VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

IMPLEMENTACE ŠIFROVÁNÍ NA DATOVÁ ULOŽIŠTĚ SPOLEČNOSTI

IMPLEMENTATION OF ENCRYPTION TO ENTERPRISE'S NETWORK ATTACHED STORAGE

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Anna Popovská**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Viktor Ondrák, Ph.D.**
SUPERVISOR

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání bakalářské práce

Ústav:	Ústav informatiky
Studentka:	**Anna Popovská**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Manažerská informatika
Vedoucí práce:	**Ing. Viktor Ondrák, Ph.D.**
Akademický rok:	2016/17

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává bakalářskou práci s názvem:

Implementace šifrování na datová uložiště společnosti

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem práce je navrhnout konkrétní implementaci šifrování dat na uložištích společnosti.

Základní literární prameny:

BITTO, Ondřej. Šifrování a biometrika, aneb tajemné bity a dotyky. Kralice na Hané: Computer Media, 2005. ISBN 80-86686-48-5.

ČSN ISO/IEC 27003 (36 9790) Informační technologie - Bezpečnostní techniky - Směrnice pro implementaci systému řízení bezpečnosti informací. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. Česká technická norma.

DOBDA, Luboš. Ochrana dat v informačních systémech. Praha: Grada, 1998. ISBN 80-7169-479-7.

POŽÁR, Josef. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

POŽÁR, Josef. Základy teorie informační bezpečnosti. Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-250-8.

SINGH, Simon. Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii. Praha: Dokořán, 2003. ISBN 80-86569-18-7.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2016/17

V Brně dne 28.2.2017

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Tato bakalářská práce se zabývá návrhem bezpečnostního opatření, konkrétně návrhem šifrování na datová úložiště společnosti. V teoretické části jsou popsány základní pojmy a informace týkající se šifrování, dat a datových úložišť. V analytické části je analyzován současný stav konkrétní společnosti se zaměřením na ukládání dat. Praktická část je zaměřena na výběr vhodného softwarového šifrovacího nástroje, organizační pokyny a další náležitosti spojené se zaváděním bezpečnostního opatření do společnosti.

Abstract

This bachelor thesis is focused on designing security measures, particularly on designing cryptography on enterprise´s network attached storage. The theoretic part describes basic concepts and information concerning cryptography, data and network attached storages. The analytic part analyses the enterprise´s current state focusing on saving data in a specific enterprise. The practical part is focused on selection of an appropriate software cryptographic tool, organizational instructions and other requisites connected with implementation of security measures in an enterprise.

Klíčová slova

šifrování disků, informační bezpečnost, bezpečnostní opatření, datová úložiště, AES

Key words

drive encryption, information security, security measures, network attached storage, AES

Bibliografická citace

POPOVSKÁ, A. *Implementace šifrování na datová úložiště společnosti*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2017. 55 s. Vedoucí diplomové práce Ing. Viktor Ondrák, Ph.D.

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracovala jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušila autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 29. května 2017

.....

podpis studenta

Poděkování

Děkuji vedoucímu bakalářské práce Ing. Viktoru Ondrákovi, Ph.D. za cenné rady, připomínky a odborné vedení a také oponentovi Ing. Marianu Rusinovi, MBA za vstřícnost, ochotu, praktické rady a konzultace.
Ráda bych poděkovala také svému manželovi a rodině za podporu v průběhu celého studia.

OBSAH

ÚVOD

V posledních dvou letech se 13% českých firem stalo obětí počítačové kriminality. Stále častějšími jsou útoky na data i aplikace [39]. V dnešní době jsou informace pro většinu společností naprosto klíčovým faktorem. Jejich ztráta či zneužití by měla pro většinu z nich velmi nákladné až likvidační následky. Je tedy přirozené, že se společnosti snaží své informace chránit.

Tato práce se zaměřuje na zavedení bezpečnostního opatření, které v konkrétní společnosti sníží riziko ztráty dat a tím zlepší bezpečnost. Konkrétně se jedná o implementaci šifrování disků na datová úložiště společnosti. Budou zde shrnuty teoretické základy spojené s touto problematikou a analýza současného stavu konkrétní společnosti. V poslední části bude vybrán konkrétní softwarový šifrovací nástroj, budou zde rozebrány potřebné organizační pokyny a další náležitosti spojené se zaváděním bezpečnostního opatření (např. analýza rizik či studie proveditelnosti).

1 CÍL A METODIKA PRÁCE

Cílem bakalářské práce je návrh zavedení šifrování na datová úložiště společnosti spolu s popisem potřebných organizačních pokynů, analýzou rizik a studií proveditelnosti projektu zavádění tohoto bezpečnostního opatření. Společnost nemůže být s ohledem na citlivost údajů zveřejněna, pro účely této práce bude tedy nazvána společností ABC. V první části práce budou shrnuty teoretické poznatky související s touto problematikou. Dále se zaměřím na analýzu současného stavu společnosti ABC, na průzkum trhu a v poslední části práce na vlastní návrh zavedení tohoto bezpečnostního opatření.

2 TEORETICKÁ ČÁST

V této části budou zpracovány teoretické podklady k mé práci.

2.1 Šifrování

Kryptologie je věda zabývající se šifrováním. Dělí se na dvě hlavní disciplíny, kryptografii a kryptoanalýzu. **Kryptografie** zkoumá šifrování: šifrovací algoritmy, jiné kryptografické nástroje, následně pak jejich implementaci, šifrovací protokoly, hashe apod. **Kryptoanalýza** se zabývá luštěním šifer a odhalováním slabin kryptografických nástrojů [2].

Významný je rozdíl mezi pojmy kódování a šifrování. Kódování transformuje text, aniž by přitom využilo nějakou utajovanou informaci, např. ASCII, UNICODE a jiné. Šifrování se provádí šifrovacím algoritmem a jedná se o proces transformace tzv. otevřeného textu (ang. plain-text, zkratka OT) na šifrovaný text (ang. cipher-text, zkratka ŠT). Tento proces využívá k zašifrování i k dešifrování určitého klíče [2].

2.1.1 Symetrická a asymetrická kryptografie

Kryptografii můžeme rozdělit na symetrickou a asymetrickou. O **symetrickou kryptografii** se jedná, pokud je k šifrování i dešifrování použit totožný klíč. Naproti tomu, pokud jsou použity klíče dva – tvoří klíčový pár (tzv. veřejný a soukromý), jedná se o **asymetrickou kryptografii**. Tyto dva klíče jsou nejen různé, ale zároveň nesmí být možné v rozumném čase zjistit pomocí jednoho klíče ten druhý. V zásadě platí, že nejdříve je vygenerován klíč soukromý a pak k němu klíč veřejný (v případě potřeby lze vygenerovat i nový klíč veřejný) [1, 4].

Hlavní výhodou symetrických šifer je jejich rychlost a nízká výpočetní náročnost. Kvalita výsledného ŠT je dána především použitým algoritmem a délkou šifrovacího klíče. Hlavní nevýhodou je, že klíč musí být sdílen s každým, kdo by potřebovat zprávu zašifrovat či dešifrovat [4].

Obr. 1: Schéma šifrování. [4]

Nevýhodou asymetrické kryptografie je rychlost šifrování. Výhodou naopak je, že se předává pouze veřejný klíč, jehož vyzrazení nenaruší bezpečnost komunikace [4].

Aby byla zajištěna důvěryhodnost v asymetrické kryptografii, jsou využívány tzv. digitální certifikáty. Jedná se o soubory, které potvrzují vztah mezi majitelem a jeho veřejným klíčem. Tento soubor je podepsán soukromým klíčem certifikační autority, je tudíž možné si platnost certifikátu ověřit [3].

Certifikační autorita má jako jediná právo vydávat, ověřovat a odvolávat platnost certifikátů. Odvolávání platnosti certifikátů se realizuje mj. tím, že certifikační autority zveřejňují seznamy neplatných certifikátů (např. těch, kterým vypršela platnost, nebo těch, které byly nějak vyzrazeny a předčasně zablokovány – revokovány). Potenciální prolomení bezpečnosti těchto autorit by tudíž značně ohrozilo bezpečnost [3, 5].

Asymetrické šifrování je v kombinaci s dalšími technologiemi používáno pro šifrování, digitální podepisování a ověřování digitálních podpisů. Rozdíl je v tom, že při šifrování se šifruje veřejným klíčem adresáta a pouze adresát si může zprávu dešifrovat svým unikátním soukromým klíčem. Při digitálním podepisování je postup opačný, šifruje se soukromým klíčem a každý, kdo má přístup k veřejnému klíči podepisovatele, může podpis tímto veřejným klíčem ověřit [4].

Obr. 2: Schéma asymetrického šifrování. [4]

V praxi se často využívá kombinace obou metod: Tajný klíč pro symetrické šifrování je zašifrován veřejným klíčem, poslán příjemci, rozšifrován soukromým klíčem (použita asymetrická kryptografie). Pro samotné šifrování komunikace se pak použije rychlejší symetrické šifrování [5].

2.1.2 Historie šifrování

Potřeba předávat si utajené zprávy je tu od pradávna. První známé šifry se datují již kolem počátku našeho letopočtu. Jednou z nejstarších šifer je například Caesarova šifra z dob starověké Římské říše. Vynalezl ji sám Caesar a její princip je založen na tom, že každé písmeno zprávy je posunuto dle abecedního pořádku o 3 znaky doprava. (Později byla šifra upravena a používala se i jiná velikost posunutí z rozmezí 1 – 25.) [1]

K velkému rozvoji šifrování došlo ale především až v období kolem světových válek. Významným milníkem bylo dešifrování elektromechanického šifrovacího stroje Enigma za druhé světové války [1].

