Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informačních technologií

Analýza zabezpečení cloud služeb

Bakalářská práce

Autor: Milan Pechánek
Studijní obor: Aplikovaná informatika

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Hradec Králové Duben 2019

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 16.4.2019 Milan Pechánek

Poděkování:

Děkuji vedoucímu bakalářské práce Mgr. Josefu Horálkovi, Ph.D. za metodické vedení práce, poskytnuté konzultace a cenné připomínky, které vedly k vypracování této práce.

Anotace

Tématem této bakalářské práce je představení cloud služeb, analýza jejich zabezpečení a praktické testy týkající se zabezpečení dat ukládaných na cloud. V úvodu bakalářské práce zaměřuji obsah na historii, základní vlastnosti a principy Cloud Computingu. V další části práce popisuji fungování cloudových služeb, jejich rozdělení do jednotlivých modelů, včetně porovnání efektivity a jejich kladných a záporných specifikací. Věnuji se zde také porovnání nejznámějších poskytovatelů cloudových služeb dle kritérií datových úložišť, které jsem stanovil. Navazující částí je analýza zabezpečení dat cloud, ve které se zaměřuji zejména na šifrování, dále na základní pojmy zabezpečení a bezpečnostní hrozby. Podrobně popisuji šifrování pomocí nástrojů třetích stran. Praktická část této práce analyzuje vybrané produkty třetích stran a jsou zde interpretovány výsledky měření, které vznikly sledováním vytížení systémových zdrojů jednotlivými produkty při procesu šifrování.

Annotation

Title: Analysis of cloud services security

The topic of this bachelor thesis is the introduction of cloud services, analysis of their security and practical tests related to data security stored in the cloud. In the introduction of the bachelor thesis I focus on the history, basic features and principles of Cloud Computing. In the next part I describe cloud services and its function and their division into individual models, including comparison of efficiency and their positive and negative specifications. I also compare the best-known cloud service providers with the data storage criteria which I have set. The next part is the cloud security data analysis, which focuses on encryption, basic security concepts and security threats. I describe in details the encryption using third-party tools. The practical part of this work analyzes the selected third party products and interprets the results of the measurements that

were generated by using the system resources of the individual products during the encryption process.

Obsah

Seznam obrázků

Seznam grafů

Seznam tabulek

1 Úvod

Cloud Computing je moderní a velmi rozšířená forma sdílení služeb a vypočetních zdrojů v oblasti informačních technologií. Samotný název Cloud vystihuje celkovou logiku tohoto systému, kdy klient využívá software, hardware a služby poskytovatele vzdáleně pouze pomocí internetového připojení. Tento trend nabývá na popularitě zejména díky dostupnosti dat v podstatě odkudkoli na světě. V dnešní době chytrých mobilních zařízení s kvalitním fotoaparátem, velkým rozlišením fotografií a tím rostoucím objemem obrazových dat je příhodné uvolnit úložiště ve svém zařízení, zálohovat snímky pro případnou ztrátu zařízení a zároveň zážitky z dovolené nebo z každodenního života zachycené fotoaparátem sdílet svým blízkým či kolegům. Právě Cloud Computing pomocí cloud úložiště v sobě zahrnuje všechny tyto možnosti.

Cílem této práce je tedy analyzovat zabezpečení cloud služeb související s vystavením citlivých obrazových či soukromých dat na úložiště poskytovatele a analyzovat možné řešení tohoto zabezpečení.

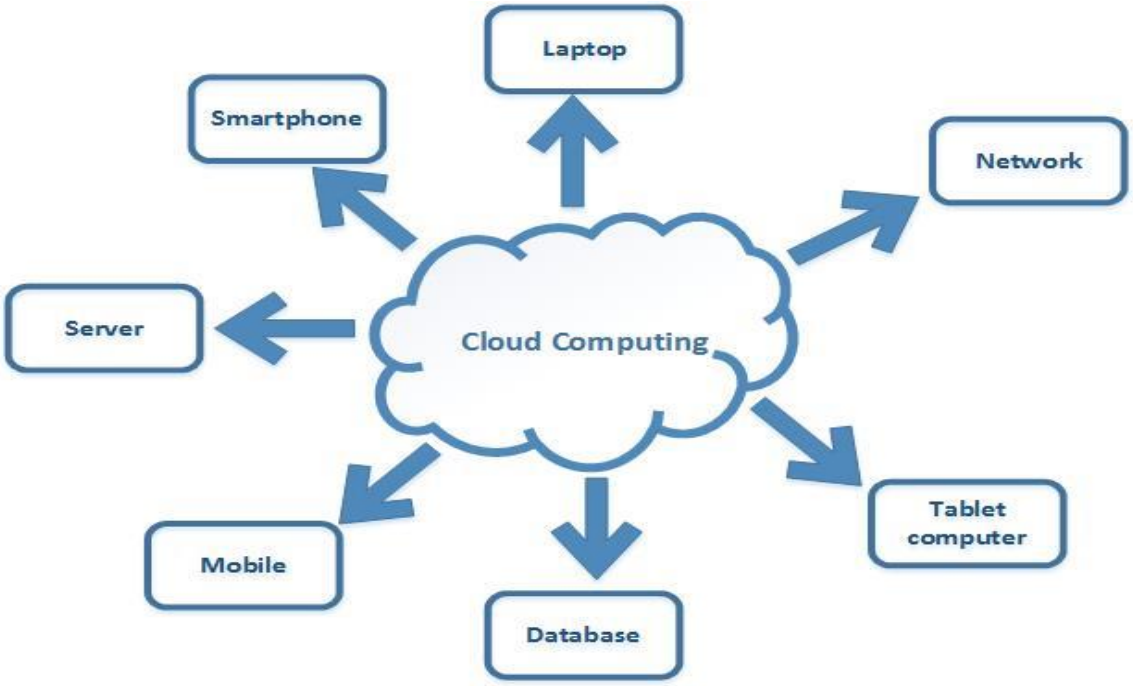
Bakalářská práce je rozdělena na dvě části – část teoretickou a část praktickou. V první části je popsána historie Cloud Computingu, jeho základní principy a vlastnosti. Popsány jsou zde všechny modely Cloud Computingu, ovšem práce je primárně zaměřena na model Public Cloud Computing. V této práci jsou také vysvětleny způsoby zpracování služeb Cloud Comutingu. V teoretické části je také zahrnuta problematika Cloud jako úložiště dat a porovnání populárních cloud úložišť. Zbylý obsah teoretické části je věnován zabezpečení dat ukládaných na cloud úložiště a způsobům zabezpečení těchto dat, zejména šifrování a nástrojům sloužícím k tomuto účelu. Celá tato část byla zpracována na základě odborné literatury.

Část praktická se zabývá analýzou a testováním nástrojů třetích stran sloužících k zabezpečení dat ukládaných uživatelem na cloud úložiště. Tyto nástroje jsou analyzovány a testovány v praxi. Během testování nástrojů probíhá analýza vytížení systémových zdrojů šifrovacími nástroji a výsledky tohoto testování jsou znázorněny a prezentovány pomocí grafů. Závěr práce shrnuje cíle, základní postřehy, poznatky a výskedky vyplývající z této práce.

2 Vymezení pojmu Cloud Computing

Pojem Cloudové služby zná v dnešní době téměř každý. Většinu z nás ve spojení s těmito službami napadne přístup ke sdíleným datům, aplikacím a souborům, zejména obrázkům, dle aktuální potřeby. Tento pojem byl zhruba před deseti lety téměř neznámý. Objevoval se pouze v odborných článcích pod zkratkami SaaS nebo ASP. Cloudové služby přitom dnes používají stovky milionů lidí po celém světě. Nejčastěji když si do Cloudové služby uloží rodinné snímky a poté si je prohlíží pomocí chytrého mobilního telefonu nebo chytré televize.

Cloud Computing jako nová technologie zažil dramatický nástup následkem globální ekonomické krize. Společnosti z důvodu propadu ekonomiky mají na informační služby stále menší rozpočty financí. Právě nedostatek financí na správu IT infrastruktury je přinutil najít méně nákladné řešení, které je možné přizpůsobovat podmínkám na trhu. Dle profesora R. Buyaa [1] bychom mohli Cloud shrnout jako „Paralelní a distribuovaný počítačový systém sestávající ze sbírky vzájemně propojených a virtuálních počítačů, které jsou dynamicky zajištěny a prezentovány jako jeden nebo více unifikovaných výpočetních zdrojů založených na dohodách o úrovni služeb (SLA) stanovených mezi poskytovatelem služeb a spotřebiteli“ nebo dle obecnější definice, Armbrust a další [2] „Hardware a software datového centra, které poskytuje služby.“[3]



Obr. 1 Schéma Cloud Computingu. (Vlastní zpracování dle [49])

2.1 Historie Cloud Computingu

První výskyt termínu Cloud Computing datujeme pouze do roku 1997. Tehdy nový pojem použil ve své přednášce profesor Ramnath Chellappa z Goizueta Business School. Tento muž první vyslovení termínu Cloud Computing rozšířil definicí [3] „počítačové paradigma, ve kterém jsou hranice výpočetní techniky stanoveny ekonomickou rozvahou místo technologickými limity“.

Ovšem myšlenka cloud služeb je daleko starší než tato definice. Koncept cloud struktury, která je přítomná všude a dostupná dle aktuální potřeby, popsal John McCarthy, profesor ze Stanfordu. McCarthy byl již v šedesátých letech přesvědčen, že úložiště budou jednoho dne uspořádány jako veřejně dostupná služba, cloud dokonce srovnává s elektrickou rozvodnou sítí.

Historie a filozofie cloud computingu jsou významné i pro aktuální pochopení cloudu. Jeho vlastnosti – dostupnost systémových prostředků a aplikací ve formě veřejné služby, zdánlivá neomezenost kapacity a flexibilita totiž přímo specifikují to, čím se cloud computing odlišuje od aplikací založených na hostingu nabízených v historii.

Hosting jako takový se podobně jako cloud computing vyznačuje škálovatelností a pro koncového klienta hostované programy a služby vypadají jako uložené v cloudu. Co se týče hostovaných služeb není v podstatě možná plynulá aktualizace aplikací nebo jejich upgrade na nový hardware bez komplikací v případě výpadku služby.

Tyto možnosti nabízí až cloud a aplikace vyvinuté se zaměřením na podporu více různých aplikací s podporou dynamických datových úložišť [3].

2.2 Modely Cloud Computingu

Cloudové služby rozdělujeme dle způsobu, jakým je služba poskytována. Lze konstatovat, že možnosti cloudových služeb je možno jednotlivě uchopit dle úrovně poskytované služby pro klienta. Zde můžeme vyjmenovat čtyři základní druhy rozdělení, které zahrnují velmi rozsáhlé pole působnosti CloudComputingu. Tyto druhy nazýváme obecně také modely nasazení [4]. Jednotlivé podkapitoly jsou zpracovány na základě zdrojů: [4], [7] a [11].

2.2.1 Public Cloud Computing (Veřejný)

Tento model, s kterým se již setkala většina uživatelů výpočetních technologií, je také označován jako klasický cloud computing. Zde jsou sdíleny a poskytovány služby široké veřejnosti, nejčastěji třetí stranou – poskytovatelem (providerem) – prostřednictvím webového rozhraní a internetového připojení, většinou na principu pay-as-you-go nebo také pay-per-use. Velmi důležitý je fakt, že veškeré starosti se správou, aktualizacemi a technickou podporou jsou na straně poskytovatele. Jako příklad můžeme uvést Skype a Microsoft Azure, které využívají miliardy klientů.

2.2.2 Private Cloud Computing (Soukromý)

Poskytuje stejné služby jako Public Cloud Computing s tím rozdílem, že tento model je postaven a provozován výhradně pro podporu obchodních operací nějaké organizace nebo soukromé sítě. Provozován je buď samotnou organizací nebo externím providerem (třetí stranou). Tudíž se výpočetní zdroje mohou nacházet v prostoru organizace nebo mimo areál. Z pohledu klienta se Private Cloud Computing od Public Cloud Computingu neliší.

2.2.3 Hybrid Cloud Computing (Hybridní)

Tento typ kombinuje prvky veřejného i soukromého cloud computingu. Jedná se o dva a více veřejných a soukromých cloudů, které vystupují navenek jako jeden cloud. Tyto jednotlivé cloudy zůstávají jedinečnými entitami, ale jsou navzájem provázány proprietární nebo standardizační technologií, pomocí které lze mezi těmito cloudy přenášet data a aplikace. Hlavním cílem a výhodou Hybridního Cloud Computingu je v případě vyčerpání kapacity soukromého cloudu možnost využití veřejného cloudu k získání dalších zdrojů, které jsou potřeba, aby organizace mohla nadále pracovat.

2.2.4 Comunity Cloud Computing (Komunitní)

V tomto modelu je infrastruktura cloudu sdílena několika organizacemi a podporuje danou komunitu, např. zaměstnance více firem pracujících na stejném projektu. Tento specifický typ cloud computingu je dostupný pouze konkrétní komunitě nebo skupině se stejným zájmem. Příkladem tohoto modelu nasazení je OpenCirrus tvořený společnostmi HP, Intel, Yahoo a dalšími. Community Cloud Computing může být spravován danou organizací nebo třetí stranou.

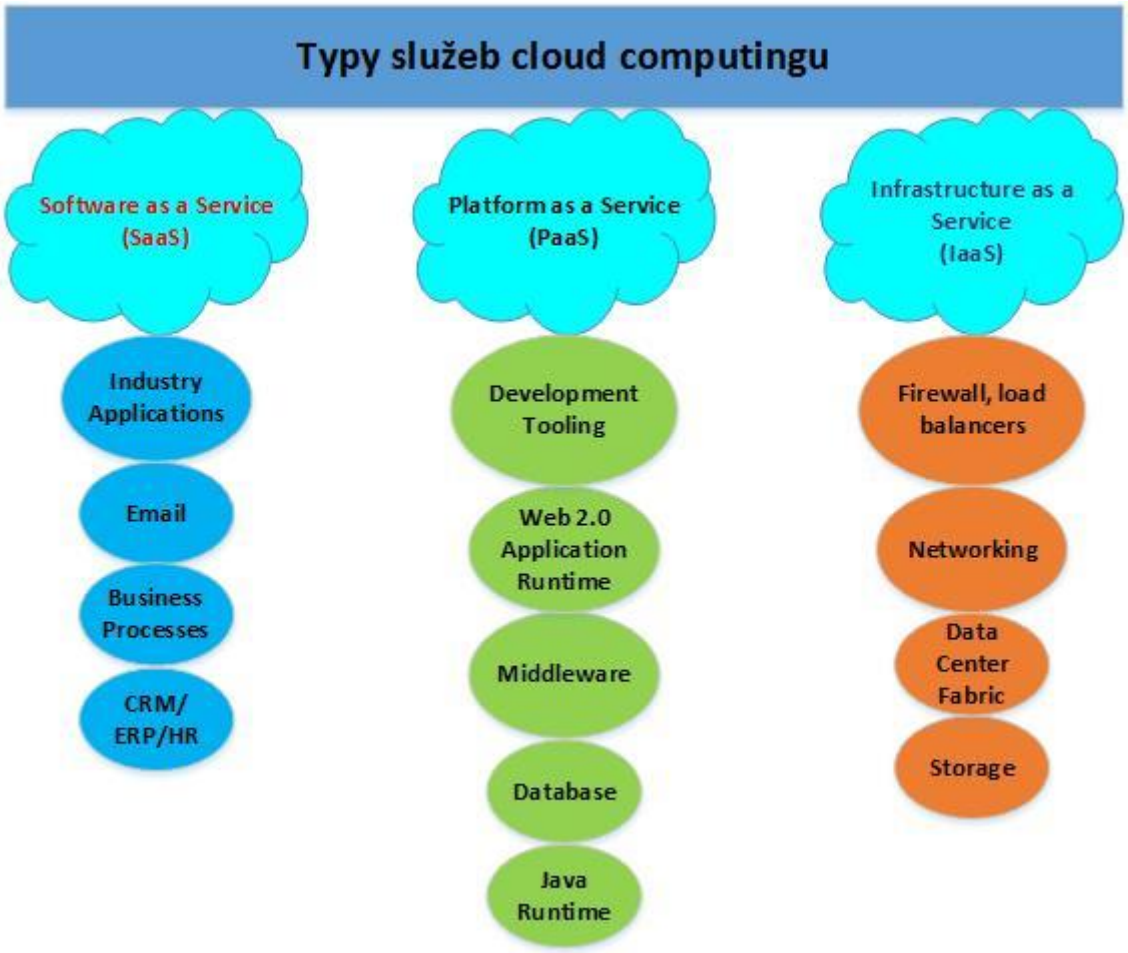
3 Způsoby zpracování služeb Cloud Computingu

Typ služby definuje, jakou úroveň abstrakce vlastních prostředků a úsilí na správu cloud computing poskytuje. Tyto služby dělíme na tři třídy a už samotný název jednotlivých typů tříd nám napovídá o úrovni služeb poskytovatele [7]. Tato kapitola se zakládá na informacích ze zdrojů [4] a [12].

