Česká zemědělská univerzita v Praze

Technická fakulta

Analýza bezpečnosti datových úložišť v počítačových sítích

bakalářská práce

Vedoucí bakalářské práce

Ing. Zdeněk Votruba

Autor

Martin Čejka

PRAHA 2015

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra technologických zařízení staveb

Technická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Martin Čejka

Informační a řídicí technika v agropotravinářském komplexu

Název práce

Analýza bezpečnosti datových úložišť v počítačových sítích

Název anglicky

Security Analysis of data storage in computer networks

Cíle práce

Cílem práce je analyzovat stávající prostředky zabezpečení velkých datových úložišť a datových center. Zabezpečení dat datových úložišť zasahuje do oblasti spolehlivosti techniky a technologií ukládání dat, požární bezpečnosti, fyzické bezpečnosti, síťové bezpečnosti a bezpečnostní politiky. Práce je rovněž zaměřena na síťovou bezpečnost, zachovává si ale myšlenku komplexního pojetí bezpečnosti. Součástí práce je i rozbor struktury sítí datových úložišť spolu s definicí potencionálních rizik. V závěru práce jsou tak nabídnuta i řešení eliminace různých bezpečnostních rizik.

Metodika

Seznámit se s hlavními prostředky a technologiemi využívanými při zabezpečení datových úložišť a počítačových sítí a provést jejich analýzu a srovnání.

Doporučený rozsah práce

30 až 40 stran textu včetně obrázků, grafů a tabulek

Klíčová slova

bezpečnost, počítačové sítě, datová úložiště

Doporučené zdroje informací

HARRIS, S: a kol.. Hacking – manuál hackera, Grada Publishing. 2008, ISBN 978-80-247-1346-5
HERMINGHAUS, V. SCRIBA, A. Storage Management in Data Centers. Springer. Berlin-Heidelberg. 2009.
SOSINSKI, B.: Mistrovství – počítačové sítě, Computer Press. 2010, ISBN 978-80- 251-3363-7

Předběžný termín obhajoby

2015/05 (květen)

Vedoucí práce

Ing. Zdeněk Votruba, Ph.D.

Elektronicky schváleno dne 8. 1. 2014

doc. Ing. Jan Malaťák, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 3. 2. 2014

prof. Ing. Vladimír Jurča, CSc.

Děkan

V Praze dne 03. 04. 2015

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením Ing. Zdeňka Votruby, Ph.D. a uvedl v seznamu všechny použité literární a odborné zdroje. Souhlasím, aby práce byla půjčována ke studijním účelům a byla citována dle platných norem.

V Praze dne ……. ……

Martin Čejka

Poděkování

Speciální poděkování bych chtěl věnovat panu Ing. Zdeňku Votrubovi, Ph.D. za cenné informace, aktivní přístup a věcné připomínky, společnosti Kimbau, stavebně-inženýrská s.r.o. za poskytnutí materiálu k porovnání ekonomického a kvalitativního hlediska hasiv, panu Ing. Janu Růžičkovi ze společnosti CESNET za možnost navštívení datového úložiště a mé rodině za podporu.

Abstrakt: Cílem této bakalářské práce bylo informovat o moderních technikách a technologiích využívaných v datových úložištích k zajištění bezpečnosti a spolehlivosti provozu. V kapitole „Datová úložiště“ jsou uvedeny výhody a způsoby využití datových úložišť, technické parametry ukládání dat, a také je nastíněn budoucí vývoj technologií pro ukládání dat. Kapitola „Bezpečnost“ pak popisuje konkrétní technologie, které se využívají pro zabezpečení. Tato kapitola je rozdělena do podkapitol „Spolehlivost a efektivita datových center“, „požární bezpečnost“, „fyzická bezpečnost“, „síťová bezpečnost“ a „komplexní bezpečnost“. Práci doplňuje autorem napsaná příloha s názvem „Ekonomické hledisko datových úložišť“. Závěr práce obsahuje diskusi o dané problematice.

Klíčová slova: datové úložiště, bezpečnost, počítačové sítě

Security Analysis of data storage in computer networks

Summary: The aim of this bachelor thesis was to inform a reader about the newest methods and technologies that are used in data storages for ensure security and reliability of their traffic. In the chapter “Data storages” are introduced advantages and methods of using data storages, technical characteristics of storing data and also the future technologies of storing data are briefly drawn up. A chapter “Security” describes concrete technologies that are used for securing data storages. This chapter is divided into subchapters “Reliability and efficiency of data centers”, “fire safety”, “physical security”, “network security” and “complex security”. Bachelor thesis is complemented by one attached file created by the author named “Economic aspects of data storages”. The conclusion includes a discussion on the issue of data storages.

Keywords: data storage, security, computer network

1. Úvod

Nacházíme se v době, kdy informace mohou mít ve společnosti nejvyšší hodnotu. Myšleno je tím například výrobní tajemství společnosti nebo citlivé informace, které lze zneužít k poškození její reputace. Informace jsou dnes z největší části drženy ve formě počítačových dat. S prudkým nárůstem objemu a důležitosti firemních i osobních počítačových dat vyvstává otázka jejich uchovávání a bezpečnosti.

Data mohou být sbírána jinými společnostmi, zločinci, či dokonce státními orgány některých států. Mohou být zničena v důsledku chyby lidského faktoru i přírodní katastrofy. Způsobů odcizení nebo zničení je ale mnohem více.

Každá větší společnost pak musí řešit nejen investice do vlastního hardwaru a jeho provozu, které jsou nemalé zvláště v době, kdy objem firemních dat dosahuje mnohonásobně vyšších hodnot, ale hlavně bezpečnost svých dat. Ochranu dat je třeba vnímat velmi komplexně, a proto je třeba řešit spolehlivost technologií, bezpečnost požární, fyzickou, síťovou, a také bezpečnostní politiku celé společnosti. Jedním z řešení uchovávání a zabezpečení dat je využití datového úložiště.

Datové úložiště, jako prostor k uchovávání počítačových dat, může být lokální, přenosné anebo provozované třetí stranou vzdáleně přes síť internet. Bakalářská práce je orientována výhradně na posledně zmíněnou variantu.

Tato práce pojednává o stavu zabezpečení datových úložišť se zvláštním zaměřením na síťový provoz. Výstupem práce je popis technik a technologií, které se používají k zabezpečení dat zákazníků datových úložišť. Vedlejším cílem práce je informovat společnost o nutné ochraně proti kyberkriminalitě.

Vzhledem k faktu, že oblast bezpečnosti se příčinou technologického vývoje, selhávání zabezpečovacích systémů a inovací zločinců neustále mění, byl při tvorbě práce kladen důraz na aktuálnost.

2. Datová úložiště

Jak již bylo zmíněno v úvodu, cílem práce je popsat datová úložiště se vzdáleným přístupem, který je zprostředkován přes internet. Data tak poskytujeme třetí straně, čímž je míněna společnost, která službu datové úschovy provozuje. Trend posledních let však není jen o poskytování datového prostoru, ale také služeb spojených se správou dat a používáním softwaru, platforem, infrastruktur a nově i řešením bezpečnosti. Takovým službám se říká cloudové a užívá se pak pojem cloudová úložiště.

Využití služeb datového úložiště má řadu hodnotných výhod. V první řadě lze oproti lokální úschově dat ušetřit čas nutný k zajištění vhodného HW, k uvedení systému ukládání dat do provozu a k zajištění bezpečnosti. Malé společnosti tak nemusí investovat do drahého HW a jeho provozu. Navíc se není nutné tolik zabývat zálohováním, protože větší část zodpovědnosti za data nese provozovatel. I přesto se musí zálohovat nebo využít zálohovacích služeb provozovatele. Dalším plusem je zmírnění obav z poškození vlastní techniky – o data firma nepřijde a svůj provoz zahájí ihned po nahrazení předchozí techniky, bez složitých instalací. Moderní a pohodlný je také přístup k datům z různých zařízeních a různých lokalit. Zvolením cloudové služby lze navíc využít online práci v textových editorech, práci s vývojářskými nástroji a nově i s virtualizovanými stroji s OS, na kterých lze dále provozovat nesčetně komerčního softwaru. Nevýhodou je nutnost přístupu k internetu. Pokud jde pouze o data, je řešením synchronizovaná složka v lokálním počítači. V případě, že je firma závislá i na cloudových službách, není jiné řešení, než přesun lehké techniky do oblasti s přístupem k internetu. Potíže mohou nastat i při samotném přechodu firmy na vzdálené úložiště.

Služby, které datové úložiště poskytuje, jsou placené. Pokud je zákazníkem firma, je pak řešení dražší, komplexnější a s větší možností konfigurace, především bezpečnosti. Byly tak zmíněny dvě nejdůležitější hlediska při rozhodování – ekonomické a bezpečnostní. Třetím, často opomíjeným faktorem, je čas. Dalšími faktory mohou být pohodlnost a přístupnost.

2.1. Trendy cloud computingu

Popularita cloudových úložišť roste, což má své opodstatnění. Oproti klasickým datovým úložištím ale skrývají ta cloudová mnohem větší bezpečnostní rizika. Prvně je nutné zmínit, že většina cloudových úložišť, včetně těch největších, jako jsou Dropbox, Onedrive a Google Drive, nešifrují uložená data. V případě prolomení ochrany serverů by pak firemní data nebyla již chráněna. Navíc k nim má přístup i samotný provozovatel, a pak záleží, do jaké míry takové společnosti můžeme věřit. Částečným řešením je šifrovat data již před přenosem nebo přejít k takovým provozovatelům, kteří data na discích šifrují a sami obsah uložených dat neznají. Mezi takové patří úložiště SpiderOak, Wuala nebo Mega. [1] Šifrování komunikace a dvoufázový přístup už je naštěstí samozřejmostí cloudových úložišť. Zajímavým českým projektem právě vstupujícím do světa cloudových úložišť, je Cryptelo Drive, který nabízí velmi silné šifrování přenosu i uložení dat. Bezpečnost odpovídá úrovni TOP SECRET podle definice NSA. Nejkomplexněji myšlenku cloudu uchopil Microsoft s produktem Azure, nabízející virtuální stroje s OS a komerčním SW, včetně všech konkurenčních řešení.

2.2. Technické parametry ukládání dat

Jsou tři známé technologie ukládání dat – DAS, NAS a SAN. Velká datová úložiště využívají posledně zmíněnou technologii SAN s komunikačním rozhraním FC, SCSI nebo iSCSI. SAN je datová síť, která umožňuje přístup k datům z více serverů. Data jsou fyzicky uložena v datových centrech, z bezpečnostních důvodů ve více než jednom. Přenos dat ze serverů podléhá komunikačnímu protokolu a z důvodu spolehlivosti a bezpečnosti může v případě poruchy využít redundantní cesty – multipathing. Na serverech je nainstalován OS, nejčastěji na unixové bázi, tedy linuxové distribuce a distribuce OS Solaris. Zastoupení mají i distribuce Novell a Windows. Nejběžnější software pro řízení a správu disků v datovém centru je VxVM od společnosti Veritas, dnes součásti Symnantecu. Správa disků datového úložiště je komplikovaná a věnují se ji specializovaní správci. [2]

Technologie RAID chrání data v případě selhání disku, a to ukládáním na více disků. RAID může být realizován jako SW, který představuje virtuální zařízení mezi serverem a fyzickým úložištěm, anebo jako HW ve formě řadiče. Technologie MAID naopak umožňuje práci jen s aktivními disky, zatímco ostatní se netočí, a tak šetří energii a prodlužuje jejich životnost.

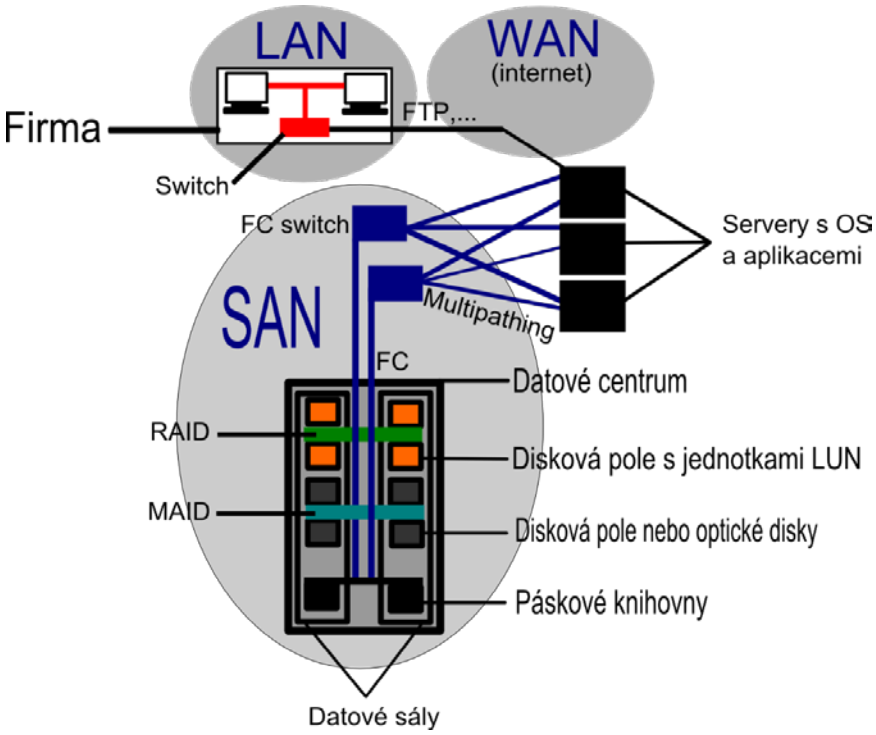
Významným příspěvkem je technologie LUN, jejímž principem je rozdělení disků na menší logické jednotky s unikátním identifikátorem, což urychluje čtení a zápis na disk. V teoretické rovině je každý svazek LUN chápán jako samostatný disk. [2]

V roce 2008 byl společností EMC ohlášen příchod pole disků využívající paměť flash. Řešení bylo velmi nákladné a až současné pořizovací ceny umožňují implementaci technologie. [2]

Vývojem a implementací technologií datových úložišť se zabývají především společnosti EMC, IBM, HP, Sun microsystems a Hitachi. Vzhledem k výhodám virtualizace a její již téměř neoddiskutovatelně potřebné aplikaci na disková pole a přepínače se stává velkým hráčem také společnost VMWare.

Při výběru médií rozhoduje výkon, spolehlivost, kapacita, flexibilita, ovladatelnost. Při požadavku vysokých parametrů prudce roste cena, a proto je trendem datových center tzv. hierarchické uspořádání, kdy jsou nepoužívaná data přesouvána do vrstvy s levnějším provozem, většinou do páskové knihovny. Naopak nejpoužívanější data jsou uložena na diskových polích s největší rychlostí. Tím se dosahuje rovnováhy mezi rychlostí, kapacitou a cenou za pořízení i provoz. [3] Hierarchii a výše zmíněné technologie vystihuje obr. 1.

obr. 1 – Jedno z možných schémat datového úložiště [vlastní]

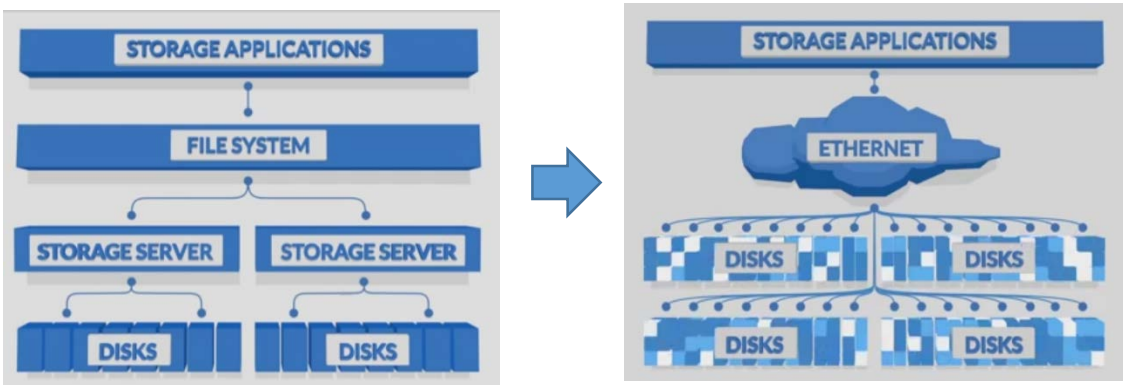


2.3. Budoucnost technologií ukládání dat

Technologie níže zmíněné jsou tím nejnovějším v relativně rychle se vyvíjející evoluci technologií ukládání dat. Najdeme je tedy spíše v budoucích datových centrech, než v těch současných.