V druhé polovině dvacátého století vznikla díky prudkému rozmachu počítačů nutnost najít šifrovací systém, který by byl dostatečně bezpečný a sloužil by jako standard. Americký národní úřad pro standardy (NBS) po veřejné soutěži vybral šifrovací

standard DES (Data Encryption Standard), jehož přihlašovatelem byla společnost IBM [1].

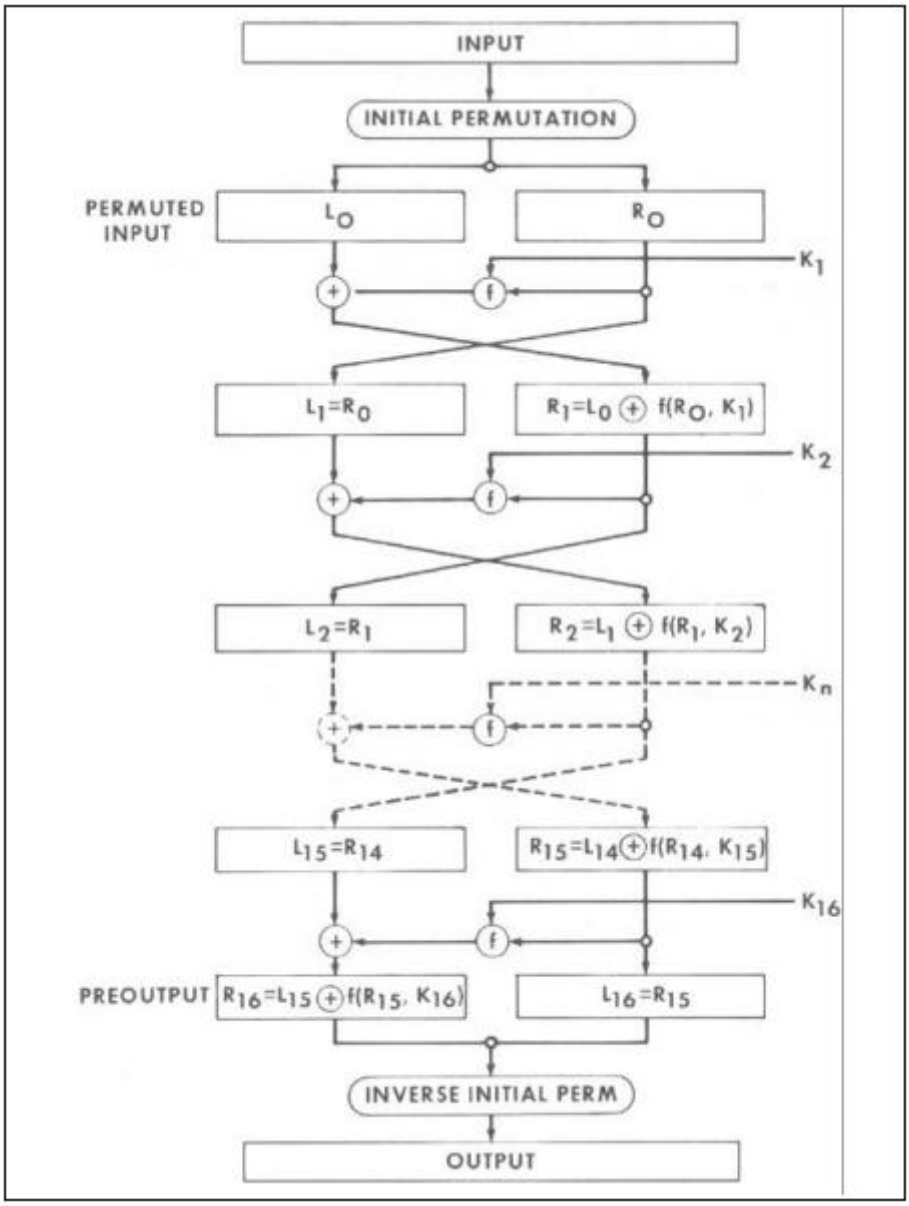
2.1.3 Moderní šifrovací algoritmy

Jedním ze základních principů moderní kryptografie je Kerckhoffsův princip formulovaný v roce 1883 nizozemským lingvistou Augustem Kerckhoffs von Nieuwenhoffem. „*Bezpečnost šifrovacího systému nesmí záviset na utajení algoritmu, ale pouze na utajení klíče.“* [6]

Pokud by byla totiž bezpečnost závislá pouze na utajení algoritmu a nikoliv klíče (jak tomu bylo např. u Ceasarovy šifry), dříve nebo později by se někomu povedlo systém prolomit. Proto jsou dnes principy šifrovacích algoritmů veřejně známy, pouze jsou utajovány klíče. Bezpečnost je pak závislá na relativní nemožnosti uhodnutí klíče, která je závislá na aktuálním možnému výpočetnímu výkonu počítačů [6, 7].

DES – Data Encryption Standard

DES je symetrická šifra, využívá tedy stejné klíče pro šifrování i dešifrování. Průběh šifry (viz obrázek níže) se skládá z úvodní permutace, poté je 16 krát provedena iterace operací (16. se mírně liší, ale princip zůstává stejný) a po závěrečné permutaci dostáváme ŠT [8, 9].



Obr. 3: Schéma DES. [8]

Permutace je zde provedena tím, že jsou přeházeny pozice bitů vždy v rámci každé 64 bitové sekvence [9].

Iterace [9]:
Rozdělení na dvě části levou (left, L) a pravou (right, R).
S pravou částí je provedena:

- permutace,

- xor s klíčem (o vytváření klíčů viz dále),
- substituce (na základě tabulky se bit na určité pozici nahradí 0 nebo 1 - novým bitem),
- permutace.

Je provedena operace xor nad pravou a levou částí -> nová levá část.
Původní pravá část je umístěna na místo levé a nová levá část je umístěna na místo pravé.
Další iterace.

Klíče potřebné pro iterace (celkem 16) mají délku 48 bitů a vytvářejí se z jednoho klíče o délce 64 bitů (ale každý 8. bit je použit pro paritní kontrolu, takže v podstatě můžeme říct, že jeho délka je pouze 56 bitů). Proces vytváření klíčů je pak složen z opakování procesu rozložení sekvence bitů (z původního klíče) na dvě stejně velké části, a poté je provedena permutace, na jejímž základě jsou vybrány bity pro první klíč. Tento proces se zopakuje 16 krát (jednou pro každý klíč) [8, 9].

Prolomení DES

Poté, co se uskutečnilo několik více či méně úspěšných útoků na tento šifrovací standard, byla agenturou RSA v roce 1997 vypsána kryptoanalytické soutěž na prolomení DES, aby se prokázala reálná možnost jeho prolomení. O pět měsíců později byl znám nejúspěšnější řešitel, který DES prolomil při použití 14 000 počítačů na Internetu. O rok později byl dokonce sestrojen DES cracker za 250 tisíc dolarů, který dokázal prolomit DES šifrovaný klíčem o délce 56 bitů [1].

Prolomení DES vedlo k vypsání veřejné soutěže o nový standard, který by nosil název AES (Advanced Encryption Standard). Vítězem se nakonec stal algoritmus s původním názvem Rijndael.

AES – Advanced Encryption Standard

Algoritmus, který je používán pro symetrické šifrování, byl přijat v roce 2001 a jeho životnost byla odhadována na minimálně tři desetiletí. Mezi jeho hlavní výhody patří rychlost a jednoduchá hardwarová i softwarová implementace [1].

Text je šifrován v hexadecimální podobě a po blocích (např. o délce 128 bitů – na této délce je založeno i vysvětlení jednotlivých tranfromací). Základem šifry jsou 4 transformace, které se několikrát opakují [17]:

SubBytes – substituce pomocí standardizované tabulky (S-box)

		y														
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Obr. 4: S-box. [18]

Shift Rows

Při šifrování 128 bitů je jeden blok tvořen tabulkou 4 x 4, kde v každé buňce je jeden znak v hexadecimální podobě. Při transformaci Shift rows první řádek ponecháme nezměněn. V druhém řádku posuneme každou buňku o jednu pozici doleva (první buňka jde na místo čtvrté). Ve třetím řádku posouváme buňky stejným způsobem o dvě pozice a ve čtvrtém o tři [19].

Mix Columns

V této fázi je každý sloupec bloku vynásoben standardizovanou maticí [19].

Add Round Key

Každý sloupec je za použití operace xor spojen s vygenerovaným klíčem, který má také formu 4 x 4 [19].

Šifrování je provedeno nejdříve přidáním základního klíče pomocí operace xor, poté se devětkrát provedou všechny čtyři transformace a ve finální fázi se provedou pouze tři transformace (je vynecháno Mix Columns) [19].

Pro každé šifrování je potřebný základní klíč, ze kterého se pomocí substituce pomocí S-boxu, změny pozice v rámci sloupců a xorování postupně vytvoří i klíče pro jednotlivá opakování (Round Keys) [19].

Kvantová kryptografie a riziko prolomení AES

V posledních několika letech se začínají objevovat první čipy a počítače částečně fungující na principech kvantové mechaniky. Vyrábí je např. společnost D-Wave. Tyto součástky a počítače ještě nemají výpočetní schopnosti, které se slibují od kvantových počítačů, ale už teď jsou mnohem rychlejší než aktuální součástky pracující s bity. Například na počátku roku 2016 byla zveřejněna informace, že společnost Google provozuje kvantový počítač, který je 100 000 000 krát rychlejší než stávající počítače (viz [13]) [11, 12, 13].