3.1.1 SaaS – Software as a Service (Software jako služba)

V tomto distribučním modelu se zavazuje poskytovatel cloudových služeb aplikace hostovat uživateli přímo přes síť, která je jediným prostředkem, jenž zákazník potřebuje. Tento hosting si uživatel nekupuje, ale jedná se o pronájem. Poskytovatel tedy mění svoji aplikaci nebo službu ve výrobek. Tímto také vzniká největší výhoda pro uživatele SaaS, a to s minimálními nebo dokonce žádnými náklady na nákup a instalaci software, správu hardware a update. Ve svém PC totiž žádnou aplikaci nemá, ale používá ji pomocí přístupu přes webový prohlížeč. Další výhodou SaaS je také správa software a hardware profesionálním odborníkem a zpravidla redundantní hardware vzhledem k minimalizaci možnosti ztráty dat. Mezi nevýhody služeb typu SaaS lze zařadit nižší rychlost aplikací než u ostatních typů služeb a nízkou validitu s non-SaaS aplikacemi. Software as a Service využívá například Google Apps, Selesforce.com, Zoho.com a další.

SaaS můžeme rozdělit do dvou kategorií. První kategorií je služba pro firmy, kde řešení pro podniky a firmy jsou poskytována zejména na základě předplacení služby. Řadí se zde převážně aplikace zaměřující se na obchodní procesy. Druhou kategorií je služba pro fyzické osoby - tyto služby jsou dostupné převážně zdarma, poskytovatel přijímá zisk z reklam. Typickým příkladem jsou e-mailové aplikace nebo on-line hry.Tento typ se nejvíce podílí na zájmu o cloudové služby vzhledem k jeho nízkým nákladům, flexibilitě a velké rychlosti nasazení [12].



Obr. 2 Rozdělení služeb Cloud Computingu. (Vlastní zpracování dle [50])

3.1.2 PaaS – Platform as a Service (Platforma jako služba)

Tato služba spočívá v poskytnutí všech prostředků výpočetní a softwarové infrastruktury klientovi, usnadňuje tak vytvoření UI v poskytovaném vývojovém prostředí. Zahrnuje software potřebný k provozování vlastních aplikací, návrhy aplikací a nástroje pro jejich update. Klient se zabývá správou vlastních aplikací, nikoliv platformou, díky které může aplikace vytvářet a provozovat pomocí internetu. O platformu, její správu a zabezpečení se nadále stará poskytovatel hostingu. Nejčastěji klient hradí využívaní hardware, operačního systému a místa na disku poskytovatele. Platformy umožňují zákazníkům vytvářet a vyvíjet aplikace daleko větších rozměrů, než by jim umožňoval vlastní hardware.

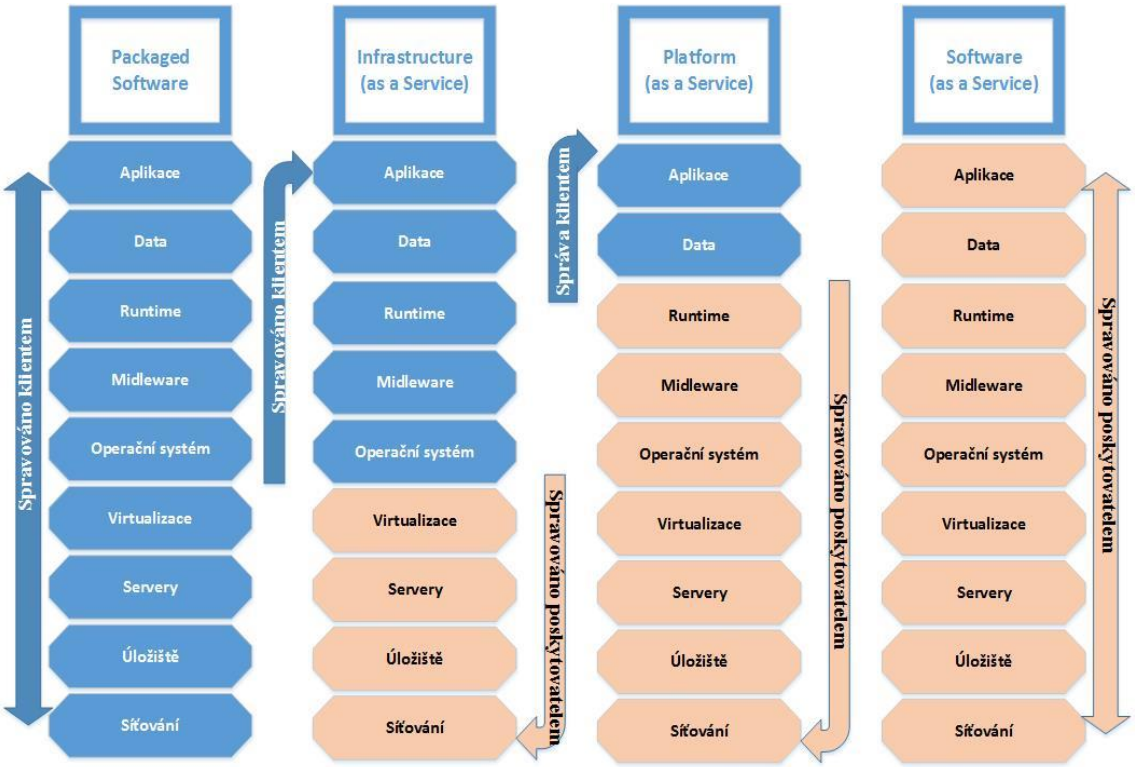
Výhodou tohoto typu je široké uplatnění pro zákazníka počínaje základními procesy vývoje aplikací, testováním a konče hostováním. Pro firmy je PaaS přínosem z důvodu možnosti spolupráce pracovního týmu na dálku odkudkoliv.

Zákazník nemusí investovat do fyzického výpočetního výkonu a zabezpečení. Jednoduše lze služby PaaS škálovat a upravovat. Nevýhodou pro uživatele může být jeho limitování ohledně rozhraní a jazyka. Za průkopníka PaaS považujeme společnost Salesforce.com se svou CRM platformou Force.com, dále tento typ využívá například Microsoft Azure, Yahoo! Open Strategy, Google a Amazon [12].

3.1.3 IaaS – Infrastructure as a Service (Infrastruktura jako služba)

Zde se poskytovatel zavazuje poskytovat infrastrukturu s odpovídajícím úložištěm, zabezpečením a servery pro vytváření aplikací. Velikost poskytované infrastruktury je flexibilní dle aktuálních požadavků klienta, který sám infrastrukturu spravuje včetně instalace software. Jedná se o absenci nákladů na vlastní zdroje, které mohou nadále pro klienta zůstat nevyužité nebo nebudou dostatečně velké a pomocí IaaS může využívat zdrojů poskytovatele na vyžádání dle vyvíjejících se výpočetních výkyvů. Poskytovatelův fyzický soubor hardwarových zdrojů (několik serverů a sítí) tvoří virtualizované výpočetní zdroje, které může klient využívat bez starostí o jejich správu, a tyto starosti připadají na poskytovatele. Klient přistupuje k těmto virtualizovaným výpočetním zdrojům pro sestavení vlastní IT platformy. Klient nespravuje OS, disk a nasazené aplikace, ale má nad nimi kontrolu.

Tento způsob je vhodný pro klienty, kteří vlastní svůj software a nemohou nebo se nechtějí starat o hardware.Příkladem IaaS jsou například Amazon AWS, Rackspace, Microsoft Live Mesh, IBM Computing on Demand (CoD).Výhodou tohoto typu nasazení je okamžitá možnost přizpůsobení zdrojů vzhledem k požadavkům klienta například u nepředvídatelných okolností. Další výhodou pro uživatele je absence pořizovacích nákladů za hardware. Nevýhodou tohoto typu služby je velké riziko týkající se důvěry uživatele v infrastrukturu poskytovatele (dostupnost, datová bezpečnost atd.) [4], [12].



Obr. 3 Typy Private Cloud Computingu.(Vlastní zpracování dle [51])

3.2 Základní vlastnosti Cloud Computingu

V této podkapitole se zaměřím na typické vlastnosti Cloud Computingu. Každý autor publikací o Cloud Computingu uvádí výčet jeho charakteristických vlastností trochu odlišný, vzhledem k individuálním názorům a požadavkům na cloud. Vybral jsem proto pět vlastností, které bych vyzdvihl a charakterizoval. Tyto vlastnosti musíme nalézt u každého efektivního a dobře propracovaného cloudu. Jak uvádí T.Erl a spol. [13] „Definice Cloud Computingu dle NIST definuje pouze pět charakteristik. Mezi tyto charakteristiky nepatří odolnost. Odolnost se objevila jako velmi významný aspekt a úroveň její podpory představuje nezbytné zahrnutí mezi charakteristiky cloudu.“ Tuto kapitolu jsem vypracoval na základě zdrojů [5], [7], [11], [13] a [14].

3.2.1 Použití na vyžádání (on-demand usage)

Uživatel cloudu může jednostranně využívat služeb, výpočetních zdrojů, serverů a úložiště automaticky po konfiguraci a nemusí angažovat providera. Výsledkem je samoobslužné využití na vyžádání, [13] [14].

3.2.2 Přístup kdykoliv a kdekoliv

Cloudové služby lze využít kdykoliv a kdekoliv, zejména s pomocí nejrůznějších klientů připojených k internetu. Připojení k internetu je zcela nezbytnou podmínkou. Ovšem tento způsob přístupu umožňuje podporu celé řady zařízení, přenosových protokolů, rozhraní a bezpečnostních technologií. Jedná se o možnost připojení obsáhlých i tenkých klientů jako například smartphone, tablet, notebook nebo stolní počítač. Tento způsob má i své nevýhody. Zásadním problémem je nemožnost připojení k internetu. Problémy však mohou vzniknout i na straně webu, ke kterému se uživatel připojuje. V této době již riziko těchto závad není příliš vysoké, nicméně můžeme si připomenout například výpadek společnosti Google počátkem roku 2017, kdy jejich služby přestaly fungovat na několik hodin a hostované aplikace byly zcela nedostupné [13], [14].

3.2.3 Měřitelnost využitých služeb (Pay-as-you-go)

Tato vlastnost je základním principem Cloud Computingu a označuje způsob platby pouze za reálně využité služby. Uživatel nehradí vysoké náklady na zřízení vlastního hardware nebo software, ale využívá a platí jenom takový rozsah služeb, který opravdu využije. Výhodou těchto řešení je tedy zejména omezení počátečních nákladů, jako je pořízení hardware, software, licencí, zálohování, náklady na IT specialisty atd. Služby jsou účtovány dle využitého času nebo dle objemu přenesených dat. Tato vlastnost je úzce spjata s vlastností použití na vyžádání. Měřitelnost využitých služeb aplikují i bezplatné cloudy a to z důvodu zpětné vazby o využívání cloudu [5], [7], [13].

3.2.4 Elasticita

Velmi důležitým prvkem Cloud Computingu je elasticita služeb a vlastností přesně dle aktuální potřeby klienta, jiným slovem na vyžádání. Tuto vlastnost nazýváme také škálovatelností. Škálovatelnost je možnost elastického přizpůsobení (rozšíření nebo snížení výkonu systému v případě potřeby) výpočetních schopností vzhledem k maximální možné efektivitě nákladů, stejně jako například poskytovatel elektrické energie řeší odchylky ve spotřebě energie. Co se týče přizpůsobení poskytovaných služeb (výpočetních schopností) klientovi, jedná se o proces, který není řízen uživatelem. Ten ho vnímá pouze podle vyúčtování

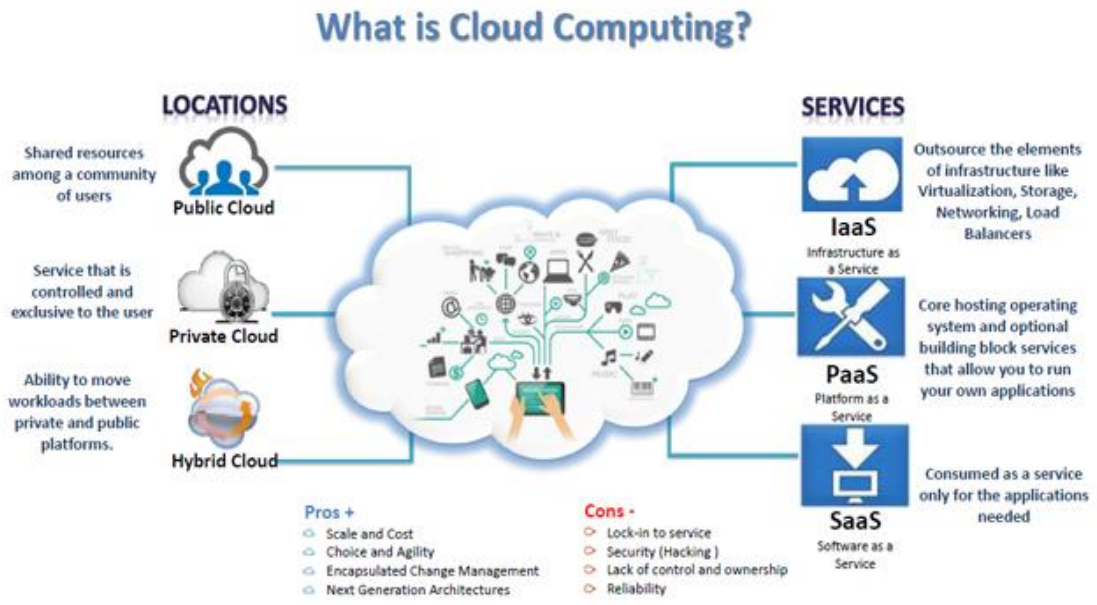
skutečného objemu využitých zdrojů. Největší škálu elasticity může nabídnout poskytovatel s velkými výpočetními zdroji [7], [13], [14].

3.2.5 Sdílení zdrojů a multitenancy

Tato vlastnost znamená sdílení software, který slouží pro několik navzájem izolovaných uživatelů (nájemců). Sdílené zdroje jsou dynamicky přiřazovány dle požadavků zákazníků. Výhodou pro poskytovatele je spojení fyzických a virtuálních zdrojů do jednoho velmi rozsáhlého zdroje. Mezi tyto sdílené zdroje patří ukládání, zpracování, paměť a šířka pásma sítě [13], [14].

3.2.6 Odolnost (Resiliency)

Odolnost u cloudových služeb zajišťuje redundanci výpočetních zdrojů na více fyzických místech. Pokud jeden zdroj přestane fungovat, může ho automaticky nahradit jiná redundantní implementace na jiném fyzickém místě v rámci stejného cloudu nebo popřípadě jiného cloudu. Pomocí odolnosti poskytovatel zvyšuje spolehlivost, dostupnost a tím i kvalitu cloudu [13].