Společnost Seagate uvedla na trh média s názvem Kinetic HDD, která jsou připojena přes rozhraní ethernet. Výrobce tvrdí, že dokáže snížit celkové náklady provozu serveru až o 50% při až čtyřnásobně zvýšeném výkonu. Důvodem je zjednodušení celé struktury, kdy se jedinou řídící jednotkou stává aplikace datového úložiště. Zlepší se tak následně i flexibilita. Technologie je znázorněna na obr. 2.

obr. 2 - Řešení Kinetic HDD od společnosti Seagate [4]



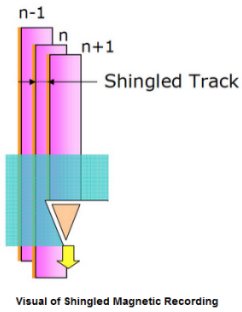
Společnost WD, konkrétně její nezávislá skupina HGST, přišla také s velmi unikátním řešením ve formě disků vyplněných heliem. V prostředí vyplněném héliem se disky otáčí s menším odporem, otáčky generují menší teplo a podle výrobce tak dojde k úspoře energie až o 23%. Disk vyplněný heliem je zobrazen na obr. 3.

Další, často diskutovanou technologií, je SMR. Její podstatou je, že se stopy datových drah překrývají, nejsou oddělené mezerou (viz obr. 4). To ve výsledku přináší úsporu místa a hustota disku může být zvýšena až o 25%. Nevýhodou je fakt, že pokud jedna dráha přenáší data, pak všechny dráhy, které ji překrývají, pracují také. To má negativní vliv na výkon. O technologii se zajímají jak HGST, tak Seagate. Obě společnosti také intenzivně pracují na využití technologie HAMR. Principem této technologie je laser, který zahřeje část disku, na kterou se bude

zapisovat. Důsledkem je tak enormní vzrůst hustoty disku, že by se na běžně používaný disk vešlo až 60TB dat. Zatímco technologie SMR je v procesu ladění, HAMR je stále ve vývoji.

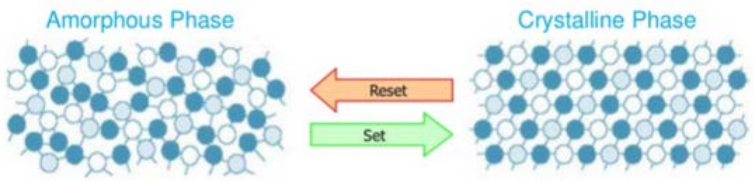
obr. 3 - HGST Ultrastar He8 [5]

obr. 4 - Princip technologie SMR [5]



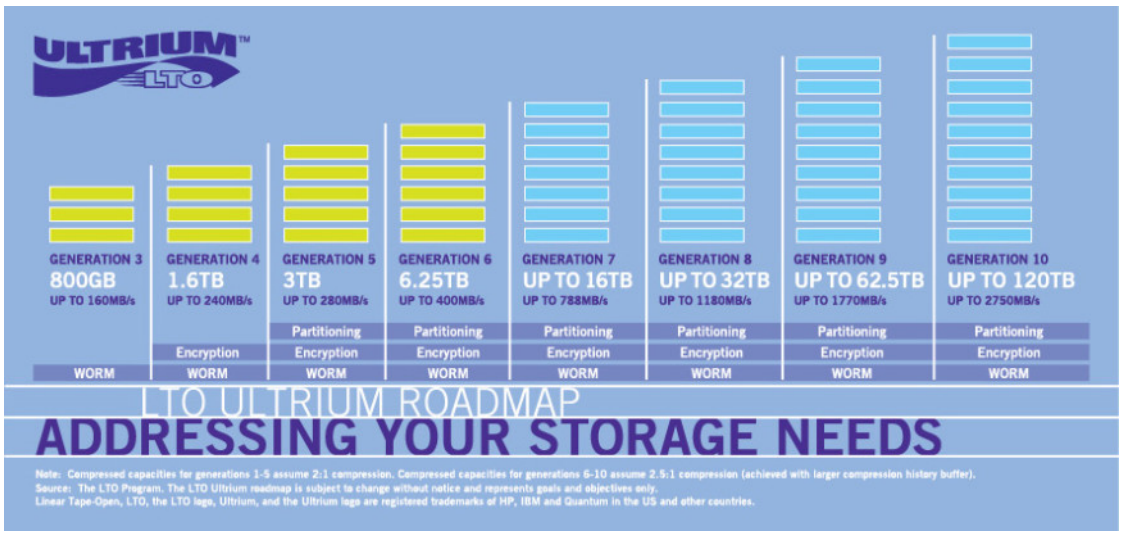
IBM nyní pracuje na vývoji energeticky nezávislé paměti PCM. Využívá se chalkogenidová slitina ve dvou skupenstvích – amorfní, které nemá pravidelné uspořádání částic, a krystalické s pravidelným uspořádáním částic. Protože se liší hodnoty jejich elektrických odporů (amorfních látky mají vyšší), můžeme uložit binární informaci – viz obr. 5, která vytrvá až do další změny. Oba stavy jsou totiž stabilní. IBM navíc tvrdí, že do jedné buňky lze zapsat až milionkrát, což by značně prodloužilo životnost v porovnání s 30 000 zápisy u technologie flash. Předpovědí je i až tisíckrát vyšší rychlost při poloviční spotřebě, opět v porovnání s flash.

obr. 5 - PCM [6]



V oblasti záznamu dat na magnetické pásky vede technologie LTO. Poslední verze LTO-6 byla vydána v roce 2012. V očekávání jsou verze LTO-7 a LTO-9. V roce 2014 společnosti IBM, HP a Quantum, které se na vývoji LTO podílejí, oznámily další rozšíření o LTO-9 a LTO10. Na ty si ale datová centra počkají déle, oficiální webové stránky odhad neuvádí. Vlastnosti jednotlivých generací LTO lze vyčíst z obr. 6.

obr. 6 – Vývoj technologie LTO [7]



V budoucnosti ještě o něco vzdálenější lze očekávat výsledek spolupráce IBM a Fujifilm, kterým se již nyní podařilo vytvořit páskové médium o kapacitě 154TB díky technologii nazvané NANOCUBIC, vyvinuté společností Fujifilm. Využívány jsou Barium Ferritové částice, které jsou menší a stabilnější. [8]

Předmětem vědy posledních let je také využití DNA k ukládání dat. EBI již provedl úspěšný pokus, kdy do DNA zapsali dokument, obrázek a zvuk, který následně přečetli se 100% úspěšností. Podobný projekt byl realizován i v USA. Výhodou je přetrvání informace po tisíce let. Člen týmu Nick Goldman také sdělil, že jeden gram DNA má potenciální kapacitu 2PB. Tým EBI také připustil, že syntetizování této molekuly, menší než smítko prachu, bylo neuvěřitelně nákladné. To je asi důvod, proč se v nejbližší době tato technologie nerozšíří, do budoucna se jí ale přikládá veliký potenciál. [9]

3. Bezpečnost

Bezpečnost firemních dat je na prvním místě. Otázkou je, zda je bezpečné data svěřit provozovatelům datových úložišť. Bez předchozí analýzy lze tvrdit, že vždy záleží na konkrétním poskytovateli této služby, a proto by se každá firma při výběru měla o zajištění bezpečnosti zajímat. Protože jsou data fyzicky uchovávána v datových centrech (dále DC), jejich bezpečnost začíná právě tam. [10]

Důležitou roli hraje strategické umístění DC. Datové centrum by mělo být v oblasti, kde je malá rizikovost přírodních katastrof, jako jsou povodně, zemětřesení a jiné. Okolí by mělo být vhodné a s nízkým indexem kriminality. Vyhledávané jsou také lokality splňující spolehlivé a kvalitní připojení objektu do rozvodné sítě. Čím více je nezávislých přívodů energie do objektu, tím vyšší spolehlivost je zaručena. Spolehlivost se zajišťuje zvolením správných technologií a technických zařízení v oblasti napájení a chlazení, a je nedílnou součástí bezpečnosti. Ztráta dat je nepřípustná.

Při projektování budovy DC je kladen důraz na odolnost stavby vůči vnějším vlivům a požárům. Používají se masivní železobetonové konstrukce. Projekt by měl brát na vědomí následnou aplikaci elementů požárního a fyzického zabezpečení.

Je-li datové centrum dobře chráněno před požárem, zločinci a ztrátou dat, je třeba obrátit pozornost k zaměstnancům DC. Rizikovost jejich činů je na bezpečnosti dat zákazníků přímo závislá, a proto musí datová centra věnovat pozornost správnému nastavení, dodržování a testování bezpečnostní politiky.

Posledním dílem pro dosažení úplného zabezpečení je zajistit bezpečnost síťového provozu datového úložiště. Od chvíle, kdy data opustí zákazníkovo zařízení, vstupují do nebezpečného prostředí – internetu. Po zajištění bezpečného přenosu dat je nutné zajistit jejich bezpečné držení.

3.1. Spolehlivost a efektivita datových center

Bezpečnost dat zákazníků je spojená se samotnou spolehlivostí používané techniky a využívaných technologií. Výběr technologie ukládání dat byl popsán v předchozí kapitole. Je samozřejmostí, že dnešní datová centra využívají uložení do více lokalit a přístup k datům je možný více než jedním způsobem.

3.1.1. Napájení

Racky jsou běžně napájeny více než jednou větví. Fakt, že je trendem směřovat k redundanci technologií je evidentní, a také často známý pod pojmem N+1. V případě výpadku elektřiny jsou racky napájeny systémy UPS a datová centra mají vlastní generátory se zásobou paliva. DC mají běžně také vlastní trafostanice. Tendencí posledních let je také využití alternativních zdrojů energie, jmenovitě solární, vodní a větrné. Efektivita využití energie DC udává hodnota PUE, což je zjednodušeně podíl celkové spotřebované energie a odběru IT zařízení. Čím je hodnota PUE nižší, tím efektivnější je provoz DC. Hodnoty se pohybují mezi 1,1 – 2,0, tab. 1 znázorňuje hodnoty PUE některých vybraných datových center, Rovnice 1 vyjadřuje výpočet.

Rovnice 1 - Výpočet hodnoty efektivnosti PUE, využívaný v DC Google. Vysvětlivky lze najít v seznamu použitých symbolů [11]

$$PUE = \frac{Celková\ spotřebovaná\ energie}{Energie\ odebraná\ IT\ technikou} = \frac{EITS + ESIS + ETX + EHV + ELV + EF}{EITS - ECRAC - EUPS - ELV - Enet1}$$

tab. 1 - Zjištěné hodnoty PUE [11] [12] [13] [14]

Datové centrum	**PUE**
Microsoft DC v Chicagu – bez redundance	1,15 – 1,22
Microsoft DC v Chicagu – s redundancí	1,5
Datová centra společnosti Google	1,11 – 1,23
Moderní datová centra Microsoftu	1,15-1,2
Datové centrum Tokyo No.6	1,2
Datové centrum Tower v Praze	1,62

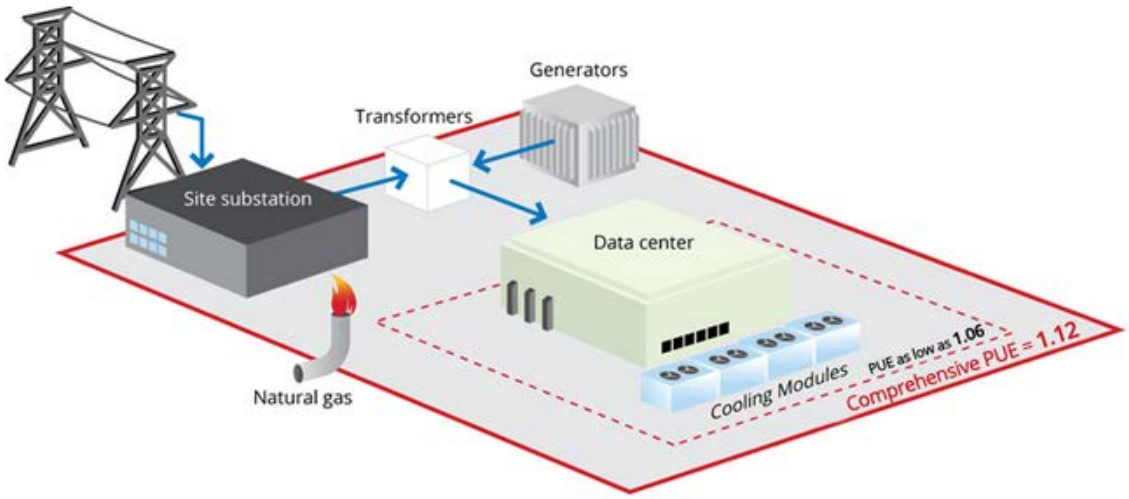
3.1.2. Chlazení

Pro chlazení se využívají různé, vyspělé chladicí systémy. Jmenovat lze filtrování vzduchu, které snižuje prašnost a zvyšuje životnost. Některé systémy chladí racky z podlahy, některé ze předu. Systém free cooling datovému centru šetří elektrickou energii využitím venkovního vzduchu, zvláště je-li venkovní teplota nízká. Pro zvýšení efektivity se používá systém studené uličky nebo odběr teplého vzduchu z prostoru.

3.1.3. Ostatní prvky a shrnutí

Chladicí systémy i napájení jsou neustále monitorovány čidly. Monitoruje a reguluje se také vlhkost. Internet je do datových center přiváděn rychlým a spolehlivým optickým vedením. Na obr. 7 je vidět řešení datových center společnosti Google. Ani menší datová centra v ČR se ale strukturou téměř neliší. Obrázky obr. 9, obr. 10, obr. 11, obr. 12, obr. 13 a obr. 13 jsou pořízeny v datových centrech a prezentují technologie popsané v této kapitole.

obr. 7 - Schéma datových center Google [11]



obr. 8 - Vzduchotechnika, Microsoft DC [12]

obr. 9 - UPS, Microsoft DC [12]

obr. 10 - Připojení k internetu, Microsoft DC [12]

obr. 11 - Filtry, Facebook DC [15]

obr. 12 - Alternativní zdroje, Microsoft DC [12]

obr. 13 - Generátor, Microsoft DC [12]

3.2. Požární bezpečnost

Požární bezpečnost je velmi složité a obsáhlé téma. Protože je práce zaměřena spíše na bezpečnost síťovou, nebude té požární věnována potřebná pozornost.

Na bezpečnost před požárem je třeba dbát již na samém počátku – při projektování stavby. V souladu s právními a technickými předpisy požární bezpečnosti staveb je při budování datového centra dbáno na stavební konstrukce a jejich požární odolnost, na požárně ochranné materiály, na únikové cesty a na požárně bezpečnostní zařízení.

3.2.1. Pasivní požární bezpečnost

Pasivní požární bezpečnost tvoří konstrukční řešení, technologie zvyšující jeho požární odolnost, pasivní bezpečnost osob a v některých případech detekce požáru. Pasivní požární bezpečností tedy rozumíme řešení snižující šíření požáru a jeho vlivu na bezpečnost osob a na konstrukci a zařízení, aniž by docházelo k samotnému procesu hašení. Patří sem například zpěňovatelné nátěrové hmoty, protipožární nástřiky, deskové obklady. K pasivní bezpečnosti osob patří správné řešení únikových cest, dělení objektů do požárních úseků, atd. [16] [17]

V některých případech lze do pasivní požární bezpečnosti zařadit i detekci požáru. Detekce je sice svým fyzikálním principem prvkem aktivním, ale neúčastní se na procesu hašení. Záleží pak na tom, jak pasivní a aktivní požární bezpečnost definujeme. Definice se mohou lišit, a také se liší.