Budoucí kvantové počítače ale právě díky svým výpočetním schopnostem mohou ohrozit bezpečnost aktuálního šifrování. Kdybychom chtěli prolomit například 128bitový klíč AES, počet možných 128bitových klíčů by byl 2^{128}. Předpokládejme, že počítač s běžným výkonem by dokázal otestovat 1 bilion klíčů za sekundu, pak by mu otestování všech možných klíčů zabralo 10,79 trilionů let, což je důvod, proč je AES

považován za bezpečnou formu šifrování a dosud nebylo prolomen. Pokud bychom ale použili na otestování klíčů kvantovou technologii se stejnou propustností, zvládnutí stejného úkolu by trvalo pouze šest měsíců [7, 14].

2.1.4 Šifrování pevného disku

Budeme se zabývat šifrováním dat, která jsou persistentně uložená na pevném disku. Šifrování těchto dat může probíhat na úrovni: souborové, adresářové, oddílové nebo diskové [20].

Naprostá většina implementací šifrování disků je pomocí tzv. on-the-fly řešení. Což znamená, že data jsou zašifrována před tím, než jsou uložena na pevný disk a dešifrována před opětovným použitím [21].

K šifrování disku lze přistupovat hardwarovým a softwarovým způsobem, který se rozlišuje vrstvou, na které šifrování probíhá. Hardwarově orientované řešení šifruje celý disk po jednotlivých bitech bez ohledu na informace, které data představují. Je považováno za bezpečnější a efektivnější. Softwarově orientované řešení musí rozlišovat jednotlivé informace, protože například část disku, kde jsou informace pro zavádění systému MBR (Master Boot Record) musí zůstat nezašifrovaná. Toto řešení je levnější, flexibilnější a lépe paralelizovatelné. V praxi se často využívají řešení, která kombinují tyto dva přístupy [20, 21].

Dále můžeme dělit šifrování na tzv. Narrow-block a Wide-block Encryption. Narrow-block Encryption šifruje data po 16-ti bajtových blocích, což je rychlejší, ale méně bezpečnější metoda. Wide-block Encryption šifruje data po 512-ti bajtových sekcích. Toto řešení je pomalejší, ale při dostatečném výpočetním výkonu je to vhodnější metoda, která poskytuje větší bezpečnost [20, 21].

2.2 Data, informace a důležitost bezpečnosti informací

Pojem **data** můžeme chápat jako určitý zápis (např. posloupnost jedniček a nul v počítači) nebo jakýsi vjem. Když tato data vezmeme a přiřadíme k nim jejich význam (např. zobrazíme si jedničky a nuly na obrazovce jako obrázek), dostáváme z dat **informaci** [10].

Informace jsou v dnešní době základním aktivem každého podniku a téměř každý podnik nějakým způsobem využívá IT technologie pro své fungování. Kyber útoky tak mohou ohrozit téměř každý podnik. Podle průzkumu zveřejněného v listopadu 2016 čelila pětina podniků za posledních 12 měsíců nějakému kybernetickému útoku a celosvětově náklady podniků spojené s těmito útoky dosahovaly za posledních 12 měsíců 279 miliard dolarů. Proto by měl otázku kybernetické bezpečnosti zvážit každý podnik [15, 16].

2.3 Datová úložiště

2.3.1 Pevný disk

Pevný disk (ang. Hard Disk Drive – HDD) je součástka, na kterou jsou ukládána všechna data, která zůstávají v zařízení i po jeho vypnutí – obsahuje tzv. persistentní data. Nejmenší jednotkou, na kterou lze uložit informace na pevném disku, je jeden sektor (512 bytů). Jeden fyzický disk lze rozdělit na několik oddílů – logických disků a pracovat s nimi jako se samostatnými disky. Na začátku pevného disku je umístěn Master Boot sektor (MBS), jenž obsahuje pokyny, které slouží k zavedení operačního systému do paměti po zapnutí počítače. Také obsahuje informace o tom, jak je fyzický disk rozdělen do disků logických [22].

2.3.2 Disková pole - RAID

Diskové pole nebo-li RAID (Redundant Array of Independent Disks) je spojení několika fyzických disků tak, že operační systém je vidí jako jeden logický disk. Toto uspořádání umožňuje realizaci datových operací paralelně. Poskytuje to také možnost využití redundance a tím zvýšení spolehlivosti. Dle redundance rozlišujeme 7 úrovní RAID, zde jsou některé z nich [26,27]:

RAID 0: Nevyužívá redundanci, data jsou rozdělena na všechny disky a operace jsou prováděny paralelně.

RAID 1: Obsahuje zrcadlení (mirroring), kdy jsou vždy na dva disky ukládány totožné informace. Tudíž když dojde k výpadku jednoho z těchto disků, může se stále bez přerušování pokračovat v činnosti.

RAID 5: Redundance, kdy na každém disku je vymezena část, kde je uložena parita. V případě výpadku jsme schopni dopočítat ztracená data pomocí parity. Dosavadní řešení dokázala nahradit výpadek jednoho disku, toto řešení dokáže nahradit i výpadek více disků.

2.3.3 Cloud – Virtuální úložiště

Společnost Gartner definuje Cloud jako způsob využití výpočetní techniky, kde jsou pružné a škálovatelné IT funkce nabízeny jako služba zákazníkům využívajícím internetové technologie. Cloud je tedy síť serverů, které poskytující nějaké služby. V našem případě se zaměříme na ukládání a přístup k datům. Data jsou pak přístupná, po přihlášení, prakticky odkudkoliv z internetu [23, 24, 25].

Určitým typem cloudu je privátní cloud. Stále se jedná o pronajímatelnou službu, ale implementace je v režii společnosti. Přístup k takovémuto cloudu bývá často omezen

pouze na uživatele ve vnitřní síti. Tímto je zajištěna vyšší bezpečnost a je garantována dostupnost [25].

2.4 Informační bezpečnost

Informační bezpečnost můžeme chápat jako ochranu informačních systémů (a v něm uložených informací) před poškozením, zničením, ztrátou či zcizením. Aby bylo možné zkoumat jednotlivé možnosti narušení bezpečnosti informačního systému, je vhodné si tento systém rozdělit na samostatné objekty [42].

Tyto objekty nazýváme aktivy. „Aktivum je přesně vymezená součást informačního systému, která je určena svojí funkcí, vazbami, svojí hodnotou a která při narušení své funkčnosti může mít vliv na bezpečnost informačního systému.“ [42, s.7]

Na informační aktiva působí z jejich okolí různé vlivy. Pokud tyto vlivy mohou způsobit nežádoucí změny aktiva, nazýváme je bezpečnostní hrozby. Pokud hrozba způsobí změnu (stavu, struktury, vazeb nebo funkce) aktiva, jedná se o bezpečnostní událost. Jestliže tato událost navíc ohrozí bezpečnost informačního systému, jedná se o bezpečnostní incident [42].

Pravděpodobnost výskytu hrozby v kombinaci s pravděpodobností způsobení bezpečnostního incidentu nazýváme riziko hrozby. Úroveň tohoto rizika se snižuje nasazením bezpečnostního opatření, které má za cíl snížit dopad na organizaci či zranitelnost aktiva [42].

V této kapitole se věnuji vysvětlení pouze několika pojmů z oblasti informační bezpečnosti. Podrobnější informace týkající se bezpečnosti informací a především systému řízení bezpečnosti informací (ISMS) lze nalézt například v publikaci Management informační bezpečnosti [42] a v normách řady ISO/IEC 27000.

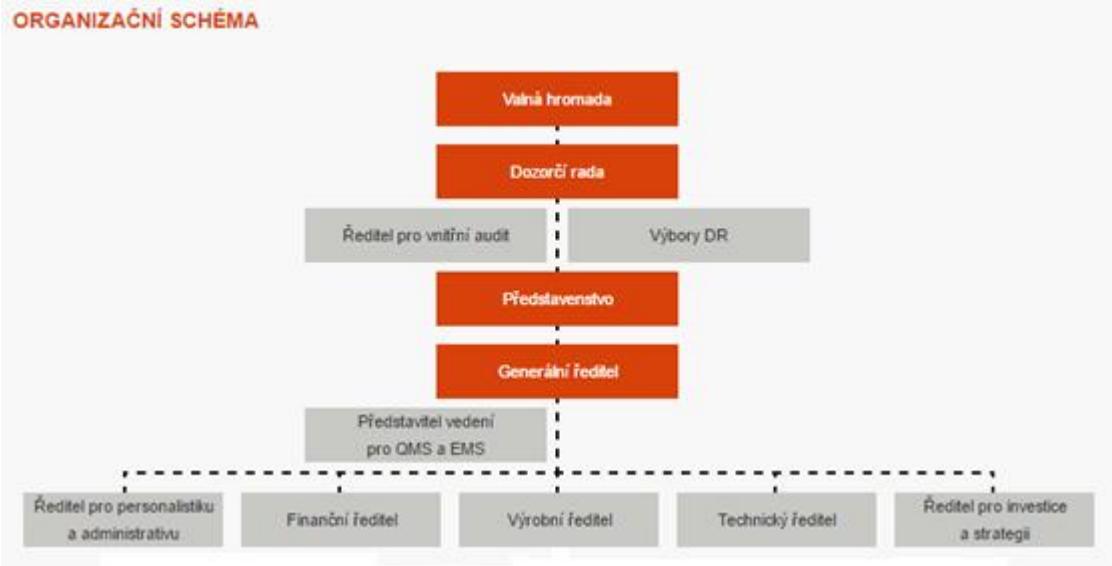
3 ANALÝZA SOUČASNÉHO STAVU

Společnost, na kterou bude zaměřena analytická a praktická část mé práce, podniká v hutním průmyslu. Počet zaměstnanců společnosti se pohybuje v řádu několika tisíc osob a její obrat se pohybuje v řádech několika desítek miliónů korun. Z důvodu ochrany citlivých informací společnosti nemůže být v této práci uveden název společnosti. Pro účely této práce bude tudíž označována jako **společnost ABC**.