Obr. 4 Principy Cloud Computingu.(Zdroj: [52])

4 Cloud jako úložiště dat

V této kapitole se zaměřím na vytyčení kritérií, dle kterých má uživatel možnost výběru cloudu pro své potřeby. V první řadě by měl uživatel zhodnotit jaký typ dat a přibližnou velikost jejich objemu bude ukládat. Dále by se měl zaměřit na nabízený výkon, tedy rychlost příjmu a dobu odezvy. Důležitým kritériem je také spolehlivost a odolnost proti chybám, například dle úrovně smlouvy SLA, a zda je potřeba funkce zálohování a obnovení dat. Rozhodujícím parametrem by měly být také cenové náklady na používání daného cloudu. Na závěr musíme vzít v potaz požadavky na zabezpečení týkající se typu šifrování, mechanismu ověřování pro připojení k datům a podobně. Parametru zabezpečení se budu věnovat v celé následující kapitole [15], [16].

Mezi největší dodavatele cloudových služeb a cloudu jako úložiště dat můžeme zařadit téměř všechny velké a všem dobře známé nadnárodní společnosti zabývající se informačními technologiemi, protože cloud computing je velmi rozšířený, u klientů oblíbený a neodmyslitelně se řadí mezi několik největších odvětví informačních technologií. Právě z tohoto důvodu ho většina těchto gigantů zařazuje do svého portfolia služeb.

4.1.1 Cenový aspekt

Uživatel s nízkými nároky na objem ukládaných dat a funkcionalitu často nalezne požadované cloudové úložiště velice levně, někdy i zcela zdarma. Je ale omezen například nízkou garancí dostupnosti, spolehlivosti nebo malým objemem úložiště. Takový druh základní služby bez záruk pro zákazníka a bez poplatků za využívání nazýváme také jako best-effort. Pokud má uživatel nároky vyšší a zvolí plně zpoplatněnou variantu, nemusí se obávat, protože v případě cloud computinguje cena bez skrytých poplatků transparentně a konečně určená [15].

4.1.2 Velikost objemu ukládaných dat

Objem úložiště může uživatel využít například již od 2 GB u společnosti Dropbox ve variantě Basic a to zdarma až po 30 TB u společnosti Google v produktu Google Drive. Toto kritérium je tedy pro výběr cloudu velmi individuální. Zákazník si může

zvolit nižší velikost objemu úložiště a v případě potřeby rozšířit tento objem dle aktuálních požadavků.

4.1.3 Dostupnost služeb

Hodnota dostupnosti služeb je velmi důležitým kritériem pro výběr cloudu, obzvláště pokud uživatel plánuje například sdílení nebo hosting dat, u kterého je třeba stálý a nepřetržitý přístup. Na tomto aspektu může popřípadě záviset i podnikání uživatele cloudu. Zde poskytovatel může uvést úroveň SLA, což je, jak volně přeložil M. Hora [16]„Dohoda o úrovni poskytovaných služeb“ a udává se v procentech. Tímto poskytovatel ručí zákazníkovi, v jakém časovém rozpětí může být cloudové úložiště nedostupné například během jednoho měsíce nebo jednoho roku.

4.1.4 Přístup

Varianty přístupu můžeme najít v podstatě čtyři. Přes webový prohlížeč, pomocí tenkého klienta, mobilního klienta anebo pomocí API. Z těchto vyjmenovaných variant je ovšem nejčastěji nabízeným způsobem přístupu k cloudu právě webový prohlížeč. Je to proto, že zpravidla každý počítač má ve svém systému nainstalován alespoň jeden webový prohlížeč. Prostřednictvím smartphone se uživatel připojí pomocí aplikace. Každý uživatel by měl tedy zvážit svůj výběr dle varianty přístupu [18].

4.1.5 Fyzické umístění cloudu

Fyzické umístění cloudu by mělo hrát určitou roli při rozhodování uživatele jaký cloud vybrat. Přeci jenom jsou data umístěna na konkrétním fyzickém zařízení, a tudíž hrozí jejich odcizení nebo znehodnocení. Z tohoto důvodu by mělo být kritériem pro výběr cloudu to, kde přesně se cloudové úložiště dat nachází, a zda splňuje legislativní podmínky - například pro zpracování osobních údajů. Cloudové úložiště by mělo být fyzicky zabezpečeno tak, aby se k němu nemohla dostat žádná třetí strana. Kvalitní cloud by měl pravidelně procházet audity.

4.2 Porovnání nabízených cloudových úložišť vybraných poskytovatelů

Tato podkapitola je porovnáním cloudových úložišť od známých poskytovatelů cloud služeb. Porovnávány jsou zde aspekty, které jsem popisoval výše.

4.2.1 Amazon (Amazon Web Services)

Společnost Amazon je hlavním průkopníkem Cloud Computingu, ale také nejznámějším dodavatelem cloudových služeb vůbec, zejména v zahraničí. Jedná se o cloud odvětví společnosti - Amazon Drive. Amazon již nenabízí cloudové úložiště zdarma, a proto musí uživatel vybírat pouze z placených variant.

100 GB Amazon Digital StoragePlan. V tomto programu Amazon nabízí 100GB cloudového úložiště za 11,99 USD ročně. Do úložiště se přistupuje pomocí aplikace Amazon Photos, lze ho využívat pomocí počítače, smartphone, tabletu atd. Amazon garantuje zabezpečení a ochranu soukromí.

1 TB Amazon Digital StoragePlan. Až na maximální objem dat (1 TB) a cenu (59.99 USD ročně) jsou parametry stejné jako 100 GB verze. Pokud si klient zakoupí členství Prime membership, nezapočítávají se fotografie uložené na cloudové úložiště do maximálního objemu dat [8].

4.2.2 Google Drive

Společnost Google garantuje a uvádí, že jsou data uložená na Google Drive neustále v naprostém bezpečí a nachází se na vysoce zabezpečených datových centrech, která jsou postavena na míru. Dále uvádí, že ke všem souborům na Google Drive má klient přístup z jakéhokoli zařízení a může je snadno sdílet. Google Drive si poradí s jakýmkoliv typem souboru, například s hudbou, filmy, dokumenty a podobně. Je také propojen se službou Gmail a Fotky Google. Maximální velikost jednoho souboru je 5TB. Uchováváno je posledních 100 verzí souboru 30 dnů zpětně. Google má servery úložiště rozmístěny po celém světě.

Tabulka 1 Srovnání variant produktu Google Drive.

Velikost úložiště	Cena/měsíc

15 GB	Zdarma
100 GB	59,99,- Kč
1 TB	299,99,- Kč
10 TB	2 999,99,- Kč
20 TB	5 999,99,- Kč
30 TB	8 999,99,- Kč

[9]

4.2.3 Microsoft OneDrive

Služba OneDrive od společnosti Microsoft poskytuje přístup k souborům klienta pomocí internetové sítě, zvládne integraci s programy balíčku Microsoft Office a nyní se prodává již předinstalovaný v OS Windows. Soubory se automaticky synchronizují se stolním počítačem, lze tak s nimi pracovat offline. Přístup k souborům je možný z počítače, notebooku, tabletu nebo mobilních zařízení. OneDrive obsahuje také velkou podporu různých typů souborů. Například soubory formátu PDF, Adobe Photoshop, Adobe Illustrator, Visio a další. Pomocí OneDrive lze rovněž provádět streaming videa v HD kvalitě. Pomocí aplikace SharePoint umožňuje OneDrive sdílení souborů v pracovním týmu nebo ve škole. U této aplikace nalezneme také historii aktivit a úprav souborů. Klient OneDrive může obnovit soubory, které byly odstraněny nedopatřením, nebo pokud by došlo k internetovému útoku [19].

Prémiové funkce OneDrive týkající se rozšíření zabezpečení:

Pro sdílení souborů lze využít odkazy s možností nastavení termínu jejich platnosti. Pomocí této vlastnosti lze poskytnout uživatelům, se kterými jsou soubory sdíleny, přístup pouze po omezenou dobu. Tyto odkazy lze rovněž chránit heslem. Existuje možnost obnovení celého úložiště do libovolného bodu maximálně 30 dnů zpětně. Další prémiovou funkcí je detekování a upozornění uživatele na útok ransomware [20].

Tabulka 2 Srovnání variant produktu OneDrive.

Ceny služeb pro fyzické osoby:
OneDrive Basic 5 GB – pouze úložiště, zdarma.

OneDrive 50 GB - pouze úložiště, 49,99,- Kč / měsíc.
Office 365 pro jednotlivce - zahrnuje OneDrive a jeho prémiové funkce, 1 TB úložiště. 1 790,- Kč/rok
Office 365 pro domácnosti – zahrnuje OneDrive a jeho prémiové funkce, 5 TB úložiště. 2 490,- Kč/rok

4.2.4 Dropbox

Prostor určený primárně pro spolupráci dává uživateli možnost lepší efektivity práce pomocí synchronizace ve všech zařízeních, jež si uživatel zvolí. Pomocí Dropbox lze odesílat velké soubory i uživatelům, kteří účet Dropbox nainstalovaný nemají. Samozřejmostí je funkce skenování dokumentů, sdílené složky, přístup offline, komentáře k souborům a další výhody. Dropbox nabízí třicetidenní zkušební verzi zdarma. Verzování souborů Dropbox podporuje a to po dobu 30 dnů zpětně. Servery se nachází v USA. Velikost souboru je neomezená při nahrávání přes synchronizační aplikaci.

Tabulka 3 Srovnání variant produktu Dropbox.

Ceník služeb pro fyzické osoby:
Basic – zdarma, 2 GB úložiště, synchronizované soubory a složky, DropboxPaper
Plus – 9,99€ / měsíc, 1 TB úložiště, offline přístup k souborům
Proffesional - 19,99€ / měsíc, 2 TB úložiště, full-text vyledávání

[21]

4.2.5 iCloud – Apple

Tato aplikace je integrována v zařízeních od výrobce Apple a umožňuje nahrání fotografií, videí i dokumentů. Fotografie a videa v zařízení Apple se automaticky ukládají na iCloud v originální kvalitě a plném rozlišení. V zařízení tak zůstává pouze „odlehčená“ verze z důvodu úspory úložiště. Toto úložiště lze sdílet s více uživateli nebo přidávat komentáře k albům. Přístup je možný pomocí aplikace přímo v zařízení nebo pomocí webového prohlížeče. Lze na více zařízeních sdílet i zprávy. Pomocí iCloud lze automaticky zálohovat všechny soubory v zařízení, tudíž se jedná o ochranu dat při ztrátě zařízení. Služba iCloud se zakládá na dvoufaktorovém ověřování Apple ID. Toto zabezpečení spočívá v tom, že si uživatel

nastaví důvěryhodné zařízení, které patří pouze jemu a pokud se přihlašuje na jiném nebo novém zařízení, vyžaduje po něm iCloud kromě hesla také šesticiferný ověřovací kód, který se uživateli zobrazí pouze na jeho důvěryhodném zařízení. Poté po prvním přihlášení již není tento kód vyžadován až do kompletního odhlášení nebo vymazání zařízení.

Tabulka 4 Srovnání variant produktu iCloud.

Objem úložiště	Cena
5 GB	Zdarma
50 GB	0,99 €/měsíc
200 GB	2,99 €/měsíc
2 TB	9,99 €/měsíc

[22]

4.2.6 Box.net

Služba Box.net na trhu cloudových úložišť začínala jako konkurence výše zmíněného Dropboxu. Jedná se o méně známou službu, avšak jednu z těch dražších v porovnání s předchozími cloudovými službami. V základním tarifu Personal nabízí tato služba úložiště 10 GB bezplatně. V nabídce je také možnost přistupovat z několika zařízení zároveň několika uživatelům. Výhodou je, že lze nastavit pro tyto uživatele jednotlivě oprávnění. Verzování souborů nabízejí pouze placené varianty úložišť. Lze využit synchronizační aplikaci pro systémy Windows i mobilní zařízení s operačním systémem iOS a Android. Servery úložišť tohoto poskytovatele se nachází na území USA. Tato služba je propojena s Office online stejně tak jako Dropbox. Úložiště je přístupné pomocí webového rozhraní.

Tabulka 5 Srovnání variant produktu Box.net.

Název varianty	Kapacita úložiště	Max. velikost souboru, počet uživatelů	Cena / měsíc
Individual	10 GB	250 MB, 1	Zdarma
Personal Pro	100 GB	5 GB, 1	9 €
Starter	100 GB	2 GB, 3 - 10	4,50 €
Business	Neomezená	5 GB, 3 - neomezeně	13,50 €

Business Plus	Neomezená	5 GB, 3- neomezeně	22,50 €

[23], [24]

4.2.7 Mega

Toto úložiště si zakládá především na bezpečnosti dat a soukromí, například šifrováním jak přenášených dat, tak i dat uložených na úložišti. K datům nemá tedy přístup ani samotný poskytovatel Mega, ale pouze uživatel vzhledem ke znalosti dešifrovacího klíče. Pokud uživatel zapomene heslo, není již žádná možnost opakovaného přihlášení, a tudíž dochází ke ztrátě uložených dat. Verzování souborů lze vytvořit pouze ručně, automaticky se neprovádí. Servery tohoto poskytovatele jsou umístěny na Novém Zélandu a v Evropě, a lze k nim přistupovat pomocí aplikací nebo webového prohlížeče. V nabídce je také rozšíření pro Chrome a Firefox. Základní a bezplatnou variantou úložiště je zde po registraci kapacita 50GB, prvních 30 dní je zde navíc 35GB kapacity, za instalaci aplikace MEGAsync obdrží uživatel navíc 20GB a mobilní aplikace 15GB po dobu 180 dní. Po doporučení nového uživatele se kapacita navyšuje o 10GB na rok.

Tabulka 6 Srovnání variant produktu Mega.

Název varianty	Kapacita úložiště	Maximální objem přenesených dat za měsíc	Cena / měsíc
Základní	15GB	-	Zdarma
Pro Lite	200GB	1TB	4,99 €
Pro I	1TB	2TB	9,99 €
Pro II	4TB	8TB	19,99 €
Pro III	8TB	16TB	29,99 €

[23], [25]

5 Zabezpečení dat v cloud

S Cloud Computingem jsou spojena rizika týkající se zabezpečení dat a informací. Pro odlišné typy služeb se požadavky na zabezpečení víceméně neliší, avšak nalezneme odlišné požadavky mezi modely nasazení. Soukromý cloud je vnímán jako bezpečnější oproti cloudu veřejnému, a tudíž je jejich zabezpečení odlišné. Data nebo informace uživatele se v Cloud Computingu nacházejí na straně poskytovatele, jedná se tedy o velké riziko odcizení, zneužití, nezákonného šíření nebo poškození dat. Můžeme se také setkat s prodejem uživatelských dat třetí osobě. Data mohou vzhledem k infrastruktuře poskytovatele překračovat hranice naší země a tato okolnost může mít dopad na právní a regulační formu ochrany dat. Problematika ochrany v digitálním světě přetrvává nejčastěji ve formě šifrování [18][11].

5.1 Základní pojmy standardního zabezpečení

V této kapitole nastíním základní pojmy a koncepty, které vymezují či souvisejí s hrozbami nebo útoky na cloud. Bezpečnostní opatření týkající se dat mají za cíl chránit před jejich zneužitím nebo únikem.

Mezi základní pojmy můžeme zařadit rozhodně důvěrnost, jelikož je to požadavek uživatele k omezení přístupu k jeho datům. Dalším pojmem je integrita, která zajišťuje nepozměnění obsahu uložených nebo přenášených dat třetí stranou. Základním pojmem v cloudu je také autentizace, která nám zajišťuje, že k určitým datům může mít přístup jenom oprávněný uživatel. Hrozba a risk jsou spolu úzce související pojmy, kde hrozba představuje možné narušení bezpečnosti, riziko je měřeno právě dle počtu a úrovně hrozeb a pravděpodobnosti jejich výskytu. Entitu, která může způsobit hrozbu a představuje riziko, protože je schopna provést útok, nazýváme agent hrozby. Dále se budu zabývat jednotlivými hrozbami, nástroji pro bezpečnostní kontroly a bezpečnostními mechanismy [13].

