sledují pohyb v jednotlivých rackových uličkách a u vstupů do serveroven. Kamerový záznam je ukládán. Samotné vchody do budovy potom sleduje bezpečnostní pracovník na vrátnici. Na fyzickou bezpečnost je ve zkoumaném datovém centru kladen velký důraz a vzhledem k daným možnostem je plně dostačující. Jako dodatečné opatření by bylo vhodné zavést přístup na principu bio senzorů např. otisku prstu, hlasu, či sítnice. Datové centrum však denně navštíví desítky osob a vzhledem k problémům při využití této technologie by to pravděpodobně nebylo příliš efektivní. Zavedení tohoto systému by však mohlo být přínosem pro vstup do firemní serverovny HC3, kam běžní zákazníci zpravidla přístup nemají, poněvadž jsou zde umístěny především klíčové technologie potřebné pro chod či zabezpečení celé síťové infrastruktury.

Základem síťové infrastruktury je celá řada klíčových prvků, jako jsou core switche či routery. Páteřní síť lze rozdělit do dvou základních částí. První část je umístěna

v serverovně Sitelu a zajišťuje mimo jiné konektivitu do zahraničí a k partnerským společnostem (společnost Telia, Hurricane Electric, Dial Telecom, uzel NIX.CZ). Druhá část se nachází přímo v datovém centru na Vinohradské ulici a zprostředkovává spojení se zbylými datovými sály. Následuje zapojení dalších switchů, na jejichž porty jsou připojeny zákaznické či firemní servery, dohledové servery, cloud, technické oddělení atd. Primární konektivita do sítě Internet je 2x 20 Gb/s v rámci uzlu NIX.CZ a 30 Gb/s v rámci zahraničního provozu. Vzhledem k využití dat zákazníky je tato kapacita v současné době plně dostačující, což lze také pozorovat na grafech datových přenosů. Tato konektivita je řešena pomocí optických vláken. K rozvodu v síti je potom využita také kroucená dvoulinka. Pro zabezpečení sítě je využíváno firewallů umístěných na klíčových místech síťové infrastruktury a také IPS – TippingPointu, který zajišťuje především zabezpečení cloudu. Případné DDoS útoky jsou řešeny blokací zdrojové či cílové IP adresy na konkrétním core switchi či routeru (tzv. black-holing) a případném přidání adresy do ACL. Zde však může figurovat pouze omezený počet IP adres. Jako dodatečná ochrana proti DDoS útokům by bylo vhodné implementovat do sítě zařízení speciálně konstruované na DDoS ochranu – tzv. anti - DDoS (např. od spol. Huawei). Nicméně pořízení takového zařízení by opět znamenalo poměrně vysoké výdaje. V serverovnách jsou použita optická vlákna či kroucené dvoulinky. Vedení kabelů v datovém centru je řešeno stropními rastry či skrze zdvojenou podlahu.

Systémů monitorujících provoz a výskyt neočekávaných událostí v datovém centru je používáno několik. Primárním dohledovým nástrojem jsou dva projektory. První sleduje energetické systémy, chlazení a teploty. Jsou zde také zobrazovány případné požární či záplavové alarmy a poruchy konkrétních zařízení. Druhý projektor sleduje páteřní síť a její dostupnost. Pro dodatečný dohled je potom využíváno několik portálů. Sledován je provoz na síti (vytížení linek), stav komponent konkrétních serverů, či zahlcení mailových serverů v případě spamu. Jako dodatečný dohledový nástroj je využíván mobilní telefon, kam o zásadních událostech přijde v případě problému SMS. Zároveň je také správcům jednotlivých částí sítě odesílán v případě problémové události automatický e-mail. Dohledové centrum, které se nachází ve druhém patře budovy je řešeno adekvátně vzhledem k rozsahu a stavu datového centra. Poměrně velkou výhodou je malá vzdálenost mezi dohledovým centrem a zbylými serverovnami. V případě jakéhokoliv problému tak můžou pracovníci Casablanca INT reagovat a fyzicky se dostat

na kýžené místo velmi rychle. Výjimku tvoří serverovna HC16, která je až v 16. patře. Zde trvá cesta výtahem delší dobu a v případě nefunkčnosti výtahů by potíže v tomto datovém sálu mohly být fatální. Celé technické oddělení je chráněno proti výpadku elektrického proudu systémem UPS.