3.1 Analýza společnosti a data ve společnosti

V této části se budu zabývat popisem a analýzou organizační struktury společnosti, jejím hardwarem, softwarem a jejími daty.

3.1.1 Organizační struktura se zaměřením na ICT



Obr. 5: Organizační struktura společnosti ABC.

Odbor informatiky a telekomunikačních technologií společnosti ABC je součástí Finančního úseku a řídí ho vedoucí odboru. Dělí se na několik částí: oddělení zabývající se centrálními aplikacemi, oddělení servisu PC a sítí, 4 oddělení zabývající se vývojem a oddělení pro telekomunikace.

3.1.2 Hardware

Hardware - servery

Stěžejním prvkem podnikové sítě je primární server se dvěma 12-ti jádrovými procesory a s operační pamětí 11 x 8 GB. Druhý server o stejných parametrech funguje jako záložní a testovací. Oba tyto servery mají Intel architekturu. Datové úložiště společnosti je realizováno RAID diskovým polem, jehož hlavní část tvoří 20 disků, každý o paměti 600 GB, které jsou propojeny přes 8GB fibre channel SAN.

Na těchto dvou hardwarových serverech je realizováno prostředí VMware, které provozuje virtuální servery. Tyto virtuální servery jsou společně se sítí SAN v clusteru, což zvyšuje dostupnost a snižuje náklady na provoz. Všechny virtuální servery tedy pracují nad jedním datovým polem (jehož parametry jsou uvedeny výše). Virtualizované servery jsou využívány především jako databázové, na ukládání souborů uživatelů a jako podpora aplikací (SAP, Lotus Notes).

Hardware – uživatelské počítače

Společnost provozuje okolo 3 000 uživatelských počítačů výhradně od společnosti Lenovo s platformou Intel.

3.1.3 Software

Software – servery

Operačním systémem je Microsoft Windows Server 2008 R2, minoritně je používán také Linux. Dalším softwarem jsou serverové části aplikačního SW: adresářové služby

Active Directory, Lotus Notes, souborové služby, monitorovací SW počítačové sítě, datové schránky a další.

Software – uživatelské počítače

Operačním systémem je Microsoft Windows, kde většina zařízení používá Windows 7, 8 nebo 10. Pro ověřování a přístup ke sdíleným zařízením je využíváno adresářových služeb Active Directory. Uživatelé pracují v OS s omezeným oprávněním. Důležitá data jsou ukládána na sdílených síťových úložištích, kde jsou jednou denně zálohována. Lokální data zálohována nejsou.

Bezpečnostní software se skládá z antivirového programu, antispyware softwaru a firewallu.

Klientské části centrálních aplikací nainstalované na uživatelské počítače jsou hlavně SAP a Lotus Notes.

Kancelářské aplikace jsou zastoupeny aplikacemi Microsoft Office.

Další aplikace jsou vždy specifické pro jednotlivé menší skupiny uživatelů.

3.1.1 Data ve společnosti

Ve společnosti funguje systém pro správu dokumentů DMS, který je pravidelně zálohován.

S daty je pracováno ve virtuálních serverech, které jsou v clusteru s diskovým polem. Ochrana dokumentů je navíc posílena zrcadlením diskového pole na pole stejného typu v jiné lokalitě.

Vybrané dokumenty jsou archivovány v tzv. Důvěryhodném archivu, kdy jsou dokumenty ukládány tak, aby byla splněna dlouhodobá právní platnost těchto

dokumentů. Tyto dokumenty jsou označeny elektronickou značkou, což garantuje rozeznání originálu, vloženého do důvěryhodného archivu, od kopie, která z důvěryhodného archivu nepochází.

V následující tabulce jsou uvedena data, která jsou v aplikacích SAP a Lotus Notes (LN). Tato data jsou ohodnocena dle důležitosti jejich ochrany stupnicí od 1 (data vyžadující nejmenší stupeň ochrany) do 5 (data vyžadující nejvyšší stupeň ochrany), jejichž ztráta by měla pro společnost nejnákladnější důsledky.

Tab. 1: Data v aplikacích Lotus Notes a SAP

Aplikace	Informace o aplikaci	Důležitost ochrany dat
Reklamace *SAP + Lotus Notes*	V SAPu jsou uložena všechna data, vybraná data se přenášejí do LN. Zde slouží pro koloběh vyřizování reklamace. Budou připojovány dokumenty obchodní a technické povahy.	4
Investiční akce *SAP + Lotus Notes*	Data v SAPu, v LN sledování celého průběhu investiční akce, vazby na další aplikace LN, přidávání dokumentů v různých fázích rozpracovanosti akce.	4
Evidence smluv *Lotus Notes*	Jednoduchá aplikace pro evidenci dokumentů převážně formátu DOC(X).	3
Evidence poptávek *Lotus Notes*	Evidence poptávek cizích společností a evidence nabídek společnosti těmto společnostem. Sledování stavu nabídky a vyhodnocování úspěšnosti nabídek společnosti.	3
Metrologie - kalib.protokoly *Lotus Notes + V.I.S.*	Evidence evidenčních karet měřidel, pro potřeby kalibrace napojeno na systém řízení výroby a evidence záznamů o kalibraci a kalibračních protokolů.	2

Datové schránky *Lotus Notes*	Koloběh dokumentů z/do datových schránek jednotlivých společností. Slouží k prokazatelnému předávání a vyřizování dokumentů v prostředí LN. Výměnu dokumentů mezi LN a datovými schránkami zajišťuje podatelna.	4
Personální kardexy *SAP + Lotus Notes*	Skeny personálních informací o zaměstnancích původní jednotné společnosti ABC jsou dnes uloženy v LN aplikaci, prostředí LN zde slouží pouze jako úložiště.	4

3.1.2 Ukládání a zálohování dat

Dle směrnice pro zálohování a archivaci dat společnosti ABC probíhá zálohování a archivace několika způsoby, dle typu dat, která je třeba uchovávat. Nejdůležitější – produkční data jsou zálohována okamžitým mirroringem (zrcadlením) na diskové pole ve vzdálené lokalitě. Takto zálohovaná data je možné okamžitě použít, v případě zničení, online.

U všech ostatních systémů se provádí záložní kopie na magnetické pásky, které jsou umístěny v magnetopáskovém robotu v Archivu společnosti ABC. Obnova dat je značně pomalejší, výhodou ale je, že na pásky se vytvářejí generační kopie, lze se proto vrátit i ke starším datům.

Data uživatelů jsou zálohována na virtuální souborový server. Každý z jednotlivých provozů má přidělen virtuální souborový server. Všichni uživatelé jsou poučeni, jak data zálohovat. Každý uživatel má v uživatelském počítači adresář, který se po zadání pokynu uživatelem, zálohuje na souborový server provozu.

Ve společnosti je několik administrátorů sítě a každý z nich má přiděleny uživatele. Ti pak těmto uživatelům dávají potřebná práva a přístup k souborovému serveru, na který mají mít oprávnění.

Souborový server je automaticky zálohován TSM serverem na magnetopáskové knihovny, umístěné v SAN síti v různých lokalitách. TSM server také zálohuje servery systému SAP a databáze Lotus Notes.

3.1.3 Řízení přístupu k datům

Dle vnitřní směrnice společnosti ABC má každá centrální aplikace svého držitele, správce a provozovatele. Administrátor přístupu pak řídí přístup uživatelů podle jejich jednotlivých oprávnění. O oprávnění pro své podřízené žádá podle vnitřní směrnice společnosti ABC jejich vedoucí prostřednictvím aplikace Lotus Notes. Rizikovým faktorem tedy přetrvává zneužití informací osobami mající dostatečné oprávnění k jejich přístupu.

3.1.4 Vývoj vlastního softwaru a pracoviště Service Desk

Společnost provozuje v rámci odboru Informatiky a telekomunikačních technologií několik oddělení zabývající se vývojem nového softwaru podporujícího především procesy spojené s výrobou společnosti (závodu). Dále probíhá stálý rozvoj prostředků pro antispamovou a antivirovou kontrolu. Vývoj vlastního softwaru je konkurenční výhodou společnosti.

Pro hlášení problémů s provozem PC pro koncové uživatele je ve společnosti ABC zřízeno pracoviště Service Desk s nepřetržitým provozem.

3.2 Analýza rizik

Společnost ABC má vypracovánu analýzu rizik. Jednou z nejvíce rizikových oblastí, na kterou tato analýza rizik upozorňuje, jsou pracovní stanice a jejich nedostatečné zabezpečení. Dle této analýzy rizik je potřeba v první fázi vytipovat pracovní stanice, na

kterých se vyskytují nejvíce rizikové dokumenty, a zvýšit jejich bezpečnost. V druhé fázi zvýšit bezpečnost i na dalších skupinách pracovních stanic. Na základě analýzy rizik bylo tedy společností zvoleno šifrování disků jako opatření proti rizikům s pracovními stanicemi. Šifrování disků má společně s organizačními pokyny podstatně snížit především rizika týkající se odcizení zařízení, či přístupu třetích stran k těmto zařízením.

3.3 Analýza trhu

V současnosti existuje na trhu několik nástrojů šifrujících datová úložiště. Pro přiblížení možností na trhu si uvedeme některé z nich.