5.1.1 Hrozby

Mezi hrozby řadíme odposlouchávání přenosu, které se může vyskytnout při přenášení dat uživatele na cloud a jeho infrastrukturu poskytovatele. Agent s nekalým úmyslem může zachytit data a nelegálně je shromažďovat. Tímto

způsobem se snaží narušit důvěryhodnost přenášených dat a vztah uživatele k poskytovateli cloudu. Touto entitou může být například externě umístěný škodlivý software, který pořizuje kopie přenášených dat. Hrozbou nazýváme i takzvaného škodlivého prostředníka, jenž zachycuje přenášená data, pozmění je nebo k nim přidá vlastní obsah. Tímto může ohrozit celé úložiště zanesením škodlivých dat.

Jako odmítnutí služby nazýváme útok DoS, kterým útočník přetíží informační zdroje na straně poskytovatele, a ty poté nefungují správně. Jedná se o umělé navýšení pracovní zátěže nebo přetížení sítě imitačními zprávami nebo opakovanými požadavky na komunikaci. Při této hrozbě ovšem dochází k nemožnosti komunikace uživatele s cloud serverem, avšak data zůstávají v bezpečí.

5.2 Šifrování

Standardně jsou data v čitelném formátu, například text známe jako čitelný prostý text. V případě, že jsou tato data přenášena po síti, jedná se o velmi snadno zranitelný a zneužitelný cíl. K předejití tohoto problému se využívá šifrovací mechanismus nazvaný digitální kódovací systém, který je určený pro zachování bezpečnosti přenášených dat. Data z prostého textu se kódují do nečitelného formátu, jenž je chráněný před nežádoucím vlivem třetí strany. Pokud jsou šifrovány textové údaje, používá se k dešifrování zpět do původního formátu šifrovací klíč, který mají jenom oprávněné strany. Tuto kapitolu zpracovávám na základě informací ze zdroje [13].

5.3 Typy šifrování

Rozlišujeme dvě základní formy šifrování nazývané jako symetrické šifrování a asymetrické šifrování, jež můžeme označit za časově náročnější. Při přenosu dat pomocí webu se setkáme s protokolem HTTP, který obsahuje vrstvu TLS (Transport Layer Security). Vzhledem k porovnání rychlostí těchto dvou šifrovacích metod TLS využívá asymetrickou metodu většinou při výměně klíčů a poté přechází na symetrické šifrování.

5.3.1 Symetrické šifrování (Symmetric encryption)

Toto šifrování nazýváme symetrickým vzhledem k tomu, že zde slouží jeden šifrovací klíč k šifrování i dešifrování a je sdílený oběma stranami přenosu. Tuto

metodu můžeme zahlédnout také pod názvem kryptografie tajného klíče. Zástupce symetrické šifry: AES, RC4, Triple DES.

5.3.2 Asymetrické šifrování (Asymmetric encryption)

Zde nalezneme na rozdíl od symetrického šifrování dva různé šifrovací klíče a to jmenovitě soukromý a veřejný. Tato metoda je také označována jako kryptografie veřejného klíče. Vzhledem k použití více klíčů je toto šifrování zpravidla poměrně pomalejší než symetrická jednodušší varianta. Ochrana dat spočívá v zašifrování pomocí soukromého klíče, k němuž má přístup pouze jeho majitel a následné dešifrování pomocí veřejného klíče, který je dostupný pro příjemce dokumentu. Pokud naopak zašifrujeme data pomocí veřejného klíče, lze je dešifrovat pouze za pomocí soukromého klíče. Každá zpráva šifrovaná tímto způsobem má své vlastní soukromé klíče a může být dešifrována libovolnou stranou s odpovídajícím veřejným klíčem. Tato metoda na rozdíl od symetrického šifrování nenabízí ochranu integrity, a tudíž ani diskrétnost, jelikož každá strana, která má veřejný šifrovací klíč může generovat šifrovaný text. Většinově používaná je implementace RSA.

5.4 Hašování

Hašování je používáno, pokud je vyžadováno zabezpečení dat pouze jednosměrně a nevratně. Typickým příkladem, kdy se využívá hašování, je ukládání hesel. Tato technologie může být také využita k odvození haše a rozložení zprávy na miniaturu, jež má pevnou délku a slouží pro kontrolu integrity zprávy. Příjemce použije ke zprávě stejnou hašovací funkci a ověří shodu s miniaturou, která zprávu doprovází. I malá změna původních dat na vstupu vede k velké změně miniatury a příjemce jasně pozná, že došlo k neoprávněnému zásahu do dat. Lze tedy nakonfigurovat bránu firewall na straně cloudu tak, aby odmítala zprávy, u nichž zjistí, že byly pozměněny a neposkytne tedy cloudové služby.

5.5 Správa identit a přístupu

Tento mechanismus zabezpečení má zkratku IAM a obsahuje kombinaci zásad a komponent potřebných k ověřování uživatelů a zajištění přístupových práv. Skládá se ze čtyř prvků. Prvním prvkem je autentizace, která zahrnuje nejčastěji

identifikaci uživatele pomocí jména a hesla, ovšem můžeme se setkat i s identifikací digitálním podpisem, certifikátem, otiskem prstu nebo IP adresou. Autorizace je dalším z prvků IAM, zajišťuje kontrolu vztahů mezi uživateli, kontrolu přístupu a dostupnosti výpočetních zdrojů. Mezi prvky IAM dále patří správa uživatelů. Tento prvek stanovuje pravidla identifikace a kontroly pro definované uživatelské účty a tím eliminuje hrozbu nedostatečné autorizace.

6 Šifrování dat v cloud pomocí nástrojů třetích stran

Jak jsem již zmiňoval v předchozí kapitole týkající se zabezpečení dat v cloud, hrozí uživateli v případě přenosu dat na cloud riziko odposlouchávání přenosu, shromažďování dat, nebo jejich pozměnění škodlivým prostředníkem neboli agentem. Z tohoto důvodu byly vyvinuty programy, které pomáhají uživateli pomocí šifrovacích mechanismů zakódovat data na jeho straně ještě před přenosem na cloud. Tyto programy zašifrují data tak, aby je bylo možné přečíst pouze pomocí klíče, jenž vlastní oprávněný uživatel a zamezí tak přístupu k soukromým datům třetím stranám. Vzhledem k výše zmiňovanému problému cloudu (konkrétně pro uživatele je možná absence znalosti infrastruktury a konkrétního zabezpečení serverů cloud úložišť na straně poskytovatele) pomáhají tyto nástroje třetích stran uživateli ochránit svá data i v případě ztráty, odcizení anebo nežádoucího přístupu k datům, protože tato data jsou bez šifrovacího klíče nečitelná a bezvýznamná a uživatel se tím pádem nemusí obávat o ztrátu úrovně zabezpečení na straně poskytovatele. Někteří poskytovatelé mohou šifrovat pouze autentizační údaje, což může být nedostačující a uživatel má možnost pomocí nástrojů třetích stran zašifrovat i data nahraná na cloud. V této kapitole uvedu několik příkladů softwarových nástrojů, které poskytují zabezpečení dat ukládaných na cloud pomocí šifrování.

6.1 Boxcryptor

6.1.1 Specifikace

Tento software od společnosti SecombaGmbH pocházející z Německa je velice rozšířený a oblíbený pro své velmi přívětivé uživatelské rozhraní. Kontroluje data pomocí end-to-end šifrování a tudíž šifrovaná data může číst pouze uživatel, kterému data patří. Boxcryptor se napojí na uživatelem vybrané cloudové úložiště a vytvoří v zařízení uživatele virtuální diskový oddíl, u platformy Windows standardně „X:“, do kterého uživatel vkládá data a ty se přesouvají zašifrována na cloud. Uživatel si však musí dávat pozor na soubor encfs6.xml, jenž Boxcryptor vytváří ve složce Boxcryptor.bc na cloudovém úložišti. Tento soubor obsahuje šifrovací klíč, tím pádem by přesunutí, odstranění nebo poškození tohoto souboru znemožnilo dešifrování dat. Boxcryptor poskytuje kombinaci asymetrického a

symetrického šifrování. U asymetrického šifrování se jedná o algoritmus RSA a u symetrického šifrování využívá algoritmus AES s délkou šifrovacího klíče 256 bitů. Tento způsob zaručuje, že každý soubor si ponechá jedinečný a náhodný šifrovací klíč. Boxcryptor je dle informací uvedených na webových stránkách Boxcryptor [26] aktuálně kompatibilní s třiceti poskytovateli cloud úložišť. Mezi kompatibilní služby patří například i několik známých služeb jako je Dropbox, Google Drive, OneDrive, Box, Amazon Cloud Drive, iCloud a další. Pro uživatele je velmi důležité nastavení dobře zapamatovatelného hesla, protože Boxcryptor je tzv. zero-knowledge šifrovací nástroj a tudíž nelze obnovit heslo. Uživatel by tedy při jeho ztrátě přišel i o všechna data [27], [28].

6.1.2 Podporované platformy

Pro správnou funkci software Boxcryptor na platformě Windows potřebuje uživatel jeden z těchto operačních systému: Windows 7, Windows 8 a Windows 10, vyjma varianty Windows 10 Insider, který není aplikací Boxcryptor oficiálně podporován. V případě Windows je nutný také .NET Framework 4.5.2. Na zařízeních od společnosti Apple je vyžadována platforma macOS 10.11 a novější, dále iOS 10.3 a novější, kde Boxcryptor je kompatibilní s iPhone, iPad a iPodtouch. Uživatel si variantu pro iOS stáhne na Appstore. Pro Android je zde funkcionalita od verze 4.4 a vyšší a Boxcryptor je kompatibilní se smartphony a tablety. Na Android zařízení si uživatel stáhne Boxcryptor v Google Play Store nebo Amazon Appstore. Portable varianta aplikace Boxcryptor je kompatibilní s Windows 7 a novější, macOS 10.10 a novější a s 64–bitovou variantou Linux.

Boxcryptor vyžaduje internetové připojení a v případě, že má uživatel zavedena nějaká síťová omezení, musí povolit připojení na domény, IP adresy, porty a protokoly Boxcryptoru [29].

6.1.3 Produkty

Boxcryptor má v nabídce verzi Free, která je zdarma a je určená pro fyzické osoby. Uživatel si zde může vybrat pouze jedno cloud úložiště a synchronizovat data na dvou zařízeních. Základní varianta nabízí také dvoufaktorovou autentizaci a tzv. inteligentní integraci, která umožňuje sdílení dat i s uživateli, kteří nepoužívají

Boxcryptor ani cloud úložiště. V této variantě nalezne uživatel technickou podporu od ostatních uživatelů nebo agentů podpory na fóru Boxcryptor. Dále je k dispozici varianta Personal, která oproti základní verzi Free nabízí navíc zvýšení bezpečnosti pomocí šifrování názvů souborů a neomezený počet cloud úložišť, na něž bude uživatel šifrovat data. Dále je zde také neomezený počet zařízení, na kterých budou data synchronizována a možnost rychlé technické podpory pomocí emailu. Poslední verzí pro fyzické osoby je varianta Business, jež poskytuje stejné výhody jako varianta Personal, ale k tomu dále umožňuje vytvoření skupin pro různé úrovně přístupu a vytváří možnost přidat ostatní uživatele Boxcryptor do skupiny. Samozřejmostí je i vyšší rychlost technické podpory [30].

Boxcryptor nabízí také varianty pro společnosti, tou základní je Company, u které se cena licence odvíjí dle počtu uživatelů a délky období licence. Ta nabízí tzv. Master key, který je určený pro administrátora skupiny a ten má s tímto klíčem možnost dešifrovat jakýkoliv soubor v úložišti bez znalosti hesla uživatele. Tento klíč se využívá i v případě obnovy hesla uživatele, kterou administrátor může provést nebo v případě vyřazení uživatele ze společnosti. Lze nastavit interní pokyny společnosti pro uživatele, omezené přístupy, minimální délku hesla a spoustu dalších user a group management výhod oproti variantám pro fyzické osoby. Varianta Company je pro 5 až 50 uživatelů. Dále je zde varianta Enterprise, která je pro početnější skupiny 50 a více uživatelů a její cena se odvíjí individuálně dle poptávky společnosti. Obě varianty nabízejí lepší uživatelskou podporu od specialistů Boxcryptor, u Enterprise dokonce telefonické konzultace během pracovní doby, video hovory pro pomoc s nastavením aplikace Boxcryptor a další [31].

Tabulka 7 Srovnání variant produktu Boxcryptor.

Název varianty	Cena
Free	Zdarma
Personal	48 $ / rok
Business	96 $ / rok
Company	10 $ za uživatele / rok nebo 8$ za uživatele / rok
Enterprise	Individuální cena dle požadavků

[32]

6.2 AxCrypt

6.2.1 Specifikace

Jedná se o software od švédské firmy AxCrypt AB. První verze byla vydána v roce 2002. Zaměřuje se na jednotlivce a malé skupiny v rámci firem. Automaticky se spojí s cloud úložištěm, jehož aplikaci má uživatel v zařízení nainstalovanou a vytvoří zde složku AxCrypt. I zde se jedná o end-to-end šifrování a v případě ztráty hesla již data nelze obnovit. Tato aplikace šifruje soubory jednotlivě anebo výběr souborů uživatelem, lze ovšem označit celou složku jako šifrovanou a při vkládání souborů do složky a případném odhlášení uživatele dojde automaticky k zašifrování souborů. Podpora jazyků je velmi široká, samozřejmostí je angličtina, němčina, ruština a další. Šifrování souborů zde probíhá pomocí algoritmu symetrického šifrování AES-128 a AES-256 v závislosti na variantě produktu. Dále je zde využíván veřejný klíč RSA-4096 pro sdílení souborů a soukromý klíč RSA-4096, který slouži pro synchronizaci mezi zařízeními a v případě ztráty zařízení jako krytí. Původní verze AxCrypt 1.x nemá tak širokou funkcionalitu jako novější verze a podporuje pouze stolní počítače Windows, avšak uživatelé ji mohou nadále využívat. Nová verze AxCrypt 2.x umí otevřít soubory zabezpečené starší verzí, naproti tomu starší verze nedokáže otevřít soubory zabezpečené novější verzí. Velikost šifrovaného souboru u této aplikace nehraje roli [33], [34].

6.2.2 Podporované platformy

Aplikace AxCrypt 1.x podporuje platformy Windows od 95 po Windows 2008, Vista, 7, 8 a 10. AxCrypt 2.x podporuje rovněž 32 a 64 bitové verze Windows 2008, Vista, 7, 8 a 10, dále potom Max OS X od varianty 10.8 a novější. Co se týče mobilních zařízení, jsou podporovány platformy Android 4.0.3 a vyšší a iOS 8.0 a vyšší [35].

6.2.3 Produkty

AxCrypt nabízí variantu Free, která je pro každého zdarma. Ovšem na zařízení MAC má uživatel k dispozici pouze čtení zašifrovaných dat. Na ostatních PC je zde kromě

čtení také možnost šifrování dat variantou AES-128 bit. Dále zálohování klíče účtu, otevření souborů zašifrovaných jinými uživateli a podpora uživatelů na komunitním fóru od pracovníků AxCrypt [38].