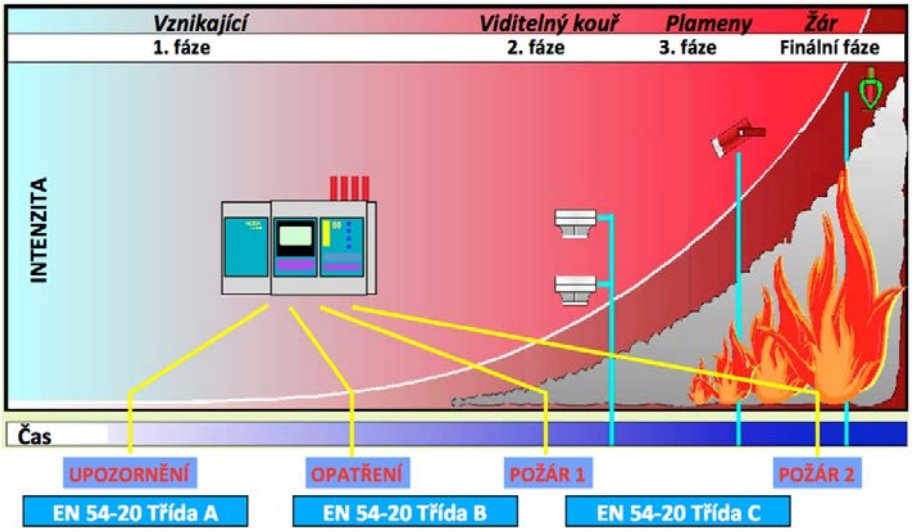
V datových centrech je téměř vždy použita dvouúrovňová detekce. První úroveň tvoří dnes již velmi populární technologie VESDA. Ve chvíli, kdy detektory VESDA vyhodnotí nebezpečí, aktivují se protipožární detektory. Vzhledem k možným teplotním výkyvům spojeným s provozem datového sálu se jednoznačně volí opticko-kouřové detektory, které detekují vznikající kouř při hoření. Pokud dojde k vyhlášení poplachu, ústředna přenáší informace o poplachu na PCO, aktivuje zvukovou a optickou signalizaci a předá prostor aktivním prvkům požární bezpečnosti.

3.2.1.1. Technologie VESDA

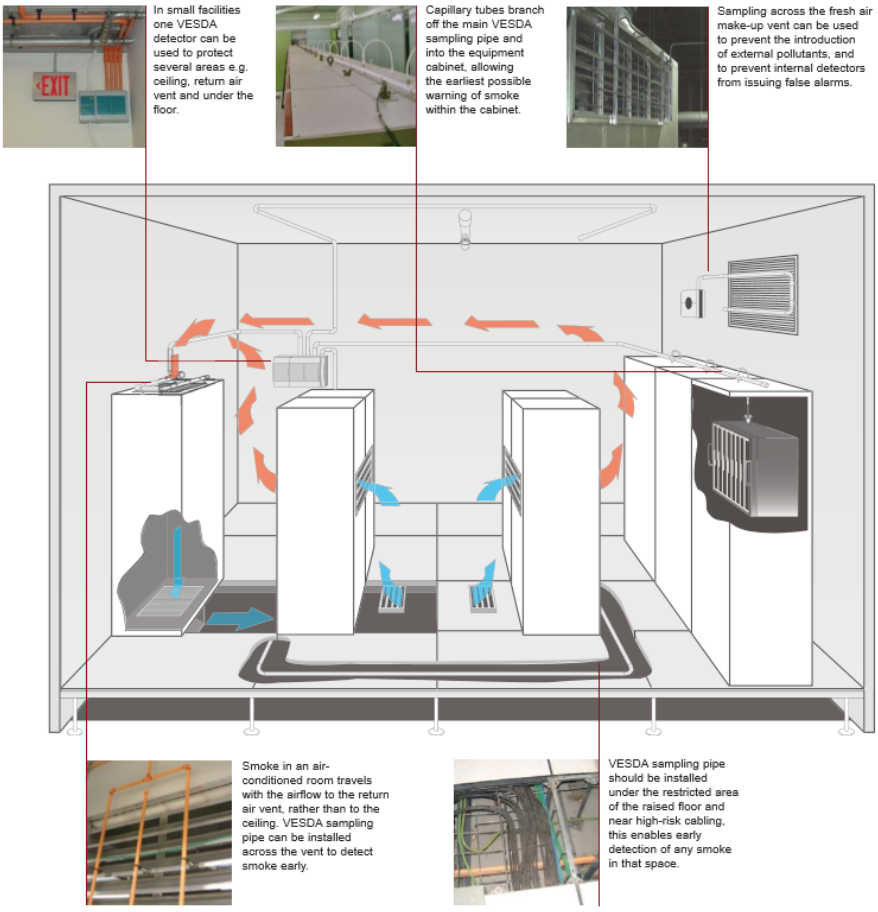
VESDA (systém včasného varování) je technologie vyvinutá společností Xtralis a patří do detektorů ASD (nasávací detekční systémy). Detektor nepřetržitě analyzuje vzorky vzduchu. Vzduch je několika přívody nasáván a přiváděn přes senzor proudění vzduchu do detekční komory chráněné filtrem zaručujícím čistý vzduch kolem povrchu optického detektoru – laseru. Laserové světlo vysílá světlo o krátkých vlnových délkách a ve spolupráci s fotodiodami a dalšími pokročilými zobrazovacími technologiemi (tisíce senzorů) dosahuje optimální reakce na široký rozsah typů kouře. Vzduch po detekci vyčerpán z detekční komory a odvětrán zpět do detektorem chráněné zóny. V případě, že kouř přesáhne povolenou hranici při měření v detekční komoře, detektor předá informaci se stavem Alert, Action, Fire1 nebo Fire2.

Detektory VESDA jsou velmi citlivé a dokáží tak detekovat požár ještě dříve, než může mít katastrofické následky, viz obr. 14. Speciální řešení pro datová centra představuje obr. 15.

obr. 14 - Znázornění včasného varování a stavů detektorů VESDA [18]



obr. 15 - Aplikace detektorů VESDA navržená přímo pro datová úložiště [18]



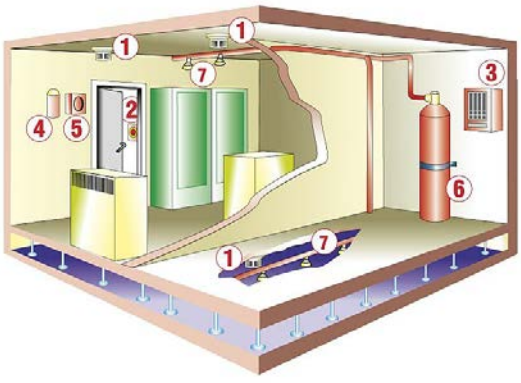
3.2.2. Aktivní požární bezpečnost

Aktivní požární bezpečnost v této práci chápeme jako hašení požáru a zabránění jeho šíření. Předpokládáme, že je požár již detekován, poplach je vyhlášen a cílem je hašení, odvedení tepla a kouře, snížení rozsahu škod a teplotního namáhání konstrukce stavby. V DC navíc hraje nejdůležitější roli bezpečnost HW. Použití správné hasící technologie má jasné podmínky – hasivo nesmí být vodivé a nesmí poškodit HW a elektroniku DC. Takové podmínky splňují plynné, práškové a nově vodní vysokotlaké hasicí přístroje. V případě DC mluvíme výhradně o samočinném hašení bez účasti lidského činitele. Práškové přístroje (hasivo ABC) se prakticky nepoužívají. Kromě požadavků na bezpečnost HW se hodnotí pokles teploty, vliv hasiva na korozi, pracnost odstranění hasiva po požáru a mnoho dalších vlastností hasiv. [19]

3.2.2.1. Plynové hasicí systémy

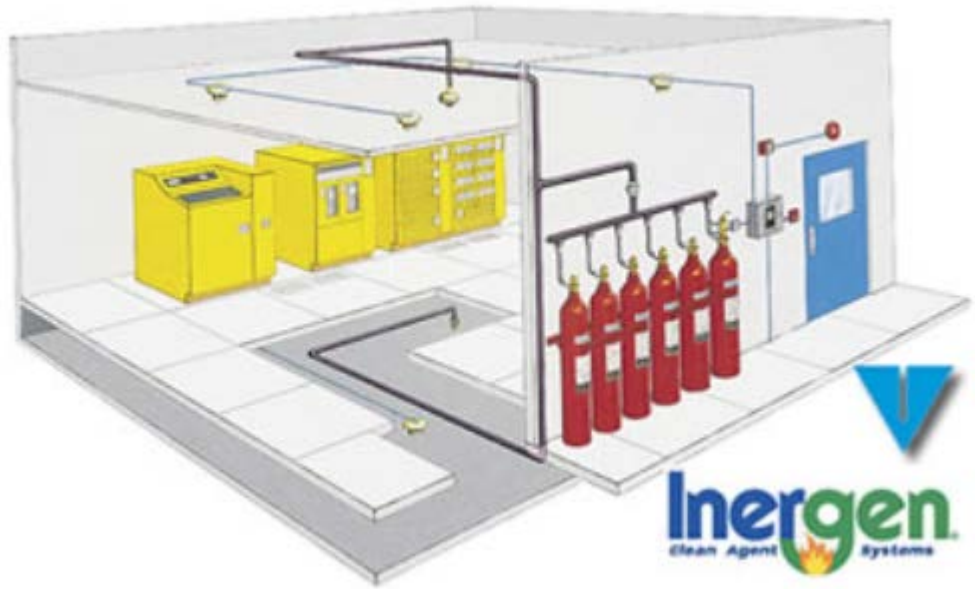
Nejpoužívanější jsou hasící systémy plynové, které můžeme dále dělit na chemické a inertní. Nejčastějším chemickým hasivem používaném v datových centrech je FM-200 se vzorcem CF3-CHF-CF3. Je zdraví nezávadné a ekologické (nerozkládá stratosférický ozón), ale může v reakci se zplodinami hoření vytvořit látky lidskému zdraví nebezpečné. Využíváme kompletní hasící systém, viz obr. 16. Hasivo je nevodivé. Některé látky vzniklé po reakci s plamenem mohou poleptat sklo. Podobnými chemickými látkami jsou Novec-1230, Fe-13. Chemická hasiva pracují na principu odebírání tepla z reakce spalování a následnému zabránění dalšího vznícení.

obr. 16 - Požární systém s FM-200 [20]



Nejpoužívanějším inertním hasivem v oblasti ochrany IT techniky je IG541, složením 52% N, 40% Ar, 8% CO_2. Je to plyn zdraví nezávadný a ekologický. Dalšími inertními hasivy jsou Argonite IG-55, Argon IG-01, Dusík IG-100, CO2 systémy. Inertní plyny využívají k hašení princip vytěsnění kyslíku, přesněji nahrazení. Koncentrace kyslíku je minimalizována na úroveň, kdy nedochází k procesu spalování. Objem hasiva inertního plynu k uhašení požáru je několikanásobně vyšší proti plynům chemickým, což zobrazuje obr. 17. Náklady na dodávku a montáž technologie jsou z tohoto důvodu mnohem vyšší. Naopak cena hasiva je nízká.

obr. 17 - Požární systém s IG-541 [21]



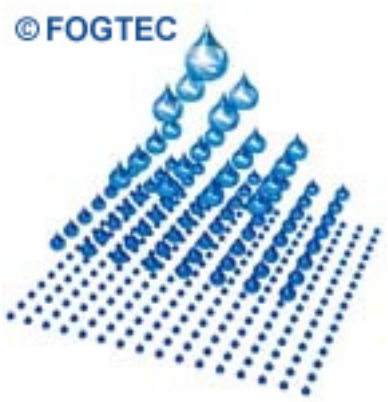
3.2.2.2. Vodní vysokotlaké hasicí přístroje a systémy

V zahraničí se velmi rozmáhá využití technologie společnosti FOGTEC, tedy vodní vysokotlaké mlhy. Tato technologie patří do kategorie vodních hasicích přístrojů. Přesto je díky demineralizaci a vysokému tlaku nevodivá a elektronice neškodná, tedy alespoň do doby kdy se případně smísí s prachem na rackových skříních, pak by mohla vodivost získat zpět.

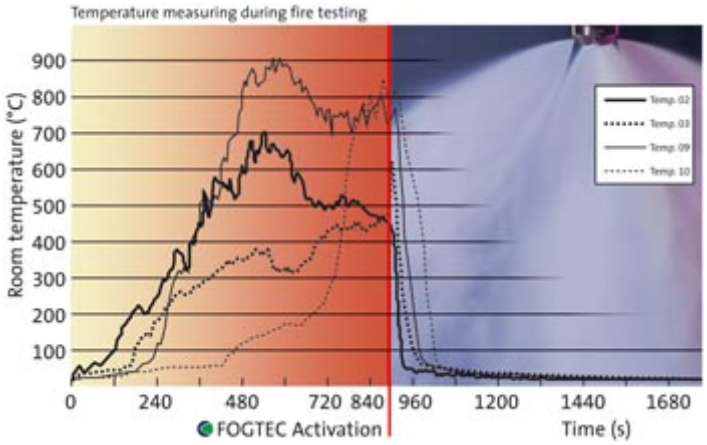
Důvodem vysoké efektivity technologie jsou extrémně malé kapičky, viz obr. 18. Tyto kapičky pod vysokým tlakem vsáknou energii (teplo) z požáru. Kapičky se při reakci s teplem odpařují a odebírají tak požáru na síle a kyslíku. Na rozdíl od inertních plynů ale dochází ke snížení kyslíku jen v místě požáru, nikoliv v celé místnosti. Zjednodušeně to tedy lze vysvětlit, že

principem je přeměna kapek vysokotlaké mlhy v páru, která dusí oheň. To, že je takové hašení efektivní, lze vyčíst z grafu na obr. 19.

obr. 18 - Běžná kapky v porovnání s FOGTEC [22]



obr. 19 – Závislost času na teplotě při hašení technologií FOGTEC [22]



3.2.2.3. Porovnání hasicích technologií

tab. 2 - Analýza hasiv pro datová centra [vlastní]

HASIVO	CENA APLIKACE / CENA HASIVA	BEZPEČNOST HW	VIDITEL-NOST	VODI-VOST	BEZPEČ-NOST ŽP a osob	ZÁPACH
ABC	1392kč/12kg i s lahví	Nízká	Špatná	Žádná do 110kV	Střední	střední
FM-200	1712kč/m^3 / 1176kč/kg	výborná	Střední	žádná	Střední	žádný
IG541	1526kč/m^3 / 112kč/kg	výborná	výborná	mírná	Výborná	žádný
FOGTEC	Několikanásobně vyšší	výborná	výborná	možná	Výborná	žádný

K tab. 2 je nutno zmínit několik upřesňujících faktů. „Uvedené ukazatele lze brát pouze za orientační, neboť záleží na velikosti, složitosti a povaze chráněných prostor, použitém předpisu, stavebním řešení daného prostoru a místě stavby.“, uvádí Ing. Bohumil Kotlík, jednatel společnosti kimbau, stavebně-inženýrská s.r.o. Uvedené ceny aplikace obsahují náklady na technologii a náklady na hasivo, neobsahují naopak detekci EPS a zajištění vzduchotechniky. „Poměrně velkou nevýhodou je zdražení média FM-200 z doporučené ceny

23 euro na doporučenou cenu 42,5 euro, které proběhlo v nedávné minulosti, a které v současně době tento plyn velmi cenově znevýhodňuje.“, dodává Ing. Bohumil Kotlík.

3.2.3. Elektronické požární systémy

Pasivní a aktivní prvky požární bezpečnosti se vzájemně doplňují. Nejvyšší účinnosti pak dosáhneme jejich správnou kombinací.

EPS – elektronická (elektrická) požární signalizace. Elektronický systém sloužící k včasné indikaci požárně nebezpečné situace. Primárním úkolem EPS je zabránit ohrožení osob, zvířat nebo ochránit materiální hodnoty před požárem. Systém se skládá z ústředny, čidel a vedení, které je propojuje. Kromě funkce indikace požáru má systém i funkce výstupní jako spouštění sirén, spínání jiných požárně bezpečnostních zařízení jako, VZT systémy, hašení, evakuační systémy apod. a funkce vstupní jako monitorování požárně bezpečnostních zařízení. [23]

Možné, výhodné a pro splnění všech předchozích požadavků dokonce nezbytné, je propojení EPS se systémy PZTS a přístupovými systémy ACS.

3.3. Fyzická bezpečnost

V posledních letech vidíme masivní slučování elektronického a fyzického prostoru. Přešli jsme od přímého fyzického zabezpečení k práci se sociální a elektronickou oblastí, abychom zajistili, že osoby jsou skutečně těmi, za koho se vydávají. S tímto vývojem však přichází i nový soubor rizik a zranitelných míst, z nichž jsme se naučili zmírnit jen některé. Aby fyzické zabezpečení fungovalo, musíme plně pochopit nové technologie, které se do něj integrují. [24]

3.3.1. Poplachové zabezpečovací a tísňové systémy

Poplachové zabezpečovací a tísňové systémy (PZTS) jsou instalovány za účelem detekování neoprávněného vstupu do hlídaného prostoru.

3.3.1.1. Ústředny

Základem úspěšného zabezpečení je ústředna připojená na PCO. Na ústřednu jsou pak napojené různé detektory, signalizace, klávesnice, moduly a doplňky. Podle typu zapojení rozdělujeme systémy smyčkové, sběrnicové a smíšené. Z bezpečnostního hlediska jsou

nejvýhodnější systémy sběrnicové, z ekonomického naopak smyčkové. V datových centrech převažují sběrnicové systémy.