Konkrétně se budeme zabývat 4 nástroji. Prvním je produkt společnosti Microsoft BitLocker. Druhým je ESET DESlock Encryption. Třetím je komplexní řešení bezpečnosti dat společnosti McAfee – McAfee Complete Data Protection Advanced. Čtvrtým je produkt AreaGuard NEO společnosti SODAT software.

Popis těchto produktů je uveden v přílohách a zhodnocení jejich požadovaných vlastností je uvedeno v kapitole 4 Vlastní návrhy řešení.

3.4 Požadavky společnosti

Hlavním požadavkem společnosti je zavedení šifrování na datová úložiště společnosti se zaměřením na uživatelské počítače. Společnost vnímá jako rizikovou práci s dokumenty společnosti, především s těmi, na které mají jejich uživatelé dostatečná oprávnění. Tato rizika navíc podporuje fakt, že velká část uživatelských počítačů ve společnosti jsou pracovní notebooky, které si zaměstnanci v případě potřeby berou domů či na pracovní cesty.

Zároveň je potřeba zohlednit v návrhu řešení to, že aktuální výpočetní kapacita serverů je plně využívána již používanými aplikacemi. V případě potřeby zavedení podpory šifrování také na servery je třeba počítat s nutností navyšování jejich výpočetní kapacity.

Počítačová síť, kde se nacházejí uživatelské počítače, je od výroby oddělená. Předmětem této práce je nalézt řešení pouze pro síť s uživatelskými počítači a nikoliv pro síť s výrobou.

3.5 Zhodnocení analýzy současného stavu

Rozsáhlost počítačové sítě společnosti ABC sebou nese určité výhody, ale i úskalí. Nevýhodou současného stavu je nekonzistentnost operačních systémů, a vzhledem k rozsáhlosti sítě, náročnost zavádění jakýchkoli změn. Společnost se také potýká s nízkou frekvencí obnovy hardwaru a softwaru, která je způsobena nedostatkem pravidelných prostředků a rozsáhlostí sítě. Bude tedy nutné najít řešení, které bude kompatibilní se všemi typy OS, které společnost používá. Musíme také uvážit riziko, že starší verze OS (ať už na serverech či na zařízeních uživatelů) nemusí poskytovat dostatečnou bezpečnost.

Velký důraz bude také kladen na dostupnost, protože jakýkoliv výpadek by byl pro společnost velmi nákladný.

Pozitivně ale vnímám stav zálohování a archivace dat a využívání virtualizace, která snižuje požadavky na hardware. Systém je propracovaný a zdokumentovaný.

Velmi znepokojující je ale těžko kontrolovatelné zacházení s daty, ke kterým mají jejich uživatelé dostatečná oprávnění. Riziko s tímto spojené (riziko ztráty dat v důsledku odcizení zařízení apod.) by mělo být šifrováním sníženo.

4 VLASTNÍ NÁVRHY ŘEŠENÍ

V této části se budu věnovat vlastnímu návrhu řešení pro společnost ABC.

4.1 Uspořádání dat na úložištích

Logické i fyzické uspořádání dat společnosti na sdílených úložištích je vyhovující. Data jsou oddělena dle typu a důležitosti logicky a nejdůležitější data jsou oddělena i fyzicky.

Uspořádání dat na zařízeních koncových uživatelů (osobní počítače a notebooky) neposkytuje dostatečnou ochranu dat. Na tato zařízení bude aplikováno opatření šifrování disků. Šifrování bude spravováno vzdáleně. Administrátoři nastaví uživatelům potřebná oprávnění, přičemž uživatelé nebudou mít právo šifrování vypnout. V případě, že by se firma rozhodla nešifrovat celé disky, je nutné, aby administrátoři nastavili k zápisu pouze adresáře, které budou šifrovány. (Typicky by se mělo jednat o adresáře Plocha, Stažené soubory a Dokumenty, které jsou umístěny na disku C.) Zbytek adresářů bude uživatelům k zápisu zakázán. Pokud má počítač více disků (ať fyzických či logických) budou tyto opět zašifrovány celé či budou šifrovány opět určené adresáře, které budou jako jediné povoleny k zápisu. Další organizační opatření jsou uvedena od kapitoly 4.5.

4.2 Požadavky na šifrovací nástroj

Hlavním požadavkem na šifrovací nástroj je bezpečnost. Nástroj musí pocházet z důvěryhodného zdroje, nesmí mít bezpečnostní rizika. Druhým nejdůležitějším požadavkem je, aby nástroj měl v ČR dodavatele, který bude poskytovat servis v průběhu zavádění a používání nástroje.

Dále je požadováno, aby nástroj splňoval požadovanou funkcionalitu. V první řadě tedy šifrování různých částí disku. Měl by tedy umožňovat šifrování jak celého disku, tak jednotlivých oddílů či adresářů. Dále by měla být umožněna práce s přenosnými

zařízeními (pro práci s šifrovanými dokumenty přes USB flash disk apod.). Nástroj by měl být také kompatibilní s firemními aplikacemi společnosti ABC a s alespoň většinou OS, které společnost používá. Společnost ABC by chtěla v rámci organizačních opatření oddělit roli administrátora od role správce klíčů, tato funkcionalita je tedy také jedním z parametrů výběru. Tato kritéria jsou uvedena níže i s produkty v tabulce (u OS se zaměřím na MS Windows 7, 8 a 10).

Významnou roli hraje samozřejmě také cena. Musíme brát ale v úvahu, že zavedení levného nástroje, který by nesplnil požadavky na bezpečnost, by bylo bezpředmětné a z dlouhodobého hlediska dražší (náklady spojené s případným útokem + cena nového opatření).

4.2.1 Možnosti šifrovacích nástrojů

Tab. 2: Možnosti šifrovacích nástrojů. [20, 28, 29, 30, 31, 32, 33, 34]

Produkt Parametry	**Area Guard Neo**	**BitLocker Drive Encryption**	**McAfee Complete Data Protection Advanced**	**ESET DESlock Encryption Pro**
Šifrování celého disku	Ano (ale bez OS)	Ano	Ano	Ano
Šifrování oddílu	Ano	Ano	Ano	Ano
Šifrování adresářů	Ano	Ano, omezeně	Ano	Ano
Šifrování USB flash disku	Ano	Ano	Ano	Ano
Oddělení role administrátora od správce klíčů	Ano	Ne	Ano	Ano
Šifrování sdílených úložišť	Ano	Ne	Ano	Ano
Kompatibilita s aplikacemi společnosti (SAP, Lotus Notes)	Ano	SAP ano, Lotus Notes nepotvrzeno	Ano	-
Kompatibilita s OS Serverů	MS Windows Server 2008 a novější	MS Windows Server 2008 a novější	MS Windows Server 2003 a novější (2003 pouze 32 bit)	MS Windows Server 2003 a novější
Kompatibilita s OS uživatelských počítačů	MS Windows Win 7, Win 8, Win 8.1, Win 10	MS Windows Vista a vyšší v edicích PRO a Enterprise	MS Windows Win 7, Win 8, Win 8.1, Win 10	MS Windows Win 7, Win 8, Win 8.1, Win 10
Šifra	AES 256	AES (128 / 256)	AES 256	AES 256
Cena (licence na 1 uživatelský počítač)	2100 Kč (servis 1 rok, další roky za příplatky)	0* Kč	2450 Kč (+ cena servisu)	2770 Kč (na 3 roky)

* Cena nového OS (např. Windows 10 Pro): 4000 Kč.

4.3 Metodika výběru šifrovacího nástroje

Nejdříve zhodnotíme nástroje dle prvních dvou nejdůležitějších kritérií – z hlediska bezpečnosti a z hlediska dostupného servisu. Porušení libovolného z těchto dvou kritérií zapříčiní vyřazení tohoto nástroje z výběru.

V tabulce jsou uvedeny funkcionality nástrojů. Neposkytnutí některého z těchto kritérií daným produktem nepovede k vyřazení produktu, ale bude to hodnoceno jako nevýhoda oproti dalším produktům, které tuto funkcionalitu poskytují.

Výhodou nástroje je samozřejmě nízká cena. V rámci této bakalářské práce ale nelze uspořádat výběrové řízení, které by mohlo cenu významně změnit. Proto v rámci objektivity bude zhodnocení na základě ceny jedné licence na jedno zařízení. Pokud budou ostatní funkcionality srovnatelné, bude jako nejlepší zhodnocen nejlevnější produkt.

4.4 Zhodnocení a výběr šifrovacího nástroje

Hlavní kritéria splňují produkty Area Guard Neo, McAfee Complete Data Protection Advanced a ESET DESlock Encryption. U produktu BitLocker bylo zjištěno, že obsahuje bezpečností rizika (viz 4.3.1). Vzhledem k tomu, že cílem opatření je, aby poskytovalo lepší zabezpečení, je použití rizikového nástroje bezpředmětné a tudíž musí být z výběru vyřazen.

Zbývající produkty poskytují požadované parametry srovnatelně. Výhodou McAfee Complete Data Protection ale je, že se jedná o komplexní řešení poskytující mnohé další funkcionality. Mírnou nevýhodou produktu Area Guard Neo by mohlo být, že nešifruje OS. Společnost ABC ale toto nepožaduje, proto to nebude bráno jako nevýhoda tohoto produktu.

Výhodou všech produktů je používání symetrické šifry AES, která je jednou z doporučovaných symetrických šifer např. ve vyhlášce o kybernetické bezpečnosti či v americkém standardu NIST Special Publication 800-131A [40, 41].