Další variantou je Premium, která již u podporovaných vlastností nerozlišuje mezi MAC a ostatními PC. Oproti všem vlastnostem varianty Free navíc nabízí silnější verzi algoritmu AES a to 256 bitů. Varianta Premium dále nabízí přístup k zašifrovaným souborům pomocí aplikace na mobilních zařízeních se systémem Android nebo iOS. Pomocí funkce Zabezpečené složky může uživatel velice snadno automaticky zabezpečovat nové soubory. Lze sdílet klíč pro dešifrování souborů s ostatními uživateli. Automaticky vytváří složku AxCrypt v cloudovém úložišti, jehož aplikaci má uživatel nainstalovanou v zařízení. Zavazuje se k možnosti bezpečného ukládání hesel a citlivých souborů na cloudvém úložišti. Premium umožňuje skrytí názvů šifrovaných souborů a bezpečné odstraňování uložených dat. Uživatelská podpora zde funguje přímo a to pomocí emailu nebo chatu. Tato varianta je pouze pro fyzické osoby [36].

Dále může zájemce využít variantu pro organizace Business, která zahrnuje všechny vlastnosti varianty Premium pro jednotlivce a navíc lepší administraci uživatelů a administrátorský učet. AxCrypt na svých webových stránkách uvádí, že pracuje na rozšíření vlastností varianty Business a brzy vydá exkluzivnější funkce [37].

Tabulka 8 Srovnání variant produktu AxCrypt.

Název varianty	Cena za rok (360 dnů) uváděná v CZK
Free	Zdarma
Premium	975,-
Business	2014,-

[38]

6.3 FolderLock

6.3.1 Specifikace

Aplikace slouží k zabezpečení dat, byla vyvinuta společností NewSoftwares.net zabývající se bezpečnostními aplikacemi. Pomocí FolderLock lze zabezpečit celé

složky nebo jednotlivé soubory. Uživatel si může vybrat mezi variantami na PC nebo na mobilní zařízení. Nabízí zaheslování a uzamčení souborů, složek nebo celých diskových oddílů. Dále poskytuje šifrování dat pomocí standardu AES-256, při němž si uživatel vybere umístění složky „trezoru“, kam se budou ukládat zašifrovaná data, poté Folder Lock vytvoří nový diskový oddíl, ve kterém budou data k zobrazení. Pomocí jednoduchého ovládání nastaví uživatel odemčení nebo uzamčení trezoru a heslo pro jeho ovládání. Šifrování lze provádět v režimu Stealth, při kterém jsou zašifrované soubory nebo složky neviditelné. Tento režim lze pohodlně ovládat pomocí klávesových zkratek. Folder Lock poskytuje uživateli možnost skartace souborů, což je žádoucí pro trvalé odstranění citlivých soukromých dat ze zařízení, přičemž odstraní i zbytková data, která standardně zůstávají po odstranění stále uložena na paměťovém médiu, dokud nedojde k jejich přepsání. Aplikace umožňuje obnovení hesla k souborům pomocí tzv. Master password, které uživatel nastavuje při instalaci a je tak hlavním administrátorským heslem. Celá aplikace je dle mého názoru velice uživatelsky přívětivá a lehce ovladatelná. Folder Lock byl vyhodnocen testovací společností Top Ten Reviews [39] se známkou 9,38 z 10 jako nejlepší šifrovací software. Vyzdvihnuta byla velmi vysoká rychlost šifrování, jednoduchost ovládání, šifrovací klíč AES-256 a další dodatkové funkce, které nabízí [40], [41].

6.3.2 Podporované platformy

Kompatibilita této aplikace je pouze se systémy Windows a to konkrétně Windows 7, Windows Vista, Windows XP, Windows 2003 a 2008 Server. Všechny zmíněné platformy jsou podporovány jak ve verzích 32-bitových, tak i 64-bitových. Platformy Apple ani Linux podporovány nejsou. Aktuální verze desktop aplikace je Folder Lock 7.7.8 z 24. září 2018. Co se mobilních zařízení týče, podporován je Android verze 4.2 a vyšší. Aktuální verze aplikace 2.3.7 pro Android je ke stažení na Google play. Pro uživatele Apple je k dispozici varianta pro iOS 9.0 a vyšší, která je ke stažení na App Store. Na webových stránkách Folder Lock je sice nabízena varianta pro Windows Phone, avšak po kliknutí na odkaz Windows Store není žádný produkt k dispozici [42], [43].

6.3.3 Produkty

Tabulka 9 Srovnání variant produktu Folder Lock.

Varianta	Cena
Folder Lock zkušební verze	Zdarma
Folder Lock pro desktop plná verze	39 $
Folder Lock pro android	109,99 Kč
Folder Lock pro iOS	3,99 $
Folder Lock pro Windows Phone	Neznámo

[43]

6.4 Shrnutí nástrojů třetích stran

V dnešní době existuje velká řada produktů, které poskytují zabezpečení dat použitelných ať už pro cloud nebo pouze v zařízení v rámci soukromí či střídání uživatelů na jednom zařízení. Vzhledem k tomu, že tyto nástroje třetích stran vyžadují zpravidla velmi silná hesla pro identifikaci uživatele a již zmíněné velké délky šifrovacího klíče, jedná se v podstatě o neprolomitelnou úroveň zabezpečení dat běžného uživatele. Tyto vlastnosti zahrnuje již zmiňované úložiště Mega, které data šifruje automaticky při přenosu na úložiště. K datům má tedy stejně jako v případě nástrojů třetích stran přístup pouze uživatel, nikoliv poskytovatel úložiště, vzhledem k neznalosti dešifrovacího klíče. Bohužel většina vývojářů nástrojů třetích stran neposkytuje informace o požadavcích na sytém. Během šifrování probíhají velmi složité algoritmy a procesy. Jedná se tedy o poměrně vysokou zátěž pro nevýkonná zařízení.

6.5 Interní zabezpečení cloudových úložišť

Zabezpečení na straně cloud úložiště se řídí dle standardů a certifikátů, které cloud provider uvádí. Vzhledem k bezpečnosti jsou ovšem detaily tohoto zabezpečení neveřejné a uživatel tedy neví, jak konkrétně toto zabezpečení funguje či naopak nefunguje. V případě interního zabezpečení se mimo šifrování dat jedná většinou o zabezpečení umístění a separace dat, pravidelný bezpečnostní audit, správu uživatelů a řízení přístupů nebo samotné fyzické zabezpečení serverů.

6.6 Shrnutí zabezpečení cloud

V současnosti se vize cloud služeb velmi rozšířila, stojí na ní provoz a existence mnoha společností a pohodlí uživatelů. Jedná se o velmi efektivní, rychlé a snadné řešení sdílení a zálohování dat. Nicméně by žádný uživatel neměl zapomínat na nebezpečí a hrozby, které s sebou tento komfort nese. I přes snahu provozovatelů cloud úložišť zajistit a zlepšovat zabezpečení dat uživatele se stále jedná o velmi rizikové úložiště dat v porovnání s daty uloženými na soukromém disku. Proto by měl uživatel cloud služeb ve svém zájmu používat zabezpečení i na své straně. Přinejmenším používat již zmíněné nástroje třetích stran, které nijak nekomplikují užívání cloud úložiště. Jakékoliv opatření nad rámec standardního a poskytovatelem nabízeného zabezpečení zvyšuje exponenciálně bezpečnost uložených dat na cloud úložišti.

7 Analýza a testování nástrojů pro zabezpečení dat

V této kapitole se budu věnovat testování nástrojů pro zabezpečení dat ukládaných na cloud. Jedná se o praktickou část této bakalářské práce.

7.1 Vlastní nástroje zabezpečení cloud úložišť

Tuto problematiku nelze zkoumat z důvodu, že interní zabezpečení probíhá na straně serveru, a tak nemáme způsob, jak měřit například vytížení serveru při probíhajícím šifrování nebo dalších úkonech zabezpečení. V tomto případě máme pouze informace, které poskytuje cloud poskytovatel.

7.2 Popis praktické části (analýza nástrojů zabezpečení třetích stran)

V této části kapitoly se zaměřím na analyzování jednotlivých nástrojů třetích stran, které jsem popisoval v části teoretické. Vyzkouším a popíši šifrovací nástroje od instalace až po náročné šifrovací operace. Budu zkoumat vytížení systémových prostředků konkrétně procesoru, operační paměti, pevného disku a síťové karty při procesu zabezpečení a přenášení dat. Toto zkoumání bude probíhat u tří výše popisovaných produktů. Aby byly výsledky měření co nejlépe porovnatelné, využiji pro všechny zkoumané nástroje třetích stran identické cloudové úložiště. Tímto zajistím objektivitu výsledků díky stejným podmínkám na straně cloud. Jako úložiště budu využívat aktuální verzi Dropbox 67.4.83.

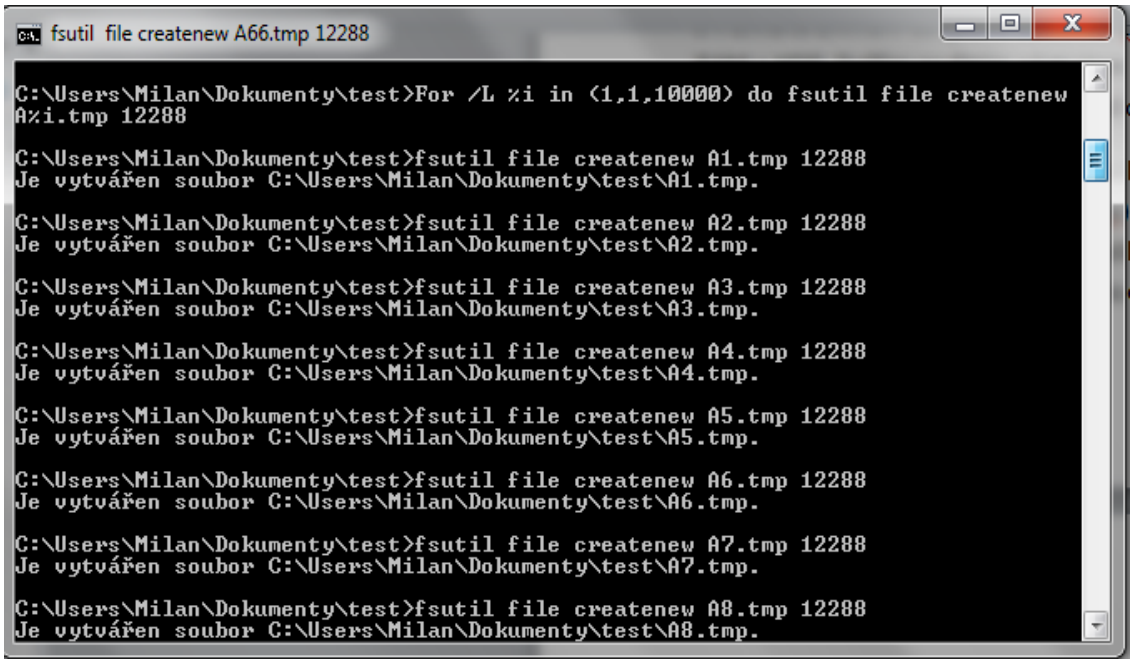
Zařízení, které bude sloužit jako jednotný nástroj k analýze, bude osobní notebook Asus s běžnými základními parametry. Popis důležitých parametrů zařízení:

- Operační systém: Windows 7 Home Premium(64-bitová verze) Service Pack 1
- Procesor: AMD A4-3300M 1,9GHz 2 Core
- Operační paměť: 6 GB
- Diskové jednotky: 1 x HDD 750 GB rozdělený na dva diskové sektory
- Aktuální rychlost internetového připojení: cca 7 Mbit/s download i upload

7.3 Postup praktické části

V praktické části jsem postupně nainstaloval tři produkty, které nabízejí šifrování dat, jež jsou uložena nebo následně budou uložena na cloud. Po instalaci a seznámení se se šifrovacím softwarem bylo nutné v zařízení nainstalovat cloud úložiště splňující nutné podmínky týkající se kapacity, která je potřebná pro otestování nástrojů třetích stran. K tomuto účelu jsem využil Dropbox ve variantě Basic, která je zdarma a poskytuje kapacitu 2 GB, což je pro účely testování dostačující. Následně jsem využil software pro sledování vytížení systémových prostředků zařízení během šifrování. Pro toto sledování jsem zvolil software SysGauge System Monitor od společnosti Flexense Ltd [44]. Tento sledovací nástroj umožňuje zaznamenávat informace o vytížení systémových prostředků během časového intervalu s frekvencí snímání dat jedna sekunda. SysGauge jsem využil k zaznamenání vytížení CPU, RAM a HDD. Dalším použitým nástrojem byl software Sledování prostředků, který je součástí systému Windows a který mi poskytl přehled o aktivitě síťové karty.

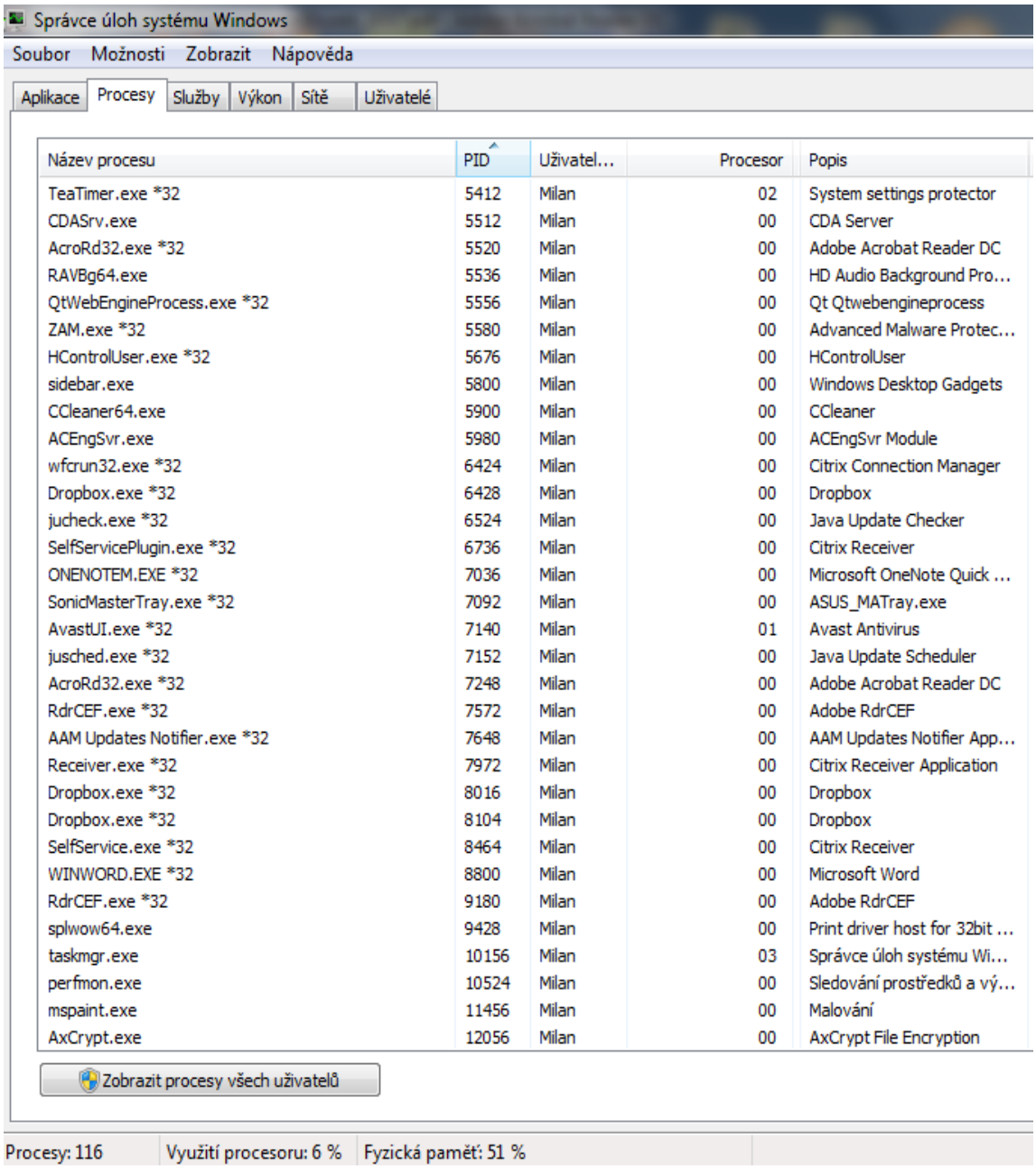
Dalším krokem bylo vytvoření zkušebních dat sloužících k testování. Byl vygenerován jeden soubor o velikosti 1 GB typu Excel (.xlsx) a 10 000 souborů o velikosti 12 kB typu Textový dokument (.txt). Testovací soubor o velikosti 1 GB byl generován nástrojem Dummy File Creator vytvořeným společností MyNikko.com zabývající se vývojem aplikací [45]. Velké množství malých souborů jsem vygeneroval pomocí příkazového řádku za použití nástroje Fsutil, který je součástí systému Windows. K tomuto generování jsem použil příkaz: For /L %i in (1,1,10000) do fsutil file createnew A%i.tmp 12288 a inspiroval jsem se dle popisu funkce na internetových stránkách zabývajících se informačními technologiemi [46]. Následně bylo analyzováno šifrování a synchronizace testovacích dat pomocí produktů třetích stran nejdříve jednoho velkého souboru a poté deseti tisíc malých souborů. Pak jsem tuto analýzu přenesl ze sledovacího software SysGauge a interpretoval ji pomocí grafů s využitím nástroje Microsoft Excel 2016.