Casablanca INT poskytuje celou řadu služeb. Služby, které jsou primárně spojeny s provozováním datového centra, jsou server housing, poskytování virtuálních serverů (cloud), zálohování dat a správa serveru. Vzhledem k těmto službám je infrastruktura řešena adekvátně. Předpokládáme-li však postup současných technologií, bude nutné podstatně rozšířit virtualizaci a cloudové služby datového centra neboť poptávka po těchto technologiích se stále zvyšuje. Zákazníci však mají k dispozici vše potřebné pro správu vlastních serverů či vzdálenou podporu. Mají možnost využít vzdáleného restartu svého serveru či připojení konzole pro vzdálený přístup. V obou případech je nutné kontaktovat podporu z autorizovaného kontaktu, případně sdělit aktuální číslo svého občanského průkazu. Návštěvníkům datového centra jsou v serverovnách k dispozici pojízdné konzole pro připojení k jejich serverům (standardně monitor, myš, klávesnice, napájecí kabely). V každém datovém sálu jsou tyto konzole po 2 až 3 kusech. Některé z konzolí by bylo vhodné obměnit a investovat do kvalitnějších zařízení, neboť již nejsou v příliš dobrém stavu. V každém datovém sálu je také několik stoliček pro přístup do vyšších míst rackových stojanů.

5.2 Předpokládaný vývoj

Při rozboru předpokládaného vývoje datového centra Casablanca INT, je opět nutné brát v úvahu především lokalitu, kde se datové centrum nachází a současné řešení daných serveroven. Již bylo zmíněno rizikové umístění některých datových sálů. Nicméně pokud jsou brány v úvahu všechny uvedené aspekty, nelze pokládat případný přesun datového centra do jiné lokality, za příliš reálný. Investice vynaložené na případné přemístění by mohly dosahovat až desítek milionů korun a lze je pokládat za příliš vysoké. Nemluvě o nutnosti vybudování nových optických tras, které by zajišťovaly spojení s okolím. Na druhou stranu je však současná lokalita velmi výhodná z hlediska dostupnosti datového centra a realizace internetového připojení pro velké množství pražských zákazníků. Lze tedy předpokládat, že THC zůstane umístěno na Vinohradské ulici. V tomto případě pak lze očekávat modernizaci jednotlivých serveroven a to především datových sálů HC5

a HC2. U těchto sálů není rozmístění rackových stojanů příliš efektivní z hlediska chlazení a rackové uličky nejsou zcela uzavřeny tak, jako je tomu v serverovně HC8. Design těchto datových sálů celkově nepůsobí příliš homogenně. Stejně tak lze předpokládat podstatnou expanzi cloudových služeb a virtualizačních technologií. V současné době (únor 2018) již probíhá rozšíření stávajícího cloudu Casablanca INT a v serverovně HC6 je tak k tomuto účelu zřizováno několik nových rackových stojanů. Pro posílení síťového zabezpečení je plánováno nasazení inteligentní automatické ochrany proti DDoS útokům. V současné době již probíhá její testování a implementace. Posun lze očekávat také ohledně dostupnosti a zabezpečení zákaznických služeb. Současné trendy totiž směřují k tzv. vrstvě Tier 0, kdy je celé fyzické datové centrum zrcadlově provozováno jako plně cloudové datové centrum a v případě výpadku fyzických technologií je nahradí technologie virtuální. Také v tomto případě však bude nutná poměrně vysoká investice a to zřejmě v podobě výstavby minimálně jednoho dalšího datového sálu. V každém případě lze říci, že rozvoj a modernizace datového centra Casablanca INT se bude v budoucnosti z velké části odvíjet především od výnosů společnosti a poptávce po jejích službách, za předpokladu udržení současného standardu a provozu služeb stávajících.

6 Závěr

Jednotlivé cíle práce byly splněny. Teoretická část je zaměřena na samotné představení datových center. Je zde uveden jejich současný stav a historický vývoj. Dále také účel, možnosti zabezpečení a související technologie. Tato problematika je řešena především v kapitole 3.3 „Infrastruktura a technologické celky datového centra“. V dalších podkapitolách jsou potom uvedeny typy datových center, jejich dostupnost a klasifikace.

V praktické části je analyzováno zkoumané datové centrum společnosti Casablanca INT. V jednotlivých kapitolách je zde představen jeho design a konkrétní datové sály. Dále jsou uvedeny služby daného datového centra a také jeho technologické celky společně se zabezpečením a používanými postupy. Konkrétně je zkoumána rozvodná síť a záložní zdroje datového centra. Dále také síťová infrastruktura a chlazení datových sálů. Z hlediska bezpečnosti je v praktické části uvedeno řešení požárního a záplavového zabezpečení a také fyzického přístupu a síťového zabezpečení. V neposlední řadě jsou zmíněny dohledové systémy a monitoring datového centra Casablanca INT.