3.3.1.2. Detektory

Dělení detektorů je velmi rozmanité. Datové centrum je obvykle vybaveno perimetrickou, plášťovou i prostorovou ochranou.

Předpokladem pro perimetrickou ochranu je oplocení. Jeho účinnost je závislá na výšce, materiálu, konstrukci, případně na použití vrcholových zábran. Datová centra bývají často obehnaná plotem vyšším, než tři metry. Oplocení ale není samozřejmostí všech datových center. Detekce může být zprostředkována mnoha způsoby, především venkovními PIR detektory, plotovými systémy, deformačními systémy, tlakovými kabely, mikrofonními a optickými kabely, laserovými systémy, klasickými a termovizními kamerami, infračervenými a mikrovlnnými bariérami atd. Vzhledem ke specifičnosti těchto detekcí v oblasti četnosti planých poplachů je vhodné kombinovat několik systémů.

Plášťová ochrana detekuje vstup do hlídaného objektu. V datovém centru je zajištěna magnetickými kontakty, které jsou kombinovány s přístupovými systémy. Datové sály pochopitelně nemají okna, ať jsou v podzemí nebo ne. Kanceláře datového centra však mohou používat pro zvýšení bezpečnosti detektory tříštění skla.

Prostorová ochrana následuje za plášťovou a detekuje osoby až po té, co hlídaný prostor naruší. Místnost datového sálu je citlivá na správnou volbu a instalaci detektorů. V případě, že dokážeme umístit detektor tak, aby v jeho sledované oblasti nebyl zdroj tepla, můžeme použít pasivní detektor PIR. V případě, že dokážeme umístit detektor tak, aby v jeho sledované oblasti nebyly veliké kovové plochy, můžeme použít aktivní detektor MW. Oba požadavky mohou být v datových sálech obtížně dosažitelné. Při návrhu jejich rozmístění navíc vycházíme také z fyzikálních principů detekce. Řešením může být použití duálních detektorů, které využívají aktivní i pasivní detekci. Samozřejmostí je využití tamperu a antimaskingu.

3.3.2. Kamerové systémy

Kamerové systémy (CCTV) umožňují vizuální kontrolu a monitorování oblastí střeženého prostoru. Systémy svou funkcí plní roli bezpečnostního nebo dohledového systému a vhodně doplňují funkci klasického zabezpečovacího systému (EZS). Prvky CCTV umožňují snímání obrazu v místě sledovaného prostoru, jeho přenos a zobrazení do stanoviště obsluhy bezpečnostního systému (dohledové centrum), případně záznam obrazu k pozdějšímu využití. Záznam obrazu je nejčastěji využíván ke zkoumání rizikových situací, případně plní i roli důkazního materiálu. [23]

3.3.2.1. Technické údaje a využití

Kamerový systém je složen z kamer, držáků a záznamového zařízení (obr. 20). Další komponenty jsou závislé na výběrů technologie kamer a na způsobu a účelu instalace. Je-li ukládacím mediem harddisk, je třeba věnovat jeho výběru pozornost, existují harddisky přizpůsobené k záznamu videa. Kamery můžeme rozdělit na analogové a IP kamery. Analogové kamery se znovu začínají instalovat s příchodem technologie HD-TVI. IP kamery nabízí nesčetně možností jako je inteligentní analýza obrazu, možnost bezdrátového přenosu a tak snadné rozšiřitelnosti, až multimegapixelové rozlišení kamer a součinnost s dalšími systémy jako jsou PZTS a přístupové systémy. Nepřítelem IP kamer je však přenos takto objemných dat po síti. Zajímavou volbou může být moderní technologie HD-SDI, která kombinuje dobré vlastnosti technologií analogových a IP. Obraz je ve Full HD rozlišení a na rozdíl od IP kamer se při přenosu nekomprimuje. Přenos je realizován pomocí koaxiálních kabelů.

obr. 20 - Kamera a DVR v technologii HD-SDI [23]

3.3.3. Přístupové a autentizační systémy

Podkapitolou přístupové a autentizační systémy je v této práci míněno řízení a monitorování pohybů a přístupů osob ve střeženém objektu. Zařadit sem lze pojmy přístupové systémy ACS, elektronické vstupní systémy EVS nebo elektronická kontrola vstupu EKV.

Mezi základní komponenty klasického vstupního systému patří čtečka a klávesnice, viz obr. 21. V případě využití na recepci lze použít vstupní audiotelefony a videotelefony. Časté je propojení s elektrickým zámkem, který vyhlásí poplach v případě násilného otevření dveří.

obr. 21 - Čtečka a klávesnice [23]

Výstupy čtečky jsou řízeny protokolem. Starším, využívaným u RFID čteček, je jednosměrný protokol Wiegand. U magnetických karet tomu je protokol clock-and-data. V nedávné době byly ale zavedené standardy oboustranného šifrovaného datového přenosu OSDP a SCP. Díky těmto protokolům navíc kromě rapidního zvýšení bezpečnosti dochází ke zjednodušení montáže a úspoře materiálu. Místo hvězdicové kabeláže s šesti-žílovým kabelem postačí sériové propojení čteček čtyř-žílovým kabelem. [25] Čtečky s OSDP a SCP od výrobce HID Global jsou na obr. 22.

obr. 22 - Čtečka od společnosti HID Global [26]

3.3.3.1. Čtečky RFID

RFID je systém, který slouží k identifikaci osob v objektu pomocí radiofrekvenčních vln. Informace se ukládají do čipu. Mezi výhody patří rychlost a spolehlivost. Má však vážné bezpečnostní nedostatky. Je možné je klonovat a lze proti nim použít útoky hrubou výpočetní silou, aniž by systém upozornil na opakované pokusy. Navíc jsou většinou identifikační čísla čipů vzestupná. Pochybné je také převádět systémy na cloudové řešení, kdy v případě prolomení se do webu lze získat přístup ke všem kartám a budovám. [26]

3.3.3.2. Heslo, PIN

Hesla nebo kódy PIN jsou vhodné především v kombinaci s čipovými technologiemi. Snižujeme tím riziko neoprávněného vstupu po odcizení čipu. Pokud jde o informační systém s počítačovými stanicemi, je důležité dodržet heslovou politiku, tedy složitost hesel (délka, využití číslic a speciálních symbolů) a jejich periodická obměna. V případě informačního systému je velkou bezpečnostní výhodou využití dvouúrovňové autentizace, kterou může například tvořit heslo a vygenerovaný token.

3.3.3.3. Rozpoznání duhovky nebo sítnice

Rozpoznání duhovky identifikuje osoby na základě barevných skvrn na duhovce oka. Vzory skvrn jsou jedinečnější než DNA. Obtížnost získat dostačující záběr již odezněla s příchodem kamer s vysokým rozlišením. Výhodou technologie je vysoká přesnost a rychlost. Uvádí se, že pravděpodobnost mylné shody je zhruba statisíckrát menší než u systémů rozpoznávání obličejů. Možným způsobem, jak systém obejít, je statická fotografie oka nebo napodobení digitálního obrazu po odcizení vzoru ze systému. Jay Hauhn, technologický ředitel a viceprezident průmyslových vztahů ve firmě Tyco Intagrated Security i Patrick Grother, ředitel biometrických standardů a testování v institutu NINST ale shodně tvrdí, že to v reálném světě je takřka nemožné. Dalšími nevýhodami jsou vysoké náklady a vysoké nároky na snímací techniku. Podobnou technologií je i rozpoznání sítnice na základě vzoru žilek na sítnici. Technologie jsou využívány ve vojenství a tam, kde jsou nároky na ochranu dat vysoké a náklady nehrají důležitou roli. Ceny ale postupně klesají a tyto technologie pronikají i do bankovnictví a zdravotnictví. Očekává se, že se technologie rozšíří i do dalších podnikatelských oblastí a do mobilních telefonů. Společnost Symantec se netají tím, že používá technologii rozpoznávání duhovky u vchodu do trezoru. Může dále usnadňovat bankovní transakce, odbavování na letišti nebo práci státních orgánů. [28] [27]

3.3.3.4. Rozpoznávání obličeje

Technologie rozpoznávání obličeje se z kvalitativního hlediska vyvíjí velmi rychle. Rozeznávání tváří je již tak pokročilé, že je lze použít nejen k ověření, ale dokonce i k nalezení osoby v davu a zjišťování, zda se nechová podezřele pomocí tepové frekvence, mimiky či změny v očích. Mezi nevýhody patří vyšší četnost mylných identifikací, možnost obejít systém obrázkem tváře dané osoby, v případě sledování nasazením klobouku, či v poslední řadě fakt, že tváře se s věkem mění. Při současném vývoji však tyto systémy jistě najdou v blízké budoucnosti své uplatnění. [27]

3.3.3.5. Snímání otisku prstu

Snímání otisků je dalším typem prokázání identifikace, která je jedinečná. Slabina systémů RFID, kdy s validní kartou může vstoupit i jiná osoba je z tohoto pohledu vyřešena. Nevýhodou systémů byla možnost sejmutí a zkopírování otisků pomocí želatinových materiálů. Tento

problém je ale údajně u nejnovějších technologií již vyřešen použitím tepelných senzorů. Jedinou méně významnou nevýhodou může být citlivost na čisté prostředí, ve výrobním průmyslovém centru pak taková technologie není vhodná. [27]

3.3.3.6. Shrnutí přístupových a autentizačních systémů

Technologie autentizačních a přístupových systémů jsou v prudkém vývoji. Pozornost se obrací zvláště na tzv. biometrické systémy, tedy takové technologie, které automaticky identifikují a autentizují osoby na základě jejich biologických vlastností, jako je otisk prstu nebo vzor duhovky. Pro kompletnost, kromě zmíněných technologií, se vyvíjí a používají technologie další. Jednou z nich je technologie pro rozpoznání hlasu na základě vzorků. Její zásadní nevýhodou však je jednoduchost vzorek hlasu zkopírovat. Dalšími technologiemi ve vývoji jsou geometrie ruky nebo vlastní podpis.

Základem pro bezpečnost je vždy vhodná kombinace bezpečnostních prvků. Použitím jen jednoho se vystavujeme příliš velkému riziku. Proto není překvapením, že abychom se dostali řekněme k bankovnímu trezoru, musíme překonat čtečku karet, zadat PIN kód, otisk prstu a například rozpoznání duhovky. Biometrické prvky jsou nejdražší, ale také nejbezpečnější, a proto se používají jen tam, kde je žádán vysoký stupeň bezpečnosti.

3.3.4. Fyzická ostraha

Fyzická ostraha se z pohledu popsaných technologií v předešlých odstavcích může zdát zastaralá a méně spolehlivá. Někdy tomu ale může být naopak, zejména používá-li společnost technologii RFID, kdy si právě fyzická ostraha může povšimnout, že daná osoba v oblasti nemá co pohledávat, i přesto že vlastní validní čip. Může zpozorovat, že fotografie na čipové kartě nesedí se vzhledem osoby nebo zkrátka nabýt pocitu, že na dané situaci něco nesedí. Výhodou je i okamžitý zásah v případě fyzického útoku či poplachu. Naopak nevýhodou je samotný lidský faktor, ať už dojde k neúmyslné chybě nebo úmyslnému zneužití. Nevýhodou mohou být i pravidelné výdaje na pracovní sílu. [27]

3.3.5. Datová centra o fyzické bezpečnosti

Dosvědčením o výše zmíněných technologií je tab. 3 citující stránky vybraných DC v ČR a SR.

tab. 3 - Datová centra o fyzické bezpečnosti

• Vyspělý monitorovací systém, který má pod kontrolou všechny prostory v budově i okolo ní. • Celý komplex je rozdělený na monitorované bezpečnostní zóny a vstup do nich podléhá dvojúrovňové kontrole (karta a PIN kód). • Nonstop profesionální bezpečnostní služba přímo v objektu Datacube s jediným posláním: chránit vaše technologie. • Každá návštěva se identifikuje podle dokladu totožnosti a seznamu oprávněných osob. Pohyb návštěv je limitovaný a jsou doprovázené bezpečnostní službou anebo personálem datového centra.	 DC Datacube http://www.data-cube.sk/sk#security
• Při navrhování našeho datového centra jsme velmi dbali na vysokou úroveň bezpečnosti. A to jak z pohledu fyzické bezpečnosti, tak i z pohledu zabezpečení software. Datové centrum se nachází z velké části pod zemí s minimem přístupových tras. • Přístup osob do objektu je monitorován a podmíněn identifikací prostřednictvím karty spolu s ověřením otisku prstu. Díky tomu máme dokonalý přehled o pohybu všech osob v rámci prostor datového centra.	 DC Izen http://dc.izen.cz/
• Vlastní holdingová bezpečnostní agentura GAN. • Kamery vně budovy, uvnitř budovy a uvnitř datového sálu. • Čidla detekce pohybu a otevření dveří uvnitř budovy a datového sálu. • Dispečink, ostraha, monitorování a evidence přístupu 24x7x365. • Uzamčené RACKy s přístupem na čipové karty. • Vstupy na čipové karty (do budovy, sálů, racků).	DC Monaco https://www.dc-monaco.cz/
• Napojení na centrální bezpečnostní systém ČRa. • Nepřetržité monitorování všech prostor i okolí objektu. • Dohled bezpečnostní agentury v režimu 24/7. • Přístup je pouze přes systém čipových karet v kombinaci se čtečkami biometrických údajů. Záznamy o přístupech jsou archivovány. • Lokalita DC je v nezátopové oblasti a s velmi omezeným letovým provozem.	DC Tower http://tower.active24.cz/
Datová centra (DC) jsou provozována ve speciálním režimu, přítomnost osob je možná vždy pouze s doprovodem, stejně tak připojení zákaznické infrastruktury podléhá supervizi správce DC.	ITS https://www.its.cz/cloud

3.4. Síťová bezpečnost

3.4.1. Kyberkriminalita

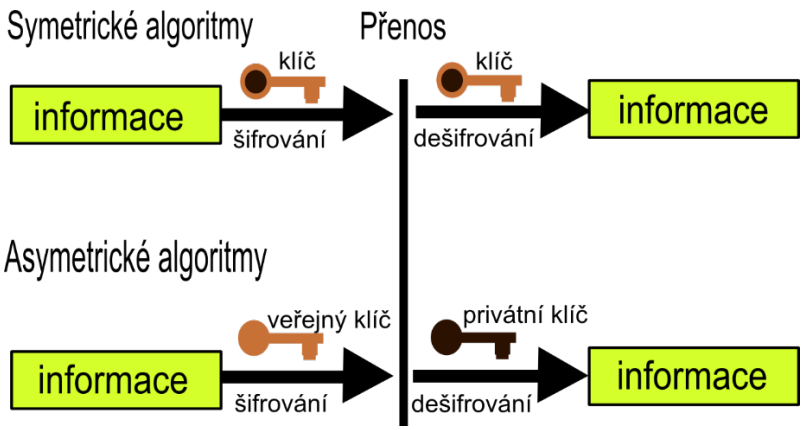
Především v posledním desetiletí, kdy se význam internetu nepředstavitelně zvýšil, vzrostlo množství firemních i osobních informací, které mohou být sbírány jinými společnostmi, zločinci, či dokonce vládou. O to horší je fakt, že takový sběr dat, stopování a sdílení, může být prováděno z pohodlí domácího křesla, a díky automatizaci některých obtížných algoritmů dokonce bez hlubších znalostí. Kriminalita se vždy zaměřovala do sfér, kde mohla nejvíce získat. Dobře to lze nastínit na vývoji společnosti, kdy v industriální éře byla kriminalita soustředěna na nejvíce ceněné materiály a zboží. V post-industriální době, kdy nejvyšší hodnotu nabyly služby, se kriminalita dokonale adaptovala, pomysleme třeba na všechny podvodné služby kolem nás. Dnešní společnost žije v době informatické, což je pojem zavedený světově známými sociology. Nejvyšší hodnotu nabývají informace a jejich přesun do prostředí kyberprostoru zapříčinil i přesun kriminality, a dal tak vzniku novému pojmu – kyberkriminalita.

3.4.2. Kryptografie a šifrování

Kryptografie je věda, která se zabývá utajováním dat pomocí matematických metod. Výsledkem aplikace kryptografických metod je šifrovaná komunikace.

Šifrování je klíčem dnešní síťové bezpečnosti. Označuje proces, kterým jsou informace transformovány do dat, jež ztratila svůj kontext. Dešifrování je pak opačný proces. Data jsou převedena zpět do podoby informací, které lze přečíst a rozumět jim. Dohromady se pak dvojice algoritmů pro šifrování a dešifrování nazývá šifra (cipher). Některé šifry jsou přitom založené na klíčích, což je informace, která parametrizuje a mění chování šifrovacích algoritmů. [29] Klíče známe symetrické nebo asymetrické, rozdíl je velmi pochopitelně popsán na obr. 23.

obr. 23 - Rozdíl mezi symetrickými a asymetrickými algoritmy [vlastní]

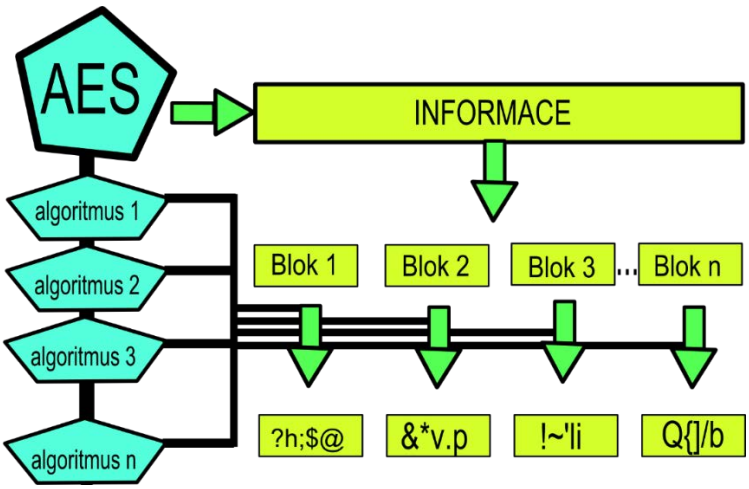


3.4.2.1. Symetrické šifrování

Symetrické algoritmy se používají v blokových a proudových šifrách, k šifrování i dešifrování je použit jediný klíč.

Blokové šifry šifrují data po blocích. Je-li informace větší, než jeden blok, rozdělí si algoritmus informaci do bloků, které samostatně zašifruje. Princip je zobrazen na obr. 24. Nejčastěji používaná bloková šifra, vlastně nejčastěji používané šifrování dnešní doby, je algoritmus AES, který je zatím neprolomený. Vychází z téměř čtyřicet let starého DES. Velikost používaných bloků je 128 bitů, velikost klíče může být až 256 bitů. Blokových šifer existuje mnoho. Za zmínku stojí šifra Blowfish používající bloky o 64 bitech a klíče o až 448 bitech, za bezpečnější než AES se ale nepovažuje. Šifra s názvem Triple DES aplikuje metodu DES třikrát po sobě, čímž se výrazně navyšuje bezpečnost. Oproti AES je ale šifrování mnohem pomalejší.

obr. 24 - Princip algoritmu AES [vlastní]



V případě proudových šifer se šifruje zpráva jedním unikátním klíčem generovaným znak po znaku pomocí funkce generující pseudonáhodné znaky. Nejznámějším zástupcem je algoritmus RC4 s délkou klíče 40-256 bitů a šifrováním pomocí XOR mezi klíčem a dvěma 8 bitovými indexy. Algoritmus RC4 je ale v současnosti již prolomen.

3.4.2.2. Asymetrické šifrování

Asymetrické algoritmy se využívají u digitálních podpisů. K šifrování je použit klíč veřejný a k dešifrování privátní. Může to být i naopak, což je případ právě digitálních podpisů. Asymetrické šifrování využívá obtížných matematických výpočtů, jejichž výsledek lze snadno vypočíst, ale těžko lze zjistit uživatelem použité hodnoty. Používají se především tři algoritmy.

První z nich spočívá ve faktorizaci celých čísel, která vznikají vynásobením velmi velkých prvočísel. [29] Rozložit velké číslo na součin prvočísel může trvat roky, zatímco jejich vynásobení a získání výsledku je téměř okamžité. Toho využívá jeden z nejpoužívanějších asymetrických algoritmus RSA, využívaný pro digitální podpisy. Na algoritmu je založen i nyní populární program PGP, který se využívá k šifrování emailové komunikace.

Podstatou šifry D-H-M je zase kalkulace velmi komplikovaných diskrétních logaritmů, využívající Rovnice 2 Rovnice 3. Výpočet výsledné hodnoty je opět snadný, ale účastníkem použité hodnoty je velmi obtížné zjistit. Alex Stamkos, ředitel bezpečnostní společnosti Artemis na konferenci Black Hat uvedl, že si pravděpodobně matematika s problémem diskrétního logaritmu brzy poradí, a šifra bude následně prolomena. [30]

Třetím metodou jsou eliptické křivky, definované Rovnice 4. Tato neprolomená metoda je ale patentována společností BlackBerry a za její licenci je nutné platit.

Rovnice 2 - Princip algoritmu D-H-M [31]

$$|(A^B)^C|_m = |(A^C)^B|_m$$

Rovnice 3 [29]

$$gx = h \quad kde\ g, h\ jsou\ členy\ konečné\ cyklické\ grupy$$

Rovnice 4 - Princip řešení nad eliptickou křivkou [29]

$$y^2 = x^3 + ax + b$$

3.4.2.3. Další kryptologické metody

Za zmínění stojí také hashovací funkce. Jedná se o matematikou funkci, jež převádí řetězec libovolné délky na hodnotu s pevnou velikostí reprezentující původní data. Výstup hashovací funkce může být zveřejněn, aniž byste museli mít obavy o důvěrnost původní zprávy [29]. Nejznámější hashovací funkcí je již prolomená MD4, která je nyní nahrazena MD5, SHA a RIPEMD. S hashovacími funkcemi je úzce svázaná kryptografická technologie zvaná MAC [29], která díky algoritmu a klíče aplikovanými na vstupní data vytváří MAC kód, který slouží jako autentizace a verifikace. Hashovací funkce nacházejí uplatnění v algoritmech pro kontroly chyb, v práci s databázemi a v mnoha dalších oborech. Pokud se kryptografická hashovací funkce aplikuje například na zprávu elektronické pošty, je výsledná hashovací hodnota v zásadě digitálním podpisem [29], k jehož naplnění stačí přidat asymetrické šifrování.

Potenciál skrývá i kvantová kryptografie, která nepoužívá matematické metody, ale metody kvantové mechaniky. Tato technologie se stále kvůli některým nedostatkům nepoužívá. Měla by být ale imunní proti odposlouchávání, kdy při využívání kvantové mechaniky se při odposlechu mění fyzické vlastnosti, což je možné detekovat.

Teoreticky se všechny šifrovací algoritmy dají prolomit, pokud je k dispozici dostatek zdrojů pro otestování všech možností. Existuje však jedna výjimka, a to je systém, v němž se používá jako klíč jednorázová tabulka (one-time pad), jejíž obsah vznikl na základě dostatečně kvalitního generátoru náhodných čísel. Důkaz o tom, že jednorázová tabulková šifra je neprolomitelná, podal Claude Shannon. Platí to za podmínky, že obsah tabulky je zcela náhodný, uplatňuje se jen jednou a má délku větší nebo rovnou datům, které šifruje. [29] Této šifře se říká Vermanova šifra a v praxi je jen velmi obtížně využitelná. Známé je použití pro krytí horké linky mezi Moskvou a Washingtonem za studené války. Pokud má Vermanova šifra nějakou budoucnost, tak je spojena právě s kvantovou kryptografií.

3.4.3. Bezpečnost datové sítě SAN

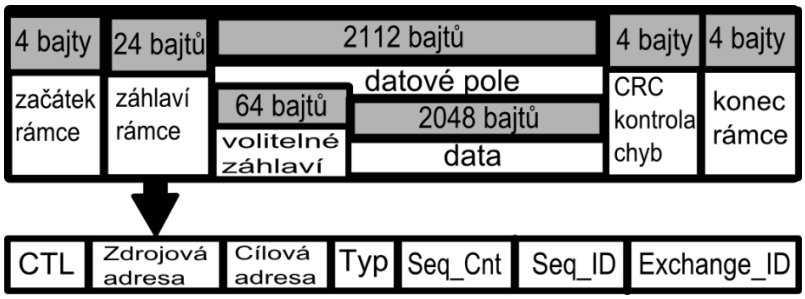
3.4.3.1. Technické parametry sítě

Sítě SAN jsou většinou propojeny technologií Fibre Channel (FC). Standard FC je definován tělesem ANSI, a obsahuje nejen popis kabeláže a spojení na fyzické vrstvě, ale i protokol FCP (Fibre Channel protokol) určený k transportu dat.

Kabely, spojení a konektory v síti Fibre Channel jsou pasivní. Signál odesílá vysílač a přijímá ho přijímač. Každé spojení nebo konektor obsahuje jeden vysílač a přijímač s tím, že data se pohybují po dvou drátech opačným směrem. [29] Tím je na rozdíl od rozhraní Ethernet zabráněno ztrátě dat způsobené interferencí. Adaptér HBA je síťové rozhraní, které slouží k připojení počítače do sítě nebo k zařízení s úložišti.

Návrh FCP počítá se zapouzdřením příkazů a dat v různých formátech, například SCSI (většinou), ATM a IP [29]. Architektura protokolu je složena z pěti vrstev – fyzické (FC-0), linkové (FC-1), síťové (FC-2), vrstvy společných služeb (FC-3) a vrstvy mapování protokolů (FC-4). Rámec rozhraní FC je vyobrazen na obr. 25.

obr. 25 - Rámec rozhraní FC [vlastní]



Port je v terminologii Fibre Channel entitou, které lze přiřadit síťovou adresu. Port je zdrojem i cílem komunikace. Portem jsou tedy nejen adaptéry HBA, ale také fyzická a logická zařízení úložišť, hostitelé, přepínače a rozbočovače [29].

Přepínané sítě Fibre Channel typu fabric (FC-SW) jsou asi nejčastějším topologickým řešením, ačkoliv ne zrovna levným. Uzly a procesy zasílají jako součást přihlašovacího rituálu ostatním portům informace o svém stavu. Každý uzel se totiž musí do sítě FC-SW přihlásit, iniciátor

a cílový port přitom nově přihlašovaný port autentizují a vyjednávají o vlastnostech připojení, včetně typu používaných protokolů a přenosových rychlostí [29].

Adresní prostor sítě FC-SW obsahuje 2^{24} (16 777 216) logických adres. V sítích SW-FC přitom narazíte na tři různá schémata adresace: jména WWN, adresy portů a fyzické adresy arbitrových smyček AL-PA [29]. Nejpoužívanějším identifikátorem je WWN, který přiřazuje unikátní sériové číslo (ID) každému portu a či přepínači. Tendencí posledních let je využití protokolů IP kompatibilních. Mezi takové patří iSCSI, FCIP a iFCP.

Síťová správa je prováděna přes protokol SNMP a pro sítě SAN bylo vyvinuto několik softwarových řešení pro správu sítě, uvádí je tab. 4.

tab. 4 -Software pro správu sítě SAN [29]

Název nástroje	**Společnost**
SANscreen	Onaro, nyní koupené společností NetApp
ControCenter SAN Manager	EMC
SAN Volume Controller (SVC)	IBM

Podle očekávání společnosti HP, EMC, IBM, Veritas a další nabízejí také software pro zálohování dat.

3.4.3.2. Zabezpečení

Úkolem zabezpečení datové sítě SAN je zajistit, aby se uživatelé dostali jen k takovým datům, ke kterým mají mít přístup, nikoliv k jiným, které mohou být i na stejném disku. V této oblasti velmi napomáhá proces virtualizace a její odvozené technologie, například LUN a zónování. LUN jednotky totiž nejen oddělují disk na samostatné jednotky, ale také je umožňují maskovat. Maskovat je možné i HBA řadiči, které obsahují maskovací SW používající adresování WWN (maskují tedy ID portů a přepínačů). Nejelegantnější řešení současnosti je zónování. Komunikace LUN vede přes FC switch a výsledkem je, že jen určitý server může přistoupit k určité části disků. Switch spojí dohromady jen takové uzly, které spolu potřebují komunikovat, a to pouze tehdy, jsou-li ve stejné zóně. Každý uzel může být členem více zón. Identifikace zón probíhá přes pWWN anebo D, P, kdy pWWN je bezpečnější, ale je nutné

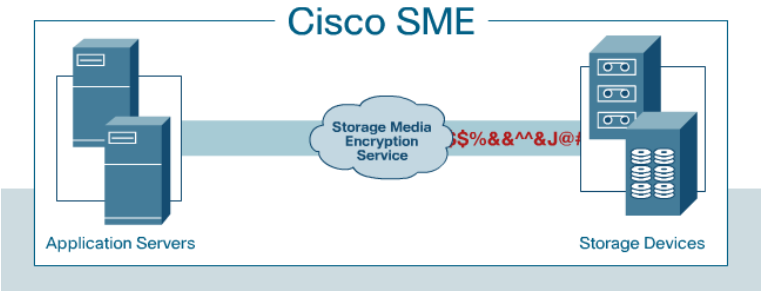
zaopatřit před spoofingem (otrávením). Jde o využití faktu, že se do zóny může přihlásit více než jedno zařízení. Útočník se pak může pokusit přihlásit do zóny s „otráveným“ pWWN a sehraje tak roli MITM. Přestože je útok obtížný, nelze ho vyloučit, a proto je dobré mu předejít pomocí pojistky DCC, známé také jako port ACLs. DCC mapuje pWWN až k cestě do portu přepínače, a pokud se tam pokusí připojit na jiný port, přihlášení zakáže. Využívá se k tomu technologie PKI, která řeší autentizaci, důvěrnost, integritu a neodvolatelnost komunikace. Jiným řešením je protokol DH-CHAP, který mezi uživatelem a přepínačem vyžaduje silnou autentizaci a chrání tak před únikem pWWN. Vhodné je DCC a DH-CHAP kombinovat. Stejně jako u běžných sítí je doporučeno všechny nevyužívané porty vypnout.

Zajištění, aby nikdo nezískal administrátorské heslo a jeho přístupová práva je nezbytné. S právy měnit zóny by útočník získal přístup k cizím datům. Údaje mohou být odposlechnuty z interní sítě. Implementace bezpečného šifrování a monitorování sítě toto riziko eliminuje.

Zranitelnou částí je velmi starý protokol SNMP. Diskutují se především útoky typu DoS. Výrobci již nyní dodávají záplaty ke svým zařízením a radí, aby zařízení komunikující přes SNMP, která nejsou nezbytná pro chod, byla odpojena. Úplné řešení zatím není a společnost CERT se snaží tlačit na prodejce SAN technologií. V řešení jsou úpravy zařízení tak, aby odmítly zprávy od neautorizovaného systému, a také rozdělení SNMP provozu na oddělené segmenty. [32] [33]

Ukázku řešení bezpečnosti sítě SAN lze najít například na webových stránkách společnosti Cisco. Ta nabízí software SME (obr. 26), který šifruje média algoritmem AES. Součástí řešení jsou moduly, switche a další HW vybavení s vlastním OS, komunikací využívající SSH, SSL, RADIUS a FC-S a dalším SW pro správu. Dále Cisco nabízí možnost šifrování komunikace TrustSec Fibre Channel a nabízí vlastní IPSec řešení pro připojení datového centra k internetu.

obr. 26 - Schéma řešení Cisco SME [19]



3.4.4. Bezpečnost v prostředí sítě WAN

V případě, že se chce útočník dostat do interní sítě SAN z externího prostředí, jsou aplikační servery datového úložiště připojené k internetu jediným přístupným bodem.

3.4.4.1. Firewall

Firewally (dále FW) lze realizovat jako HW i jako SW. Úkolem klasických FW je analyzovat data skrz procházející komunikace, a na základě výsledků analýzy je filtrovat. Tím nejmodernějším, co se ve světě FW děje, je postupný přechod na novou generaci nazývanou NGFW. Souvisí to s virtualizací datových center a cloudových úložišť. Virtualizované FW se nezaměřují na provoz paketů a portů, ale na aplikace samotné. To vychází ze zkušenosti, že ani běžný FW v kombinaci s dobře zabezpečeným OS nestačí, protože samotné aplikace nejsou chráněny. Je snahou FW propojovat s dalšími technologiemi. Jsou to především systémy detekce a prevence průniku, webové filtry, FW pro webové aplikace a DLP. [35]

V datových úložištích se FW příliš neuplatňují. Důvodem je již dostačující zabezpečení pomocí šifrování, zónování a LUN jednotek interní sítě, a také fakt, že filtrace FW snižuje propustnost a výrazně zpomaluje provoz, což je komerční riziko.