Obr. 5 Znázornění příkazu fsutil v cmd. (Zdroj: vlastní zpracování)

7.4 Popis měření

Všechna měření probíhala pomocí sledovacího nástroje ihned při spuštění šifrování dat nástrojem třetí strany. Tato data byla zároveň synchronizována na cloud úložiště, aby došlo k co nejvěrnějším podmínkám využívání cloud služeb. Vzhledem k náročnosti internetového přenosu dat a dobám synchronizace měření probíhalo v intervalech maximálně 5 minut. Pokud samotný proces proběhl a skončil dříve, bylo sledování ukončeno. Tento interval je postačující pro znázornění vytížení systémových prostředků a porovnání tří zkoumaných produktů. U všech produktů je měřeno šifrování se shodnou délkou šifrovacího klíče AES – 256 bit.K navození uživatelských podmínek šifrování jsem ponechal všechny procesy, které běží při standardním provozu testovacího zařízení, viz obrázek č. 5.



Obr. 6 Seznam aktuálně běžících procesů. (Zdroj: vlastní zpracování)

7.5 Folder Lock

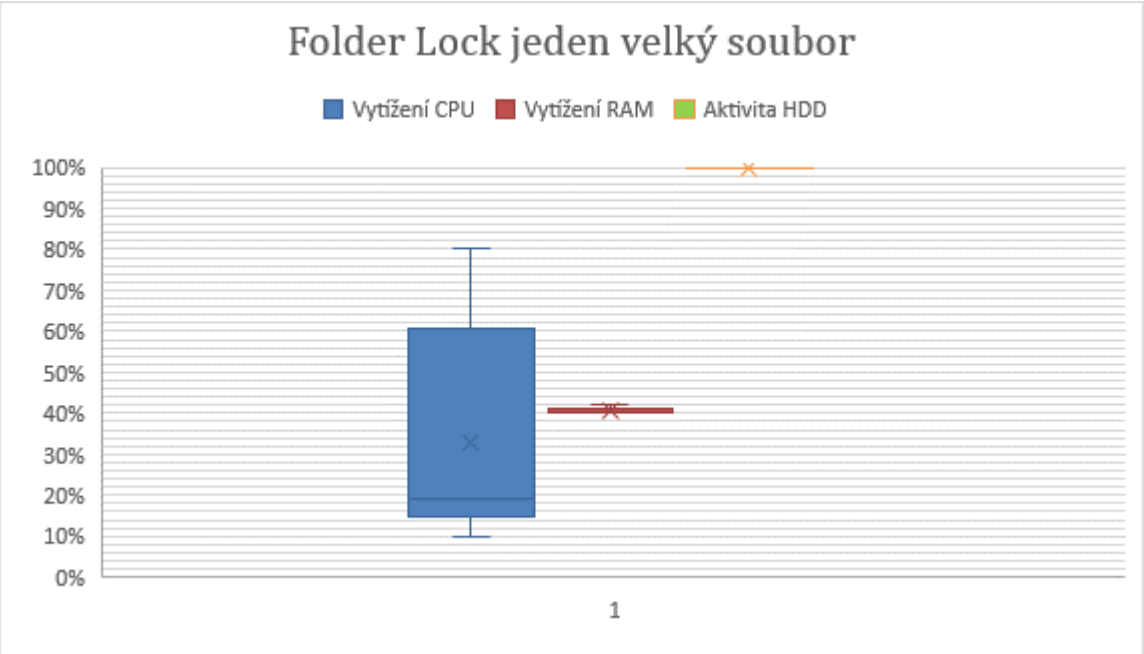
Pro otestování tohoto šifrovacího nástroje jsem nainstaloval aktuální verzi Folder Lock 7.7.8, kterou jsem stáhl přímo na stránkách vývojáře NewSoftwares [43]. Jedná se o verzi Free (Trial), u které je nastavený omezený počet spuštění programu. Poté musí uživatel v případě zájmu zakoupit verzi Full. Samotná instalace zabrala jenom několik málo minut, není třeba vyplňovat žádné osobní informace ani registrace. Po instalaci program vyžaduje nastavení hlavního hesla, které může být libovolné délky i složitosti. Lze využít virtuální klávesnice, která je

součástí formuláře pro zadání hesla a slouží k bezpečnostní prevenci proti aplikacím typu keylogger. Dále jsem vytvořil nový trezor neboli Locker, což je složka, do které se ukládají data k zašifrování a má své vlastní heslo. Vytvořil jsem tento trezor ve složce Dropbox a nastavil mu při výběru maximální kapacity 2 GB. Souborový systém se přidělí automaticky FAT32, samotný trezor zabírá cca 5052 kB. Po otevření trezoru se automaticky vytvoří nový diskový oddíl Z:, který je propojený přímo s trezorem a všechny operace s daty se provádí přímo v tomto oddílu. V Dropboxu je tedy umístěna složka, která slouží pouze jako úložiště zašifrovaných dat. Šifrování a dešifrování dat probíhá otevřením nebo uzavřením trezoru, to znamená, že při otevření trezoru lze s daty ihned pracovat. Přesunul jsem do diskového oddílu Z: nejprve jeden velký soubor, zavřel trezor a provedl měření. Poté jsem toto měření opakoval i s velkým množstvím malých souborů.

Software je velice uživatelsky přívětivý, ale na rozdíl od některých jiných nástrojů třetích stran se nespojí automaticky s cloud službou. Součinnost nástroje a cloud úložiště musí uživatel zajistit sám.

V následujícím grafu Graf 1 je znázorněno vytížení systémových prostředků během šifrování jednoho velkého souboru. Vidíme zde maximální dosažená vytížení a to 80% výkonu CPU, v případě RAM 42% a v případě aktivity HDD dokonce 100%. Průměrné hodnoty CPU dosahovaly 32,8%. Paměť RAM byla v průměru vytížena 40,5%. Aktivita HDD byla průměrně dokonce 100%, proto také rozptyl hodnot aktivity HDD je velmi malý, jelikož disk pracoval téměř po celou dobu na plný výkon.

U zaznamenaných hodnot vytížení systémových prostředků jsem vypočítal také modus neboli nejčastější hodnotu. V případě CPU byl modus 15%, RAM 40% a HDD 100%. Medián neboli střední hodnota vytížení CPU byla 19%. V případě RAM byl medián 40% a u vytížení HDD byl medián 100%, jelikož tato hodnota byla konstantní a HDD byl vytěžován stále na maximální hodnotu.



Graf 1 Grafické znázornění vytížení systémových prostředků během šifrování velkého souboru nástrojem Folder Lock. (Zdroj: vlastní zpracování dle grafu z aplikace SysGauge)

V následujícím grafu Graf 2 je zachyceno vytížení síťové karty během šifrování jednoho velkého souboru nástrojem Folder Lock. Zde byl průměr vytížení 11,4%. Modus stejně jako medián byl 0%. Nebylo zjištěno žádných neobvyklých hodnot.

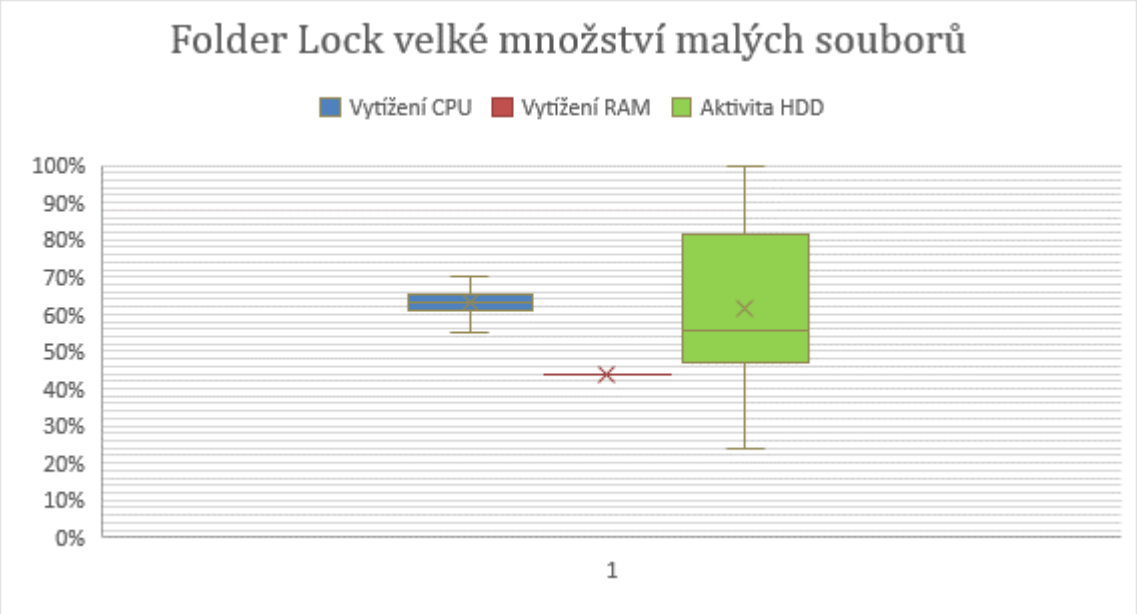
Graf 2Grafické znázornění vytížení síťové karty během šifrování velkého souboru nástrojem Folder Lock. (Zdroj: vlastní zpracování dle grafu z aplikace Sledování prostředků)

V následujícím grafu Graf 3 je znázorněno vytížení systémových prostředků během šifrování 10 000 malých souborů. Jsou zde znázorněna maximální dosažená

vytížení a to 70% výkonu CPU, v případě RAM 44% a v případě aktivity HDD rovných 100%. Průměrné hodnoty vytíženíCPU dosahovaly 63,1%, paměť RAM byla v průměru vytížena 44% a aktivita HDD byla průměrně 61,6%.

U zaznamenaných hodnot vytížení systémových prostředků jsem vypočítal stejně jako v předchozím případě modus neboli nejčastější hodnotu. V případě CPU byl modus 70%, RAM 44% a modus aktivity HDD 100%.

Medián neboli střední hodnota vytížení CPU byla 63%. V případě RAM byl medián 44% a u vytížení HDD byl medián 55,5.



Graf 3 Grafické znázornění vytížení systémových prostředků během šifrování velkého množství malých souborů nástrojem Folder Lock. (Zdroj: vlastní zpracování dle grafu z aplikace SysGauge)

V následujícím grafu Graf 4 je zachyceno vytížení síťové karty během šifrování 10 000 malých souborů. Zde bylo stejně jako v předchozím případě ze zachycených hodnot vypočítáno průměrné vytížení 13,9% a modus 0%. Medián vytížení síťové karty dosáhnul 14%.

Graf 4 Grafické znázornění vytížení síťové karty během šifrování velkého množství malých souborů nástrojem Folder Lock. (Zdroj: vlastní zpracování dle grafu z aplikace Sledování prostředků)

7.6 AxCrypt

Testování tohoto produktu probíhalo nejprve instalací, která byla stažena přímo z webových stránek produktu [47]. K dispozici je zde instalace vhodná jak pro 32-bit, tak i 64–bit verzi Windows. Obdržel jsem automaticky zdarma 30 dnů Premium verze AxCrypt, která provádí šifrování pomocí klíče AES-256. Konkrétně se jednalo o verzi AxCrypt 2.1.1573.0. Na webových stránkách produktu proběhla registrace pod emailovou adresou a nastavení hesla do AxCrypt. Poté bylo nutné přihlášení a spárování software s tímto účtem. Aplikace automaticky vyhledala cloudové úložiště a vytvořila ve složce Dropbox novou složku My AxCrypt. Šifrování probíhá dvěma způsoby. Buď uživatel vybere soubory určené k šifrování ručně, nebo vytvoří tzv. Secured Folder, do které poté stačí pouze přesunout požadované soubory a pomocí tlačítka, které umožňuje šifrovat vybrané Secured Folder složky a soubory, které jsou aplikací AxCrypt střeženy, ale byly dešifrovány pro práci s nimi. Ze způsobů šifrování pomocí AxCrypt plyne, že v případě tohoto produktu můžeme šifrovat soubory buď před jejich přesunem na cloud úložiště, anebo soubory nacházející se na úložišti. Testování šifrování jsem tedy provedl přesunutím testovacích dat do složky My AxCrypt umístěné ve složce Dropbox a poté použil tlačitko zašifrování všech nových souborů ve složce. Toto měření

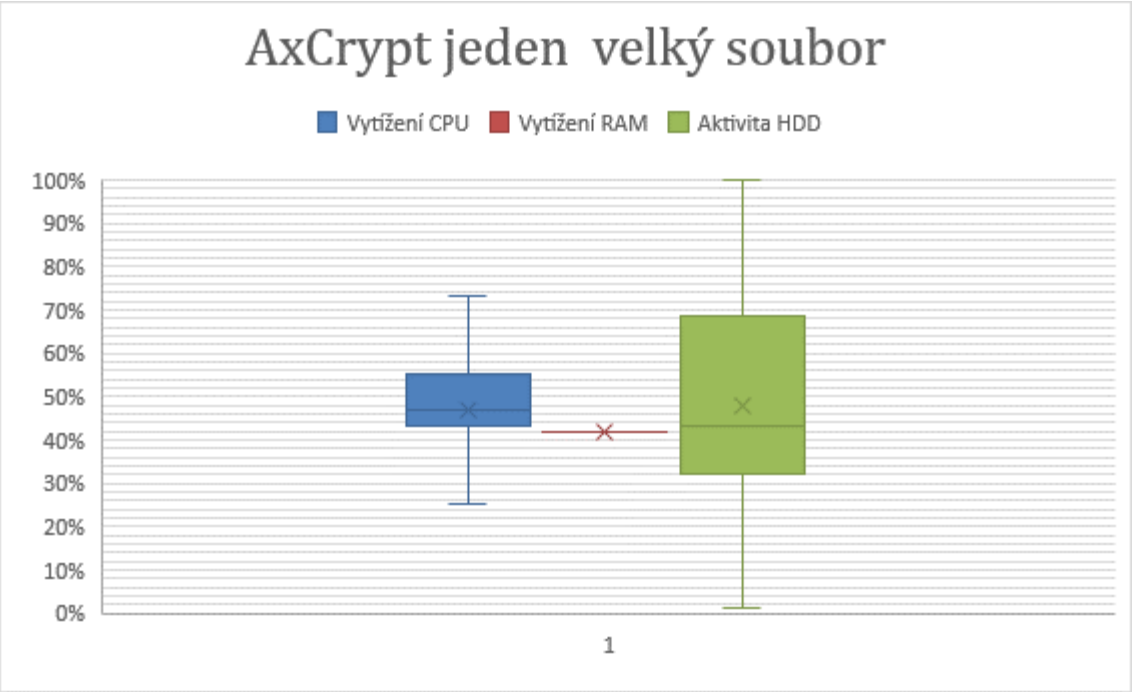
probíhalo nejprve s jedním velkým souborem a poté s velkým množstvím malých souborů.