Na základě teoretických východisek a praktických zkušeností z provozu zkoumaného datového centra je zhodnoceno jeho stávající řešení a navrženy možnosti ke zkvalitnění jeho služeb a zabezpečení. V zásadě lze říci, že největší nevýhodou z hlediska zabezpečení datového centra je lokalita, ve které se nachází. Umístění serveroven v přízemí či suterénu šestnáctipatrové kancelářské budovy je rizikové, neboť budovou prochází vodovodní a odpadní rozvody a existuje tak zde možnost havárie zaviněné třetí stranou. Také riziko požáru je z tohoto pohledu vyšší. V ideálním případě by datové centrum mělo být provozováno v samostatné a jednoúčelové budově. Přesun zkoumaného datového centra na jiné místo by byl však velmi problematický a nákladný vzhledem k již existujícím datovým uzlům. Na druhé straně je současná lokalita výhodná z pohledu dostupnosti datového centra pro zákazníky. Síťové zabezpečení by bylo vhodné posílit bezpečnostním zařízením, určeném pro eliminaci DDoS útoků. V současné chvíli jsou takovéto útoky řešeny blokováním zdrojové či cílové IP adresy, což vyžaduje aktivní zásah administrátora. Cloudové služby jsou nicméně chráněny systémem IPS a zálohovány na dvou dalších geograficky odlišných místech. Díky tomu lze považovat současné zabezpečení cloudu za plně dostačující. Samotná síťová infrastruktura je vzhledem k účelu a možnostem zkoumaného datového centra řešena adekvátně a kapacita datových linek pro zákaznické

služby je plně dostačující. V neposlední řadě je doporučeno zvýšení zabezpečení přístupu do firemní serverovny HC3, zavedení stabilního hasicího zařízení do všech serveroven, a výměna zastaralých konzolí v některých serverovnách. Dále by také byla vhodná modernizace datových sálů HC5 a HC2, což se v budoucnu také předpokládá. Stejně tak lze očekávat expanzi cloudových a virtualizačních technologií.

7 Seznam použitých zdrojů

1. GENG, Hwaiyu. *Data center handbook*. 1. Hoboken, New Jersey: Wiley, ©2015, 720 s. ISBN 978-1-118-43663-9.
2. The evolution of the data center : Timeline from the Mainframe to the Cloud - SiliconANGLE. *SiliconANGLE* [online]. United States: SiliconANGLE Media, 2014 [cit. 2017-07-20]. Dostupné z: https://siliconangle.com/blog/2014/03/05/the-evolution-of-the-data-center-timeline-from-the-mainframe-to-the-cloud-tc0114/
3. The Data Center: Past, Present and Future. *Wikibon* [online]. United States: Wikibon, 2014 [cit. 2017-05-20]. Dostupné z: http://wikibon.org/wiki/v/The_Data_Center:_Past,_Present_and_Future
4. Datacentra. *Živě.cz* [online]. ČR: CN Invest, ©2017 [cit. 2017-05-20]. Dostupné z: https://www.zive.cz/datacentra/sc-690/default.aspx
5. Understanding the Different Types of Data Center Facilities. *CyrusOne* [online]. United States: CyrusOne, ©2017 [cit. 2017-06-14]. Dostupné z: https://cyrusone.com/corporate-blog/understanding-the-different-types-of-data-center-facilities/
6. ARREGOCES, Mauricio a Maurizio PORTOLANI. *Data Center Fundamentals*. 1. Indianapolis: Cisco Press, ©2004, 1104 s. ISBN 1-58705-023-4.
7. Inteligentní koncepty klimatizace pro datová centra. *Novinky – elektrotechnika elektronika energetika průmyslová automatizace* [online]. ČR: Ing. Jakub Slavík, 2017 [cit. 2017-07-21]. Dostupné z: http://www.proelektrotechniky.cz/elektroinstalacni-technika/14.php
8. Moderní datová centra: Bezpečné zázemí pro cloud. *BusinessIT* [online]. ČR: BusinessIT.cz, 2013 [cit. 2017-07-21]. Dostupné z: http://www.businessit.cz/cz/moderni-datova-centra-bezpecne-zazemi-pro-cloud.php
9. Datová centra realisticky. *SystemOnLine.cz* [online]. ČR: CCB, ©2010 [cit. 2017-08-05]. Dostupné z: https://www.systemonline.cz/sprava-it/datova-centra-realisticky.htm
10. Bezpečnost v datových centrech? *SystemOnLine.cz* [online]. ČR: CCB, ©2016 [cit. 2017-08-05]. Dostupné z: https://www.systemonline.cz/clanky/bezpecnost-v-datovych-centrech.htm

11. Fyzická bezpečnost datových center. *Hospodářské noviny* [online]. ČR: Economia, ©2016 [cit. 2017-08-05]. Dostupné z: https://ictrevue.ihned.cz/c3-65470890-0ICT00_d-65470890-fyzicka-bezpecnost-datovych-center
12. Uptime Institute LLC - publications. *Uptime Institute LLC* [online]. United States: Uptime Institute, ©2013-2017 [cit. 2017-01-11]. Dostupné z: https://uptimeinstitute.com/publications
13. Jsou datacentra s TIER certifikací opravdu bezpečnější? *ITBIZ* [online]. ČR: Nitemedia, 2014 [cit. 2017-08-03]. Dostupné z: http://www.itbiz.cz/clanky/jsou-datacentra-s-tier-certifikaci-opravdu-bezpecnejsi
14. Virtualizace v kostce. *SystemOnLine.cz* [online]. ČR: CCB, 2010 [cit. 2017-08-06]. Dostupné z: https://www.systemonline.cz/clanky/virtualizace-v-kostce.htm
15. Co je cloud computing? *Microsoft Azure: Cloudová výpočetní platforma a služby* [online]. ČR: Microsoft, 2017 [cit. 2017-08-06]. Dostupné z: https://azure.microsoft.com/cs-cz/overview/what-is-cloud-computing/
16. Cloud computing *Cloud.cz* [online]. ČR: Cloud.cz, 2017 [cit. 2017-08-06]. Dostupné z: http://www.cloud.cz/cloud/158-cloud-computingco-ty-pojmy-znamenaji.html
17. Facebook opens its first data center outside the US, near the Arctic Circle in Luleå, Sweden. *The Next Web* [online]. The Netherlands: The Next Web, 2013 [cit. 2017-08-08]. Dostupné z: https://thenextweb.com/facebook/2013/06/12/facebook-opens-its-first-data-center-outside-the-us-near-the-arctic-circle-in-lulea-sweden/#.tnw_lsAwQoP0
18. PRONIX dokončil dodávku záložních zdrojů pro datové centrum Kokura společnosti Seznam.cz. *PRONIX s.r.o.* [online]. ČR: Pronix, 2017 [cit. 2017-08-08]. Dostupné z: http://www.pronix.cz/PRONIX-dokon-Til-dod-vku-z-lo-n-ch-zdroj-pro-datov-centrum-Kokura-spole-Tnosti-Seznam.cz-news59.html
19. 2016 Industrial Chiller Trends That Will Affect Your Bottom Line. *Industrial Chillers* [online]. United States: Oklahoma Chiller, 2016 [cit. 2017-08-08]. Dostupné z: http://okchiller.com/2016-industrial-chiller-trends-that-will-affect-your-bottom-line/
20. Distributed Denial of Service Attacks. *Cisco* [online]. United States: Cisco, 2017 [cit. 2017-08-08]. Dostupné z: https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-30/dos-attacks.html

21. HP Unveils Expanded Enterprise Security Solutions for the Instant-On Enterprise. *HP* [online]. United States: HP, 2011 [cit. 2017-08-08]. Dostupné z: http://www8.hp.com/us/en/hp-news/press-kit.html?id=1110585
22. MoNet. *Novicom, s.r.o.* [online]. ČR: Novicom, 2017 [cit. 2017-08-08]. Dostupné z: https://www.novicom.cz/monet
23. How Cloud Computing Saves You Money. *IntelliSyn Communications Inc.* [online]. United States: IntelliSyn Communications, 2017 [cit. 2017-08-08]. Dostupné z: http://www.intellisyn.com/2017/07/24/cloud-computing-saves-money/
24. Datacentrum MasterDC. *Server Hosting, Housing, Virtuální servery VPS - Master Internet* [online]. ČR: Master Internet, ©1998-2017 [cit. 2017-08-08]. Dostupné z: https://www.master.cz/datacentrum/
25. Google. *Mapy Google* [online]. Mountain View: Google, 2017 [cit. 2018-03-17]. Dostupné z: https://www.google.cz/maps/place/Vinohradsk%C3%A1+2396%2F184,+130+00+Praha+3-Vinohrady/@50.0784861,14.4723295,14z/data=!4m13!1m7!3m6!1s0x470b936f19e14885:0x357ee85f7bec9889!2sVinohradsk%C3%A1+2396%2F184,+130+00+Praha+3-Vinohrady!3b1!8m2!3d50.0780669!4d14.4721313!3m4!1s0x470b936f19e14885:0x357ee85f7bec9889!8m2!3d50.0780669!4d14.4721313?hl=cs
26. Spiceworks. *Network Monitor proposal? Really? - Spiceworks* [online]. Austin: Spiceworks, 2014 [cit. 2018-03-17]. Dostupné z: https://content.spiceworksstatic.com/service.community/p/topic_images/0000000522/53cffcea/attached_image/mini_magick20140723-8986-1jrbxxg.png