Posledním parametrem rozhodování je tedy cena. Z hlediska ceny je nejvýhodnějším produktem AreaGuard Neo. (Vycházíme-li z ceny pro jedno zařízení, po jednání s dodavateli produktů může dojít k množstevním a jiným slevám, které nejsou do rozhodování zahrnuty.) Na základě dostupných informací doporučuji společnosti ABC použití produktu AreaGuard Neo.

4.5 Doporučené organizační pokyny a jejich dokumentace

Zavedení šifrování bude organizačně zdokumentováno ve dvou hlavních dokumentech. Nejdůležitějším dokumentem je Technicko-organizační pokyn, kdy již do existujícího dokumentu budou přidány informace, o šifrování z informatického hlediska. Tento dokument plní informační funkci, že se v závodu bude šifrovat a obsahuje odkaz na dokument Pracovní postup, který upřesňuje detaily a pokyny. Dokumenty o pracovních postupech jsou v podniku běžné. Pro šifrování tedy bude vytvořen nový dokument s patřičným číslem a názvem Pracovní postup: Šifrování úložišť.

V pracovním postupu bude mj. upřesněno:

- Povinná délka a náležitosti bezpečnostního hesla pro šifrování:
    - minimální počet znaků,
    - povinné použití číslic či speciálních znaků,
    - pokyny pro obnovu hesla,
    - pokyny, co udělat, v případě vyzrazení hesla,
    - pokyny v případě opakovaně zadaného špatného hesla,
    - pokyny o utajení hesla (heslo nesmí být v na lístečku vedle počítače, nesmí být řečeno jiné osobě apod.).

- Rozdělení všech dokumentů dle důvěrnosti informací. A vydat pokyny pro jednotlivé stupně důvěrnosti. Například pro nejdůvěrnější dokumenty:
    - zákaz šíření dokumentů v nezašifrované podobě a definice případných postihů,
        - Definice výjimek (např. zákazníkovi, který nevlastní klíč k dešifrování musíme zaslat dokumenty nezašifrovány).
    - dokumentovat počet kopií nejdůležitějších dokumentů a uživatele, kteří k nim mají přístup.

4.6 Stanovení rolí, činností, odpovědností

Základní role zaměstnanců pro zavedení a provoz šifrování:

- vedoucí,
- zástupce vedoucího,
- správce šifrovacích klíčů,
- administrátor,
- uživatel.

Vedoucí je osoba, která má zodpovědnost za celý proces zavádění i provozu šifrování. Tato osoba musí být zaměstnancem společnosti ABC. Může svou práci delegovat, zodpovědnost však zůstává na vedoucím.

Činnosti a pravomoci vedoucího:

- komunikuje s dodavatelskou firmou,
- komunikuje s vedením společnosti,
- řeší závažné potíže,
- připravuje a dohlíží na provedení zkušebního provozu (zde je nutné ověřit kompatibilitu se všemi důležitými aplikacemi, funkčnost sdílení souborů apod.),
- připravuje a dohlíží na provedení jednotlivých částí zavádění šifrování,

- v rámci šifrovacího programu vytvoří jednotlivé role s jejich pravomocemi a přidělí je členům týmu pro zavádění šifrování,
- vytvoří nové směrnice, upraví staré, vedení firmy musí změny potvrdit.

Zástupce vedoucího je osoba, která pomáhá vedoucímu, v případě nutnosti se střídají na směnách či v pohotovosti (společnost ABC funguje totiž s nepřetržitým provozem). Vedoucí mu deleguje úkoly. Spolupracují na tvorbě a provádění zkušebního provozu, zavádění i provozu šifrování. Jeho hlavním úkolem je stanovit jednotlivé skupiny zaměstnanců, u kterých se zavede šifrování v jednotlivých fázích. Zavádění se bude provádět za nepřetržitého provozu, proto je nutné, aby skupiny zaměstnanců, kteří mezi sebou komunikují a poskytují si dokumenty, byly ve stejné fázi zavádění šifrování. Dále je jeho úkolem přiřadit určené skupiny zaměstnanců jednotlivým administrátorům. Také má na starosti ve spolupráci s dodavatelskou firmou vyškolit tým pro šifrování a následně také proškolit uživatele (seznámit je s novými směrnicemi, dát jim pokyny).

Správce šifrovacích klíčů má jako hlavní činnost spravování záloh šifrovacích klíčů. V případě nutnosti má možnost obnovit zašifrované dokumenty. Tato role by neměla být slučitelná s jinou rolí pro šifrování, aby byla zaručena bezpečnost. Veškerá činnost správce šifrovacích klíčů je monitorována (o přístupech k jednotlivým heslům jsou vytvářeny logy, které jsou zasílány vedoucímu šifrování).

Několik osob bude disponovat rolí **administrátor.** Hlavní činností a zodpovědností administrátorů je správa uživatelských počítačů. Tento tým administrátorů má za úkol nastavit na uživatelských počítačích patřičné složky pro zápis, zbytek složek nastavit pouze pro čtení. Dále budou vzdáleně nastavovat počítače pro šifrování a vzdáleně, ve spolupráci s uživateli, data zašifrují. Také nastaví, aby uživatelé neměli právo vypnout šifrování. Řeší problémy v běžném provozu, komunikují s uživateli.

Uživateli jsou všichni ostatní zaměstnanci společnosti ABC, kterých se šifrování dokumentů týká (tzn. pracují s počítačem či jiným zařízením do šifrování zahrnutým). Uživatelé budou proškoleni o zásadách používání šifrování disků tak, aby poskytovalo dostatečnou bezpečnost.

Povinnosti uživatelů:

- vytvořit a používat pro šifrování dostatečně bezpečné heslo,
    - alespoň 8 znaků: malá a velká písmena, číslice a speciální znaky,
    - nepoužívat nejčastěji používaná hesla či jejich části (password, heslo, jméno manželky, apod. – o tomto budou uživatelé poučeni v rámci školení),
- v případě podezření vyzrazení hesla, okamžitě tuto skutečnost nahlásit a heslo změnit,
- dodržovat vydané směrnice.

4.6.1 Organizační začlenění rolí pro společnost ABC

Podrobný popis struktury oddělení informatiky se nalézá v kapitole 3.1.1. Roli vedoucího šifrování převezme oddělení správy PC a sítí. Jeho zástupce převezme roli zástupce šifrování. Správce šifrovacích klíčů bude vybrán z jiného oddělení – bude jím vedoucí oddělení telekomunikací. Správce šifrovacích klíčů tedy nebude organizačně podřízeným vedoucímu šifrování a také nebude mít administrátorská práva k počítačům. Tato opatření zvýší bezpečnost a sníží hrozbu zneužití obnovovacích klíčů.

Administrátoři z oddělení správy PC a sítí převezmou také roli administrátorů pro šifrování. Uživateli budou všichni uživatelé, na jejichž zařízení se vztahuje šifrování.

4.7 Studie proveditelnosti

V této kapitole se budu zabývat studií proveditelnosti projektu nasazení šifrování disků ve společnosti ABC. Rizika, která by mohla nasazení a později bezpečnost produktu ohrozit jsou uvedena níže.

Tab. 3: Analýza rizik projektu nasazení šifrování

Pořadové číslo	Hrozba	Pravděpodobnost	Míra dopadu	Hodnota rizika
1	Nekompatibilnost produktu se sítí společnosti (s aplikacemi apod.)	Střední	Střední	Vysoká
2	Ukončení činnosti dodavatele	Nízká	Střední	Střední
3	Objevení bezpečnostního rizika v produktu	Střední	Vysoká	Vysoká
4	Rozšíření kvantových počítačů a prolomení šifry AES	Nízká	Vysoká	Střední

Po aplikaci opatření budou hodnoty rizik následující:

Tab. 4: Analýza rizik projektu nasazení šifrování po aplikaci opatření

Pořadové číslo	Hrozba	Vybrané řešení	Pravděpodobnost	Míra dopadu	Hodnota rizika
1	Nekompatibilnost produktu se sítí společnosti (s aplikacemi apod.)	Provedení zkušebního provozu před nákupem, vybrání jiného produktu	Střední	Nízká	Nízká
2	Ukončení činnosti dodavatele	Smluvně ošetřit zachování důvěryhodnosti informací. Servis převezmou zaměstnanci společnosti ABC.	Nízká	Nízká	Nízká
3	Objevení bezpečnostního rizika v produktu	Vybrání důvěryhodného dodavatele, který v takovémto případě rychle zveřejnění update.	Nízká	Střední	Střední
4	Rozšíření kvantových počítačů a prolomení šifry AES	Aktuálně tato technologie není zcela vyvinuta a než bude, může dodavatel přejít na používání jiné šifry.	Nízká	Nízká	Nízká

Riziko nekompatibilnosti produktu se sítí společnosti a jejími aplikacemi je střední. Dodavatelé všech produktů dokládají, že by s tímto problém být neměl. Navíc produkty jsou kompatibilní s OS, které firma používá. Přesto se jisté komplikace mohou vyskytnout. Proto opatřením je provedení zkušebního provozu před nákupem produktu. V případě, že se projeví komplikace, které by znemožnily úspěšné nasazení produktu, bude vybrán jiný produkt a zkušební provoz zopakován. Vzniknou tedy pouze provozní náklady na stávající zaměstnance a stávající hardware.