Tak jako u předchozího produktu byly výsledky testování software AxCrypt zaznamenány do grafů. Následující graf Graf 5 zachycuje hodnoty získané pomocí nástroje SysGauge během testování, při kterém bylo provedeno šifrování jednoho velkého souboru. V tomto grafu jsou znázorněna maximální dosažená vytížení, konkrétně se jedná o hodnoty 73% výkonu CPU. V případě RAM bylo dosaženo maximálně 42% vytížení, což byla zároveň odlehlá hodnota. V případě HDD bylo maximum dosažené aktivity 100%.

Průměrné hodnoty vytížení CPU dosahovaly 46,8%, paměť RAM byla v průměru vytížena 42% a u HDD byla aktivita průměrně na 48%. U aktivity HDD byl zjištěn velký rozptyl hodnot díky rozsahu mezi minimální hodnotou 1% a maximální hodnotou 100%.

Modus u tohoto testování byl v případě CPU 47%, v případě RAM z důvodu konstantních hodnot opět 42% tak jako průměr a maximum. Modus aktivity HDD byl 43%.

Medián hodnot, který lze vidět v tomto grafu pro každou položku byl v případě CPU 47%, v případě RAM 42% a HDD 43%.



Graf 5 Grafické znázornění vytížení systémových prostředků během šifrování velkého souboru nástrojem AxCrypt.(Zdroj: vlastní zpracování dle grafu z aplikace SysGauge)

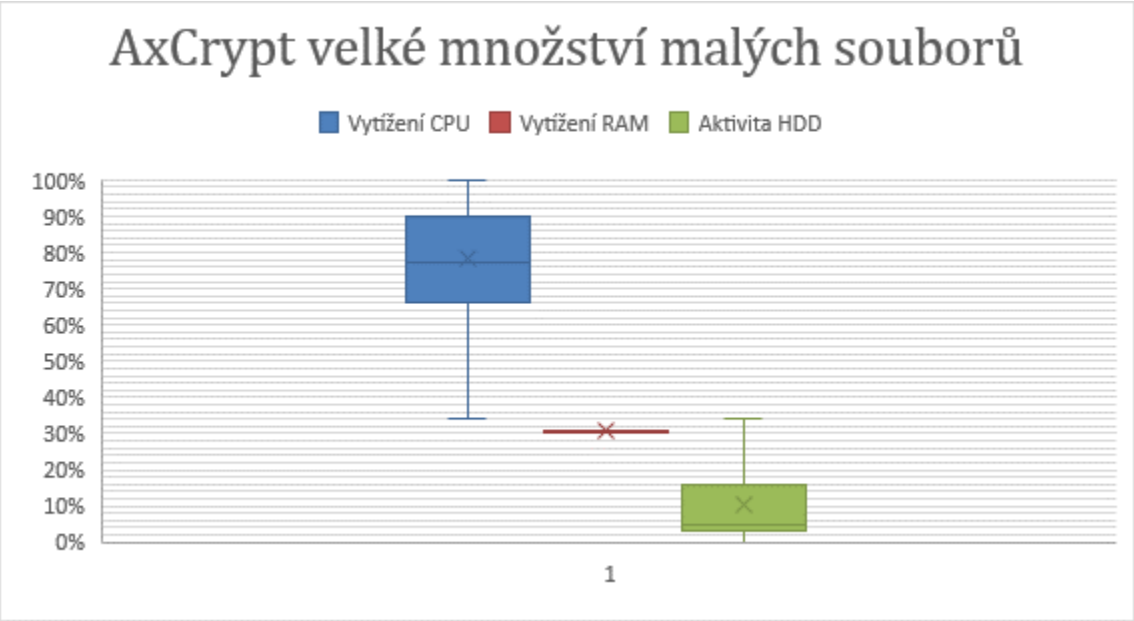
V následujícím grafu Graf 6 je zachyceno vytížení síťové karty během šifrování jednoho velkého souboru. Zde byl vypočítán průměr vytížení 27,5% a modus 0%. Medián v tomto případě byl 20%.

Graf 6 Grafické znázornění vytížení síťové karty během šifrování velkého souboru nástrojem AxCrypt. (Zdroj: vlastní zpracování dle grafu z aplikace Sledování prostředků)

V následujícím grafu Graf 7 jsem interpretoval vytížení systémových prostředků během šifrování 10 000 malých souborů produktem AxCrypt. Zde si lze

povšimnout maximálního dosaženého vytížení a to 100% výkonu CPU, v případě RAM 31% a v případě HDD 76%. Průměrné hodnoty vytížení CPU dosahovaly 78%, paměť RAM byla v průměru vytížena 30,6% a HDD byl vytížen průměrně pouze z 10,3%.

U zaznamenaných hodnot vytížení systémových prostředků a aktivity HDD jsem vypočítal stejně jako v předchozím případě modus neboli nejčastější hodnotu. V případě CPU byl modus 65%, RAM 30,5% a HDD 5%. Medián vytížení CPU byl 77%, RAM 30,5% a medián aktivity HDD byl 5%.



Graf 7 Grafické znázornění vytížení systémových prostředků během šifrování velkého množství malých souborů nástrojem AxCrypt. (Zdroj: vlastní zpracování dle grafu z aplikace SysGauge)

V následujícím grafu Graf 8 je zachyceno vytížení síťové karty během šifrování jednoho velkého souboru. Zde byl zjištěn průměr vytížení 36,5% a modus 0%. Medián v tomto případě byl 25%.

Graf 8 Grafické znázornění vytížení síťové karty během šifrování velkého množství malých souborů nástrojem AxCrypt. (Zdroj: vlastní zpracování dle grafu z aplikace Sledování prostředků)

7.7 Boxcryptor

Testování probíhalo instalací aktuální verze software (2.33.933) stažené z oficiálních webových stránek produktu Boxcryptor [48]. Po instalaci následovala registrace a vytvoření účtu Boxcryptor pomocí emailu, který je nutno ověřit. Uživatel musí souhlasit s rizikem ztráty dat při zapomenutí hesla k účtu. Při výběru varianty jsem zvolil variantu Free, která je zdarma a podporuje možnost propojení jednoho cloud úložiště, což je pro moji analýzu dostačující. Po spuštění aplikace Boxcryptor je pro začátek k dispozici stručný a přehledný tutoriál.

Boxcryptor sám vytvořil nový diskový oddíl (X:), který automaticky propojil s cloud úložištěm Dropbox nainstalovaným v zařízení a v diskovém oddílu (X:) přidal složku Dropbox. Šifrování pomocí tohoto software probíhá kliknutím pravým tlačítkem myši na soubor, výběrem položky Boxcryptor a dále zvolením Encrypt či Decrypt. Tuto akci lze provést i pro složku, a tím lze šifrovat či dešifrovat všechny soubory ve složce najednou. Všechny soubory, které budou následně přeusnuty do zašifrované složky, se automaticky zašifrují také. Při přesouvání souboru do diskového oddílu (X:) Boxcryptor automaticky nabízí možnost výběru přesouvané soubory šifrovat či ne. Proces šifrování tedy probíhal přímo při přesouvání souborů na cloud úložiště. Velkou výhodou, kterou jsem u

Boxcryptor objevil, je automatické dešifrování souborů při jejich přesunutí z cloud úložiště do úložiště v zařízení, tudíž lze s daty ihned pracovat.

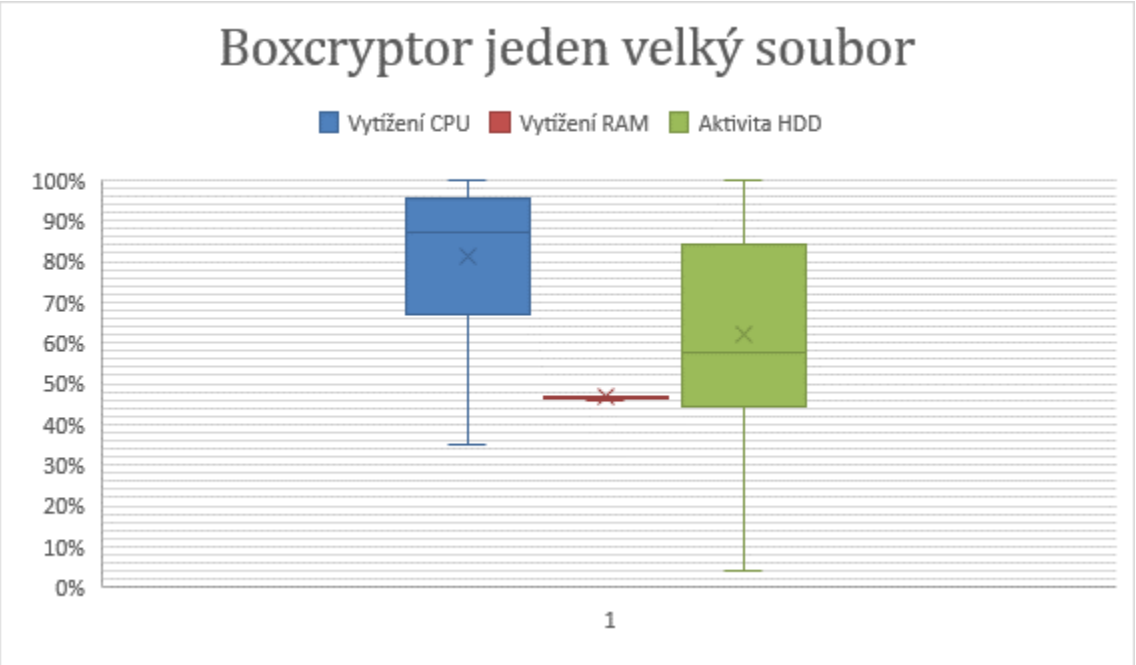
Toto měření probíhalo nejprve s jedním velkým souborem a poté s velkým množstvím malých souborů. Během analýzy tohoto produktu jsem si kromě delší doby šifrování oproti předchozím produktům nepovšiml žádných anomálií.

I v tomto případě byly výsledky testování zaznamenány do grafů. Následující graf Graf 9 opět zachycuje hodnoty získané pomocí nástroje SysGauge během testování, při kterém bylo provedeno šifrování jednoho velkého souboru. V tomto grafu jsou znázorněna maximální dosažená vytížení, konkrétně se jedná o hodnoty 100% výkonu CPU. V případě RAM bylo dosaženo maximálně 47% vytížení. V případě HDD bylo maximum dosažené aktivity 100%.

Průměrné hodnoty vytížení CPU dosahovaly 81,3%, paměť RAM byla v průměru vytížena 46,7% a u HDD byla aktivita průměrně na 61,8%. U aktivity HDD byl zjištěn velký rozptyl hodnot díky rozsahu mezi minimální hodnotou 4% a maximální hodnotou 100%.

Modus u tohoto testování byl v případě CPU 100%, v případě RAM z důvodu konstantních hodnot opět 47% tak jako průměr a maximum. Modus aktivity HDD byl 100%.

Medián hodnot, který lze vidět v tomto grafu pro každou položku, byl v případě CPU 87%, v případě RAM 47% a HDD 57,5%.



Graf 9 Grafické znázornění vytížení systémových prostředků během šifrování velkého souboru nástrojem Boxcryptor. (Zdroj: vlastní zpracování dle grafu z aplikace SysGauge)

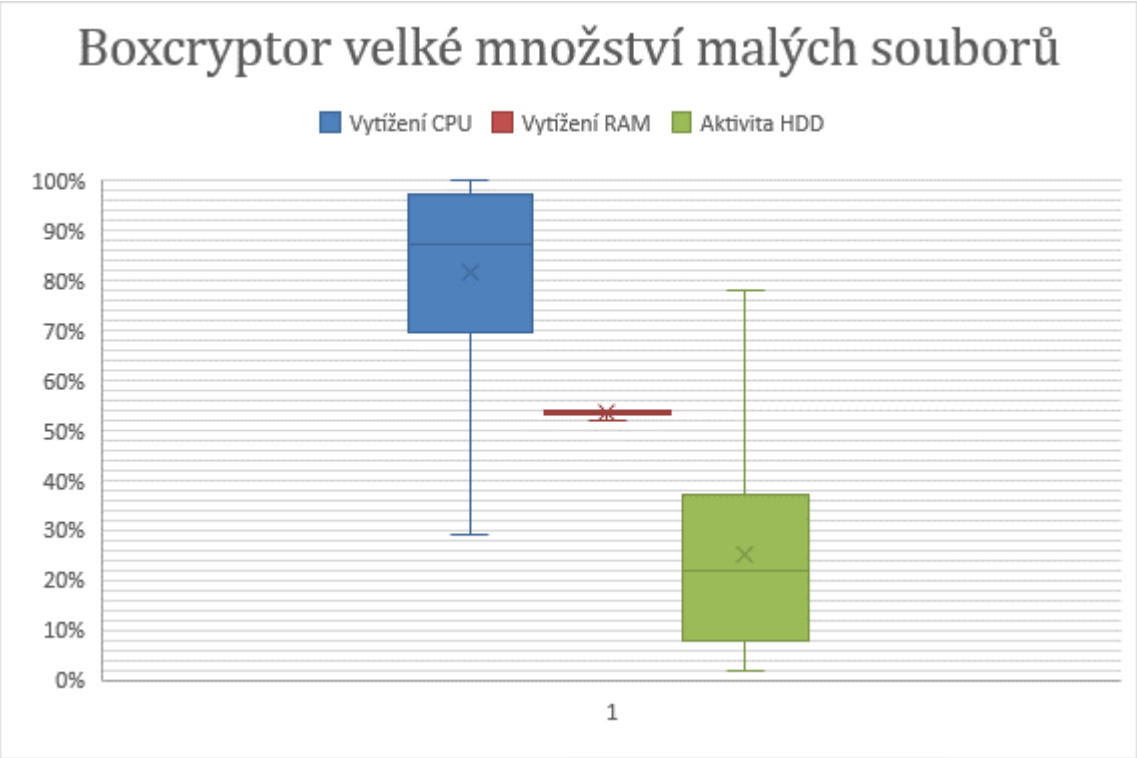
V následujícím grafu Graf 10 je zachyceno vytížení síťové karty během šifrování jednoho velkého souboru. Zde byl vypočítán průměr vytížení 69,2% a modus 70%. Medián v tomto případě byl 71%.

Graf 10 Grafické znázornění vytížení síťové karty během šifrování velkého souboru nástrojem Boxcryptor.(Zdroj: vlastní zpracování dle grafu z aplikace Sledování prostředků)

V následujícím grafu Graf 11 jsem interpretoval vytížení systémových prostředků během šifrování 10 000 malých souborů produktem Boxcryptor. Zde jsou

zachycena maximální dosažená vytížení a to 100% výkonu CPU, v případě RAM 54% a v případě HDD byla maximální dosažená aktivita 78%. Průměrné hodnoty vytížení CPU dosahovaly 81,4%, paměť RAM byla v průměru vytížena 53,3% a HDD byl vytížen průměrně pouze z 25,1%.

U zaznamenaných hodnot vytížení systémových prostředků a aktivity HDD jsem vypočítal stejně jako v předchozích případech modus neboli nejčastější hodnotu. V případě CPU byl modus 99%, RAM 54% a HDD 8%. Medián vytížení CPU byl 87%, RAM 53,5% a medián aktivity HDD byl 22%.



Graf 11 Grafické znázornění vytížení systémových prostředků během šifrování velkého množství malých souborů nástrojem Boxcryptor. (Zdroj: vlastní zpracování dle grafu z aplikace SysGauge)

V následujícím grafu Graf 12 je zachyceno vytížení síťové karty během šifrování jednoho velkého souboru. Zde byl zjištěn průměr vytížení 3,4%. Modus i medián v tomto případě byly rovných 0%.

Graf 12 Grafické znázornění vytížení síťové karty během šifrování velkého množství malých souborů nástrojem Boxcryptor. (Zdroj: vlastní zpracování dle grafu z aplikace Sledování prostředků)

8 Závěr a shrnutí výsledků

Cílem této práce byla analýza zabezpečení cloud služeb, konkrétně zabezpečení cloud jako úložiště dat pomocí nástrojů třetích stran, které jsou určeny k šifrování dat ukládaných na cloud úložiště a data jsou tak zabezpečena proti případnému selhání zabezpečení na straně cloud poskytovatele.

V teoretické části byl popsán cloud computing od historie a vymezení pojmu přes základní vlastnosti, jednotlivé modely až po způsoby zpracování služeb. Následně byla teoretická část zaměřena na cloud jako úložiště dat včetně porovnání aktuálně nabízených cloud úložišť. Dále se teoretická část skládala ze zabezpečení dat v cloud, vysvětlení bezpečnostních hrozeb a popisu způsobů zabezpečení dat. Ze způsobů zabezpečení dat bylo popsáno detailně šifrování, jelikož poslední kapitola teoretické části byla zaměřena na představení širovacích nástrojů třetích stran. Teoretická část byla tedy koncipována tak, aby popisované šifrování a zmiňované nástroje třetích stran navázaly na část praktickou a tyto nástroje byly v této části analyzovány a testovány.

V praktické části byly analyzovány a testovány šifrovací nástroje třetích stran představené v teoretické části. Jednotlivé nástroje byly popsány od instalace až po samotné zabezpečení dat pomocí šifrování. Testování šifrování je vždy znázorněno graficky a interpretováno krabicovým grafem. Pro co nejlepší analýzu nástrojů probíhalo testování šifrování vždy nejprve s jedním velkým souborem a poté s velkým množstvím malých souborů.

Nejideálnějších výsledků v případě šifrování jednoho velkého souboru dosáhl nástroj AxCrypt, kde průměrná hodnota vytížení CPU byla 46,8%, modus stejně jako medián byl v tomto případě 47%. Paměť RAM byla vytížena konstantně a aktivita HDD byla průměrně 48% s modusem a mediánem 43%. Rozptyl hodnot vytížení byl nejmenší ze všech testovaných nástrojů. Tento případ je nejlepší vzhledem k nejmenším výkyvům vytížení a aktivity CPU, RAM a HDD.

V případě šifrování velkého množství malých souborů byly nejlepší výsledky dosaženy nástrojem Folder Lock. Zde byly průměrné hodnoty vytížení CPU 63,1%, modus 70% a medián 63%. Páměť RAM byla vytížena konstantně 44% a aktivita

HDD dosahovala průměrně 61,6%, modus byl 100% a medián 55,5%. Vzhledem k nejmenším rozptylům hodnot a nejmenším výkyvům hodnot ze všech testovaných nástrojů byl v případě šifrování velkého množství malých souborů nejideálnějším nástrojem Folder Lock.

9 Seznam použité literatury

1. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, Cloudcomputing and emerging IT platforms: Vision, hype, and reality fordeliveringcomputing as
   the 5th utility, FutureGenerationComputer Systems, 25:599616, 2009.
2. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, and R. Katz, AbovetheClouds: A BerkeleyViewofCloudComputing, UC BerkeleyReliableAdaptiveDistributed Systems LaboratoryWhitePaper, 2009.
3. Karpeta, J.: Počítače v oblacích(1):Cloud je všude kolem, Computerworld.cz, [online].
4. Mácha, P.: Historie a základní principy cloudcomputingu, Systemyonline.cz, [online].
5. Dočekal, D.: Cloudcomputing … je všude okolo nás, Lupa.cz [online].
6. Zikmund, M.: Co je to cloudcomputing a proč se o něm mluví, Businessvize.cz [online].
7. JOSYULA, Venkata, Malcolm ORR a Greg PAGE. Cloudcomputing: automatingthevirtualized data center. Indianapolis, IN: Cisco Press, c2012. ISBN 978-1-58720-434-0
8. Amazon: Amazon Drive [online]. Seattle: Amazon, ©1996-2018 [cit. 2018-11-13]. Dostupné z: https://www.amazon.com/b/?_encoding=UTF8&node=15547130011&ref_=cd_auth_home
9. Google. *Google: Google Drive* [online]. MountainView, Kalifornie, USA, [2018] [cit. 2018-11-17]. Dostupné z: https://www.google.com/intl/cs_ALL/drive/pricing/Google. Google: Google Drive [online]. MountainView, Kalifornie, USA, [2018] [cit. 2018-11-17]. Dostupné z: https://www.google.com/intl/cs_ALL/drive/pricing/
10. Microsoft: Azure. Microsoft: Azure [online]. Seattle, ©2018 [cit. 2018-11-18]. Dostupné z: https://azure.microsoft.com/cs-cz/
11. BUYYA, Rajkumar, James BROBERG a Andrzej GOŚCIŃSKI. Cloudcomputing: principles and paradigms. Hoboken, N.J.: Wiley, c2011. ISBN 978-0-470-88799-8.

12. SORIANO, Miguel a Pavel BEZPALEC. Cloudcomputing [online]. České vysoké učení technické v Praze Fakulta elektrotechnická: TechPedia, 2017 [cit. 2018-11-20]. ISBN 978-80-01-06211-1. Dostupné z: techpedia.fel.cvut.cz/download/?fileId=802&objectId=77
13. ERL, Thomas, Richardo PUTTINI a Zaigham MAHMOOD. Cloudcomputing. UpperSaddle River, NJ: PrenticeHall, [2013]. ISBN 978-0-13-338752-0
14. MELL, Peter a Timothy GRANCE. The NIST DefinitionofCloudComputing: RecommendationsoftheNational Institute ofStandards and Technology [online]. In: . Gaithersburg, září 2011, s. 7 [cit. 2018-12-01]. DOI: 800-145. Dostupné z: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf
15. Kritéria pro výběr úložiště dat: Obecné aspekty [online]. Washington: Microsoft, 2018 [cit. 2018-12-02]. Dostupné z: https://docs.microsoft.com/cs-cz/azure/architecture/guide/technology-choices/data-store-comparison
16. IT Systems [online]. Mladá Boleslav, 2012, 2012(1-2) [cit. 2018-12-02]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/virtualizace/cloud-cena-az-na-druhem-miste.htm
17. IT Systems [online]. Mladá Boleslav, 2005, 2005 [cit. 2018-12-02]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/outsourcing-ict/tajemstvi-zkratky-sla-1.htm
18. ANTONOPOULOS, Nick a Lee GILLAM. Cloudcomputing: principles, systems and applications. New York: Springer, ©2010. Computercommunications and networks. ISBN 978-1-84996-240-7.
19. Microsoft: OneDrive [online]. Redmond, Washington, USA: Microsoft, ©2018 [cit. 2018-11-21]. Dostupné z: https://products.office.com/cs-cz/business/teamwork/online-file-storage-and-sharing
20. Microsoft: OneDrive [online]. Redmond, Washington, USA: Microsoft, ©2018 [cit. 2018-11-21]. Dostupné z: https://onedrive.live.com/about/cs-cz/plans/

21. Dropbox: Individual [online]. San Francisco: Dropbox, ©2018 [cit. 2018-11-21]. Dostupné z: https://www.dropbox.com/individual
22. Apple: iCloud [online]. Cupertino, ©2018 [cit. 2018-12-12]. Dostupné z: https://www.apple.com/cz/icloud/
23. JANŮ, Stanislav a Vladislav KUSKA. Kde nejlevněji uložit 1 TB dat: Srovnali jsme aktuální ceny cloudových úložišť. Živě: Počítače [online]. Praha, ©2019, 20. března 2018 [cit. 2019-01-02]. Dostupné z: https://www.zive.cz/clanky/kde-nejlevneji-ulozit-1-tb-dat-srovnali-jsme-aktualni-ceny-cloudovych-ulozist/sc-3-a-186707/default.aspx#part=1
24. Box [online]. Redwood City: Box, ©2018 [cit. 2019-01-02]. Dostupné z: https://www.box.com/
25. MEGA: User-encryptedcloudservices [online]. Auckland: Mega, ©2019 [cit. 2019-01-04]. Dostupné z: https://mega.nz/
26. Boxcryptor: SecurityforyourCloud [online]. Augsburg: Secomba, ©2019 [cit. 2019-01-05]. Dostupné z: https://www.boxcryptor.com/en/
27. SEGUN, Daniel. 5 bestcloudencryptiontoolsfor Windows PC users [online]. September 18, 2018 [cit. 2019-01-05]. Dostupné z: https://windowsreport.com/cloud-encryption-tools/#.XDB2RFVKjIV
28. PCWorld: Software [online]. Praha: IDG Czech Republic, 2012 [cit. 2019-01-05]. Dostupné z: https://pcworld.cz/software/tip-jak-si-zdarma-zasifrovat-cloudove-uloziste-3-dil-44946
29. Boxcryptor: Help [online]. Augsburg: Secomba, ©2019 [cit. 2019-01-06]. Dostupné z: https://www.boxcryptor.com/en/help
30. Boxcryptor: forIndividuals [online]. Augsburg: Secomba, ©2019 [cit. 2019-01-06]. Dostupné z: https://www.boxcryptor.com/en/for-individuals/
31. Boxcryptor: forTeams [online]. Augsburg: Secomba, ©2019 [cit. 2019-01-06]. Dostupné z: https://www.boxcryptor.com/en/for-teams/
32. Boxcryptor: Pricing and Features [online]. Augsburg: Secomba, ©2019 [cit. 2019-01-06]. Dostupné z: https://www.boxcryptor.com/en/pricing/
33. AxCrypt: Information [online]. Stockholm: AxCrypt AB, [2018] [cit. 2019-01-08]. Dostupné z: https://www.axcrypt.net/information/

34. AxCrypt: Frequentlyaskedquestions [online]. Stockholm: AxCrypt AB, [2018] [cit. 2019-01-08]. Dostupné z: https://www.axcrypt.net/support/faq/
35. AxCrypt: Requirements [online]. Stockholm: AxCrypt AB, [2018] [cit. 2019-01-08]. Dostupné z: https://www.axcrypt.net/information/requirements/
36. AxCrypt: Premium [online]. Stockholm: AxCrypt AB, [2018] [cit. 2019-01-08]. Dostupné z: https://www.axcrypt.net/axcrypt-premium/
37. AxCrypt: Business [online]. Stockholm: AxCrypt AB, [2018] [cit. 2019-01-08]. Dostupné z: https://www.axcrypt.net/axcrypt-business/
38. AxCrypt: Pricing [online]. Stockholm: AxCrypt AB, [2018] [cit. 2019-01-08]. Dostupné z: https://www.axcrypt.net/pricing/
39. Top Ten Reviews: Buy better [online]. Ogden, USA: Purch, ©2019 [cit. 2019-01-12]. Dostupné z: https://www.toptenreviews.com/
40. Top Ten Reviews: Folder Lock 7 Review [online]. Ogden, USA: Purch, ©2019 [cit. 2019-01-12]. Dostupné z: https://www.toptenreviews.com/software/security/best-encryption-software/folder-lock-review/
41. NewSoftwares.net: Folder Lock - features [online]. Beaverton, USA: NewSoftwares.net, ©2002-2018 [cit. 2019-01-12]. Dostupné z: http://www.newsoftwares.net/folderlock/features/
42. NewSoftwares.net: Folder Lock FAQs [online]. Beaverton, USA: NewSoftwares.net, ©2002-2018 [cit. 2019-01-12]. Dostupné z: http://www.newsoftwares.net/folderlock/faq/
43. NewSoftwares.net: Folder Lock [online]. Beaverton, USA: NewSoftwares.net, ©2002-2018 [cit. 2019-01-12]. Dostupné z: http://www.newsoftwares.net/folderlock/
44. SysGauge: System monitor [online]. Rishon Lezion (Israel): Flexense, ©2007-2019 [cit. 2019-03-05]. Dostupné z: https://www.sysgauge.com/index.html
45. MyNikko: Dummy File Creator [online]. MyNikko.com, ©2002 [cit. 2019-03-05]. Dostupné z: http://www.mynikko.com/dummy/

46. The Back Room Tech: Howto: Generate Many Files of a Particular Size in Windows [online]. The Back Room Tech.com, ©2010-2019 [cit. 2019-03-05]. Dostupné z: http://www.mynikko.com/dummy/
47. AxCrypt: Download [online]. Stockholm: AxCrypt AB, [2018] [cit. 2019-03-09]. Dostupné z: https://www.axcrypt.net/download/
48. Boxcryptor: download [online]. Augsburg: Secomba, ©2019 [cit. 2019-03-16]. Dostupné z: https://www.boxcryptor.com/en/download/
49. RosiGroup: cloudove-sluzby [online]. Male Bielice: Rosi Group, 2015 [cit. 2019-03-05]. Dostupné z: https://rosigroup.com/sluzby/cloudove-sluzby/
50. Barkat consulting: cloud computing [online]. Libertyville IL: Barkat consulting, ©2010-2019[cit.2019-03-13].Dostupnéz: http://www.barkatconsulting.com/consolidation-and-virtualization/
51. Silverlight hack: cloud [online]. 2011 [cit. 2019-03-21]. Dostupné z: www.silverlighthack.com
52. QuoteColo: Cloud [online]. QuoteColo, 2015 [cit. 2019-03-13]. Dostupné z: https://www.quotecolo.com/whats-the-difference-between-cloud-computing-and-software-defined-networks-sdn/

Univerzita Hradec Králové
Fakulta informatiky a managementu
Akademický rok: 2016/2017

Studijní program: Aplikovaná informatika
Forma: Prezenční
Obor/komb.: Aplikovaná informatika (ai3-p)

Podklad pro zadání BAKALÁŘSKÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Pechánek Milan	Zahrádkářská 481, Hradec Králové - Svobodné Dvory	I1500409

TÉMA ČESKY:

Analýza zabepečení cloud služeb

TÉMA ANGLICKY:

Analysis of cloud services security

VEDOUCÍ PRÁCE:

Mgr. Josef Horálek, Ph.D. - KIT

ZÁSADY PRO VYPRACOVÁNÍ:

Cílem práce bude provést analýzu a testování zabezpečení dat uložených ve veřejných cloud službách. Autor práce představí principy cloud služeb zaměřených na veřejný cloud, představí možnosti zabezpečení dat uložených v cloudu a provede jejich testování. Autor se zaměří na možnosti zabezpečení a šifrování dat v samotných cloud službách a zabezpečení dat pomocí nástrojů třetích stran.
V praktické části pak autor provede komparativní analýzu zabezpečení dat ve veřejných cloud jak pomocí interních i externích nástrojů.

Osnova práce:
Úvod
Rešerše problematiky
Formy cloud služeb
Stanovení kritérií pro využití cloud jako úložiště dat
Analýza standardního zabezpečení dat v cloud
Výběr řešení třetích stran pro šifrování dat v cloud
Stanovení výchozích hypotéz
Stanovení metodiky testování
Realizace testování
Vyhodnocení testů
Vyhodnocení hypotéz
Závěr

SEZNAM DOPORUČENÉ LITERATURY:

ADAMS, Niall M. a Nicholas. HEARD. Data analysis for network cyber-security. London, UK: Imperial College Press, 2014. ISBN 9781783263745.

RAJANI, Sharma a Trivedi RAJENDER. Data Security in a Cloud Environment Using Multilevel Uec. 1. United States: LAP Lambert Academic Publishing, 2014. ISBN 9783659586958.

(c) IS/STAG , Portál - Podklad kvalifikační práce , I1500409 , 03.04.2019 16:23

Podpis studenta: ..... Datum: .....

Podpis vedoucího práce: ..... Datum: .....

(c) IS/STAG , Portál - Podklad kvalifikační práce , I1500409 , 03.04.2019 16:23