3.4.4.2. Současná řešení

Datová úložiště nezabezpečují každý server, propustnost dat by tím byla velmi snížena. Řešení spočívá v analyzování veškeré komunikace na vstupu do interní sítě ze zařízení nezávislých na chodu datového úložiště, jak ukazuje obr. 28. Sledování provádí tým administrátorů, kteří k práci používají různé nástroje. Dříve se jednalo zpravidla o systémy detekce průniku IDS. Síťové detekční systémy jsou založeny na principu analýzy síťového provozu a vyhledávání známých vzorků útoků neboli signatur, anebo vyhledáváním anomálií. [36] Důležité je při tom mít aktuální databázi. Ze stále používaných IDS lze jmenovat jen freewarové nástroje Snort, Squil, Hogwash, a několik komerčních nástrojů.

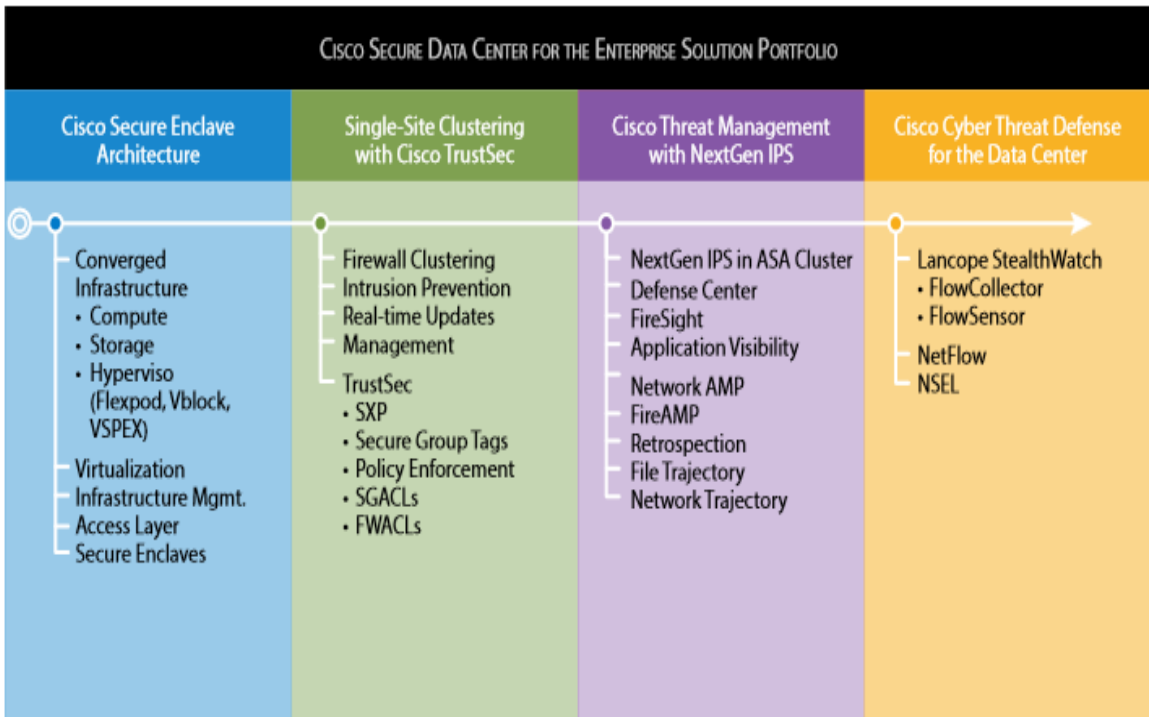
Dnes jsou IDS nahrazeny specializovanými softwarovými i hardwarovými řešeními o mnoha funkcích, včetně IDS, IPS a monitoringu. Často se obecně nazývají Threat Protection, často je ale názvem řešení samotný produkt, respektive je pro komplexnost bezpečnosti poskytováno několik produktů.

Z tab. 5 lze vyčíst distributory dřívějších IDS a současných řešení. Mezi všemi zmíněnými společnostmi také často figuruje zcela nový pojem Security-as-a-service.

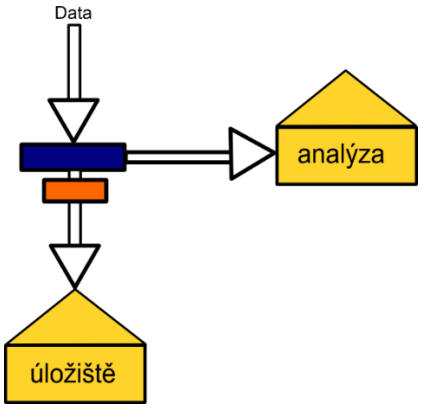
tab. 5 - Předchozí a současná řešení bezpečnostního SW [vlastní]

Společnost	Dřívější produkt IDS	Současné aktivity, produkty
Cisco	Cisco Secure IDS	Speciální produkty. Pro DC na obr. 27
CA technologies	eTrust Intrusion Systém	Řešení pro bezpečnost cloudových úložišť
Intrusion	SeureNet a SecureHost	Savant, TraceCop™, SecureTAP™, Commander™ pro monitorování, stopování, analýzu, obranu před odposlechy a únikem dat
NFR	IDS NFR Security	odkoupena spol. CheckPoint, NG Threat Prevention, NGFW, cloudové služby
Další společnosti a současná řešení: McAfee (Data Center Security Suite, Cloud Security Suite a další), HP (SIEM a další), AlienVault (IDS, SIEM a další), IBM, Juniper, SourceFire, Stonesoft, Symantec, Netapp, Brocade		

obr. 27 - Řešení pro datová centra od společnosti CISCO [37]



obr. 28 - Současné řešení zabezpečení datových úložišť [vlastní]



3.4.4.3. Útok a obrana

Prvním krokem, který síťový narušitel zvolí, je sběr informací. První informace získá vyhledáváním na internetu, další skenováním sítě a jejích počítačů. K tomu slouží nepřeberné množství nástrojů, jako je scanrand nebo nmap. Ty zjistí otevřené porty a v případě, že je útočník za firewallem v interní síti, tak i topologii celé sítě. Obranou před takto lehkým prozrazením je zakázání UDP a ICMP echo paketů, jejichž zpětná vazba je zdrojem informací. Některé nástroje, jako je paratrace, mohou běžný firewall obelstít. Pak je obranou úplný zákaz ICMP zpráv typu 11. Další cenou informací, kterou útočník může získat, je používaný OS a služby. Opět existuje spoustu nástrojů, například xprobe2, nmap. Obranou sice je stejně jako u skenování sítě, omezení provozu ICMP, konkrétně zprávy typu 3. Ty jsou ale zároveň v dnešních sítích potřebné. Záleží pak na kvalitě FW či jiného SW, zda situaci dokáže rozlišit. Pokud ano, útočník se musí spolehnout na méně přesnou pasivní identifikaci, například nástrojem p0f. Pro identifikaci služeb lze použít nástroj amap. Pokud jsou služby veřejně přístupné, předejít jejich identifikaci je obtížné. Program amap ale lze detekovat a upozornit správce. Nebezpečným zdrojem informací je odposlech sítě. Většinou síť nelze pasivně odposlouchávat, a tak je snahou útočníka docílit odklonění provozu, například otrávením ARP cache nástroji arpspoof, WinARP-sk, ettercap, hunt nebo zdvojením MAC adresy nástrojem macchanger a SMAC nebo zahlcením přepínače MAC adresami nástroji macof, EtherFlood nebo otrávením DNS. V případě datového úložiště se nabízí otrávení DNS, po kterém lze následně odposlouchávat vzdálené podsítě a virtuální sítě v pozici MITM. Cílem útočníka je samozřejmě odposlechnout uživatelská jména, hesla, emaily, soubory, zprávy, historii operací. K tomu pak slouží nástroje ettercap, dsniff, Wireshark. Obranou nemůže být vzhledem

k povaze nabízených služeb datového úložiště filtrace MAC adres. Řešením je šifrování, případně detekce odposlechů nástroji ARPWatch či WinARPWatch. DNS se dá zabezpečit pomocí DNSSEC, což je rozšíření DNS o asymetrickou kryptografii a digitální podpisy DNS zón [38]. Datová úložiště dále šifrují celou komunikaci. Využívají k tomu šifrované protokoly nebo doplnění IPSec v případě, že protokol šifrovaný není. V případě protokolu Kerberos je nutné zmínit, že již existuje nástroj kerbsniff, který jeho síťový provoz umí zachytit. V případě kvalitně zvoleného hesla je ale bezmocný.

Má-li útočník ještě vyšší cíle, než získání cenných informací, pak je to přístup k počítači. K němu využije automatizované nástroje pro hledání zranitelnosti, jako jsou core IMPACT, Immunity CANVAS, Nessus nebo Metasploit, některé dokáží i útočit. Následně se pokusí počítač napadnout (exploitovat) kódem vybraným v závislosti na operačním systému a nalezených slabin. Pro OS Linux jsou exploity většinou založené na přetečení bufferu (zásobníku) nebo haldy (oblast, kam si programy alokují prostor pro proměnné). Obranou před těmito exploity je využití knihovny Libsafe či záplaty a skripty pod hlavičkou GRSSecurity. Pro Windows jsou samozřejmé jiné exploity, například nabourání procesu meet.exe. Proces napadení serveru probíhá přidáním shell kódu do paketu. Shell kód pro další exploit nastaví tzv. zadní dvířka, a to otevřením portu, nebo pomocí zpětného připojení v případě, že server má firewall. [38]

Pozornost vyžaduje i obrana před útoky typu DoS, jejímž cílem není odcizení dat, ale znepřístupnění serveru. Takový scénář si datová úložiště nemohou dovolit. Jedním z útoků je DoS Flood, technika, kdy server zahltíme dotazy, na které musí odpovědět. Nebezpečný může být DoS Flood především ve formě DDoS, při němž se do útoku pouští více strojů, v realitě až statisíce, připojených do sítě botnet. Rozlišují se Flood útoky typu ICMP, UDP a TCP. Kromě nich jsou ještě DoS útoky, které zneužívají chyby v HW nebo SW. Staršími proslulými útoky tohoto typu jsou Teardrop, Ping of death, SYN Flood či Banana Attacs, proti kterým jsou aktualizované systémy imunní. Vývoj útoků DoS pokračoval využitím reflektivních metod, které ve své podstatě posílají na větší počet zařízení pakety se zfalšovanou IP (IP oběti), přičemž tato zařízení, například routery, následně odpovídají právě oběti, a to mnohem většími daty. Výhodou je, že se reflektivní útok výrazně zesílí a navíc je útočník jen těžko stopovatelný. Nejznámější útok tohoto typu nese název Smurf. Lze ale využít mnohem efektivnějšího DNS Amplification Attack, kdy útočník umístí na DNS server doménu s vlastním

obsahem, na který se pak vyptává falšovanými pakety s IP oběti. DNS server může poslat odpověď o více než sedmdesáti násobném objemu. [39]

3.4.5. Bezpečnost v prostředí sítě LAN

Zaměstnanci datového úložiště jsou připojeni do sítě LAN, oddělené od sítě SAN. Síť LAN a počítačové stanice musí být zabezpečeny před úniky a ztráty dat. Data mohou obsahovat například plán budovy, prvky využité při zabezpečování nebo informace zneužitelné metodami sociálního inženýrství. Uživateli sítě LAN jsou i firmy, zákazníci datového úložiště. Zranitelnost je velmi vysoká. Všechny výše popsané bezpečnostní prvky datového úložiště se mohou stát jen málo platnými, pokud bude mít neoprávněná osoba přístup k datům firmy, ať už díky špatně zabezpečené síti LAN nebo díky lidskému faktoru.

3.5. Komplexní bezpečnost

Nejnovější trendy úplně mění pohled na bezpečnost a obrací pozornost na řízení rizik a na lidský faktor. Důvodem této změny je vysledování z mnoholetých zkušeností, že primární důraz na obranu zařízení nestačí a neodpovídá realitě.

3.5.1. Řízení rizik

Protože cílem firmy je finančně prosperovat, bezpečností se pak rozumí ochrana před čímkoliv, co prosperitu ohrožuje. V případě datového úložiště to není jen ztráta dat, ale také přerušení provozu, poškození reputace, nedodržení závazných požadavků či vlivy externí. Řízení rizik (risc management) se snaží odhalit okolnosti vzniku rizik a předcházet jim. Netýká se jen známých oblastí bezpečnosti, protože rizika bývají často skrytá v běžném provozu.

3.5.2. Lidský faktor

Lidský faktor se jeví jako největší zdroj nebezpečí. Příkladem za vše je kauza s Edwardem Snowdenem, bývalým pracovníkem americké vládní organizace NSA a CIA. Klíčem úspěchu těchto orgánů je bezpečnost, které je věnována nevyšší pozornost. Zpráva, že NSA v rámci projektu PRISM masově odposlouchává internetovou komunikaci, přišla právě od Snowdena, z prostředí, kam se žádný hacker nedostal. Studie dokazují, že většina bezpečnostních

incidentů pochází z vnitřního prostředí. Zaměstnanci mají mnohem větší možnosti, včetně legálně získaných oprávnění. Poškodit firmu mohou nevědomě nebo vědomě. V případě nevědomého poškození může dojít k pochybení nebo ke zneužití v důsledku technik sociálního inženýrství považovaných za vůbec nejnebezpečnější. Důvodem vědomého poškození může být touha po moci či penězích, pomsta atd., to jsou velmi silní protihráči. Ačkoliv jsou osobní postihy nezbytné, lepším řešením je preventivní práce se zaměstnanci, kdy je v jejich zájmu nepoškodit společnost a jejich kolektiv.

3.5.3. Bezpečnostní politika

3.5.3.1. Bezpečnostní pravidla

Bezpečnostní pravidla vedou zaměstnance a procesy ve firmě tak, aby neohrožovali její bezpečnost. Nacházejí se v pracovních smlouvách a v interních předpisech. Při jejich tvorbě je kladen důraz na přesnost a aktuálnost. Cílem je také pravidla a zmíněné procedury a pravidla kontrolovat a testovat.

V případě DC se limituje, kontroluje a monitoruje pohyb všech osob v objektu a v prostředí sítě. Určuje se, jak pracovat s citlivými daty a kdo je zodpovědný za řešení různých situací. Každý zaměstnanec, včetně administrátorů, má mít vlastní přihlašovací údaje a specifická práva a role. Důležité je i zpracování vyřazených médií, zpravidla destrukcí a sešrotováním.

3.5.3.2. Sociální sítě na pracovišti

Výhody sociálních sítí pro firmy jsou známé – oslovení velké části trhu za nízké finanční náklady a online osobní přístup k zákazníkům. Firmám s kvalitním internetovým marketingem pak roste reputace a výsledky hospodaření. Naopak produktivita zaměstnanců s přístupem k sociálním sítím klesá a především klesá i bezpečnost. Řešením může být školení a vzdělávání zaměstnanců. Sociální sítě by měly být řešeny v bezpečnostní politice.

3.5.4. Audit a zálohování

Auditem rozumíme zaznamenávání porušení pravidel bezpečnostní politiky informačního systému. Záznamy se ukládají do databáze. Čím lepší SW je použit, tím více informací lze získat. Mezi ně patří zobrazení času, data, terminálu a identifikace událostí. Výstupem je například

zjištění, že z kanceláře „X“ se zaměstnanec pětkrát pokusil přihlásit jako administrátor. Celou databázi by firma měla považovat za citlivý soubor a náležitě ji chránit. V datovém centru to může mít klíčovou roli pro detekci narušitele.

Cílem zálohování je předejít ztrátě dat a konfigurací různých systémů. Využívanou výhodou nejen datovými centry je držení zálohy na geograficky odlišném místě.

3.5.5. Red teaming

Bezpečnost nekončí jejím zavedením, musí se testovat a kontrolovat. Jedna z nejmodernějších možností je red teaming, metoda najmutí společnosti simulující nepřítele, zaměstnávající bezpečnostní specialisty a etické hackery. Na základě podepsané smlouvy se nepřátelský tým snaží dostat k co nejvíce citlivým údajům a místům. Provádí penetrační testy, testuje fyzické zabezpečení a zaměstnance. Ti o testování nevědí, a tak je simulováno reálné napadení. [38]

3.5.6. Aditivní model

Aditivní model je moderně pojatá teorie zpracovaná B. Mathaiselem, T. Retterem a G. Grumanem, popisující filosofii zabezpečení firmy. Prvním bodem je zúžení zaměření ochrany. Říká, že čím více prvků chce firma chránit, tím obtížnější je jejich ochrana. Proto by firmy měly na základě posouzení rizik více chránit rizikovější oblasti a méně oblasti s rizikem nižším. Druhý bod nabádá k využití více vrstev zabezpečení. Třetím bodem je alternativní pojetí lidského faktoru. To, že jsou lidé hlavním rizikem, není to samé, jako že jsou hlavním problémem. Jsou totiž i řešením. Pomocí školení, motivace a zařazování do programů dosáhneme opaku – zaměstnanci informují o hrozbách, které samo vedení neznalo, sdílí odpovědnost a snaží se bezpečnost udržet. Čtvrtý bod se týká důvěry třetím stranám. Firmy mají vybírat takové partnery, kterým důvěřují, a s kterými na zabezpečení mohou spolupracovat. Poslední bod pojednává o tom, že cílem je zabezpečit celou firmu, nikoliv jen IT oddělení. [40]

4. Závěr

Průměrný každoroční nárůst dat je zhruba 22%. Každá současná společnost musí řešit otázku uchovávání dat a vzhledem k jejich citlivosti i jejich bezpečnost. Datové úložiště, jako řešení této problematiky, je často diskutovaná záležitost. Největší obavou je poskytování firemních dat třetí straně – provozovateli datového úložiště. Principem je pronajmutí kapacitního prostoru.

Cílem práce bylo informovat o používaných technologiích k zajištění bezpečnosti a spolehlivosti dat, a také o stavu zabezpečení. Práce může pomoci firmám rozhodujícím se mezi vlastním HW a úložištěm. Významným stavebním kamenem práce byla návštěva datového úložiště. V důsledku důrazu na aktuálnost převládají anglické zdroje informací.

Výsledkem je unikátní práce uvádějící ty nejnovější technologie ze světa zabezpečení dat, viz tab. 6, několik užitečných poznatků autora uvedených níže, ekonomické porovnání různých variant (viz Příloha 1) a náhled do budoucnosti ukládání dat.

tab. 6 - Technologie využívané pro zabezpečení dat [vlastní]

Kategorie	Technologie	Důsledek
spolehlivost a efektivita	redunandance dat	přístup více cesty, prevence ztráty dat
	generátory, UPS, více zdrojů	nepřetržitý chod
	studená ulička, chlazení ze spoda, hiarchie médií	nižší náklady, vyšší efektivita (PUE)
požární bezpečnost	VESDA	detekce požáru v předčasném stádiu
	FM-200, IG-541	plynové hašení bez poškození HW
	FOGTEC	hašení vysokotlakou mlhou bez poškození HW
fyzická bezpečnost	vícefázový přístup, šifrování ACS	výrazný nárůst bezpečnosti
	biometrické systémy	jedinečnost biometrie lze těžko obelstít
	Propojení ACS a PZTS	přístup doplní detekce a přenos poplachu
	Kamery (IP, HD-SDI)	monitorování objektů, práce se záznamy
	fyzická ostraha	okamžitý zásah, vypozorování nesrovnalostí
síťová bezpečnost	zónování, maskování LUN, šifrování komunikace a médií	zabezpečení interní datové sítě SAN
	šIfrované protokoly	bezpečené přihlášení a komunikace přes WAN
	tým správců, nástroje a spec. SW	detekce a obrana před hrozbami
komplexní bezpečnost	pravidla, audit, zálohování, red teaming, risc man.	snížení rizika lidského fakoru, kontrola

4.1. Poznatky autora

Autor práce ze svých poznatků vyvozuje několik závěrů. Jedním z nich je fakt, že pro běžnou firmu nelze dosáhnout takové úrovně zabezpečení a spolehlivosti, jaká je dosažena v datových úložištích, navíc by taková řešení byla ekonomicky nevýhodná. Kromě bezpečnostní a ekonomické stránky ještě můžeme na účet datových úložišť přidat flexibilitu pro práci, adaptabilitu s nejnovějšími technologiemi, ušetřený čas a starosti. Kritickým parametrem je ale správná volba poskytovatele úložiště. Sám autor byl během získávání poznatků svědkem téměř nezabezpečeného datového sálu. Firma si musí pečlivě analyzovat, kam svá data uloží. Chybí jakékoliv závazné normy, předpisy a standardy pro provozování datového úložiště, v čemž autor vidí chybu a domnívá se, že jejich zavedení by bylo obrovským přínosem do světa bezpečnosti. Dále autor práce vidí riziko spíše v bezpečnostní politice a síťové bezpečnosti konkrétních firem, zákazníků datového úložiště. Kromě toho, že datová úložiště spíše doporučuje, pro snížení rizika výpadku provozu firmy dále radí zajistit spolehlivý přístup k internetu. Upozorňuje také na riziko velkých cloudových úložišť, kdy jsou uložená data nešifrovaná a přístup k nim má jak provozovatel, tak útočník, který překoná bezpečnostní prvky. Problematika je spojená i se sledováním obsahu internetu světovými vládními orgány, viz kauza projektu PRISM o spolupráci NSA se společnostmi Dropbox, Microsoft a Google. To je možná více otázka soukromí, než konkurenčních bojů a firemních tajemství. Neodmyslitelná rizikovost se zde ale jistě skrývá.

4.2. Budoucnost datových úložišť

Potenciál datových úložišť je již v plném proudu využíván a autor předpovídá, že se směr vývoje nebude výrazně měnit a zájem o datová úložiště poroste. Rozvíjet se budou především cloudová úložiště, která budou nabývat na nepřeberném množství dalších služeb, a z nichž je největší potenciál skryt v Microsoft Azure. Na datová úložiště je kladen tlak ohledně bezpečnosti ze stran zákazníků, výrobců technologií i certifikačních organizací. Proto si pravděpodobně hůře zabezpečená datová úložiště dají na bezpečnosti více záležet a ta dobře zabezpečená se budou držet nejvyšších bezpečnostních standardů. Tento fakt ale vzhledem k neexistující legislativě, která by se problematikou zabývala, nelze plně potvrdit. Budoucí technologie ukládání dat znázorňuje tab. 7.

tab. 7 - Technologie budoucích datových center [vlastní]

Technologie	Princip	Význam
Kinetic HDD	rozhrání ethernet	zjednodušení architektury SAN
helium v HDD	zmenšení odporu	rychlejší HDD, vyšší životnost
SMR	překrývání drah	ušetření místa, vyšší koncentrace dat
HAMR	laser předehřívá místo uložení	vyšší koncentrace dat
PCM	stavy v upořádání částic	energeticky nezávislá paměť
LTO-7 př. 8,9,10	magnetické pásky	zvýšení rychlosti přenosu, kapacity
uložení do DNA	stavy ve struktuře DNA	tisíciletá trvanlinost, miniaturní velikost

Seznam zdrojů

[1] tri-uloziste-bezpecnejsi-nez-dropbox-google-drive-ci-onedrive. *http://www.lupa.cz/.* [Online] http://www.lupa.cz/clanky/tri-uloziste-bezpecnejsi-nez-dropbox-google-drive-ci-onedrive/.

[2] HERMINGHAUS, V., SCRIBA, A. *A Storage Management in Data Centers - Understanding, Exploiting, Tuning an Troubleshooting.* Berlin : Springer-Verlag Berlin Heidelberg, 2009. ISBN 978-3-540-85022-9.

[3] http://www.cesnet.cz/e-infrastruktura/datova-uloziste/. datova-uloziste. *http://www.cesnet.cz.* [Online] http://www.cesnet.cz/e-infrastruktura/datova-uloziste/.

[4] Seagate Kinetic HDD. *www.seagate.com.* [Online] 28. http://www.seagate.com/gb/en/products/enterprise-servers-storage/nearline-storage/kinetic-hdd/.

[5] Shingled Magnetic Recording (SMR). *www.hgst.com.* [Online] http://www.hgst.com/science-of-storage/emerging-technologies/shingled-magnetic-recording.

[6] A Prototype Storage Subsystem based on Phase Change Memory. *http://www.slideshare.net.* [Online] IBM. http://www.slideshare.net/IBMZRL/theseus-pss-nvmw2014.

[7] what is LTO technology. *http://www.lto.org.* [Online] http://www.lto.org/technology/what-is-lto-technology/.

[8] Fujifilm achieves new data storage record of 154TB on advanced prototype tape. *http://www.fujifilm.com.* [Online] http://www.fujifilm.com/news/n140521.html.

[9] DNA 'perfect for digital storage'. *http://www.bbc.com.* [Online] http://www.bbc.com/news/science-environment-21145163.

[10] http://www.ictsecurity.cz/130201-datove-trezory-bez-uloziste-zalohovani/hodnoceni-bezpecnosti-cloudovych-ulozist.html. *http://www.ictsecurity.cz.* [Online] http://www.ictsecurity.cz/130201-datove-trezory-bez-uloziste-zalohovani/hodnoceni-bezpecnosti-cloudovych-ulozist.html.

[11] Efficiency: How we do it. *http://www.google.com.* [Online] Google. http://www.google.com/about/datacenters/efficiency/internal/.

[12] Global datacenters. *http://www.microsoft.com.* [Online] http://www.microsoft.com/en-us/server-cloud/cloud-os/global-datacenters.aspx.

[13] NTT Communications Tokyo No. 6 Data Center . *https://www.youtube.com.* [Online] https://www.youtube.com/watch?v=OiWYxOi4VyY.

[14] PUE. *http://tower.active24.cz/.* [Online] http://tower.active24.cz/pue/.

[15] facebook data center . *https://www.youtube.com.* [Online] https://www.youtube.com/watch?v=5d9s_Dxs9ck.

[16] pozarni-bezpecnost-staveb_N2292. *http://www.casopisstavebnictvi.cz.* [Online] http://www.casopisstavebnictvi.cz/pozarni-bezpecnost-staveb_N2292.

[17] pasivni-protipozarni-ochran. *http://www.konstrukce.cz/.* [Online] http://www.konstrukce.cz/clanek/pasivni-protipozarni-ochrana/.

[18] Nasávací automatické hlásiče VESDA. *http://www.fireton.cz.* [Online] http://www.fireton.cz/index.php/elektricka-pozarni-signalizace/nasavaci-automaticke-hlasice-vesda.

[19] pozarni-ochrana-budov. *http://www.kimbau.cz/.* [Online] http://www.kimbau.cz/pozarni-ochrana-budov.html.

[20] *http://www.fass.cz.* [Online] http://www.fass.cz/data/1239292023308Funktionsweise-%28Raum%29.jpg.

[21] Inergen-ig-541. *https://nationalfireinc.com.* [Online] https://nationalfireinc.com/suppression-systems/inergen-ig-541.html.

[22] Research & Development. *http://www.fogtec-international.com.* [Online] http://www.fogtec-international.com/en_water_mist/research/technology/index.php.

[23] Plus, Variant. *KATALOG PRODUKTŮ 2014/15.* místo neznámé : Variant Plus.

[24] Nickerson, Chris. místo neznámé : Lares Consulting.

[25] ŠNAJDR, Petr. Identifikujte se, prosím. *Security World.* 1, 2014.

[26] Smart card readers. *http://www.hidglobal.com.* [Online] http://www.hidglobal.com/products/readers/iclass-se/smart-card-readers.

[27] HATCHIMONJI, Grant. Klady a zápory metod fyzického zabezpečení. *Security World.* 2, 2014.

[28] RAK, R. MATYÁŠ, V., ŘÍHA A KOL. *Biometrie a identita člověka ve forenzních a komerčních aplikacích.* Praha : Grada Publishing, a.s, 2008. ISBN 978-80-247-2365-5.

[29] SOSINKY, B. *Mistrovství - počítačové sítě.* Brno : Computer Press, a.s., 2010. ISBN 978-80-251-3363-7.

[30] kryptografie-ma-problem-matematika-mozna-brzy-znici-sifrovani-rsa. *http://www.zive.cz.* [Online] http://www.zive.cz/bleskovky/kryptografie-ma-problem-matematika-mozna-brzy-znici-sifrovani-rsa/sc-4-a-170055/default.aspx.

[31] Pavel Mička. Diffie-Hellman. *http://www.algoritmy.net/.* [Online] http://www.algoritmy.net/article/84/Diffie-Hellman.

[32] Institute, SANS. *Is Your Storage Area Network Secure? An Overview.* 2015.

[33] BROCADE. *Secure SAN Zoning Best Practice.* 2015.

[34] SME. *http://www.cisco.com/.* [Online] http://www.cisco.com/assets/cdc_content_elements/flash/sme/.

[35] MESMMEROVÁ, E. Kam směřují firewally. *Security World.* 1, 2014.

[36] Nový, Roman T. *Maximální bezpečnost : hackeři radí jak nejlépe zabezpečit vaši síť.* Praha : SoftPress, 2004. 8086497658 .

[37] HOGUE, T., STORM, M., MCGLOTHIN, N., KANEKO, M. *Secure Data Center for Enterprise.* místo neznámé : Cisco.

[38] HARRIS, S., HARPER, A., EAGLE, CH., NESS, J., LESTER, M. *Manuál Hackera.* Havlíčkův Brod : Grada Publishing, a.s., 2008, 2008. 978-80-247-1346-5.

[39] utoky-typu-dos. *http://www.lupa.cz.* [Online] http://www.lupa.cz/serialy/utoky-typu-dos/#ic=serial-box&icc=title.

[40] MATHAISEDL, B. RETTER, T. GRUMAN, G. Přehodnoťte své zabezpečení, dokud je čas. *Security World.* 2, 2014.

Seznam zkratek

NSA	National Security Agency
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
AES	Advanced Encryption Standard
DES	Data Encryption Standard
PGP	Pretty Good Privacy
D-H-M	Diffie-Hellmanův algoritmus
MAC	Message Authentication Code
SME	Storage Media Encryption
SMR	Shingled Magnetic Recording
HAMR	Hear-Assisted Magnetic Recording
PCM	Phase Change Memory
DDoS	Distributed Denial of Service
LTO	Linear Tape Open
DCC	Device Connnection Control
PKI	Public Key Infrastructure
DoS	Denial of Service
MITM	Man-In-The-Middle

VxVM	Veritas Volume Manager
RAID	Redundand Array of Inexpensive/Independent Disks
MAID	Massive Array of Idle Disks
LUN	Logical Unit Number
HDD	Hard Disk Drive
EBI	European Bioinformatics Institute
ACL	Access Control List
PUE	Power Usage Effectiveness
PCO	Pult Centralizované Ochrany
CCTV	Closed Circuit TeleVision
RFID	Radio Frequency IDentification
DLP	Data Loss Protection
EZS	Elektrické Zabezpečovací Systémy
IDS	Intrusion Detection System
IPS	Intrusion Prevention Systém
RSA	Rivest, Shamir, Adleman
MAC	Media Access Control (fyzická adresa)
	Message Authentication Code (kryptografie)
HBA	Host Bus Adapter
WWN	World Wide Name
pWWN	port World Wide Name

D, P	Domain, Port
DC	Datové centrum
FW	Firewall
SW	Software
HW	Hardware
OS	Operační systém
ESIS	Energy consumption for supporting infrastructure power substations feeding the cooling plant, lighting, office space, and some network equipment
EITS	Energy consumption for IT power substations feeding servers, network, storage, and computer room air conditioners (CRACs)
ETX	Medium and high voltage transformer losses
EHV	High voltage cable losses
ELV	Low voltage cable losses
EF	Energy consumption from on-site fuels including natural gas & fuel oils
ECRAC	CRAC energy consumption
EUPS	Energy loss at uninterruptible power supplies (UPSes) which feed servers, network, and storage equipment
ENet1	Network room energy fed from type 1 unit substitution