Dodavatelé, kteří jsou ve výběru, jsou na trhu úspěšně již několik let, tudíž jejich brzké ukončení činnosti je nepravděpodobné. Pro případ, že by k tomu ale došlo, je potřebné, aby bylo smluvně ošetřeno, že dodavatel, nikdy (ani po svém skončení) nezveřejní o produktu informace, které by mohly bezpečnost jeho používání ohrozit. Je také pravděpodobné, že by mohl produkty této firmy někdo převzít, což by problém také vyřešilo. Jedním z řešení by také mohlo být, že by funkce servisu převzali zaměstnanci oddělení informatiky ve společnosti, což je samozřejmě možné. Problematickou by se ale mohla stát kompatibilita např. s novými OS v kombinaci s ustáním podpory těch starých. Během této doby by ale samozřejmě měla firma dostatek času, přejít na jiný produkt.

Aktuálně je známým faktem, že každý software obsahuje chyby. [38] Je tedy téměř jisté, že i vybrané produkty chyby obsahují. Opatřením je vybrat produkt od výrobce, který na vývoji stále pracuje, odhalené chyby a bezpečnostní mezery opravuje a zveřejňuje opravy v updatech.

Kdyby došlo k rozšíření kvantových počítačů a prolomení šifry AES, byl by tento fakt velmi brzy zveřejněn. Výrobce by tedy měl dostatek času na výběr nové šifry. Také společnost ABC by měla dostatek času na provedení potřebných opatření. Dále se dá předpokládat, že takto nákladné útoky budou v první řadě provedeny na největší světové firmy. Společnost ABC je ve světovém měřítku malou firmou. K odrazení útočníka také může přispět, že čeština je těžkým a málo rozšířeným jazykem.

4.7.1 Shrnutí studie proveditelnosti

Podmínkou proveditelnosti projektu je aplikování výše uvedených opatření, především tedy: uskutečnění zkušebního provozu před nákupem produktu, smluvní ošetření zachování důvěryhodnosti informací s dodavatelem, vybrání výrobce, který bude dál pracovat na vývoji a opravování produktu.

Pokud budou splněny tyto podmínky, hodnotím projekt jako proveditelný.

4.8 Analýza rizik

Celkovou analýzu rizik má společnost ABC zpracovánu. Ale vzhledem k tomu, že se jedná o velmi důvěrné informace, nemůže být v rámci této práce zveřejněna. Zaměřím se tedy jen na rizika, na která je aplikováno opatření šifrování disků.

Tab. 5: Analýza rizik

Pořadové číslo	Hrozba	Pravděpodobnost	Míra dopadu	Hodnota rizika
1	Zcizení notebooku zaměstnance a zneužití dat	Vysoká	Vysoká	Vysoká
2	Ztráta notebooku zaměstnance a zneužití dat	Střední	Střední	Střední
3	Vynášení dat ze společnosti zaměstnancem	Střední	Vysoká	Vysoká
4	Odeslání dat omylem nesprávné osobě a jejich zneužití	Nízká	Střední	Střední

Po aplikování opatření šifrování disků bude zhodnocení rizik následující:

Tab. 6: Analýza rizik po aplikování opatření

Pořadové číslo	Hrozba	Vybrané řešení	Pravděpodobnost	Míra dopadu	Hodnota rizika
1	Zcizení notebooku zaměstnance a zneužití dat	Zašifrování dat	Nízká	Nízká	Nízká
2	Ztráta notebooku zaměstnance a zneužití dat	Zašifrování dat	Nízká	Nízká	Nízká
3	Vynášení dat ze společnosti zaměstnancem	Zašifrování dat, omezení přístupu k datům	Nízká	Střední	Střední
4	Odeslání dat omylem nesprávné osobě a jejich zneužití	Posílání zašifrovaných dat, pouze přijímce může dešifrovat	Nízká	Nízká	Nízká

Hrozba zcizení notebooku zaměstnance a následné zneužití těchto dat je snížena tím, že disky tohoto notebooku budou zašifrovány. I kdyby tedy někdo notebook zcizil, k otevřeným datům společnosti se nedostane, protože budou zašifrována.

Obdobně je tomu u ztráty notebooku. Původní riziko by zde bylo ještě o něco nižší. Pravděpodobnost, že by někdo náhodně nalezl ztracený notebook, nevrátil ho majiteli, dostal se k citlivým datům a ještě je poskytl třetím stranám tak, aby poškodila společnost, je jistě nižší, než když je notebook cíleně odcizen, ať už za účelem získání samotného zařízení či dat společnosti.

Střední hodnota rizika u hrozby č. 3 je z toho důvodu, že šifrování zcela nezruší hrozbu vynášení informací zaměstnanci, protože zaměstnanci stále budou mít přístup k dokumentům a informacím, které souvisejí s jejich kompetencemi. Riziko je ale přesto sníženo kvůli faktu, že šifrování a opatření, která budou společně se šifrováním

zavedena, toto zaměstnancům znesnadní. Zasílané dokumenty totiž budou šifrovány, rovněž přenášená data prostřednictvím přenosných zařízení budou šifrována.
Co se týče odeslání dat omylem nesprávné osobě, zde platí obdobné vztahy. Omyl samotný a následné zneužití dat je méně pravděpodobné, než cílené poškození firmy. A opět dokumenty zasílány v rámci firmy mohou být šifrováya, což riziko opět sníží.

Jak je v tabulkách zobrazeno, aplikace opatření šifrování disků bude mít velmi pozitivní vliv na výše uvedené hrozby. Celková hodnota se sníží z hodnot střední až vysoké na hodnoty nízké až střední.

4.9 Časový plán

Nejdříve je potřeba, aby byl projekt zahájen a aby bylo vypsáno výběrové řízení a aby toto výběrové řízení proběhlo. Poté bude vyhodnoceno a bude vybrán produkt. Následovat bude zkušební provoz. V případě, že by se ukázalo, že produkt není kompatibilní, bude vybrán jiný produkt a znovu proveden zkušební provoz (toto se může opakovat). Každé takové zopakování bude mít za následek zpoždění projektu o 3 měsíce. Následuje podpis smlouvy a implementace.

Tab. 7: Časový plán

Činnost	Délka trvání	Termín dokončení
Zahájení projektu	1 den	1.7.2017
Výběrové řízení na produkt	2 měsíce	1.9.2017
Vyhodnocení výběrového řízení	1 měsíc	1.10.2017
Zkušební provoz	2 měsíce	1.12.2017
Výběr nového produktu	1 měsíc	*
Zkušební provoz	2 měsíce	*
Smlouva o implementaci (nákup)	1 měsíc	1.1.2018
Implementace	6 měsíců	1.7.2018

* Nekompatibilita vybraného produktu prodlouží projekt o 3 měsíce.

Nasazení šifrování ve společnosti ABC (pokud bude produkt kompatibilní) proběhne během jednoho roku.

4.10 Ekonomické zhodnocení

Cena pořízení jedné licence softwarového nástroje Area Guard Neo na jedno uživatelské zařízení činí 2 100 Kč. Množství zařízení, na které si přeje společnost šifrování zavést, se pohybuje okolo 3 000 ks. Vycházíme-li z těchto informací, cena pořízení licencí je 6 300 000 Kč. (Na tuto cenu budou samozřejmě aplikovány množstevní slevy a cena také může být snížena výběrovým řízením. V rámci této práce z důvodu objektivnosti počítám se základní cenou za jednu licenci.) Dalším nákladem jsou provozní náklady na stávající zaměstnance. Vzhledem k tomu, že se ale nejedná o zaměstnance za tímto účelem přijaté, náklady firmy na zaměstnance se nezmění, a proto nebudou momentálně zohledněny. Je třeba také počítat s cenou budoucího servisu (v ceně je servis na jeden rok), která bude určena až konkrétní smlouvou či výběrovým řízením. Celkové náklady tedy nepřesáhnou 7 250 000 Kč.

Zavedení bezpečnostního opatření samo o sobě negeneruje zisk, ale do budoucna šetří náklady spojené s potenciálním úspěšným útokem, kterému toto opatření zabrání či jeho dopad sníží. V případě, že by došlo k odcizení informací, které by zapříčinilo ztrátu zakázky, či dokonce přerušení provozu, byly by náklady pro společnost v řádu stovek až tisíců miliónů Kč.

Z tohoto důvodu, zavedení bezpečnostního opatření, které toto riziko sníží, je z dlouhodobého hlediska pro společnost výhodné. S ohledem na výsledek hospodaření společnosti je částka za toto opatření pro společnost akceptovatelná.

ZÁVĚR

Cílem bakalářské práce bylo navrhnout zavedení šifrování na datová úložiště společnosti. Byla provedena analýza současného stavu společnosti ABC a analýza trhu. V analýze trhu byly porovnávány čtyři produkty: BitLocker, Area Guard Neo, ESET DESlock Encryption a McAfee Complete Data Protection Advanced. Nástroj BitLocker byl vyřazen kvůli bezpečnostním rizikům. Zbylé produkty splnily požadované parametry, včetně dostupného servisu. Na základě ceny za jednu licenci byl tedy vybrán produkt Area Guard Neo.

Pro zavádění byla učiněna doporučení týkající se organizačních pokynů, začlenění pokynů do stávající dokumentace společnosti, byly určeny potřebné role pro zavádění a provoz šifrování a přiřazení těchto rolí konkrétním pracovníkům firmy. Byla provedena analýza rizik, na která má být aplikováno toto bezpečnostní opatření. Analýza rizik také ukázala, že aplikací tohoto bezpečnostního opatření dojde k podstatnému snížení rizika u zmíněných hrozeb a tím ke zlepšení úrovně bezpečnosti ve společnosti. Byla provedena studie proveditelnosti projektu zavádění a provozu šifrování ve společnosti, která ukázala, že při provedení určitých opatření je tento projekt proveditelný. Ekonomické zhodnocení ukázalo, že z dlouhodobého hlediska je zavedení tohoto bezpečnostního opatření pro společnost výhodné. Dle časového plánu bude délka zavádění tohoto opatření pravděpodobně jeden rok.