Seznam obrázků

Seznam tabulek

Seznam rovnic

Seznam příloh

Příloha 1

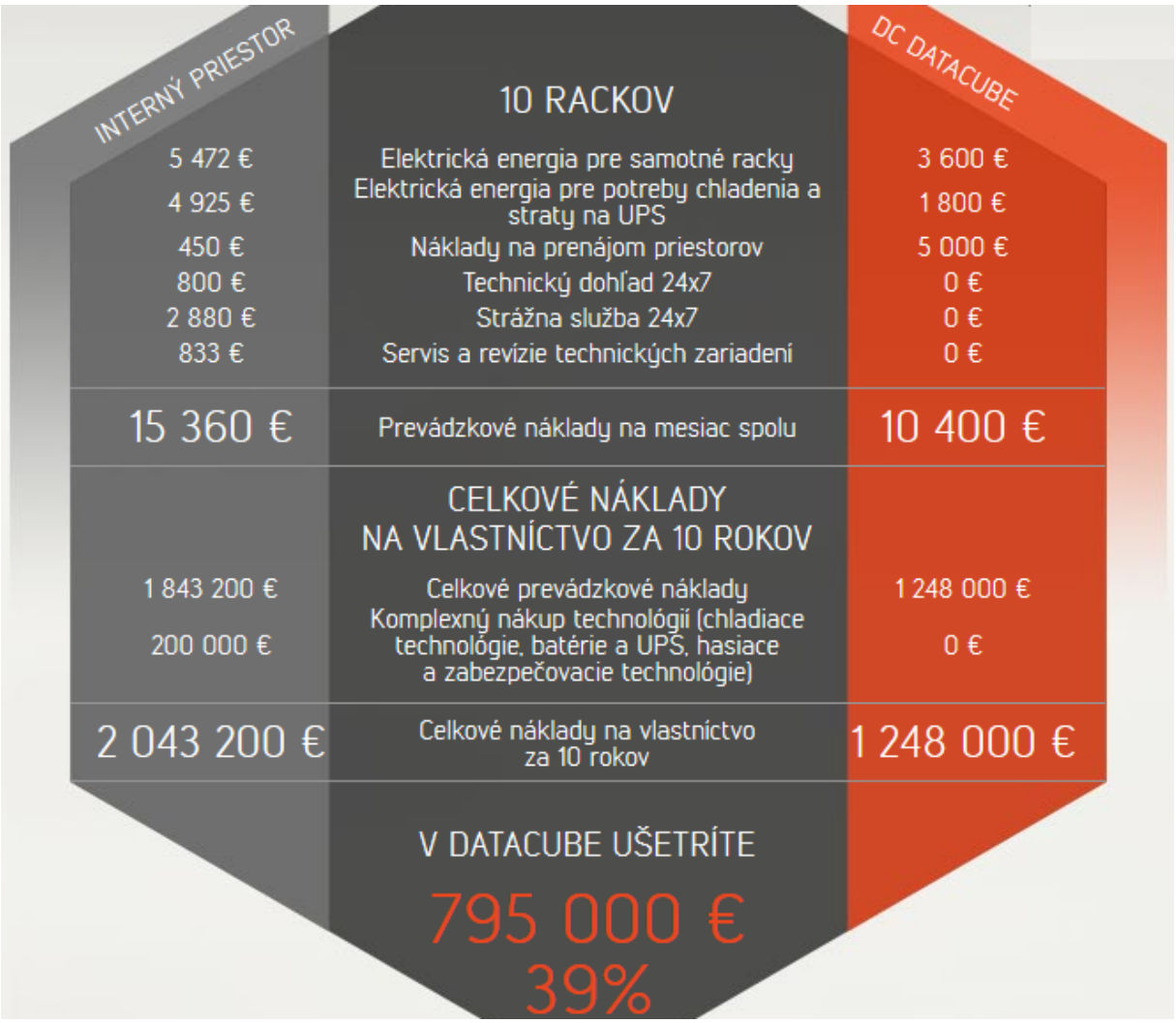
Ekonomické hledisko datových úložišť

Autor: Martin Čejka

1. Porovnání datového centra Datacube.

Datové centrum Datacube na svých stránkách zveřejnilo modelový příklad ekonomického porovnání pro 10 racků. Porovnává variantu, kdy si datové úložiště sestaví firma sama (vlevo) a variantu, kdy svěří svá data datovému centru Datacube.

obr. 29 - http://www.data-cube.sk



2. Nákup v Microsoft Azure

Následující tabulku autor vytvořil za účelem porovnání nákupu technologie oproti jejímu pronájmu v Microsoft Azure.

2.1. Úkol

Autor si vzorový příklad sestavil sám a stanovil si za úkol vybavit kanceláře IT firmy, které žádá pět funkčních strojů s linuxovým operačním systémem a patnáct funkčních strojů s operačním systémem Windows. Na všech strojích běží databáze od Oracle (EE), pro kterou v případě využití služby Azure stačí objednat dva samostatné virtuální stroje.

IT firma se skládá z pětičlenného týmu programátorů, kteří tvoří program v Microsoft Visual Studio. Dále firma zaměstnává penetračního testera, který využívá jeden stroj Windows a jeden stroj Linux, oba s vyšším výkonem a v případě interního řešení může využít dual-boot a snížit tak celkový počet strojů na devatenáct. Pět strojů Windows je využito v oddělení marketingu, čtyři stroje Linux a jeden stroj Windows je využit v oddělení monitoringu a síťové zprávy, přičemž fyzicky jsou zapotřebí jen tři počítače a jeden má vyšší výkon. Zbylé tři stroje Windows jsou rozmístěné na vrátnici a ve dvou manažerských kancelářích. Bylo vypočteno, že stroje pro provoz budou dohromady potřebovat 15TB datového úložiště.

2.2. Řešení

tab. 8 [vlastní]

	Microsoft Azure	Interní řešení
Nákup počítačů	72 000kč	174 000kč
Nákup monitorů	42 500kč	52 500kč
Poplatek za HW	20 500kč / měsíc	0kč
Oracle Database (EE)	100 000kč / měsíc	700 000kč
Microsoft Visual Studio	4 600kč / měsíc	150 000kč
Licence za OS Windows	0kč	22 500kč
Datové úložiště	32 000kč / měsíc	360 000kč při vysoké kvalitě
SOUČET	114 500 + 157 100kč /měsíc	1 459 000kč

K tabulce je třeba zmínit, že ceny jsou přibližné, i když jsou stanoveny na základě analýzy. Nepokrývají navíc všechny nákladové jednotky, ale jen ty nejdůležitější.

2.3. Shrnutí

Závěrem lze říci, že by se firmě investice do vlastního zařízení vyplatila již po přibližně devíti měsících, kdy by se náklady na pořízení vlastní technologie vyrovnaly nákladům spojeným s placením služby Azure. Z toho vyplývá, že Microsoft Azure se více vyplatí spíše malým firmám, kde návratnost investice do vlastní infrastruktury může činit až několik let, a to se především začínajícím firmám, které nemají dostatek finančních prostředků, velmi vyplatí. Speciálně se vyplatí v případě, kdy je vhodné z jednoho počítače ovládat více virtuální strojů.

3. Úložiště vs. vlastní HW

Následující tabulky srovnávají trochu odlišné věci, a to kompletní datové úložiště se všemi službami a prodejní ceny médií. Autor se i tak domnívá, že tabulky mohou pomoci k získání přehledu o tématu.

3.1. Cloudová úložiště

Současně nejlevnějším nalezeným cloudovým úložištěm je MediaFire. Kromě toho je důležité vnímat i ostatní služby, v kterých se cloudová úložiště liší, a které právě můžou určovat cenu.

tab. 9 [vlastní]

Úložiště	Prostor (GB/uživatele)	Cena (uživatel/rok) v Kč
Dropbox for business	1000	3 984
Google drive for work	neomezený	2 638
One Drive for business	1000	1 264
Wuala business	100	2 143
MEGA Pro account	500	2 720
SpiderOak Blue Enterprise	neomezený	1 786
Box business	neomezený	3 957
MediaFire Pro / MediFire Business	1000 / 100 000	765 / 7 650
Cubby Pro / Enterprise	100 / 1000	1 224 / 2 448
Egnyte Hybrid Cloud Business	10 000	4 590
OpenDrive Business	neomezený	9 180
Mozy by EMC	100	9 343
Amazon Cloud Drive	1000	12 750
Microtsof Azure	1000	11 211, neomezeno uživateli
Cryptelo Drive	274 800kč, 25 uživatelů, 50 externistů, údržba 55 000kč / rok	

Projekt http://www.bitcasa.com/ nabízí neomezené datové úložiště cloudového typu v současné době zcela zdarma. Počítá ale s pozdějším zpoplatněním.

3.2. Klasická úložiště

Na obr. 30 a obr. 31 lze nalézt cenové nabídky externích datových úložišť ze stránek https://www.coolhousing.net a https://www.hosting90.cz, jejichž podmínky využití platí za předpokladu používání další jejich služby – virtuálního privátního serveru.

obr. 30 - zdroj: https://www.coolhousing.net/cz/externi-datove-uloziste

Externí datové úložiště	
25 GB	99,- Kč /měsíc
50 GB	190,- Kč /měsíc
100 GB	380,- Kč /měsíc
150 GB	510,- Kč /měsíc
250 GB	750,- Kč /měsíc
500 GB	1.290,- Kč /měsíc
1 000 GB	2.190,- Kč /měsíc
5 000 GB	9.900,- Kč /měsíc
10 000 GB	17.900,- Kč /měsíc

Službu externího datového úložiště není možné objednat samostatně, ale pouze jako součást služeb VPS, dedikovaných serverů a server hostingu.

obr. 31 - zdroj: https://www.hosting90.cz/virtualni-servery-datova-storage

Ceník datového úložiště

Služba	bez DPH	s DPH 21%
Cena za 1 GB prostoru až do výše 1 TB	5,- Kč/měs.	6,- Kč/měs.
Cena za 1 GB prostoru nad 1 TB až do výše 10 TB	1,- Kč/měs.	1,21 Kč/měs.

Příklad čtyř založených datových storage v rámci účtu jednoho zákazníka:

Služba	bez DPH	s DPH 21%
Storage A o kapacitě 10 GB prostoru *(sazba 5 Kč za 1 GB do 1 TB)*	50,- Kč/měs.	60,50 Kč/měs.
Storage B o kapacitě 100 GB prostoru *(sazba 5 Kč za 1 GB do 1 TB)*	500,- Kč/měs.	605 Kč/měs.
Storage C o kapacitě 1500 GB prostoru *(1024 GB v sazbě 5 Kč do 1 TB + 476 GB v sazbě za 1 Kč nad 1 TB)*	5 596,- Kč/měs.	6771,16 Kč/měs.
Storage D o kapacitě 5000 GB prostoru *(1024 GB v sazbě 5 Kč do 1 TB + 3976 GB v sazbě za 1 Kč nad 1 TB)*	9 096,- Kč/měs.	11006,16 Kč/měs.

Datové centrum ADAPTIVITY ve Zlíně přichází s následující nabídkou:

obr. 32 - zdroj: http://www.adaptivity.cz/datove-centrum

Ceník Server Housingu

Velikost serveru	Napájení	Cena
1U server	100W	960 Kč/měsíc
2U server	100W	1.290 Kč/měsíc
4U server	100W	1.750 Kč/měsíc
	každých 50W navíc	+220 Kč
	DUAL	+570 Kč

Pro umístění Miditoweru počítejte s velikostí 4U.
Uvedené ceny jsou bez DPH.

Ceník Rack Housingu

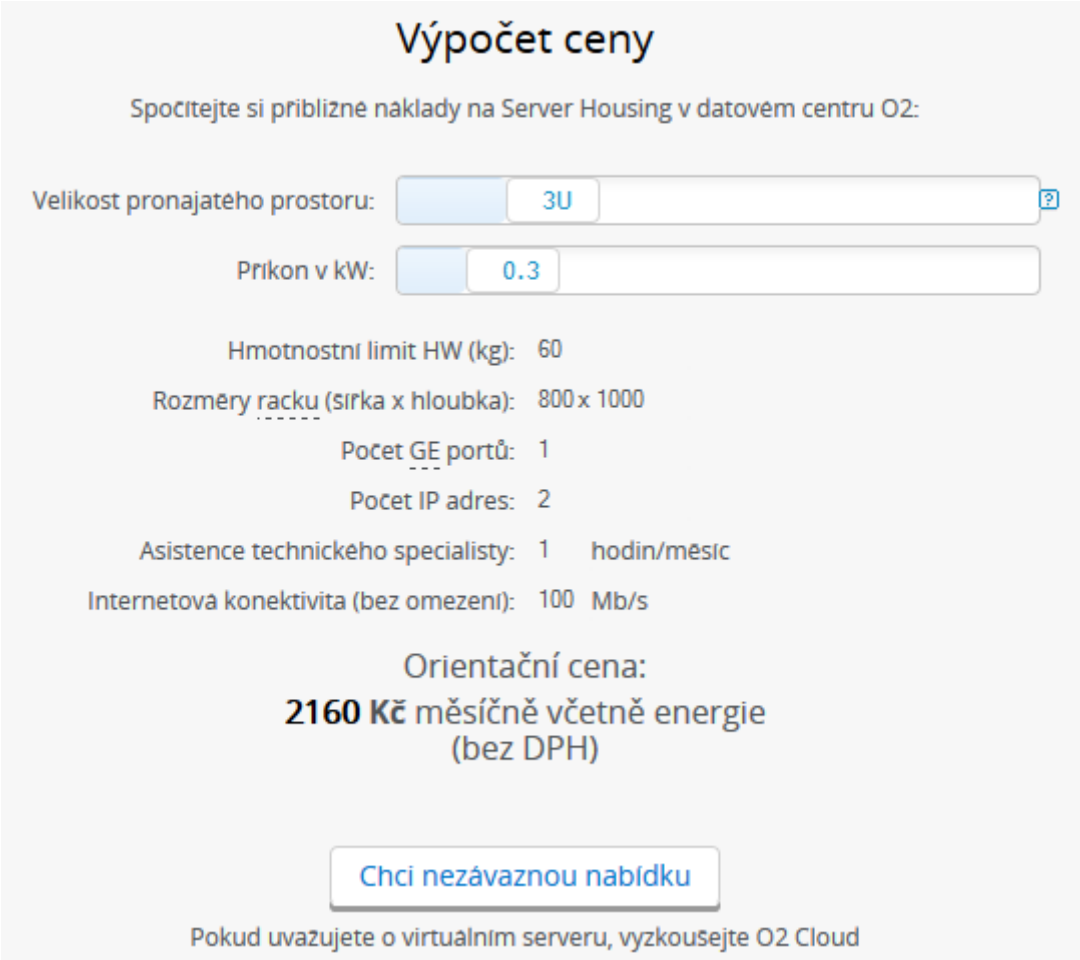
Nabízíme 42U racky CONTEG, hluboké 120 cm s přední a zadní perforací.
Ceny jsou včetně dodávky energie.

Příkon	Jištění	Konektivita	Cena
do 2kW	2 x 16A	1 Gbps	22.900 Kč/měsíc
do 3kW	4 x 16A	1 Gbps	26.900 Kč/měsíc
do 4kW	4 x 16A	1 Gbps	30.900 Kč/měsíc
nad 4kW			individuálně
1/2 rack (21U)			
do 1kW	2 x 16A	1 Gbps	13.000 Kč/měsíc
nad 1kW			individuálně

Jsme schopni měřit reálnou spotřebu racku a cenu přizpůsobit spotřebě.
Uvedené ceny jsou bez DPH.

Na stránkách O2 si lze pomocí kalkulačky vypočítat cenu pronájmu technologií pro uložení dat do datových center O2. Vzorový příklad je na obr. 33.

obr. 33 - zdroj: https://www.o2.cz/pa/191733-managed_hosting/sluzby-datovych-center.html



Následující seznam odkazů informuje o dalších cenových nabídkách uložení dat:

http://www.datahousing.cz/cz/servery/server-housing

https://www.czechia.com/clanek/serverhousing/

http://online-storage-service-review.toptenreviews.com/

http://www.top10cloudstorage.com/

http://www.remotedatastorage.net/index.asp?idName=Pricing

http://www.thecloudcalculator.com/calculators/build-vs-buy.html

http://www.datacentre.co.nz/pricing.html

3.3. Ceny HW

tab. 10 [vlastní]

Technologie	Kapacita (GB)	Cena za pořízení (Kč)
Externí HDD	500	1 500 – 2 200
Externí HDD	1000	2 000 – 3 200
Externí HDD	2000	2 800 – 4 000
Externí Cloud úložiště	4000	10 000
Externí Cloud úložiště	6000	12 000 – 15 000
Externí Cloud úložiště	8000	13 000 – 18 000
Interní HDD SATA	500	2 000 – 2 500
Interní HDD SATA	1000	2 000 – 3 500
Interní HDD SATA	2000	2 600 - 6 500
Interní HDD SATA	4000	4 800 – 11 000
Interní HDD SATA	6000	8 300 – 15 000
Disk SSD	480 a 512	5 500 – 15 000

tab. 11 [vlastní]

Technologie	Kapacita (GB)	Cena (Kč)
Úložiště NAS – nižší třída	6 000	12 000
Úložiště NAS – vyšší třída	1 000 – 64 000	305 000 – 540 000

4. Závěr

Cílem bylo vytvořit základní přehled o problematice datových úložišť z ekonomického hlediska. Snahou také bylo využít co nejvíce internetových zdrojů. To se podařilo jen částečně, ekonomické srovnání takového charakteru na internetu naprosto schází. V mnoha případech to může být i ten nejdůležitější faktor pro pronájem kapacity či přechod na cloudové nebo outsourcingové služby.