SEZNAM POUŽITÝCH ZDROJŮ

[1] BITTO, Ondřej. *Šifrování a biometrika, aneb, Tajemné bity a dotyky*. Kralice na Hané: Computer Media, 2005. ISBN 80-86686-48-5.

[2] BITTO, Ondřej. *Historie kryptologie* [online]. [cit. 2017-05-25]. Dostupné z: http://www.fi.muni.cz/usr/jkucera/pv109/2003/xbitto.htm

[3] TRUSCHKA, Jakub. Asymetrická kryptografie v praxi. *System Online: S přehledem ve světě informačních technologií* [online]. [cit. 2017-05-25]. Dostupné z: https://www.systemonline.cz/it-security/asymetricka-kryptografie-v-praxi.htm

[4] Úvod do kryptografie. *Earchivace.cz* [online]. [cit. 2017-05-25]. Dostupné z: http://www.earchivace.cz/technologie/uvod-do-kryptografie/

[5] Úvod do kryptografie. *Bezpečnostní riziko* [online]. [cit. 2017-05-25]. Dostupné z: http://www.bezpecnost.estranky.cz/clanky/zpravodajske-techniky/uvod-do-kryptografie.html

[6] Úvod do kryptologie. *Mendelova univerzita v Brně* [online]. [cit. 2017-05-25]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=7021

[7] Nastal čas na změnu principů šifrování? *Computerworld* [online]. [cit. 2017-05-25]. Dostupné z: http://computerworld.cz/securityworld/nastal-cas-na-zmenu-principu-sifrovani-1-48441

[8] NIST: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Data encryption standard (DES)*. 1999, 27 s. Dostupné také z: http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[9] Data Encryption Standard. *Tutorials point* [online]. [cit. 2017-05-25]. Dostupné z: https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm

[10] LESSNER, Dan. Data a význam. *Univerzita Karlova* [online]. [cit. 2017-05-25]. Dostupné z: http://popelka.ms.mff.cuni.cz/~lessner/mw/index.php/U%C4%8Debnice/Informace/Data_a_v%C3%BDznam

[11] FEIBERGER, Marianne. Do quantum computers exist? *Plus magazine* [online]. [cit. 2017-05-25]. Dostupné z: https://plus.maths.org/content/do-quantum-computers-exist

[12] JAVŮREK, Karel. Kvantový počítač se utkal s dnešními procesory. Zvítězil? *VTM.cz - věda, technika, zajímavosti, budoucnost* [online]. [cit. 2017-05-25]. Dostupné z: http://vtm.e15.cz/kvantovy-pocitac-se-utkal-s-dnesnimi-procesory-zvitezil

[13] ČÍŽEK, Jakub. Google: Náš kvantový počítač je 100 000 000× rychlejší. *Živě.cz - O počítačích, IT a internetu* [online]. [cit. 2017-05-25]. Dostupné z: http://www.zive.cz/clanky/google-nas-kvantovy-pocitac-je-100-000-000-rychlejsi/sc-3-a-180725/default.aspx

[14] SALVET, Pavel. Kvantové počítače: Hrozba pro dnešní úroveň šifrování? *Interval.cz* [online]. [cit. 2017-05-25]. Dostupné z: https://www.interval.cz/clanky/kvantove-pocitace-hrozba-pro-sifrovani/

[15] Realistic resilience: taking a pragmatic approach to cybersecurity. *Grant Thornton* [online]. [cit. 2017-05-25]. Dostupné z: https://www.grantthornton.global/en/insights/cybersecurity/

[16] Kybernetické útoky stojí globální business více než 300 mld dolarů ročně. *Grant Thornton* [online]. [cit. 2017-03-25]. Dostupné z: kyberneticke-utoky-stoji-globalni-business-vice-nez-300-mld-dolaru-rocne

[17] *Kryptografie: AES* [online]. [cit. 2017-05-25]. Dostupné z: http://www.kryptografie.wz.cz/data/aes.html

[18] NIST: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Advanced Encryption Standard (AES)*. 2001. Dostupné také z: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

[19] AES Rijndael Cipher - Visualization. *YouTube* [online]. [cit. 2017-05-25]. Dostupné z: https://www.youtube.com/watch?v=mlzxpkdXP58

[20] CHROMEČKA, Jiří. *ANALÝZA ŠIFROVACÍCH METOD PRO KLONOVÁNÍ DISKŮ*. Dostupné také z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=132102. Diplomová práce. Vysoké učení technické v Brně. Vedoucí práce Doc. Ing., Dipl.-Ing. MARTIN DRAHANSKÝ, Ph.D.

[21] *DiVA Portal* [online]. [cit. 2017-01-25]. Dostupné z: http://www.diva-portal.org/smash/get/diva2:347753/FULLTEXT01.pdf

[22] Pevný disk. *Ostravská univerzita: WWW server uživatelů na Ostravské univerzitě* [online]. [cit. 2017-05-25]. Dostupné z: http://www1.osu.cz/home/matejka/soft/data/harddisk.htm

[23] ČAMBALA, Lukáš. Co je to Cloud? Patří mu budoucnost dat? *Lenovo blog* [online]. [cit. 2017-05-25]. Dostupné z: http://www.lenovoblog.cz/2014/05/co-je-to-cloud-patri-mu-budoucnost-dat.html

[24] Gartner Says IT Organisations Will Invest More in Private Cloud Services than in External Cloud Providers Through 2012. *Gartner* [online]. [cit. 2017-05-25]. Dostupné z: http://www.gartner.com/newsroom/id/1193913

[25] Co je a co není cloud. *Lupa.cz: Server o českém internetu* [online]. [cit. 2017-05-25]. Dostupné z: https://www.lupa.cz/clanky/co-je-a-co-neni-cloud/

[26] *Technika personálních počítačů: materiály k předmětu (FIT)* [online]. [cit. 2017-05-25]. Dostupné z: http://www.fit.vutbr.cz/study/courses/ITP/public/itp07/raid00.pdf. Vysoké učení technické v Brně.

[27] Disková pole – RAID. *Prostředky informačních technologií* [online]. [cit. 2017-05-25]. Dostupné z: http://pit.wz.cz/Konstrukce/raid.php

[28] OHLHORST, Frank. BitLocker review. *Techworld* [online]. [cit. 2017-05-25]. Dostupné z: http://www.techworld.com/review/encryption/bitlocker-review-3212400/

[29] ESET. *Deslock Encryption: Produktový list*. Dostupné také z: https://cdn3-prodint.esetstatic.com/ESET/CZ/Produktove_listy/firmy/deslock-by-eset.pdf

[30] MCAFEE. *Complete Data Protection Advanced: Produktový list*. Dostupné také z: http://www.mcafee.cz/fileadmin/user_upload/Produktove_listy/McAfee/McAfee-Complete-Data-Protection-Advanced-PL-CZ.pdf

[31] MCAFEE. *Complete Data Protection Advanced: Data sheet*. Dostupné také z: http://www.mcafee.com/us/resources/data-sheets/ds-complete-data-protection.pdf

[32] *SAP's Standards, Processes, and Guidelines for Protecting Data and Information*. Dostupné také z: https://assets.cdn.sap.com/sapcom/docs/2016/05/4c6b54a2-707c-0010-82c7-eda71af511fa.pdf

[33] *Area Guard Neo: Data sheet*. Dostupné také z: http://www.areaguard.cz/download/AreaGuard_Neo_DatasheetA4_web.pdf

[34] McAfee Complete Data Protection Advanced. *Comguard* [online]. [cit. 2017-05-25]. Dostupné z: https://www.comguard.cz/produkty/mcafee/mcafee-data-protection/total-protection-for-data/

[35] Why Microsoft stores your Windows 10 Device Encryption Key to OneDrive. *The Windows Club* [online]. [cit. 2017-05-25]. Dostupné z: http://www.thewindowsclub.com/microsoft-windows-10-device-encryption-key

[36] Útok na Windows BitLocker není podle Microsoftu velkým rizikem. *Computerworld* [online]. [cit. 2017-05-25]. Dostupné z: http://computerworld.cz/securityworld/utok-na-windows-bitlocker-neni-podle-microsoftu-velkym-rizikem-47316

[37] Press Shift + F10 during Windows 10 Upgrade to Launch Root CLI & bypass BitLocker. *The Hacker News* [online]. [cit. 2017-05-25]. Dostupné z: http://thehackernews.com/2016/11/windows-bitlocker-bypass.html

[38] Proč nedávat záruku na software. *Net magnet* [online]. [cit. 2017-05-25]. Dostupné z: http://www.netmagnet.cz/blog/zaruka-na-software/

[39] Útoky na firmy jsou stále častější, přispívá k nim i mobilní internet. *BusinessInfo.cz* [online]. [cit. 2017-05-25]. Dostupné z: http://www.businessinfo.cz/cs/clanky/utoky-na-firmy-jsou-stale-castejsi-prispiva-k-nim-i-mobilni-internet-86035.html

[40] *Vyhláška o kybernetické bezpečnosti: č. 316/2014 Sb*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-316#prilohy

[41] NIST: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*. Dostupné také z: http://csrc.nist.gov/publications/drafts/800-131A/sp800-131a_r1_draft.pdf

[42] ONDRÁK, Viktor. *Management informační bezpečnosti*. 2015. Studijní opora pro předmět Management informační bezpečnosti. Vysoké učení technické v Brně.

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

OT – otevřený text

ŠT – šifrovaný text

SW – software

HW – hardware

OS – operační systém

LN – aplikace Lotus Notes

MS – Microsoft

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH