VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

IMPLEMENTACE NOVÝCH KONCOVÝCH UZLŮ DO FIRMY A JEJICH MANAGEMENT

IMPLEMENTATION OF NEW TERMINAL NODES TO THE COMPANY AND IT'S MANAGEMENT

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR
Bc. Pavel Lukeš

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

BRNO 2016

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2015/2016
Ústav informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Lukeš Pavel, Bc.

Informační management (6209T015)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

Implementace nových koncových uzlů do firmy a jejich management

v anglickém jazyce:

Implementation of New Terminal Nodes to the Company and it's Management

Pokyny pro vypracování:

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

Seznam odborné literatury:

BIGELOW, S. Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů. 1. vydání. Brno: Computer Press, 2004. 990 s. ISBN 80-251-0178-9.
ČSN ISO/IEC 27001. Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky. Praha: Český normalizační institut, 2006.
JANEČKOVÁ, E. a V. BARTÍK. Kamerové systémy v praxi. 1. vydání. Praha: Linde, 2011. 240 s. ISBN 978-80-7201-850-5.
PUŽMANOVÁ, R. Moderní komunikační sítě od A do Z. 2. aktualizované vydání. Brno: Computer Press, 2006. 430 s. ISBN 80-251-1278-0.
TVRDÍKOVÁ, M. Aplikace moderních informačních technologií v řízení firmy. 1. vydání. Praha: Grada Publishing, 2008. 176 s. ISBN 978-80-247-2728-8

Vedoucí diplomové práce: Ing. Viktor Ondrák, Ph.D.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2015/2016.

L.S.

doc. RNDr. Bedřich Půža, CSc. Ředitel ústavu	doc. Ing. et Ing. Stanislav Škapa, Ph.D. Děkan fakulty

V Brně, dne 29.2.2016

Abstrakt

Diplomová práce se zabývá analýzou a následným návrhem řešení problémů, ve starším objektu ze dvou, vlastněným společností MBG, spol. s r.o.. Mezi tyto problémy patří nedostatečný monitoring, zastaralé některé technologie a absence jakéhokoliv systému řízení bezpečnosti informací. V první části práce budou zpracována veškerá teoretická východiska potřebná pro danou problematiku, následně pak zpracována kompletní analýza všech výše zmíněných problémů společnosti. Na závěr bude, na základě předchozích informací, navrženo řešení všech zmíněných problémů, s ohledem na požadavky společnosti.

Abstract

This thesis deals with analysis of company's MBG, spol. s r.o. problems, following with teoretical basis for these problems and in the end, it suggests the solutions. These problems are insufficient monitoring, any of used technology are old and absent of any information security management system. The first part is focused on a teoretical basis for the described problems, the second part will completely analyze all mentioned problems of a company. Final part will contain a solution for every company's problem, based on theory and analysis with taking care about company's demand too.

Klíčová slova

Datová síť síť, CCTV, kamerový systém, terminály, systém řízení bezpečnosti informací, ISMS, stará technologie, server, záznamová zařízení, NVR

Keywords

Data network, CCTV, monitoring system, terminals, Information Security Management Systém, ISMS, old technology, server, digital video recorder, NVR

Bibliografická citace

LUKEŠ, P. *Implementace nových koncových uzlů do firmy a jejich management.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2016. 92 s. Vedoucí diplomové práce Ing. Viktor Ondrák, Ph.D..

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/200 Sb., o právu autorském a o právech souvisejících s právem autorským)

V Brně dne xx.května 2016 …….

Pavel Lukeš

Poděkování

Tímto bych rád poděkoval Ing. Viktoru Ondrákovi, Ph.D. za cenné připomínky při tvorbě této práce, jeho odborné vedení a také čas, který při strávil formováním mé práce do této podoby.

Obsah

Úvod

V dnešní době, kdy je vývoj technologií znát téměř každý nový den, jsou dnes nasazené technologie velmi brzo zastaralé, avšak z hlediska funkčnosti ve většině případů stále vyhovující. Pokud však je technologie neměnná 10 let a více, jak se děje například ve starším objektu společnosti MBG, spol. s r.o., je tento technický dopad velmi znatelný na fungování celé společnosti. (4)

Dalším potřebným aspektem v dnešní době, na který je třeba brát v zřetel, je informační bezpečnost. Nestačí IT techniku a vše okolo s ní spojené jen používat, nýbrž i chránit. Při jakékoliv absenci ochrany v rozsáhlém a moderním systému se totiž celý systém vystavuje velmi vysoké hrozbě ze strany útočníků, kteří mohou, ale i nemusí mít za svůj cíl oslabení společnosti na trhu či její úplnou likvidaci. Skrze nechráněný přístup k citlivým datům není tento záměr zcela nereálný, proto je v dnešní době na informační bezpečnost organizací kladen stále vyšší důraz. Jistá úroveň se již stala standardem a až na výjimky ve formě poměrně stále početných řad malých podniků, se jakákoliv absence systému řízení bezpečnosti informací v podniku stala spíše výjimkou, jak pravidlem. (7), (9)

Cíl a metodika práce

Cílem této diplomové práce je vytvoření návrhu řešení poměrně široké škály problémů, které společnost MBG, spol. s r.o. v posledních měsících zaznamenává. Organizace má problém s nedostatečným monitoringem, zastaralou technologií docházky a absencí tak, v tomto směru, jakékoliv kompatibility a „synchronizace“ mezi svými dvěma objekty. Při řešení otázky fyzické bezpečnosti (monitoringu) by také ráda vyřešila i otázku informační bezpečnosti, která na staré hale aktuálně chybí.

V první části budou představena veškerá teoretická východiska, která budou základem pro navržení řešení všech problémů popsaných v analýze současného stavu.

Ve druhé části práce tedy budou hlouběji analyzovány všechny problémy, které společnost trápí, včetně popisu stávajícího vybavení, náčrtu půdorysu (skrze vyšší přehlednost), kde se daná zařízení nachází a také úrovně aktuálního informačního zabezpečení organizace.

V závěrečné části se práce bude věnovat řešením veškerých problémů zmíněných v analytické části práce, které bude vypracovávat na základě teoretických poznatků z teoretické části. Navržená řešení budou samozřejmě respektovat v maximální možné míře požadavky společnosti, která v daném objektu působí.

1. Teoretická východiska

1.1 Komunikační sítě

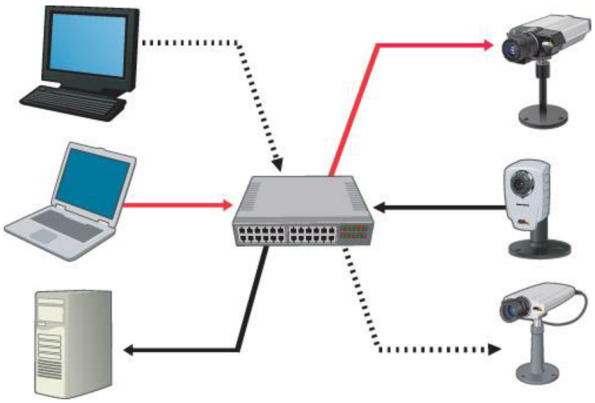
Počítačové sítě standardně dělíme na 3 typy a to na LAN, MAN a WAN. Rozdíly mezi jednotlivými druhy nejsou v počtu připojených stanic, ale v rozloze, na které se tyto sítě rozprostírají. V dnešní době se však rozdíly mezi jednotlivými druhy pomalu stírají, jak jsou jednotlivé druhy sítí vzájemně čím dál více propojovány, společně s neustálým vývojem nových technologií. (1)

1.1.1 LAN

Lokální počítačová síť LAN (Local Area Network) je termín používaný pro stanice umístěné ve vzájemné blízkosti (geograficky, zpravidla do 1km), které jsou vzájemně propojeny v jednotně adresovaném segmentu – všechny stanice v této síti mají IP adresy ze stejného intervalu hodnot (např.: 192.168.1.xxx). Komunikace na tomto druhu sítě probíhá, oproti ostatním zmíněným druhům, nejrychleji. (6)

Sítě LAN mohou mít různou topologii (Ring, Star, Bus,…) a stanice v této síti jsou nejčastěji spojovány pomocí aktivních prvků, které nepoužívají tzv. routing – swich, hub nebo bridge. Patří tak mezi nejjednodušší a zároveň nejbezpečnější typ sítě (absence komunikace s vnějším světem). (6)

Tento typ sítí se používá jako domácí počítačové sítě, podnikové sítě, ve školách, úřadech apod., do definice sítě LAN však spadají už i 2 vzájemně propojené stanice například pomocí kabelu. (1)

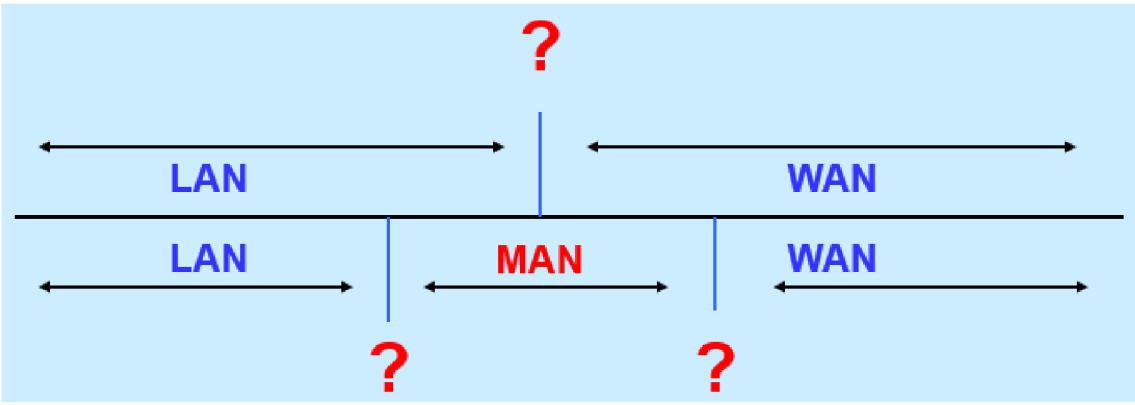


Obrázek 1: Síť typu LAN (Vlastní zpracování)

1.1.2 MAN

Metropolitní síť (Metropolitan Area Network) je prostředníkem mezi sítěmi LAN a WAN, geograficky se rozprostírá na území měst, obcí, univerzitních kampusů apod. (4)

Jelikož však není stanovena přesná hranice, kde MAN začíná a končí, nebudu se tímto typem sítě v práci podrobněji zabývat.

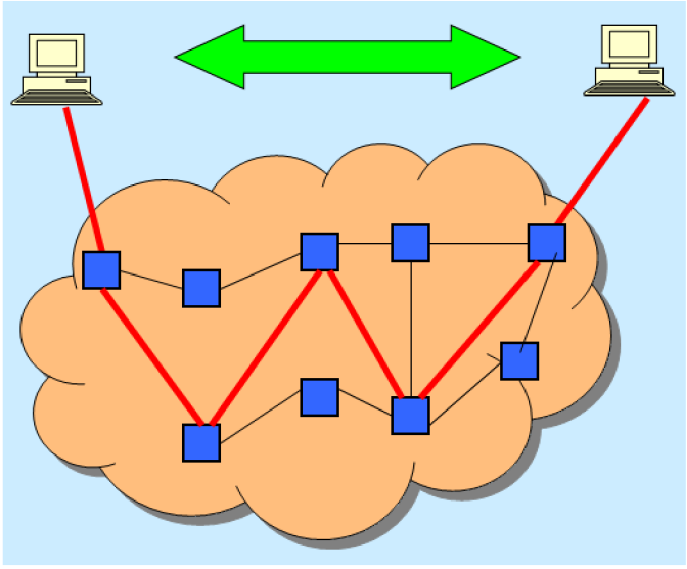


Obrázek 2: Síť typu MAN (6)

1.1.3 WAN

Geograficky nejrozsáhlejším druhem sítě je síť typu WAN – Wide Area Network. Logicky si tuto síť můžeme představit jako síť, která spojuje sítě typu LAN (případně MAN). Komunikace v síti tohoto typu probíhá s nižší rychlostí, vyšším zpožděním a jednotlivé komunikující uzly se „nevidí“ – většinou nejsou propojeny přímou cestou, ale spíše přes nižší či vyšší počet dalších aktivních prvků. Takovýchto cest mezi uzly pak existuje celá řada – je zajištěn provoz (i za cenu nižších rychlostí a vyšší odezvy) mezi uzly i v případě poruchy některého aktivního prvku na nejkratší (neideálnější) cestě. To se děje pomocí STP (Spanning Tree Protocolu). (6)

S neustálým vývojem nových technologií se pak rozdíly v rychlostech a zpoždění mezi sítěmi LAN a WAN, jak již bylo zmíněno, neustále snižují. Cílem vývoje je dosáhnout stejných přenosových vlastností jako u sítě LAN a tím tak mezi těmito typy sítí eliminovat jakékoliv rozdíly. Příkladem celosvětové sítě WAN je síť Internet. (1)



Obrázek 3: Síť typu WAN (6)

1.2 CCTV (Closed Circuit Television)

Jelikož se v návrhu budou instalovat i nové IP kamery (CCTV), práce v této kapitole vysvětlí základní problematiku systému CCTV.

Systém CCTV je, jak již překlad zkratky napovídá, uzavřený televizní okruh, který funguje nezávisle na datové síti společnosti (analogové kamery). To přináší výhodu v momentě, kdy je datová síť nefunkční nebo napadena, v případě výpadku elektřiny je zde ale nevýhoda v nutnosti dalšího záložního zdroje energie – záložní zdroj UPS či dieselový agregát napojený na datovou síť tento okruh nepokryje. (3)

Systém CCTV se používá k monitorování důležitých částí organizace, ve kterých bývají velmi často fyzicky porušována pravidla či bezpečnost v organizaci osobami, kterými jsou u výrobních podniků ve valné většině zaměstnanci společností. U obchodních řetězců jsou pak těmito „narušiteli“ většinou zákazníci. (3)

Systém CCTV je tvořen těmito komponentami (19):

- **Kamery** – sledují požadované prostory a obraz těchto prostor je posílán skrze přenosové médium do zobrazovacích zařízení
- **Objektiv** – objektiv kamery je velmi důležitým parametrem při výběru kamer. Kvalita objektivu je přímo úměrná výsledné kvalitě vytvářeného obrazu a tudíž i možnosti na vytvářeném obrazu rozpoznat objekty či osoby
- **Zobrazovací zařízení** – obrazovky, na které je obraz přenášen (živě)
- **Kamerové přepínače** – dovolují zobrazit více kamerových obrazů na jednom zobrazovacím zařízení
- **Záznamová zařízení** – uchovávají obraz z kamer po určitou, organizací či legislativou danou dobu

Tento výčet je pouze základním výčtem komponent, který může CCTV systém obsahovat. Dále tak může být doplněn například o mikrofony, reproduktory, dálková ovládání apod. (19)

1.2.1 Kamery

Kamery jsou stěžejním prvkem CCTV systému, protože bez nich by nebylo možné využít princip celého CCTV systému – monitorovat prostor, ať už se jedná o prostory uvnitř budovy, či vně.

Obraz, který kamery vytvoří, je živě přenášen do zobrazovacích prvků a zároveň i do záznamových zařízení, pro možnost zpětného dohledání určité situace. V zobrazovacích zařízeních je pak obraz vyhodnocován buď za pomocí personálu (hlídač,…) nebo pomocí automatického softwaru, který může například v dobu, kdy by ve sledovaném prostoru neměl nikdo být upozornit vedení společnosti, bezpečnostní složky apod. V dnešních kamerách pak není problém mít i funkci nočního vidění, která funguje pouze za pomoci několika málo červených diod. Není tak nutné sledovanou oblast v případě pohybu osvětlovat velkým reflektorem. (3)

1.2.1.1 Analogové kamery

Jedná se o standardně používané kamery, které využívají jako přenosové médium napětí a proud v různých výškových hladinách, které jsou na zobrazovacích zařízeních jednoznačně identifikovány a převedeny na výsledný obraz. Tento obraz je limitován možnostmi formátu PAL. (3)

V dnešní době jsou velmi časté situace, kdy má organizace již z minulosti nainstalovány analogové kamery, výsledný obraz je ale vyžadován v digitálním formátu skrze lepší skladovatelnost a následnou práci se záznamem. V takových případech se informace o obrazu uloží na záznamové zařízení a následně se pomocí příslušného SW překonvertuje do digitální podoby. (3)

1.2.1.2 Digitální kamery

Digitální IP kamery pro svůj provoz mohou, ale nemusí používat datovou kabeláž objektu, ve kterém jsou nainstalovány. V případě samostatného okruhu je zajištěn provoz systému i při poruše primární datové lince, v opačném případě jsou ušetřeny náklady na

tvorbu tohoto celého okruhu. Skrze ušetřené náklady na samostatný okruh bývají v dnešní době vyhledávanější, než analogové kamery, skrze vyšší pořizovací cenu se však, v závislosti na typu a počtu kamer, mohou náklady vyšplhat na podobnou úroveň, jaká by byla v případě použití kamer analogových. (3)

Komunikace mezi jednotlivými prvky digitálního kamerového systému probíhá na základě protokolu TCP/IP, kdy každá z kamer má přiřazenou svoji vlastní IP adresu. Díky tomuto lze informace o obrazu přenášet i bezdrátově (wifi, bluetooth,…), což je výhoda oproti klasickému analogovému řešení. (3)

Výhody těchto typů kamer jsou: (3)

- Neomezené rozlišení
- Přístup odkudkoliv – díky vlastní IP adrese lze provést připojení na kameru přes internet
- Možnost využít stávající datové rozvody (kroucené páry)

1.2.1.3 Parametry

Při výběru kamer by nejdůležitějším aspektem výběru neměly být pořizovací náklady, nýbrž i vlastnosti, které kamera za danou cenu nabízí. Může se velmi lehce stát, že z levně pořízené kamery bude potřebný natolik nekvalitní, že nebude možné jej jakýmkoliv způsobem pro dané potřeby použít. Jelikož se jedná o komponenty zahrnující optiku, je dobré při výběru věnovat pozornost podobným parametrům, jakým je věnována pozornost například při výběru nového fotoaparátu: (19)

- Světelnost – schopnost rozpoznatelně zachytit objekt i v nižší světelné hladině
- Ohnisková vzdálenost – výrazně ovlivňuje úhel záběru, který je kamera schopna zachytit
- Možnost zoomu (digitální, optický) – optický zoom je vždy kvalitnější
- Rozlišení – důležitá vlastnost, přímo ovlivněná použitým čipem, u analogových udáváno v počtu TV řádků, u digitálních v počtu pixelů

- Poměr stran – výsledná velikost obrazu v poměru osy x ku y, v dnešní době nejčastěji širokoúhlé 16:9
- Čip – nejčastěji CCD nebo CMOS

1.2.1.4 Typy konstrukcí

Kamery můžeme podle typu konstrukce primárně dělit na interní a externí, kdy u každého tohoto rozdělení existuje nespočet dalších konstrukčních řešení. V rámci této práce budou uvedeny jen základní typy: (19)

- **Standardní** – tělo kvádrového tvaru doplněno o objektiv, ten je možné vyměnit
- **Kompaktní** – jako celek, nemodifikovatelné, včetně příslušenství pro montáž
- **Bezdrátové** – výhodou je nenutnost instalace datové kabeláže až ke kameře
- **Dome** – stropní kamery
- **Deskové** – většinou fungují jako skryté kamery díky malým rozměrům
- **Antivandal** – již dle názvu lze odvodit, že se jedná o kusy odolávající velkému mechanickému působení
- **PTZ** – otočné kamery, často schovány „v kopuli“ – není vidět, kterým se kamera „dívá“
- **S termovizí** – schopné zachytit tepelné záření např. lidského těla

1.2.2 Záznamová zařízení

Záznamová zařízení slouží pro uchovávání obrazu vytvořeného kamerami pro možnosti pozdějšího přezkoumání dění ve snímané oblasti. Tato doba je u každé organizace různá, v některých odvětvích jsou podniky nuceny držet záznamy po dobu určenou legislativou, v jiných pak je zcela na organizaci, jakou dobu si zvolí. V zásadě by však neměly být kamerové záznamy drženy déle jak několik dnů (ve velkých obchodních domech je například maximum 3 dny na základě zákona o ochraně osobních údajů – §2 zákona č. 101/200 Sb.) (15) (19)

Aktuálně nejčastěji používanými záznamovými zařízením pro analogové kamery jsou DVR (Digital Video Recorder). Tato záznamová zařízení ukládají obrazy vytvořené pouze analogovými kamerami, které ale po uložení překonvertují do digitálního formátu a poté znovu uloží na pevný disk. Pro digitální kamery nelze DVR použít skrze absenci ethernetových vstupů, proto je u digitálních kamer nutno použít NVR (Network Video Recorder), které jsou již ethernetovými vstupy vybaveny. Obě zmíněná zařízení ukládají výsledný obraz na pevné disky, které mohou být jak interní, tak externí, díky osazeným SATA konektorům. Na obě záznamová zařízení, DVR i NVR, je možné se připojit i z prostor mimo společnost přes síť internet, což starší záznamová zařízení, především analogových kamer (ukládání na pásky), neumožňovala. (3) (19)

1.3 Docházkové systémy

Docházkové systémy jsou v dnešní době tvořeny většinou čtečkou čipů / čipových karet, které jsou následně pomocí datové kabeláže organizace připojeny do switche, ke kterému je připojen i server. Na tomto serveru je pak nainstalováno jedno z mnoha možných dodavatelských řešení softwaru, které údaje z terminálů dokáže korektně zpracovat.

V rámci této práce nebude řešeno softwarové řešení docházkového systému, pouze fyzický návrh instalace jednotlivých terminálů, jejich připojení na datovou síť společnosti a následné propojení se serverem skrze switch v datovém rozvaděči (pouze docházkové terminály). (5)

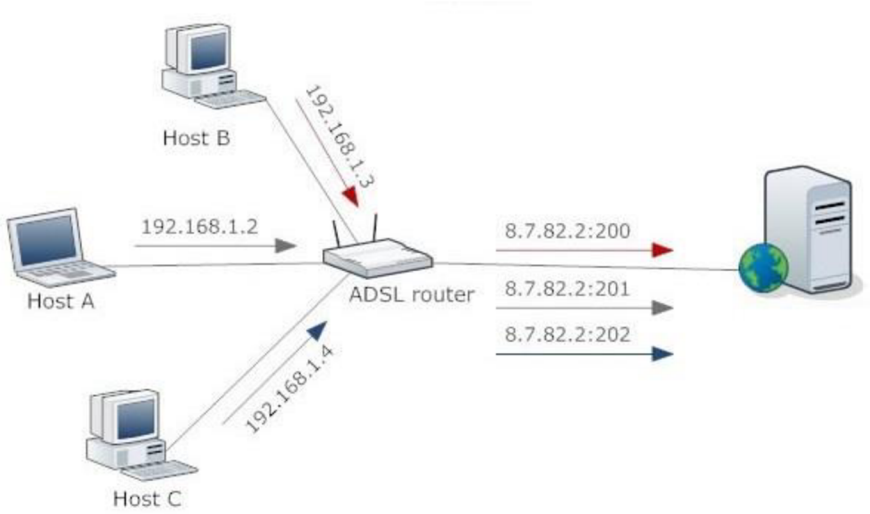
1.4 Informační bezpečnost

1.4.1 Základní pojmy

- **Aktivum (Asset)** – veškerý hmotný a nehmotný majetek organizace, v rámci ISMS to pak mohou být data, HW, SW, apod. (8)
- **Bezpečnost informací** - jedná se o kombinací 3 následujících částí: (8)
    - **Dostupnost (Availability)** – zajištění přístupu v době potřeby
    - **Důvěrnost (Confidentionality)** – zajištění přístupu pouze oprávněným osobám. Oprávnění osoby získají na základě autentizace a následné autorizace
    - **Integrita (Integrity) - zajištění správnosti a úplnosti informací.**
- **Zranitelnost -** slabé místo aktiva, které může být napadeno. (8)
- **Hrozba –** potenciální událost, která využívá zranitelnosti a následně má určitý dopad. V rámci ISMS to může být například ztráta citlivých dat (8)
- **Riziko** – míra pravděpodobnosti naplnění hrozby. Zpravidla generuje ztrátu. (8)
- **Bezpečnostní událost –** promítnutí hrozby do reality (8)
- **Bezpečnostní incident** – bezpečnostní událost s kritickým dopadem na organizaci (8)

1.4.2 Informační bezpečnost obecně

Se stále vyšší mírou používání informačních technologiích, ať už pro osobní účely či ve firmách/organizacích pro účely pracovní, nabývá pojem Informační bezpečnost na stále větším významu. Především u běžných uživatelů, a v mnoho případech i u menších firem, bývá tento pojem často spojen pouze s instalací antivirového SW, využitím systémového firewallu, případně „skrytím“ celé sítě pomocí routeru podporujícího NAT (Network Address Translation). Firewall na tomto routeru již takovou samozřejmostí nebývá. (8)



Obrázek 4: Skrytí sítě pomocí funkce NAT na routeru (Vlastní zpracování)

Tato opatření sice přispívají k vyšší bezpečnosti provozu na dané síti, v rámci pojmu Informační bezpečnost se však jedná pouze o část zabezpečení. Pojem samotný zahrnuje mnohem širší portfolio věcí zajišťujících bezpečnost, ať už se jedná o další bezpečnostní prvky (např. již zmíněný firewall), ochrana proti ztrátě informací (zálohování), chování uživatelů na síti (školení o bezpečnosti apod.), předcházení rizik, efektivní řešení bezpečnostních incidentů apod. Celý tento systém se souhrnně nazývá Systém řízení bezpečnosti informací – ISMS. (8)

1.4.3 Systém řízení bezpečnosti informací (ISMS)

1.4.3.1 Důvody zavedení ISMS

Důvodů pro zavedení informační bezpečnosti je poměrně široká škála a určitě je nelze brát na lehkou váhu. Tyto důvody mohou, v případě úspěšného napadení, stát firmu nejen její know – how, ale také pozici na trhu nebo minimálně náklady na obnovu do původního stavu. (14)

Obrázek 5: Ilustrace úrovně zabezpečení IT/IS po úspěšném zavedení ISMS (Vlastní zpracování)

- **Know-how** – odlišení společnosti od konkurence, jedná se o soubor znalostí a pracovních postupů získaných dlouhodobým působením firmy na trhu. Při zpronevěření ztrácí firma velkou část své jedinečnosti a jen těžko ji získává zpět. (14)

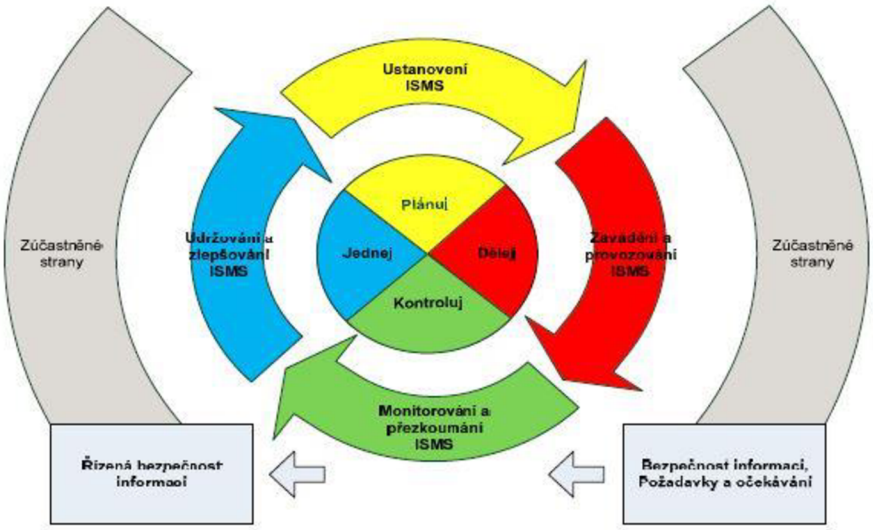
- **Zákony** – v dnešní době již prakticky v každém vyspělém státu existuje zákon o ochraně osobních údajů, který musí společnost podnikající v daném státě ctít. V ČR tento zákon definuje povinnost - *„Správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům...“* (Zákon č. 101/2000 Sb.) (14)

- **Marketing** – díky úspěšnému zavedení ISMS je společnost certifikována na základě normy ISO/IEC 27001. Při uvedení této certifikace do propagačních materiálů pak firma působí důvěryhodněji. (14)

1.4.3.2 Fáze ISMS

Principem celého ISMS je tzv. Demingův modelu (PDCA cyklus), jehož fáze se v ISMS nazývají následovně: (7)

- **Ustanovení ISMS** – v první řadě je potřeba získat souhlas od vedení společnosti s nasazením ISMS. Norma (ISO 27001) tento souhlas požaduje, protože ISMS by mělo být vždy zaváděno stylem „shora dolů". Po získání souhlasu je třeba ustanovit přesný rozsah ISMS, stanovit jasné zadání a vybrat nutná opatření na základě analýzy rizik a jejich ohodnocení.
- **Zavádění a provoz ISMS** – ve druhé fázi se bezpečnostní opatření z první fáze prosazují do chodu firmy
- **Monitorování a přezkoumání ISMS** – třetí fáze je z hlediska zlepšování stávajících řešení nejdůležitější. Jde o zpětnou vazbu na základě monitorování již aplikovaných řešení. Pokud zjištěná data z monitoringu správně interpretujeme, jsme k nim schopni v následující fázi přiřadit i adekvátní opatření, které účinnost celého ISMS následně zvýší.
- Ú**držba a zlepšování ISMS** – v poslední fázi cyklu postupujeme na základě dat získaných z monitoringu v předchozí fázi. Buď můžeme odstraňovat zjištěné slabiny, nebo stávající řešení nadále vylepšovat, aby lépe splňovaly zadané požadavky.



Obrázek 6: ISMS v modelu PDCA (7)

PDCA cyklus, vytvořil Edwards Deming, který byl průkopníkem v managementu na poli postupného zlepšování kvality, ať už vyráběných výrobků, či nabízených služeb. PDCA cyklus tedy není vázaný pouze k ISMS, ale je využitelný v mnoha různých tržních odvětvích. Historickým příkladem může být situace, kdy Edwards Deming pomohl po II. světové válce Japonsku v hospodářské obnově právě pomocí uvedení PDCA cyklu do praxe. Na základě úspěchů demingova modelu v Japonsku byl pak tento systém převzat do podniků v celém světě skrze velké množství tržních odvětví. Metoda PDCA cyklu je založena na 4 základních činnostech, které plně korespondují s jednotlivými fázemi ISMS: (7) (9)

- PLAN (plánuj)
- DO (dělej)
- CHECK (kontroluj)
- ACT (jednej)

1.4.3.2.1 Fáze PLAN

V ISMS je tato fáze zastoupena „Ustanovením ISMS“. Nejprve je nutné získat souhlas organizace, protože tato změna by měla být zavedena organizačně „shora“ a také proto, že stojí nemalé finanční a lidské prostředky na zavedení, i na následnou certifikaci. (9)

Po získání souhlasu je třeba definovat rozsah ISMS, stanovit jasné zadání (co se od zavedení očekává), vytvořit analýzu rizik a na základě výsledků analýzy pak vybrat příslušná opatření. (7)

Fáze PLAN má, z pohledu celého PDCA cyklu, největší vliv na veškeré jeho další fáze, stejně tak jako fáze check, která je velmi důležitá pro určení správného směru zlepšení stávajících řešení. (7)

1.4.3.2.2 Fáze DO

Druhá část PDCA cyklu je v rámci systému řízení bezpečnosti informací zastoupena fází Zavádění a provozování ISMS a jsou zavedena veškerá opatření na rizika, která jsme zjistili v analýze rizik z předchozí části. Činnosti nutné pro správný průběh celé fáze: (7)

- Vytvořit plán zvládání rizik a začít ho zavádět do prostředí firmy.
- Po zavedení veškerých opatření vytvořit příručku bezpečnosti informací dle normy ČSN ISO/IEC 27002.
- Začít vytvářet bezpečnostní povědomí všech uživatelů
- Zvolit způsob, jakým budeme účinnost zavedených opatření hodnotit.
- Zavést systémy rychlé detekce nově vzniklých bezpečnostních incidentů – nejčastěji pomocí monitoringu. Dále pak vytvořit soubor postupů, jak vzniklé bezpečnostní incidenty co nejrychleji a nejefektivněji řešit.
- Řídit zdroje, dokumenty a záznamy pro monitorovací fázi check
    - Vytvořit pravidla pro tvorbu, schvalování a distribuci dokumentace
    - Již neplatné verze dokumentů vyřadit
    - Provádět záznamy o veškerých provedených úkonech

1.4.3.2.2.1 Plán zvládání rizik (plán opatření)

Jedná se o dokument, ve kterém jsou uvedeny veškeré činnosti ISMS a jejich priority, omezující faktory, potřebné zdroje či odpovědné osoby, které jsou nezbytné pro zavedení veškerých požadovaných opatření. Z výše uvedeného tedy vyplývá, že plán opatření nezůstává neměnný, ale je vždy aktualizován při zjištění nových skutečností (při průběhu nového cyklu). (8)

Plán zvládání rizik se na počátku vytváří podle podkladů organizace, později na základě podnětů a zkušeností získaných zaváděním a postupným vylepšováním ISMS. (8)

1.4.3.2.2.2 Příručka bezpečnosti informací

Příručka bezpečnosti informací je soubor dokumentů, který obsahuje bezpečnostní principy, pravidla, zásady a odpovědnosti všech bezpečnostních opatření. Součástí této příručky je i plán zvládání rizik. Soubor dokumentů bezpečnosti informací je připravovány v různých úrovních: (8)

- Na **nejvyšší úrovni** jsou dokumenty potřebné pro systém řízení organizace, společně s požadavky ISMS – rozsah, politika, hodnocení rizik, prohlášení o aplikovatelnosti, plán zvládání rizik apod.
- Na **druhé úrovni** se jedná o seznam všech potřebných procesů a postupů, včetně toho, kdo, kdy a kde je má vykonat.
- **Nejnižší úroveň** není vždy nutná, jedná se především o postupy, pomocí kterých dosáhneme procesů popsaných ve druhé úrovni

1.4.3.2.2.3 Prohlubování bezpečnostního povědomí

Prohlubování bezpečnostního povědomí znamená zajistit, aby všichni uživatelé IT prostředků v organizaci získali povědomí o bezpečnosti svého chování při práci s těmito prostředky. Toto povědomí je získáváno především na bázi nejrůznějších školení, které

má za cíl toto povědomí předat a eliminovat tak největší hrozbu pro firmu skrze IT prostředky – uživatele samotného. (8)

1.4.3.2.2.4 Měření účinnosti ISMS

Měření účinnosti ISMS je velmi důležitou částí celého ISMS, na které pak závisí jakékoliv další zlepšování již zavedeného systému. Je potřeba monitorovat správné údaje, které nejvíce vypovídají o reálném přínosu zavedení systému řízení bezpečnosti informací v organizaci. Pokud sledujeme objektivní údaje, můžeme i objektivně posoudit, jestli jsou daná opatření efektivní, nebo je nutné je patřičně upravit. (8)

Velmi důležité kroky pro měření účinnosti se nachází již ve fázi Ustanovení ISMS. V této části probíhá analýza rizik a na základě její kvality se pak odvíjí i celková účinnost zaváděného ISMS. Chyby v případné špatné specifikaci a jejich dopad, vyjádřený ve formě nákladů na odstranění těchto chyb, je vyjádřen v tabulce níže: (7)

Tabulka 1: Vliv chybné analýzy rizik na jednotlivé fáze ISMS (7)

Etapa PDCA modelu	*Výše relativních nákladů v %*
Plan	*1,0*
Do	*6,5*
Check	*15,0*
Act	*100,0*

Ve fázi DO nestačí pouze zavést vybraná opatření, ale také integrovat systém pro monitorování účinnosti těchto opatření. V rámci monitorování je pak možné sledovat finanční, personální či technické ukazatele. (8)

Většina organizací, má ve velké oblibě sledovat finanční ukazatele, jejich vypovídací schopnost objektivně zhodnotit danou problematiku je však velmi omezená, protože je obtížné určit, které finance byly použity na provoz podniku, a které na zavedení systému bezpečnosti informací. Vypovídací hodnota těchto ukazatelů je také přímo závislá na lidech, kteří tyto ukazatele vykazují - např. při vzniku bezpečnostního incidentu a

následné kalkulaci ztrát, bývají do kalkulace zahrnuty pouze přímé náklady (ztrácená data, know – how, výrobní dokumentace apod.), kdežto náklady na práci všech lidí, kteří se na odstranění bezpečnostního incidentu podílejí, velmi často nebývají zahrnuty. Vypovídající hodnota bezpečnostních incidentů tak při hodnocení z čistě finančních ukazatelů bývá často nevědomě snížena. (8)

Odlišné bezpečnostní incidenty vyžadují sledování odlišných ukazatelů, včetně odlišné četnosti jejich aktualizování. Nejdůležitější je sledovat ukazatele v kategorii krizové řízení, které je vhodné vyhodnocovat ze všech nejčastěji – denně či týdně. (7) (8)

Tabulka 2: Schéma ukazatelů (7)

<table>
<tr><td rowspan="2">Význam</td><td>Vysoký</td><td><u>Krizové řízení</u>
Indikátory hrozeb
Detekce průniků do systému</td><td><u>Strategické plánování</u>
Řízení pomocí rozpočtu
Alokace zdrojů
Soulad s požadavky řízení aktiv</td></tr>
<tr><td>Nízký</td><td><u>Operativní řízení</u>
Ochrana proti škodlivým programům
Řízení sítí
Řízení bezpečnosti
Údržba/správa</td><td><u>Taktické plánování</u>
Řízení zdrojů
Ukazatele pro řízení životního cyklu vývoje aplikací
Analýza auditních a logovacích záznamů</td></tr>
<tr><td colspan="2" rowspan="2"></td><td colspan="2">Frekvence měření</td></tr>
<tr><td>Vysoká</td><td>Nízká</td></tr>
</table>

U volby ukazatelů se můžeme řídit radou **méně je více** – zvláště ze začátku zavádění ISMS může být snaha podchytit veškerá rizika kontraproduktivní. Lepší je soustředit se na začátku pouze na klíčové problémy ohrožující činnost firmy, ostatní pak přidat později v rámci zlepšování, až bude mít implementační tým dostatek zkušeností. Také snaha zavést opatření na všechna zjištěná rizika není vhodná, protože při určité míře zabezpečení je jakákoliv další přidaná hodnota zabezpečení minimální, avšak vykoupená astronomickými náklady. (8)

1.4.3.2.3 Fáze CHECK

Fáze Check se v systému řízení bezpečnosti informací nazývá Monitorování a přezkoumávání ISMS. V této části je nedůležitějším bodem získání komplexní zpětné vazby ze všech zavedených opatření v předchozí fázi a následné porovnání, zdali splňují očekávané požadavky. Porovnávání probíhá ze strany nadřízených odpovědných osob za dané činnosti (popsáno v plánu zvládání rizik), či manažera celého zavádění ISMS do prostředí organizace. Další porovnávání splnění požadavků jsou prováděna pomocí interních auditů, které by měly být na projektu zavádění ISMS nezávislé. Výsledky tohoto měření jsou poté porovnány vrcholným vedením společnosti s požadovaným stavem a následně je rozhodnuto, které činnosti budou, a jakým způsobem, modifikovány. (7)

Kontroly ze strany vrcholového managementu probíhají ve valné většině případů jednou ročně, u nově zavedeného ISMS je však roční interval příliš dlouhý a tak by měl být výrazně kratší, aby bylo možné ISMS vylepšovat operativně. Porovnávání výkonnosti probíhá na základě silných a slabých stránek ISMS, ke kterému je velmi vhodná SWOT analýza. Mezi výstupy této analýzy by nemělo chybět: (7) (9)

- Zlepšení účinnosti ISMS (nová požadovaná míra zlepšení účinnosti vs. klesající náročnost na zavedení se získáváním potřebných zkušeností)
- Nová analýza rizik, včetně jejich ohodnocení a zapsání do příslušných dokumentů
- Seznam všech procesů, které bude nutné pro zlepšení účinnosti ISMS upravit
- Ohodnocení změn v ISMS v přímé vazbě na zdroje (finanční, lidské, technologické)

1.4.3.2.4 Fáze ACT

Fáze Act se v systému řízení bezpečnosti informací nazývá „Údržba a zlepšování ISMS“. V této části jde o udržení nebo zlepšení stávajícího stavu ISMS na základě dat z monitoringu, který proběhl v předchozí fázi. Je však třeba zdůraznit, že zejména ve stavu, kdy je již ISMS nějakou dobu zavedeno, je pravděpodobně dosaženo bodu tzv. přiměřené bezpečnosti, a proto více než snaha systém vylepšit zde bude probíhat snaha systém udržet ve stávajícím stavu. (7) (9)

Ve fázi Act by měly proběhnout tyto činnosti: (7) (9)

- Zavést nová opatření pro zlepšení ISMS
- Revidovat stávající opatření

1.4.3.2.4.1 Soustavné zlepšování ISMS

Soustavné zlepšování je jedna z nejdůležitějších částí ISMS a i základním principem PDCA cyklu. Díky systému soustavného zlepšování není nutné podchytit veškeré požadované problémy hned na počátku, ale rozprostřít tyto opatření do více „cyklů“. Zavedení daných opatření bude díky tomu, velmi pravděpodobně, pečlivější a efektivnější, než při snaze pochytit vše na začátku. Na počátku zavádění by měla být věnována pozornost pouze rizikům, jejichž dopad je na činnost podniku kritický. (14)

1.4.3.2.4.2 Odstraňování nedostatků ISMS

Odstraňování nedostatků ISMS můžeme provádět pomocí dvou různých opatření: (14)

- Opatření odstraňující nedostatky ve stávajícím řešení
- Opatření preventivní

Opatření, která odstraňují zjištěné nedostatky ve stávajícím řešení je nutno řešit v co nejkratší době, jedná se nejen o zjištěné vady v systému, nýbrž i o vady projevené. (14)

Naproti tomu opatření preventivní je formou prevence do budoucna – chyby v systému sice zjištěny byly, doposud se však neprojevily. Při zvažování těchto druhů opatření je nutné porovnat míru dopadu na činnost organizace s náklady na zavedení opatření. Pokud náklady převyšují, riziko bývá akceptováno. (14)

U obou výše zmíněných opatření se však jedná až o řešení následků příčin. Je tedy velmi vhodné zjistit i příčiny, které k těmto nedostatkům vedly, ať už se jedná o chybně nastavená pravidla na začátku ve fázi PLAN, chybně zavedené řešení či chybně interpretovaná data z monitorování. Zjištění příčin těchto chyb je velmi cennou informací z hlediska potenciálního se opakování v budoucnu napříč celým zavedeným ISMS. (14)

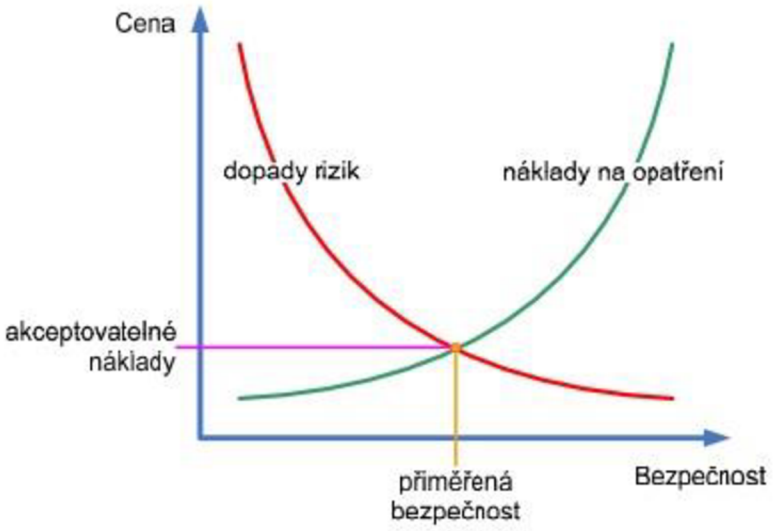
1.4.3.3 Náklady na zavedení informační bezpečnosti

Náklady na zavedení informační bezpečnosti mohou být ve formě financí, informací, personálu či pořízeného materiálu. Dále je tako potřeba mít jisté know-how, jak informační bezpečnost v podniku zavést, protože se nejedná o jednoduchý proces. (14)

Obrázek 7: Náklady vs. přínosy (Vlastní zpracování)

Určení hodnoty nákladů také není zcela jednoduché. Je zcela jasné, že s rostoucími náklady bude růst i úroveň bezpečnosti, avšak tento růst není vzájemně rostoucí, ale spíše odpovídá pravidlu o klesajícím mezním užitku – s dodatečnou jednotkou nákladů se přidaná hodnota bezpečnosti neustále snižuje. V extrémních případech tak při vynaložení neúměrně vysokých nákladů dostaneme jen nepatrné zlepšení bezpečnosti. (7) (14)

Odpovědí na otázku, kolik nákladů je výhodné vynaložit na ISMS je tzv. **přiměřená bezpečnost**. Přiměřená bezpečnost je výsledkem protnutí nákladové křivky na jednotlivá opatření s křivkou hodnot dopadů rizik na činnost společnosti. V bodě, kde se křivky setkávají, se nachází bod, za kterým již na každé další opatření bude potřeba vynaložit vyšší náklady, než na odstranění případných následků bezpečnostního incidentu z daného rizika. Investice do bezpečnosti se již od této míry zabezpečení nevyplácí. (7)



Obrázek 8: Přiměřená bezpečnost (7)

Cílem informační bezpečnosti není eliminovat veškeré potenciální hrozby, to je v dnešní době nereálné, ale najít rovnováhu mezi vloženými náklady a jistou mírou ochrany před bezpečnostními incidenty. Tuto rovnováhu (a následné sestavení grafu) můžeme určit na základě porovnání finančního dopadu všech potenciálních rizik s výší nákladů na opatření, které je proti těmto rizikům třeba zavést (14)

1.4.3.4 Metodiky pro ISMS

Jelikož je informační bezpečnost poměrně rozsáhlé téma, které se navíc velmi úzce prolíná se všemi odděleními podniku, které nějakým způsobem využívají IT prostředky firmy, jedná se komplexní problematiku, ve které se jednotlivec jen složitě orientuje. Z tohoto důvodu vznikly nejrůznější metodiky, návody, normy apod., které orientaci v této problematice velmi výrazně pomáhají. (14)

Obrázek 9: Důvod existence metodik – pracovní postupy (Vlastní zpracování)

Tyto materiály vznikly na základě praktických zkušeností, a jsou i v dnešní době postupně aktualizovány, jak postupuje vývoj nových technologií. (14)

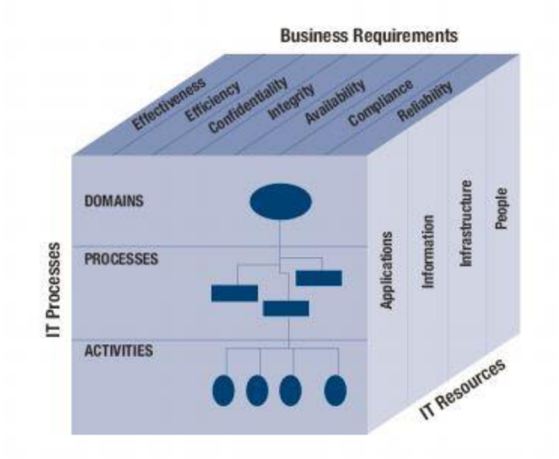
- **ITIL (Information Technology Infrastructure Library)** – jedná se o soubor postupů, konceptů a nejrůznějších doporučení, které jsou prověřené v praxi a které umožňují efektivnější plánování, využívání a zkvalitňování používání IT technologií jak ze strany zákazníků, tak i ze strany dodavatelů IT služeb. Tato knihovna začala vznikat v roce 1980 kvůli požadavku ze strany britské vlády zefektivnit stávající úroveň poskytování IT služeb. V době vzniku se jednalo o 46 knih s doporučeními z praxe. Později, v letech 2000 – 2004 byl ITIL přepracován na verzi 2, označovanou jako ITIL V2, která byla ještě v roce 2007 rozšířena o třetí verzi, značenou jako ITIL V3. V roce 2011 pak byly ve verzi 3, oproti původní verzi, realizovány změny především ve sjednocení osnovy všech obsahovaných knih, a tudíž tak došlo k celkovému zlepšení orientace ve všech 5 ústředních knihách. Verze 2 pak byla ukončena právě s přepracováním verze 3 v roce 2011. ITIL se zaměřuje především na procesní řízení organizace a je tak tudíž určen pro střední a vyšší management. (7)

Obrázek 10: Princip fungování souboru postupů ITIL (14)

- **COBIT** (**Control Objectives for Information and Related Technology**) – Framework vytvořený mezinárodní asociací ISACA v roce 1996 pro tzv. IT Governance (správa a řízení informačních prostředků). Od doby vzniku již byl tento framework (nebo také metodika) několikrát upravován, až do současné verze, která se nachází ve verzi COBIT 5. Pomocí COBITu by měly být organizace schopny dosáhnout svých strategických cílů, za efektivního využití IT zdrojů a minimalizace IT rizik. (7)

  Princip frameworku COBIT je založen na tzv. COBIT kostce, ve které jsou zaneseny 3 základní směry: (7)

  - Business Requirements (požadavky bussinessu nebo také strategie firmy)
  - IT Processes (IT procesy)
  - IT Resources (IT Zdroje)



Obrázek 11: COBIT kostka (8)

COBIT je komplexnější než ITIL, ITIL je však v určitých oblastech o poznání podrobnější. (14)

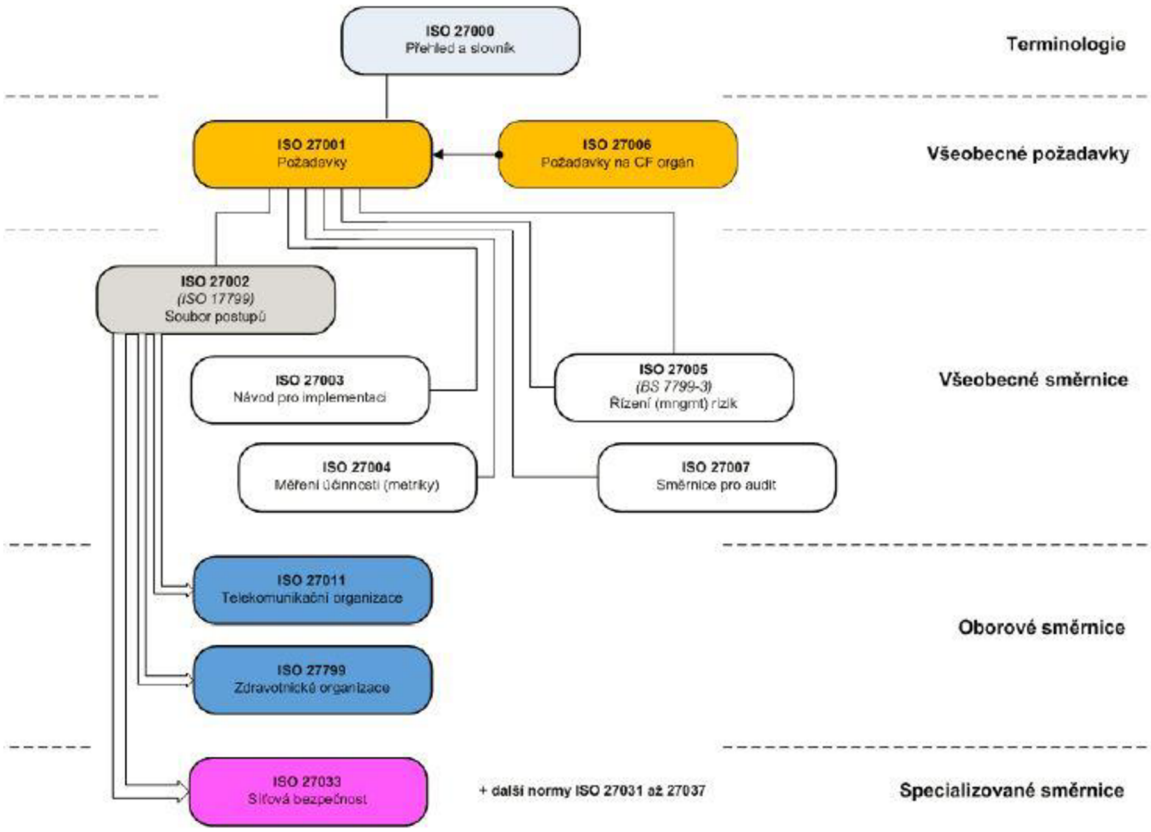
- **Common Criteria (společná kritéria, zn. CC)** – jedná se o mezinárodní standard ISO/IEC 15408, díky kterému je prováděna certifikace IT bezpečnosti. Cílem CC bylo vytvořit kvalitní a především respektovaný systém hodnocení IT bezpečnosti, který dává jistotu, že hodnocení IT bezpečnosti bude prováděno přísným a standardizovaným způsobem.
  Díky CC dochází také ke zvyšování efektivity a snižování nákladů na certifikaci, jelikož se zaměřují na použití určitých norem a snížení rizika duplikování jejich určitých částí (např. duplikování bezpečnostních prověrek).
  CC vznikly ze standardů ITSEC, CTCPEC a TCSEC a aktuálně se nachází ve verzi 3.1. (7)

1.4.3.5 Normy pro ISMS

Historie dnešních norem je datována od roku 1995, kdy ve Velké Británii vznikla britská norma BS7799, vytvořená dle nejlepších zkušeností lidí ze souvisejících oborů. Jelikož byla tato norma na velmi vysoké úrovni, co se zpracování týče, velmi rychle se začala používat v organizacích po celém světě pro zabezpečení firemních procesů a také pro zajištění dostupnosti, důvěrnosti a integrity uchovávaných dat. Tato norma tak představuje kompletní soubor návodů, metodik, postupů apod. pro problematiku

bezpečnosti informačních systémů, ať už se jedná o odhalování hrozeb, identifikaci a hodnocení rizik či následného návrhu opatření. V roce 2000 byla tato norma přepracována mezinárodní organizací ISO na normu ISO/IEC17799 a v roce 2005 pak zařazena do skupiny norem ISO 27000. (8)

1.4.3.5.1 Normy řady 27000



Obrázek 12: Dělení normy ISO 27000 (7)

Pro potřeby práce budou dále rozebrány následující normy:

- ČSN ISO/IEC 27001, ČSN ISO/IEC 27002, ČSN ISO/IEC 27004, ČSN ISO/IEC 2005

1.4.3.5.2 ČSN ISO/IEC 27001 Systémy managementu bezpečnosti informací – Požadavky

Tato norma má svého původce v normě ISO/IEC 27001:2005, liší se od ní jen tím, že je přeložena do českého jazyka. Svým vznikem pak nahrazuje starší normu ČSN BS 7799-2 která byla vydána v prosinci 2004. (2)

Norma ISO/IEC27001 vznikla skrze potřebu podpory ustavení, zavádění, provozování , monitorování, udržování a zlepšování systému managementu bezpečnosti informací (Information Security Management Systém – tzv. ISMS). Přijetí ISMS by mělo, v ideálním případě, přijít shora ve formě strategického rozhodnutí organizace. Samotný návrh, včetně zavedení ISMS je pak v organizaci podmíněn potřebami, business cíli, požadavky na bezpečnost, aktuálními procesy, velikostí a strukturou každé organizace individuálně. (2)

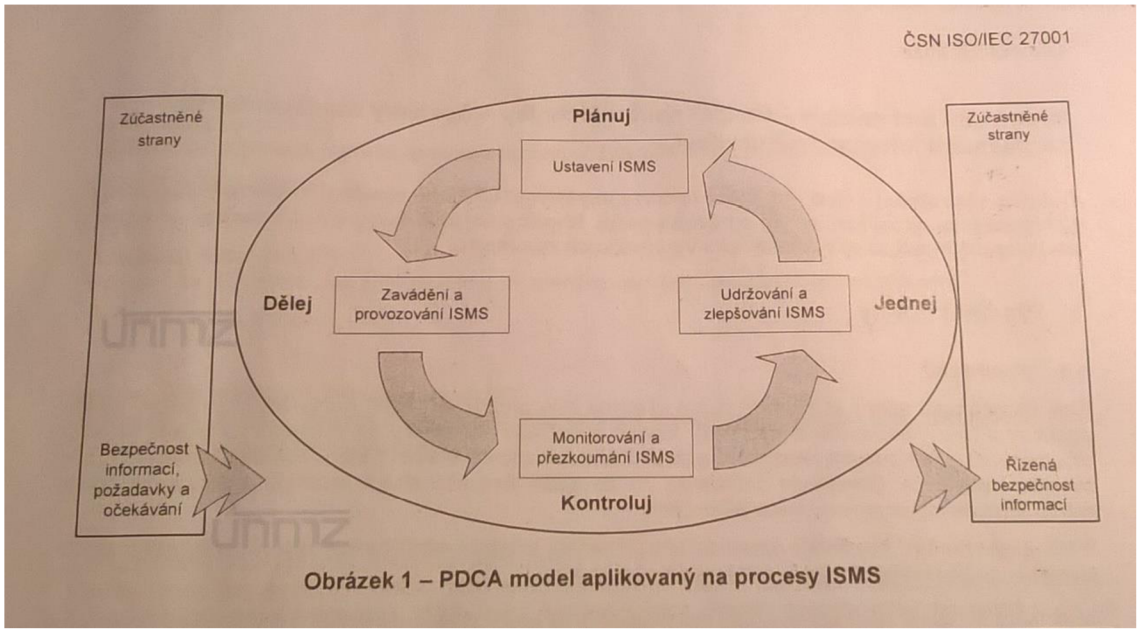
Pro efektivní fungování organizace je potřeba identifikace a následné řízení velkého množství vzájemně propojených činností. Činnost, která využívá zdroje a přeměňuje vstupy na výstupy, je možné považovat za proces. Aplikaci těchto procesů, společně s jejich identifikací, vzájemným působením a řízením pak v organizaci označujeme jako procesní přístup. (2)

Použití procesního přístupu pro ISMS podle této normy klade důraz na (viz. obr. 13): (2)

1. Pochopení požadavků, stanovení politiky a cílů bezpečnosti informací v organizaci
2. Zavedení a provozování ISMS v kontextu s řízením celkových rizik činností organizace
3. Monitorování stávající situace, zkoumání účinnosti zavedených opatření
4. Zlepšování ISMS na základě předchozího kroku

Norma ČSN ISO/IEC27001 je vzájemně propojena s normou ISO 9001:2000 a normou ISO 14001:2004 v takové míře, aby bylo podpořeno konzistentní a jednotné zavedení a provoz těchto norem. Jediný vhodně navržený ISMS tak může splňovat všechny požadavky těchto výše uvedených norem. (2)

Dále pak norma obsahuje přílohu A, která obsahuje jednotlivé cíle a jejich bezpečnostní opatření. Tyto cíle a opatření jsou uvedeny v tabulce A 1 a jsou vzájemně odvozeny a propojeny s normou ISO/IEC 17799:2005. (2)



Obrázek 13: PDCA cyklus v normě ISO 27000 (2)

1.4.3.5.3 ČSN ISO/IEC 27002 Soubor postupů pro management bezpečnosti informací

Tato norma obsahuje více než 5000 bezpečnostních opatření, které podporují strategii firmy, u které je každý z cílů přiřazen odpovědné osobě, společně s veškerými potřebnými funkcemi. Díky tomuto systému delegování je pak je jednodušší analýza aktuálního stavu informační bezpečnosti společnosti a také výběr potřebných opatření, nutných pro zlepšení aktuálního stavu. Norma se zabývá bezpečností nejen IT systémů, ale i informačních aktiv. (10)

1.4.3.5.4 ČSN ISO/IEC 27004 Řízení bezpečnosti informací – Měření

Jedná se o normu, která dává doporučení ohledně vývoje a používání metrik či měření, díky kterým je pak možno hodnotit účinnost stávající bezpečnosti informací (ISMS) a

účinnost jednotlivých opatření v organizaci. Tato doporučení se týkají politky, řízení rizik, opatření a procesů v bezpečnosti informací a také podporují následný proces revize zavedených opatření. Díky revizi je pak jasně patrné, které ISMS procesy jsou v pořádku, a které naopak potřebují zlepšení. Norma vznikla jen jako podpora pro měření účinnosti ISMS, samotné měření žádnou bezpečnost nezaručuje. (11)

1.4.3.5.5 ČSN ISO/IEC 27005 Řízení rizik bezpečnosti informací

Tato norma obsahuje doporučení pro řízení rizik bezpečnosti informací organizaci v souladu s požadavky na řízení bezpečnosti informací (ISMS) podle ČSN ISO/IEC 27001. Norma ale nespecifikuje konkrétní metodiku pro řízení rizik bezpečnosti informací, tu si musí každá organizace určit sama např. na základě rozsahu ISMS či průmyslovém odvětví, ve kterém firma podniká. V souladu s přístupem k řízení rizik popsaným v této normě lez pro implementaci požadavků ISMS použít některou z celé řady existujících metodik pro řízení rizik. Norma je určená manažerům a pracovníkům, kteří jsou v rámci organizace odpovědní za řízení rizik bezpečnosti informací a lze ji aplikovat na veškeré druhy organizací (komerční, vládní, neziskové), které mají v úmyslu řídit rizika potenciálně narušující bezpečnost informací v organizaci. (12)

1.4.3.6 Analýza rizik a jejich potlačení

Analýza rizik je stěžejní částí ISMS její výsledky do systémů vstupují hned v úvodní fázi. Stěžejní částí ISMS je tato analýza z důvodu, že na základě analýzy rizik se odvíjí v ISMS vše ostatní – od návrhu opatření, přes výslednou účinnost ISMS až po návrhy na jeho zlepšení. Pokud nejsme schopni identifikovat důležitá rizika a na ně navázané kritické činnosti, nemůžeme čekat, že zavedení ISMS nějak zásadně zlepší informační bezpečnost celé organizace. (7) (14)

V analýze rizik můžeme na zjištěná rizika buď vytvořit vhodné opatření, nebo toto riziko akceptovat. Riziko bývá akceptováno především v situaci, kdy náklady na jeho opatření převyšují míru dopadu (náklady bezpečnostní incident z tohoto rizika). (14)

1.4.3.6.1 Metodiky analýzy rizik

Analýzu rizik můžeme rozdělit na několik úrovní z hlediska detailnosti: (9)

- Hrubá úroveň
- Neformální přístup
- Kombinovaný přístup
- Detailní přístup

Na počátku každé analýzy je vhodné udělat hrubou úroveň analýzy, a poté na základě kritičnosti systému a výsledků této analýzy zvolit, jaký bude další postup, zda se bude systém analyzovat podrobněji, nebo ne. (9)

1.4.3.6.1.1 Analýza na hrubé úrovni

Při analýze hrubé úrovně pouze určíme pro každý IT systém jeho význam pro celou organizaci, společně s riziky, které z tohoto významu vyplývají. Po tomto výčtu pak je nutné určit, jakou další úroveň analýzy je nutné na daných IT systémech provést na základě těchto kritérií (posuzován bude každý systém prošlý hrubou analýzou zvlášť): (9)

- Kterých ze strategických cílů organizace je dosaženo při použití daného IT systému?
- Jaká je míra investic na vývoj, údržbu nebo nahrazení daného IT systému?
- Jaká je celková hodnota aktiv, které do daného IT systému patří?
- Jsou kritické oblasti organizace na daném IT systému závislé?

Výše uvedená kritéria nám určí kritičnost jednotlivých IT systémů pro organizaci a na základě toho určíme i potřebnou úroveň analýzy na každém z IT systémů. V praxi to tedy znamená, že čím kritičtější pro organizaci je, tím detailnější analýzu je potřeba zvolit. (9)

1.4.3.6.1.2 Neformální přístup

Neformální přístup analýzy rizik vyplývá především ze zkušeností jednotlivých osob, nikoliv ze strukturovaných (formálních) metod. (9)

Mezi výhody tohoto přístupu patří především nízká náročnost na čas a další, především finanční, zdroje a dále pak možnost využití stávajících znalostí – není třeba se učit nové postupy pro provedení této analýzy. (9)

Mezi nevýhody tohoto přístupu pak patří především obtížná obhajitelnost zvolených opatření jednotlivých rizik, protože je poměrně vysoká šance, že se některé z potřebných detailů pro kompletní analýzu opomenou a také proto, že při absenci jakékoliv formálnosti je obtížné jednotlivé výsledky analýzy mezi sebou porovnat – analýza kritičnosti je závislá především na subjektivitě jednotlivých osob. (14)

1.4.3.6.1.3 Kombinovaný přístup

Kombinovaný přístup analýzy kritičnosti IT systémů je třetí možností, jak lez tyto systémy analyzovat. Je založen na hrubé analýze všech IT systémů v první fázi, ve druhé fázi je pak u kritických, či vysoce rizikových IT systémů pro organizaci provedena podrobná analýza. Pro zbylé IT systémy je provedena pouze analýza základní. Kombinovaný přístup kombinuje minimální čas potřebný pro analýzu, společně se

zajištěním adekvátní míry pozornosti na kriticky důležité IT systémy pro danou organizaci. (9) (14)

1.4.3.6.1.4 Podrobný přístup

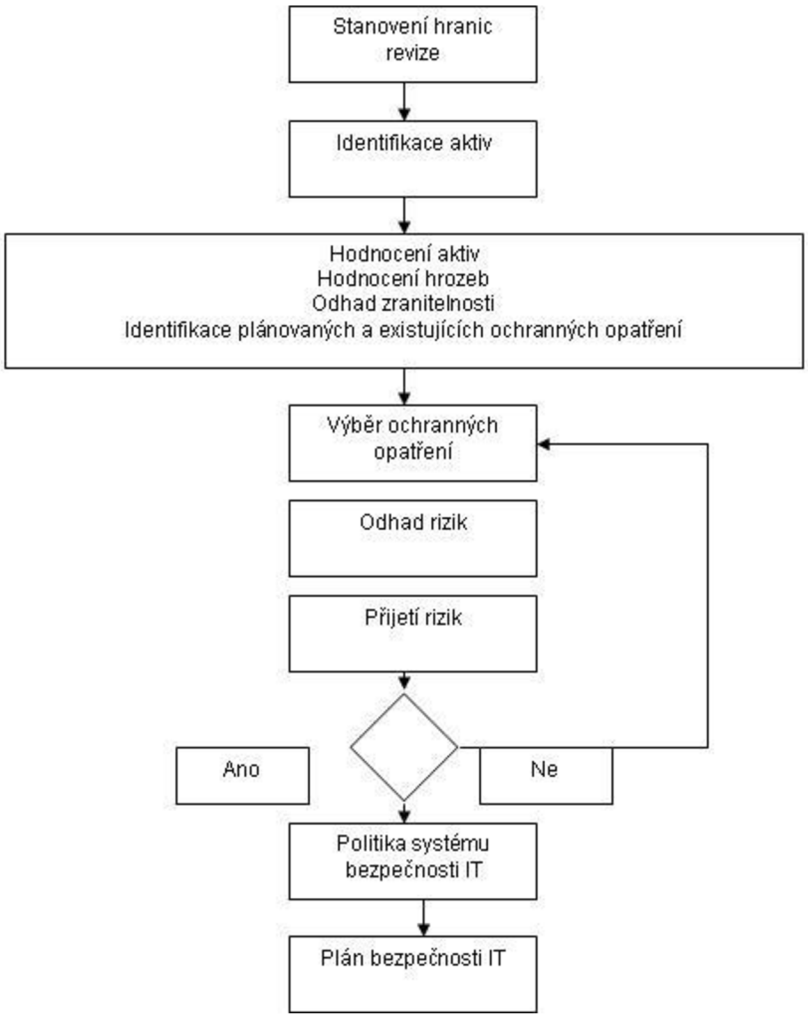
Podrobný přístup analýzy rizik rizika daného IT systému identifikuje, určí jejich velikost a poté i míru dopadu na činnost organizace v případě bezpečnostního incidentu. Výše míry rizika pak plně koresponduje s kombinací atraktivity jednotlivých IT systémů pro útočníka a jednoduchosti jejich zneužití v případě napadení. (8) (9)

Nyní si postupně rozebereme hlavní kroky podrobného přístupu analýzy (8) (9):

- Stanovení hranic revize – jako první krok podrobného přístupu analýzy rizik je potřeba stanovit hranice revize – např. čistě jen IT aktiva (HW, SW, data,…). Díky těmto hranicím se vyvarujeme hodnocení nesouvisejících činností.
- Identifikace aktiv – jedná se o identifikaci veškerého majetku, které společnost dává nějakou hodnotu a tudíž je zde i potřeba tento majetek chránit.
- Ohodnocení aktiv – nejčastěji se aktiva hodnotí pomocí stupnice 1-5, kdy 1 znamená nejmenší vliv na činnost organizace, stupeň 5 pak značí kritický vliv na fungování organizace. Hodnotí se tedy míra významu jednotlivých aktiv na fungování celého podniku..
- Hodnocení hrozeb – hodnota jednotlivých hrozeb značí velikost pravděpodobnosti, že bude daný systém poškozen – vyšší hodnota hrozby – vyšší pravděpodobnost poškození IT systému nebo aktiv. Tyto hrozby pak mohou být buď lidského, nebo přírodního charakteru.
- Odhad zranitelnosti – zjištění veškerých slabých míst v jednotlivých částech organizace (v personálu, managementu, administraci nějaké části podniku – HW, SW apod., fyzickém prostředí, pracovních postupech,…).
- Identifikace existujících / plánovaných ochranných opatření – na základě dokumentů výše je v tomto kroku vypsán seznam všech existujících opatření, společně se všemi, které je třeba nově zavést.

- Výběr ochranných opatření – výběr takových opatření, která daná rizika sníží na naprosté minimum, případně je zcela eliminují. Výběr nejdůležitějších opatření je vypsán v seznamu tzv. všeobecně aplikovatelných ochranných opatření, který lze nalézt v normě ČSN ISO/IEC TR 13335-4, ve kterém jsou rozdělena do těchto kategorií:
    - Řízení a politiky bezpečnosti IT
    - Kontrola bezpečnostní shody
    - Řešení incidentů
    - Personální opatření
    - Provozní problémy
    - Plánování kontinuity činnosti organizace
    - Fyzická bezpečnost
- Odhad rizik – v tomto kroku je nutné zjistit veškerá rizika, která IT systémům či aktivům hrozí (co a proč).
- Přijetí / nepřijetí rizik – v této části výsledná rizika buď přijmeme – vytvoříme na ně příslušná opatření, nebo nepřijmeme – akceptujeme (označíme za tzv. zbytková rizika). Akceptace rizika probíhá na základě porovnání reálného dopadu bezpečnostního incidentu na organizaci vůči nákladům, které je třeba vynaložit na opatření pro toto riziko. Pokud náklady na opatření příliš převyšují náklady na dopad daného rizika, riziko se označí za zbytkové neboli pro organizaci akceptovatelné.
- Implementace nápravných opatření – v tomto kroku veškerá rizika, označná jako přijatelná, z předchozího kroku snížíme, nebo zcela eliminujeme na požadovanou úroveň pomocí zavedení příslušných opatření
- Politika bezpečnosti IT systému – jedná se o dokument, ve kterém by měly být vypsány veškeré podrobnosti o zavedených opatřeních, včetně informace, proč jsou tato opatření nezbytná
- Plán bezpečnosti IT – dokument, ve kterém by měl být uveden podrobný plán bezpečnosti IT, stručně tedy popis veškerých akcí potřebných k tomu, aby mohla být vybraná opatření implementována

Schéma podrobného přístupu pro vyšší názornost:



Obrázek 14: Schéma podrobného přístupu analýzy (9)

1.4.3.6.2 Metodiky potlačení rizik

Tak jako je možné provést různé metody analýzy rizik, je možné tato rizika následně pomocí různých metod snižovat (9):

- Retence
- Redukce
- Transfer

1.4.3.6.2.1. Retence rizika

Jedná se o nejběžnější metodu řešení rizik. Princip retence spočítá ve vědomé či nevědomé akceptaci rizika, tedy že se proti němu nebudou vytvářet žádná opatření z důvodu, že se nejedná o rizika s velkým dopadem na společnost a zároveň vysokou mírou nákladů na odstranění tohoto rizika. Při vědomé retenci rizika je riziko rozpoznáno, ale není proti němu vytvořeno jakékoliv opatření. Při nevědomé retenci se ve většině případů jedná o riziko s tak mizivým dopadem, že analýza toto riziko zcela přehlédne. (9) (14)

Akceptace tedy probíhá v případě, že se společnosti vytvoření bezpečnostního opatření nevyplatí viz. přiměřená bezpečnost v kapitole a grafu výše. (9) (14)

1.4.3.6.2.2. Redukce rizika

Redukce rizika je používána v případě, kdy je sjednání pojištění na bezpečnostní incident daného rizika příliš nákladné, skrze velmi vysokou pravděpodobnost vzniku, a také v případě, kdy je riziko příliš vysoké, ne aby na něho mohla být uplatněna retence. (9)

Redukce rizik dělíme na 2 základní typy: (14)

- Redukce odstraňující příčiny vzniku bezpečnostních incidentů
- Redukce odstraňující následky bezpečnostních incidentů

1.4.3.6.2.3. Transfer rizika

Transfer rizika neboli pojištění proti jeho vzniku je využíván v případech, kdy je dopad rizika pro společnost často až likvidační, skrze jeho nízkou pravděpodobnost je však pojištění tohoto rizika cenově dostupné. (9)

Pod transferem rizika je možno si představit například pojištění proti živelným pohromám, požáru budovy, apod. (14)

1.4.3.7 Řízení rizik

„Cílem řízení rizik je identifikace a kvantifikace rizik, kterým je třeba čelit a poté vhodným způsobem rozhodnout o zvládnutí těchto rizik. Snížení rizika je jedna z nejčastěji používaných metod.“ *(7, str. 95)*

Výše uvedenou citaci si můžeme představit ve formě obrázku níže – 4 vzájemně na sebe navazující činnosti, které jsou v uzavřeném kruhu. Řízení rizik je tedy neustále aktuálním tématem, které po dobu života podniku nikdy nekončí. (7)

Obrázek 15: Řízení rizik (7)

Každá z, na obrázku uvedených, činností znamená: (7)

- Stanovení kontextu – v této fázi si celou oblast řízení rizik vymezíme a stanovíme role jednotlivým osobám, společně s odpovědností za tyto role. Ve stanovení kontextu rovněž určujeme metodiku, kterou budeme rizika analyzovat, její kritéria a způsoby, jakým budeme rizika hodnotit a následně zvládat.
- Analýza rizik – v této fázi identifikujeme veškerá aktiva a přiřadíme k nim hrozby a zranitelnosti.
- Vyhodnocení rizik – zde jednotlivá rizika prioritizujeme a vybíráme k nim příslušná opatření. Správný výběr opatření je klíčový pro úspěch celého řízení rizik.

Zvládání rizik – závěrečná fáze jednoho z nekonečných cyklů řízení rizik. Jedná se o nasazení opatření do praxe, většinou se tak děje pomocí retence, transferu, pojištění či jinému způsobu, jak se riziku vyhnout nebo jak je eliminovat.

1.5 Další normy

V této kapitole jsou uvedeny další normy potřebné pro zpracování projektu, jelikož se však netýkají ISMS, je nutné je zařadit zvlášť.

1.5.1 ČSN EN 50110-1 ed.3 – Obsluha a práce na elektrických zařízeních – Část 1: Obecné požadavky

Tato norma platí pro obsluhu a práci na elektrických zařízeních, s elektrickými zařízeními nebo v jejich blízkosti. Jedná se o elektrická zařízení provozovaná s úrovní napětí od malého, až po vysoké včetně. Termín vysoké napětí pak zahrnuje úrovně vysokého, velmi vysokého a zvlášť vysokého napětí. V rámci normy jsou pak uvedeny paragrafy (§1-11), na které musí být každá osoba oficiálně prozkoušena, aby je mohla získat. Zkoušky se pak v určitých intervalech musí neustále obnovovat. Osoby jsou pak na základě těchto paragrafů oficiálně schopny pracovat na elektrických zařízeních od úrovně pod dozorem kvalifikované osoby, až po úroveň samostatného projektování, vedení projektových týmů, případně pak speciální případy. (13)

1.5.2 Soubor norem ČSN EN 50132-1 – Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích: Část 1: Systémové požadavky

Soubor norem popisující veškeré požadavky systému CCTV (systémové, funkční, technické), bez kterých tento systém nelze vybudovat. Výčet všech norem, které soubor obsahuje, můžeme vidět v tabulce níže. (19)

Tabulka 3: Soubor norem ČSN EN 50132 (19)

Část souboru ČSN EN 50132	Název
Část 1	Systémové požadavky
Část 2-1	Černobílé kamery
Část 2-2	Barevné kamery
Část 2-3	Objektivy
Část 2-4	Příslušenství
Část 3	Lokální a hlavní řídící jednotka
Část 4-1	Černobílé monitory
Část 4-2	Barevné monitory
Část 4-3	Záznamová zařízení
Část 4-4	Zařízení pro okamžitý výtisk obrazu
Část 4-5	Video detektor pohybu
Část 5	Přenos videosignálu
Část 6	Pokyny pro aplikaci

2. Analýza současného stavu

2.1. Představení společnosti

Obecné informace

Obchodní jméno:	MBG, spol. s r.o.
Sídlo firmy:	Sadová 2323/4, 789 01 Zábřeh
Datum založení:	16.3.1993
Zakladatelé:	Ing. Karel Melichařík, Hubert Beck
Jednatelé:	Ing. Karel Melichařík

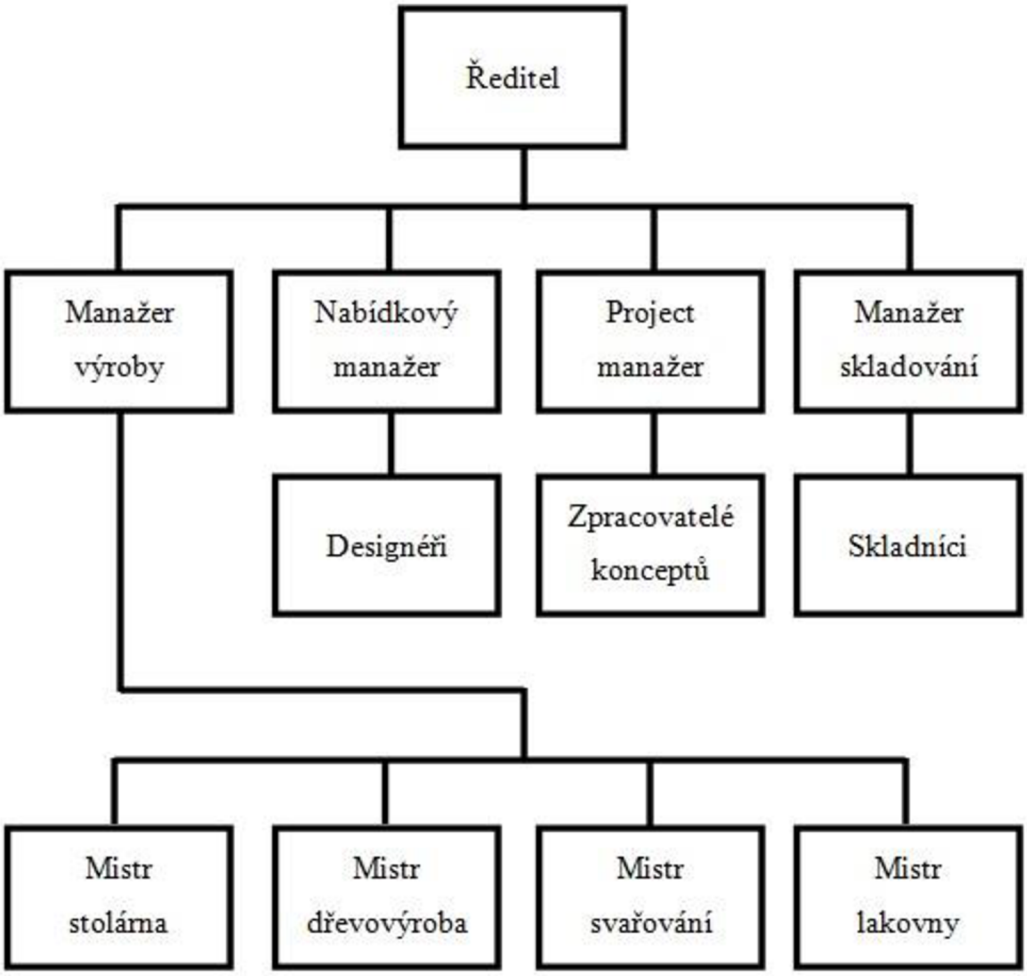
Obrázek 16: Logo společnosti MBG, spol. s r.o. (16)

Společnost MBG s.r.o. je společnost s letitou tradicí, zabývající se kovovýrobou, dřevovýrobou a truhlářstvím na zakázku. Založena byla 16.3.1993 v Olomouckém kraji, Zábřehu na Moravě.

Z počátku se společnost soustředila pouze na kovovýrobu nejrůznějšího typu - měla pouze 2 investory – z jejich příjmení je taky tvořen název společnosti – Melichařík, Beck.

Společnost se stala průkopníkem na poli úložných systémů, konkrétně nejrůznějších polic a regálů, které lze často vidět ve skladech či na čerpacích stanicích. Z tohoto segmentu se společnost rozvinula do dnešní podoby, kdy nevyrábí pouze úložné systémy, ale navrhuje kompletně design celých prodejen, včetně elektroinstalace, datové kabeláže a inženýrských sítí. Od roku 2014 se společnost zaměřuje i na zahraniční zákazníky. (16)

2.2. Organizační struktura



Obrázek 17: Organizační schéma společnosti (Vlastní zpracování)

2.3. Budovy

Společnost má nyní k dispozici celkem 2 různé objekty, oba umístěné ve městě Zábřeh na Moravě, ve vzájemné vzdálenosti asi 3km vzdušnou čarou. Jelikož se ale bude práce zabývat inovací pouze staré budovy, nebude zde uvedeno schéma budovy nové.

Obrázek 18: Stará budova (17)

Obrázek 19: Nová budova (18)

2.4. IT vybavení staré haly

2.4.1. Síť

Síť ve staré hale je typu LAN, jedná se tak o velmi jednoduchou a malou interní síť. Na tuto síť je připojeno všech 27 počítačů společnosti, server, sdílený disk a sdílená síťová tiskárna. Dále pak router, přes který stará hala komunikuje s novou halou.

Veškerá kabeláž je vedena stejnými cestami, ale po jiných médiích (datová, telefonní, kamerová).

2.4.2. Switch

Všechna zařízení společnosti jsou připojena do jednoho switche umístěného v datovém rozvaděči. Jelikož však všechny PC nemají mít přístup ke všem zařízením (disk s kamerovými záznamy, tiskárna, apod.), je rozdělen na 2 VLANY, kdy v jedné VLAN jsou veškeré sdílené počítače z dílenských prostor, ve druhé pak počítače z kanceláře a sdílená tiskárna. V obou VLAN je nastavené propojení s dalším portem switche, ve kterém je připojen sdílený disk.

2.4.3. Router

Umístěn v datovém rozvaděči, pomocí něj komunikuje stará hala s novou. Tento router je dále připojený na směrovou wifi anténu umístěnou na střeše objektu, přes kterou jsou přenášena mezi objekty veškerá potřebná data. Router umožňuje funkci NAT, schovává tedy celou vnitřní síť před okolním světem. Bohužel je to, společně s antiviry a firewally na všech počítačích jediná zavedená ochrana informační bezpečnosti.

2.4.4. Osobní počítače

Společnost disponuje 27 osobními počítači rovnoměrně rozdělenými do všech místností v hale podle potřeb zaměstnanců. Počítače v pracovních prostorách jsou sdílené pro více zaměstnanců na jednou, dělníci na nich zaznamenávají do systému stavy jednotlivých zakázek.

Všechny počítače společnosti jsou připojené na síť, všechna přípojná místa jsou využita (jsou připojeny i některé stroje – např. obráběcí CNC automaty). Je zde však příprava v podobě zaslepených zásuvek pro případné budoucí rozšiřování přípojných zařízení.

2.4.5. Server, sdílený disk

Server je umístěn v datovém rozvaděči ve 2.NP v malém skladu, ve kterém není takový provoz a tedy i prašnost jako v hlavním skladu. V případě potřeby je možné do serveru za běhu zapojit monitor i ovládací periferie z počítačů stojících hned vedle rozvaděče, primárně však správa probíhá z počítačů v kanceláři ve 2.NP přes vzdálený přístup.

Sdílený disk společnosti je taktéž umístěn v datovém rozvaděči. Přístup na něj mají všichni zaměstnanci, ovšem s odlišným nastavením oprávnění řízeným přes Active Directory (dělníci fungující na sdílených účtech mohou data pouze číst).

2.4.6. Sdílená tiskárna

Jedná se o multifunkční zařízení umožňující i skenovat a kopírovat, přístup k ní je v rámci firmy velmi omezen, využívat ji mohou jen zaměstnanci pracující v kanceláři v 2.NP

2.4.7. CCTV

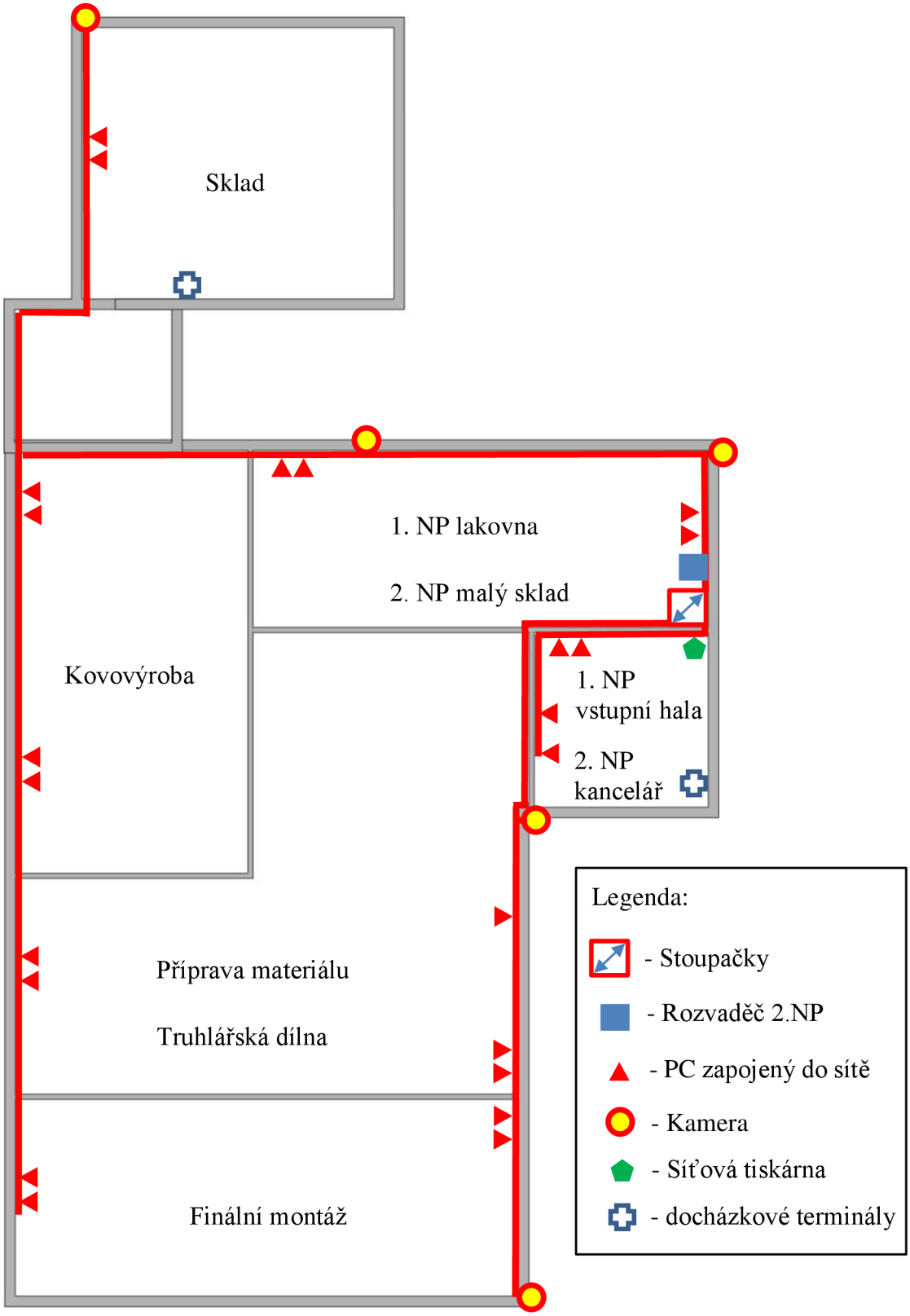
Kamery televizního systému jsou zaznačeny v náčrtu půdorysu, jedná se o IP kamery od společnosti AVTECH, konkrétně typ AVM501. Výsledný obraz se ukládá na samostatný pevný disk pomocí NVR zařízení. Toto zařízení je taktéž uloženo v datovém rozvaděči.

Dalším zařízením v datovém rozvaděči je pevný disk, již zmíněný v předchozím odstavci, který je sice zapojený do sítě, ale není sdílený všem. Tento disk slouží pouze pro potřeby ukládání obrazových záznamů z kamer a přístup k jeho datům má pouze ředitel staré haly. Permanentní zobrazovací zařízení u této instalace systému CCTV neexistují, společnost nemá personál ani potřebný SW, který by záznamy kontroloval živě. Na živý přenos z kamer je samozřejmě možné se podívat z počítače ředitele, primárně se ale záznamy ukládají pro případnou budoucí potřebu zkontrolovat situaci na sledovaném místě (v případě nehody, pracovního úrazu apod.). Z náčrtu půdorysu na další straně je zřejmé, že monitorovaný je pouze exteriér společnosti. Skrze krádeže materiálu ve vnitřních prostorách budovy, kterým aktuální rozmístění kamer jakkoliv nebrání, požaduje společnost zavedení monitorovacího systému i do vnitřních prostor budovy.

2.4.8. Terminály

Docházkové terminály jsou na půdorysu naznačeny taktéž, oba v 1.NP budovy. Nejsou však připojeny do sítě, protože se jedná o starý typ „píchaček“ s hodinami a časovým razítkem, které je vždy nutné doplnit do papírové docházky zaměstnanců. V tomto problému spočívá největší nekompatibilita s novou halou, kdy někteří zaměstnanci mnohdy, v rámci potřeby, mezi halami cestují a na nové hale si značí docházku čipovou kartou. U lidí, co takto přejíždí, je tedy vždy nutné na konci každého měsíce sbírat data potřebná pro mzdu ze dvou různých zdrojů, což není v žádném případě efektivní.

2.5. Náčrt půdorysu staré budovy s aktuálním IT vybavením



Obrázek 20: Náčrt půdorysu staré budovy s aktuálním IT vybavením (Vlastní zpracování)

2.6. Problémy s dodávkou elektrické energie

Tyto problémy bývají způsobeny především v letních měsících roku, kdy stroje používané pro zpracování zakázek kladou vysoké nároky na stávající elektrické připojení, skrze velký objem práce, který standardně v letních měsících firma má. Na základě tohoto množství zakázek je firma nucena uvést do provozu všechny dostupné stroje. Z části za tyto problémy může stará elektroinstalace, u které nebylo počítáno s tak velkým vytížením. Skrze vysokou energetickou náročnost tak dochází, v částech objektu se starou elektroinstalací, k přetížení a výpadkům jističů, v některých případech i následně hlavního jističe.

Před nápravou jakýchkoliv chyb na elektroinstalaci je nejprve nutné celou elektrickou síť podrobit analýze, díky které bude zjištěn původce veškerých problémů. Chyba nemusí být jen jedna, může se jednat o kombinaci nejrůznějších chyb. Tyto chyby mohou být následující:

- Příliš velký příkon všech, do sítě, zapojených strojů → nízká kapacita elektroinstalace
- Připojení zařízení na jiný, než zásuvkový obvod (například světelný, kde je 10A jistič, místo zásuvkového s 16A jistič) → přetížení daného obvodu
- Chyba na straně distributora → nedostačující distribuční transformátor

2.7. Požadavky společnosti MBG s.r.o.

- Rozšířit kamerový systém o minimálně 16 nových IP kamer, umístěných v interních prostorách budovy. Společnost se k tomuto kroku rozhodla na základě neustálých krádeží uskladněného materiálu z řad stálých zaměstnanců
- Z bodu výše vyplývá i potřeba zakoupení dalších NVR záznamových zařízení
- Instalovat nové elektronické terminály pro docházku, skrze potřebu vedení dat v elektronické podobě. Nyní jsou data vedena jen na papíře. Hlavním důvodem je nekompatibilita s novým objektem, kdy za stávající situace musí mít zaměstnanec čipovou kartu do nové budovy a papírovou docházku do budovy staré

- Vyřešit problém s občasnými výpadky dodávky elektrické energie a s tím spojené výpadky všech systémů, včetně serverů umístěných v daném objektu.
- Minimalizovat náklady – pořizovat se budou jen koncové prvky, připojení bude provedeno na stávající kabeláž (pokud to bude možné).
- Zachovat nepřetržitý provoz objektu
- Vyřešit problémy v období letních prázdnin – měsíce 07 a 08 roku 2016

2.8. Zhodnocení stávajícího stavu

Společnost MBG, spol. s r.o. vykonává svou činnost na trhu výborně, nezávisle na výše uvedených problémech. Ty ale její snahu mnohdy maří skrze krádeže materiálu, a jelikož je materiál objednáván přesně na danou zakázku, posléze při výrobě chybí, je nutné objednávat nový, čímž se zpozdí celý proces výroby a společnost je za opoždění smluvených termínů penalizována. Věřím tedy, že se investice do interního monitorovacího zařízení velmi rychle vrátí.

Interní datová síť je na poměrně vysoké úrovni, její obměna by tedy neměla být nutná, nepřetržitý provoz dalších IP kamer by měl být zajištěn bez větších problémů. Po zavedení elektronické docházky ale ve firmě vzniká rozpor se zákonem o ochraně osobních údajů, kdy díky elektronické docházce bude společnost udržovat data o zaměstnancích v elektronické podobě, ne jako dosud, na papíře. Aktuální bezpečnost informací, a tedy i osobních údajů o zaměstnancích, v prostorách staré haly nepřiměřeně nízká. Navrhnul jsem tedy společnosti i zavedení ISMS, a po předložení veškerých důvodů, proč ISMS zavést, byla tato potřeba zahrnuta mezi požadavky.

Problémy se stálou dodávkou elektrické energie, resp. jejími výpadky jsou pro společnost poměrně důležitou záležitostí k řešení, jelikož zatím nemá žádný záložní zdroj energie, a tak je v době výpadku kompletně vyřazeno veškeré vybavení na elektřinu, včetně monitorovacích zařízení nebo strojů na dílně, mnohdy zaseklých uprostřed procesu, který již nelze obnovit a aktuálně zpracovávaný materiál působí společnosti další finanční ztráty.

3. Vlastní návrhy řešení

3.1. Návrh vyřešení problémů s dodávkou elektrické energie

Jelikož je hlavním cílem práce instalace monitorovacího systému CCTV a následné zavedení ISMS do prostředí společnosti, nebude tato kapitola rozebrána do veškerých potřebných detailů.

Jak již bylo zmíněno v analýze společnosti, problém s napájením veškerých zařízení, připojených do elektrických rozvodů staré budovy, může být způsoben mnoha faktory - od připojení na distribuční transformátor, až po špatně koncipované elektrické rozvody v budově.

V prvním kroku návrhu řešení tohoto problému je nutné podrobit celou elektroinstalaci analýze. Po provedení této analýzy je pak potřeba zvolit takové opatření, které danou chybu zcela eliminuje. Budoucí výpadky energie není možno, ze strany společnosti, tolerovat. V analýze byly zjištěny tyto chyby:

- Přetěžování elektrické sítě v místnosti kovovýroby – toto je způsobeno použitím špatných materiálů vodičů v místnosti. Původní (hliníkové) vodiče je tedy nutné odebrat a nahradit je měděnými. Skrze tento problém je tedy nutné počítat s navýšením celkové časové náročnosti celého projektu a i nákladů za práci a vodiče samotné.
- Nedostatečný distribuční transformátor pro dané uskupení průmyslových objektů (při výpadku energie v celé budově jsou všechny jističe stále zapnuty) – tento problém bohužel nelze ze strany organizace nijak ovlivnit, proto nebude časová náročnost ani náklady na projekt jakkoliv navýšeny.

Zapojení přístrojů na jiné, než zásuvkové okruhy, v rámci analýzy zjištěno bylo, avšak jen v případě několika málo osobních počítačů. Při plném vytížení okruhu není překročena jeho kapacita, jsou tak splněny požadavky norem pro elektroinstalaci. Z tohoto důvodu nebude v časové náročnosti a nákladech projektu počítáno s přepojováním na správné okruhy, s čímž by souvisel i nákup a následná instalace nových vodičů k daným sdíleným stanicím.

3.2. Návrh implementace nových zařízení

3.2.1. Rozšíření stávajícího systému CCTV

Rozšířením stávajícího CCTV systému by mě dojít k zabezpečení vnitřních prostor staré haly, a díky tomu i k minimalizaci poměrně častých krádeží materiálu. Obraz z kamer bude ukládán na nová záznamová zařízení NVR, která budou umístěna v datovém rozvaděči umístěném v prostorách menšího ze dvou skladů.

Návrh celého systému je koncipován tak, aby dodržel jak požadavky souboru norem ČSN EN 50132, ale i veškeré požadavky společnosti. Samotné rozmístění jednotlivých kamer je zaznačeno v náčrtu půdorysu staré haly.

3.2.1.1 Požadavky společnosti na systém CCTV

Do požadavků společnosti na systém CCTV patří především snaha o minimalizaci nákladů a narušování směnného provozu tím, že budou kamery instalovány na stávající kabelové rozvody, které disponují dostatečnou kapacitou i rezervními kabelovými chráničkami.

Mezi požadavky dále patři zajištění nepřetržitého provozu, kabely ke kamerám tedy budou vedeny v lištách na omítkách zdí. Vodící lišty dovolují rychlou a jednoduchou montáž, bez potřeby bourání.

Posledním požadavkem společnosti je eliminace veškerých slepých míst kamerového systému, včetně prostor pod kamerami, je tedy nutné zajistit, mimo jiné, i vzájemnou viditelnost kamer.

3.2.1.2 Komponenty systému CCTV

3.2.1.2.1 Kamery

Pro návrh interního CCTV systému budou použity kamery společnosti HIKVISION, konkrétně model DS-2CD2622FWD-I. Tyto kamery disponují variabilní ohniskovou vzdáleností (schopnost kamery přiblížit objekt), infračerveným přísvitem pro noční vidění, vysokým rozlišením výsledného obrazu, a také funkcí pro kompresi vytvářeného obrazu a tím i snížení datového toku každé kamery.

Tabulka 4: Parametry vybraného modelu kamer (20)

Parametr	Hodnota
Senzor	CMOS
Rozlišení obrazu	Max. 1920 x 1080
Světelnost	F1.4
Ohnisková vzdálenost	2,8 – 12mm
Citlivost objektivu	0.01Lux @(F1.2,AGC ON); 0.014 Lux @(F1.4,AGC ON); 0 Lux s IR
Rychlost závěrky	1/3s – 1/10 000s
Rozsah IR přísvitu	20 - 30m
Přepínání režimu den a noc	Auto, dle času, při spuštění alarmu
Rozhraní	RJ45 – 10M/100M Ethernet
Provozní teplota	-30°C – 60°C
Povolená vlhkost	95%, nekondenzující
Třída ochrany	IP66
Energetická náročnost	5,5W (s nočním viděním 7,5W)
Rozměry	95 x 105 x 258,6mm
Váha	1200g

Obrázek 21: Ilustrace vybraného modelu kamery (20)

Dle obrázku je možno vidět, že pro instalaci kamery není třeba žádné další příslušenství (držáky apod.), stačí pouze šrouby pro přichycení na zeď. Napájecí zdroj pro uvedení kamery do provozu není potřeba, kamery budou napájeny přes síť ethernet (PoE).

3.2.1.2.2 NVR

Digitální kamery je vždy nutno doplnit záznamovým zařízením (NVR), které je schopno vytvářený obraz z kamer jak zobrazit na zobrazovacím zařízení, tak i uložit na pevný disk. Tento pevný disk nemusí být pouze externí, nýbrž i integrovaný přímo v záznamovém zařízení. Takováto zařízení snižují počet komponent celého systému, šetří místo v datovém rozvaděči, avšak oproti NVR bez pevného disku jsou dražší.

Z důvodu zajištění maximální možné kompatibility je pro návrh vybráno NVR od společnosti HIKVISION, konkrétně se jedná o model DS-7616NI-E2/16P/A. Toto zařízení disponuje 16 vstupy pro IP zařízení, která mohou být napájena přes PoE.

Obrázek 22: NVR HIKIVISION zvolené pro návrh CCTV (21)

Tabulka 5: Parametry záznamového zařízení NVR HIKIVISION (21)

Parametr	Hodnota
Videovstupy	16x RJ45
Rozlišení	5MPx
Max. zázn. rychlost	100 Mb/s
Formát komprese	H.264 / MJPEG
Rozhraní pro HDD	2 x SATA
Max. kapacita HDD	2 x 4TB
Výstup pro monitor	VGA, HDMI
Ethernet - výstupní	1 x 10 / 100 / 1000 Mbps
PoE	16 x 10 / 100 Mbps, max 120W
Energetická náročnost	15W
Rozměry (Š x V x H)	290 x 48 x 380 mm
Váha	998g

3.2.2. Docházkové terminály

3.2.2.1 Požadavky společnosti

Docházkové terminály by dle požadavků společnosti měly zůstat na původních místech, skrze chybějící kabeláž však je tento požadavek, bez rozšíření sítě nemožný. Tvorba nových tras je ale v přímém rozporu s dalším požadavkem společnosti na minimalizaci nákladů a využití stávajících kabelových rozvodů, proto bude navrženo nové umístění na trasách stávající kabeláže.

Funkčně by měly být terminály schopny zaznamenat nejen příchod a odchod (možno využít obyčejné čtečky karet), nýbrž i obsahovat volby jako dovolená, odchod k lékaři, na oběd, mimo pracoviště apod.

3.2.2.2 Výběr terminálu

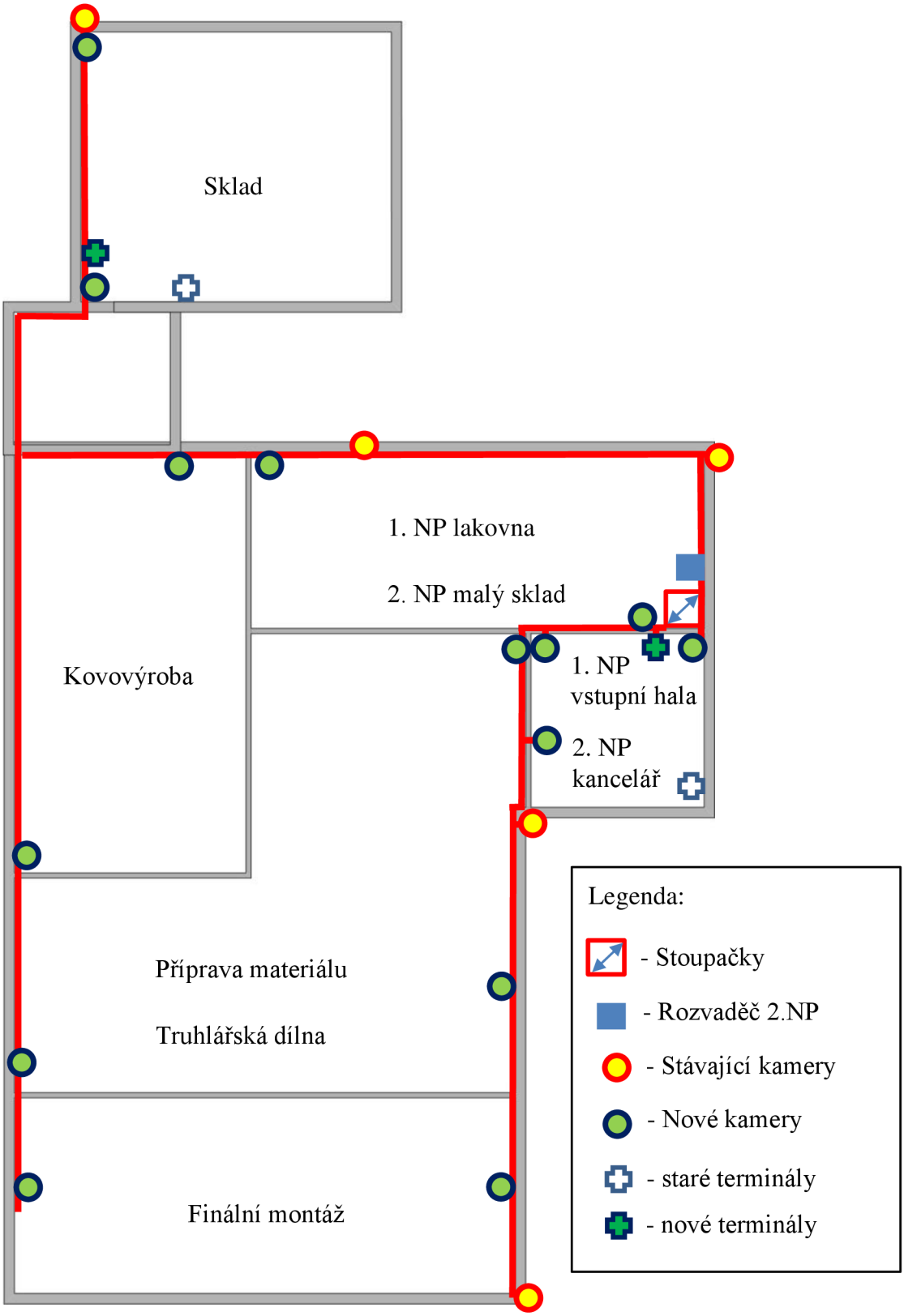
Pro návrh docházkových terminálů byl vybrán terminál DT3000 SA od společnosti ADI Global Distribution. Jedná se o dvanácti tlačítkový terminál s dvouřádkovým displejem a integrovanou čtečkou čipových karet typu HID.

Obrázek 23: Docházkový terminál ADI DT3000 SA ve dvou barevných provedeních (22)

Tabulka 6: Parametry terminálu ADI DT3000 SA (22)

Parametr	Hodnota
Napájení	12Vss nebo PoE
Počet docházkových důvodů	20
LCD	Grafický, inverzní, podsvětlený, 2x20zn.
Čtečka karet	HID, 1x Interní, 1x externí
Paměť karet	6 000
Paměť událostí	20 000
Rozhraní	RS-232, RS-485, Ethernet
Hodiny	8 časových zón, zálohovány baterií

3.2.3. Rozmístění nově implementovaných prvků



Obrázek 24: Náčrt půdorysu staré haly s rozmístěním nově implementovaných prvků (Vlastní zpracování)

Rozmístění nových prvků bylo částečně limitováno požadavkem společnosti využít pro implementaci stávající rozvody - kamery tedy nemohly být instalovány v nových trasách, ač by to bylo v určitých případech vhodnější. U terminálů pak s instalací na stávající rozvody nebyl problém.

U kamer bylo nutné dále dbát na eliminaci „slepých míst“, především v prostorách budovy, kde se nachází jakýkoliv majetek společnosti, který by mohl být poškozen nebo odcizen. Umístění terminálů pak bylo navrženo s ohledem na minimální vzdálenost od původních terminálů, a také s ohledem na dobrou viditelnost nově instalovanými kamerami.

3.2.3.1 Trasy systému CCTV

Jelikož byla kabeláž systému vedena pouze do míst, kde jsou umístěny staré kamery, nebylo by možné splnit nejdůležitější podmínku – eliminovat slepá místa. Kabeláž ke kamerám na jiho-východní stěně v kovovýrobě, truhlářské dílně a dílně finální montáže tedy musela být nově natažena, vznikla tak nová větev systému. Tato větev ale vede podélně s datovou kabeláží v rezervní kabelové chráničce, nebylo tedy za potřebí vysekávat nové trasy.

3.2.3.1.1 Sklad

Kamery v hlavní skladu jsou umístěny na jiho-východní straně budovy a snímají docházkový terminál a všechny úložné prostory na materiál, které se ve skladu nachází. Díky kolmému natočení úložných prostor, vůči stěně s kamerami, je počet navržených kamer pro splnění všech požadavků dostačující.

3.2.3.1.2 Kovovýroba

V dílně zpracovávající zakázky ze segmentu kovovýroby je jedna kamera umístěna na jiho-východní stěně, další pak na severo-východní stěně. Obě kamery na sebe vzájemně vidí a snímají i pracovní stanice s CNC stroji.

3.2.3.1.3 Lakovna

V lakovně jsou kamery umístěny v dostatečné vzdálenosti od všech lakovacích míst a přístrojů jak vertikálně, tak i horizontálně. Nemělo by tedy docházet k častému znečištění objektivů kamer. Kamery jsou umístěny v jiho-západním a severo-východním rohu místnosti.

3.2.3.1.4 Truhlářská dílna

Truhlářská dílna je jedinou místností, kde je vyšší počet kamer jak 2 a kde není splněna vzájemná viditelnost všech instalovaných kamer. 2 kamery jsou umístěny na severo-západní části místnosti, třetí pak na stejné zdi jako kamera v kovovýrobě. Kamery snímají všechny počítačové stanice a pracoviště na dílně.

3.2.3.1.5 Finální montáž

2 kamery jsou zde umístěny na stejných zdech jako v truhlářské dílně, je zde zajištěna vzájemná viditelnost kamer a jako jediná místnost nemá, při aktuálním rozmístění, jakékoliv slepé místo.

3.2.3.1.6 Malý sklad

Jelikož se jedná o místnost rozměrově přesně kopírující lakovnu, rozhodl jsem se umístit kamery do malého skladu na stejná místa, jako v lakovně. Kamery zde zabírají všechny úložné prostory a díky nevysokým úložným prostorům i datový rozvaděč.

3.2.3.1.7 Kancelář

V kanceláři je jako v jediné místnosti umístěna pouze jedna kamera, snímající všechny osobní počítače a sdílenou tiskárnu.

3.2.3.1.8 Vstupní hala

Rozměrově je vstupní hala sice rozměrově totožná s prostory kanceláře, která je umístěna nad halou, oproti kanceláři je zde však mnohem větší provoz lidí, navíc s potřebou monitorovat vstupní dveře (naproti kamery na jiho-východní stěně) haly a docházkový terminál kamerou umístěnou v severním rohu budovy.

3.2.3.2 Trasy k docházkovým terminálům

Jak již bylo zmíněno výše, při instalaci docházkových terminálů bylo dbáno na co nejkratší vzdálenost vůči umístění starých terminálů, avšak za podmínky použití stávajících rozvodů. Terminál ve vstupní hale tak byl nainstalován na protilehlou stěnu, oproti původnímu umístění, ve skladu pak byl instalován na druhé straně vstupních dveří z haly do skladu. Rozvody s případným rozšířením kabeláže počítaly, na trasách se tak nacházely rezervní kabelové chráničky. Díky využití těchto rozvodů bylo třeba pouze natáhnout nové kabely, místo vysekávání nových tras do zdí.

3.3. Návrh zavedení informační bezpečnosti

Implementovat informační bezpečnost do svého prostředí se společnost MBG, spol. s r.o. rozhodla jak skrze nové řešení vedení docházky v elektronické podobě, tak i využití této situace a digitalizaci větší části dalších personálních dat, z původní papírové podoby. S tímto přesunem tak vznikla urgentní potřeba tato data chránit, v opačném případě by jednání organizace bylo nezákonné (zákon o ochraně osobních údajů).

Z důvodu absence jakékoliv informační bezpečnosti, kromě SW instalovaného přímo na uživatelských stanicích, bude v této kapitole navržena obecná forma komplexní informační bezpečnosti organizace. V první části bude uveden plánovaný rozsah informační bezpečnosti, včetně analýzy rizik, v následující části pak navržena opatření na zjištěná rizika, určení kontrol účinnosti těchto opatření a případné další zlepšování informační bezpečnosti.

3.3.1. Ustanovení informační bezpečnosti

3.3.1.1. Souhlas společnosti

Společnost MBG, spol. s r.o. je moderní společností, splňující veškeré legislativní zákony a používající pro svůj provoz moderní technologie. Jelikož však tyto technologie je nutné užívat předem daným způsobem a představují pro organizaci, kromě veškerých dostupných výhod, vyplývajících z jejich použití, také jistá nebezpečí, je nutné společnost před tímto nebezpečím chránit.

Z tohoto důvodu se společnost rozhodla pro zavedení informační bezpečnosti do svého každodenního působení, pro kterou se zavazuje vyčlenit veškeré prostředky (finanční, technické a lidské zdroje), potřebné pro dosažení požadované úrovně informační bezpečnosti, a také se zavazuje plně podporovat tento proces ze strany vedení společnosti.

Dále se společnost MBG, spol. s r.o. zavazuje, že bude všechna doporučená opatření, na základě vytvořené dokumentace, dodržovat a kontinuálně vylepšovat.

3.3.1.2. Role a odpovědnosti

Vzhledem ke skutečnosti, že na nové hale již veškeré procesy týkající se systému řízení bezpečnosti informací fungují bez problémů, navrhuji implementační tým provádějící správu ISMS na nové hale, jako tým zodpovědný za implementaci a údržbu i na hale staré. Vzhledem k rozsahu použití IT prostředků na staré hale, společně s krátkou dojezdovou vzdáleností mezi oběma halami, navrhuji tento tým nejen pro počáteční inicializaci ISMS, ale i pro následující monitorování, vyhodnocování a zlepšování stávajícího systému.

Tento tým se skládá z následujících osob IT oddělení nové haly:

- Security manager – zodpovědný za celý projekt
- 2 IT zaměstnanci pro zavádění potřebných opatření
- 2 IT zaměstnanci pro monitoring a vyhodnocování stávajících opatření

Vybraní zaměstnanci jsou vysokoškolsky vzdělaní v oboru IT, protože jak již bylo nastíněno v teoretické části práce, pro maximální efektivitu je třeba nejen zkušeností s ISMS, ale také jeho teoretickou znalostí a znalostí potřebných metodik (ITIL, COBIT,…). I pro případné nové členy tohoto týmu tedy doporučuji absolventy VŠ v oboru IT, při současném zachování minimálního počtu dvou členů v každém týmu, pro zajištění vzájemné zastupitelnosti.

3.3.1.3. Bezpečnostní dokumentace a její řízení

Pro tvorbu a i následné aktualizace veškeré dokumentace k ISMS navrhuji osoby z týmu, které mají za úkol zavádět příslušná opatření, jelikož díky své činnosti nejlépe ví, jaké procesy je nezbytné vykonat pro úspěšné zavedení daných opatření. Odpovědnost za finální vzhled a obsah dokumentace by měl mít security manager, se kterým je nutné každou změnu nejprve konzultovat a nechat schválit.

Aktualizace dokumentace systému řízení bezpečnosti informací by měla probíhat minimálně jednou ročně, při výskytu výjimečné situace by měla být tato aktualizace však

provedena okamžitě po eliminaci daného rizika z důvodu minimalizace rizika opakování. Do aktualizace těchto dokumentů je nutné zařadit nejen analýzu rizik, ale i analýzu aktiv.

3.3.2. Analýza aktiv

V této kapitole budou uvedena aktiva pouze staré haly, jelikož se projekt zavádění ISMS týká právě jen tohoto objektu společnosti.

3.3.2.1. Identifikace aktiv

Aktiva společnosti na staré hale je možno dělit následující souhrnné skupiny:

- **Data v papírové a elektronické podobě** – účetní knihy, docházka apod.
- **Finance** – tato aktiva mají dopad na finanční zdroje společnosti, jedná se tak například o bankovní účty, faktury, finanční transakce apod.
- **Mentální aktiva** – image společnosti a její know-how
- **Majetek** – veškerý hmotný a nehmotný majetek – HW, SW, apod.

3.3.2.2. Hodnocení aktiv

Aktiva budou hodnocena číselnou stupnicí v rozsahu 1-5, kdy jednotlivá čísla znamenají výši kritičnosti (úroveň dopadu) na organizaci – 1 nulový, 5 kritický.

Tabulka 7: Legenda hodnocení aktiv (Vlastní zpracování)

1	Nulový
2	Zanedbatelný
3	Náklady na incident lehce převyšují náklady na opatření
4	Vysoká míra nákladů na odstranění problému
5	Ohrožuje činnost podniku

Výsledná váha aktiv bude zařazena do dané kategorie pomocí zaokrouhlení na celá čísla.

Tabulka 8: Hodnocení aktiv metodou CRAMM (Vlastní zpracování)

Skupina	Aktivum	Dostupnost	Důvěrnost	Integrita	Váha
Data v papírové a elektronické podobě	*Faktury*	3	2	4	3
	Pohledávky	3	2	4	3
	Závazky	3	2	4	3
	Účetní knihy	3	3	4	3
	Docházka	2	3	2	2
	Smlouvy	3	4	4	4
	Obchodní partneři, zákazníci	2	3	3	3
	Skladové informace	3	2	2	2
	Výplatní pásky	3	5	4	4
	Kompromitace hesel	2	4	4	3
Finance	*Napadení účtu*	2	4	4	3
	Kurzové ztráty	2	3	2	2
	Krach banky	5	4	4	4
Mentální aktiva	*Know-how*	4	5	5	5
	Image společnosti	4	5	5	5
Majetek	*Krádeže skladových zásob*	4	2	3	3
	Krádež a poškození HW	3	3	3	3
	Znehodnocení licence k SW	4	4	4	4
	Výpadek internetu	3	2	2	2
	Výpadek elektřiny	5	4	5	5

3.3.2.3. Seskupení aktiv

V této kapitole jsou aktiva z tabulky 8 seskupena podle váhy a také jsou vynechána všechna zanedbatelná či nulová rizika (váha menší než 3).

Tabulka 9: Seřazení vybraných aktiv dle váhy (Vlastní zpracování)

Image společnosti	**5**
Know-how	**5**
Výpadek elektřiny	**5**
Krach banky	**4**
Smlouvy	**4**
Výplatní pásky	**4**
Znehodnocení licence k SW	**4**
Faktury	**3**
Kompromitace hesel	**3**
Krádež a poškození HW	**3**
Krádeže skladových zásob	**3**
Napadení účtu	**3**
Obchodní partneři, zákazníci	**3**
Pohledávky, Závazky	**3**
Účetní knihy	**3**

3.3.2.4. Identifikace hrozeb

V této kapitole jsou uvedeny všechny možné hrozby pro výše zmíněná aktiva.

Tabulka 10: Identifikace hrozeb (Vlastní zpracování)

1.	**Image společnosti**	**5**
Hrozby	Ztráta důvěry, pozici na trhu, celý tržní segment	
Útoky	Konkurence, stěžejní dodavatelé a odběratelé	
Slabá místa	Nízká kvalita, špatná firemní politika, špatný servis	
2.	**Know-how**	**5**
Hrozby	Odchod velkého počtu zkušených zaměstnanců, penále, odcizení výrobních materiálů	
Útoky	Nespokojený zákazník, krádež	
Slabá místa	Nízká motivovanost a ohodnocení zaměstnanců, nedodržování smluvených termínů, nízká úroveň fyzického zabezpečení	
3.	**Výpadek elektřiny**	**5**
Hrozby	Zastavení výroby, ztráta všech neuložených dat, zničení HW	
Útoky	Vyhoření distribučního transformátoru	
Slabá místa	Absence náhradního zdroje energie	
4.	**Krach banky, napadení účtu**	**4**
Hrozby	Ztráta cash flow, platební neschopnost	
Útoky	Elektronický útok, pokles akcií banky	
Slabá místa	Finance v jednom bankovním ústavu	
5.	**Smlouvy**	**4**
Hrozby	Zjištění citlivých údajů smluvních partnerů a následné rozvázání poměru	
Útoky	Vloupání, omyl zaměstnance	
Slabá místa	Nízké fyzické zabezpečení (zámek na skříni s šanony)	

6.	Výplatní pásky	4
Hrozby	Vyšší konkurenceschopnost ostatních společností, závist mezi zaměstnanci a jejich odchod	
Útoky	Vloupání, omyl zaměstnance	
Slabá místa	Nízké fyzické zabezpečení (zámek na skříni s šanony)	

7.	Znehodnocení licence k SW	4
Hrozby	Nefunkční SW, potřeba zakoupení nového, nedodržení smluvených termínů a penalizace	
Útoky	Elektronický útok, vloupání, zneužití	
Slabá místa	Nízká správa dostupných licencí a kontrola jejich platnosti	
8.	**Faktury**	**3**
Hrozby	Krádež, chyba na faktuře, zneužití	
Útoky	Vloupání, omyl zaměstnance, elektronický útok	
Slabá místa	Nízká úroveň elektronické a fyzické ochrany (šanony ve skříni), lidský faktor	
9.	**Kompromitace hesel**	**3**
Hrozby	Vyzrazení citlivých informací, možná manipulace se systémy a daty	
Útoky	Vloupání, elektronický útok, omyl zaměstnance	
Slabá místa	Nízká úroveň elektronické ochrany, nízká frekvence zálohování, bezpečnostní politika hesel, liský faktor	
10.	**Krádež a poškození HW**	**3**
Hrozby	Vyzrazení citlivých informací, možná manipulace se systémy a daty, ztráta aktuální rozdělané práce	
Útoky	Vloupání, elektronický útok, virus, špatné zacházení nebo provozní prostředí (potřeba dalšího chlazení,…)	
Slabá místa	Nízké fyzické zabezpečení	
11.	**Krádeže skladových zásob**	**3**
Hrozby	Krádež, zdržení projektů, nedodržení termínů, penalizace	
Útoky	Vloupání ze strany vlastních zaměstnanců i externích lidí	
Slabá místa	Fyzické zabezpečení skladů	

13.	Obchodní partneři, zákazníci	3
Hrozby	Krádež, chyba při zadání, zneužití	
Útoky	Vloupání, elektronický útok, omyl zaměstnance	
Slabá místa	Nízké fyzické a elektronické zabezpečení dat, lidský faktor	

14.	Pohledávky, Závazky	3
Hrozby	Odcizení důležitých dokumentů, zneužití, chyba při zadání	
Útoky	Vloupání, omyl zaměstnance, elektronický útok	
Slabá místa	Nízká úroveň elektronické a fyzické ochrany (šanony ve skříni), lidský faktor	
15.	**Účetní knihy**	**3**
Hrozby	Odcizení důležitých dokumentů, zneužití, chyba při zadání, konflikty s finančním úřadem	
Útoky	Vloupání, omyl zaměstnance, elektronický útok	
Slabá místa	Nízká úroveň elektronické a fyzické ochrany (šanony ve skříni), lidský faktor	

3.3.3. Analýza rizik

Po analýze aktiv a identifikaci potenciálních hrozeb je zpracovat na základě zjištěných údajů analýzu rizik, která pak bude následně podkladem pro veškerá navržená opatření.

Skrze opakování zavedu souhrnné označení – Důležité dokumenty, které bude obsahovat Smlouvy, výplatní pásky, obchodní partnery a zákazníky, Pohledávky, zakázky a účetní knihy.

Tabulka 11: Analýza rizik (Vlastní zpracování)

Hrozba	Aktiva	Metoda potlačení rizika
Manipulace neoprávněnou osobou	Důležité dokumenty Znehodnocení licence k SW Kompromitace hesel Krádež a poškození HW	Redukce
Chyby uživatele	Důležité dokumenty Krádež a poškození HW Kompromitace hesel Znehodnocení licence k SW Krach banky, napadení účtu	Retence
Poškození aktiv	Krádež a poškození HW Důležité dokumenty Kompromitace hesel Znehodnocení licence k SW Výpadek elektřiny	Redukce
Krádež aktiv	Krádež a poškození HW Krádež skladových zásob	Transfer
Ztráta peněžních prostředků	Krach banky, napadení účtu	Transfer, redukce
Přerušení dodávky el. energie	Výpadek elektřiny Krádež a poškození HW	Redukce
Odchod klíčových zaměstnanců	Know - how	Redukce

3.3.4. Návrh bezpečnostních opatření

Na základě předchozích údajů a výsledků analýzy rizik vede tato kapitola návrh všech opatření, která pomohou potlačit výše zmíněná rizika, která není vhodné akceptovat (metoda potlačení - retence).

V případě jakéhokoliv výskytu bezpečnostního incidentu je nutné bezprostředně informovat tým zodpovědný za implementaci a správu ISMS, který na základě typu bezpečnostního incidentu provede nápravu. Tyto akce by měly být uvedeny v tzv. havarijním plánu, ve kterém by měly být všechny různé druhy bezpečnostních incidentů a postupů, jak tyto incidenty řešit. Postupem času je nutné tento dokument aktualizovat a rozšiřovat, společně s tím, jaké bezpečnostní incidenty budou nastávat. Výhoda v této situaci je, že bezpečnostní tým má již velké množství bezpečnostních incidentů, v havarijním plánu, podchycen z fungování systému informační bezpečnosti na nové hale.

3.3.4.1. Manipulace neoprávněnou osobou

Metoda potlačení rizika: **Redukce**

Redukce jako forma potlačení rizika znamená, že proti zjištěnému riziku budou vytvořena opatření, která ho potlačí nebo zcela eliminují. V případě rizika manipulace s aktivy neoprávněnou osobou proto navrhují tato opatření:

- Digitalizaci dat a jejich kryptování
- Zavedení firemní politiky hesel
- Zálohování dat
- Spravovat licence k SW

Jako prvním účinným opatřením, které by mělo eliminovat zneužití důležitých dokumentů, navrhuji jejich převedení do digitální podoby, následné zakryptování a uložení na pevný disk, který nebude připojen k síti internet. Klíč k dešifrování těchto dat by pak byl umístěn v trezoru ředitele, společně s papírovými dokumenty, které bude

potřeba ponechat i v jiné, než digitální formě. Takto uložená data by byla především ta, ke kterým není nutné často přistupovat (např. smlouvy). Ostatní data, často potřebná pro přístup by měla být zničena v papírové podobě a uložena na sdílený disk, ke kterému jsou přiřazena přístupová oprávnění – v případě napadení uživatelského účtu nejsou ohrožena data, ke kterým nemá uživatel přiřazen přístup.

Dalším opatřením, které navrhuji zavést je politika hesel, kdy uživatelé budou nuceni dodržovat jistou formu hesla – minimální počet znaků, malá a velká písmena, čísla, případně speciální znaky, které budou pro tvorbu hesla povinné. Dalším bezpečnostním prvkem by pak měla být neopakovatelnost hesla pro předem daný počet cyklů (např. neopakovatelnost v rámci posledních 5 hesel) a jeho expirace po předem stanovené době. Po zavedení tohoto hesla je jeho zjištění pro útočníka značně komplikovanější, navíc v případě jeho zjištění, není vzdálený přístup trvalý.

Zálohování všech dat navrhuji z důvodu případné kompromitace, kdy budou data na disku zašifrována (vir), smazána, ať už omylem nebo cíleně, či jinak znehodnocena. Záloha by měla být denní rozdílová, prováděna vždy v noci v době minimálního provozu na síti, jednou měsíčně pak záloha kompletní. Rozdílové zálohy by měly být umístěny síťovém disku, s přístupem pouze pro bezpečnostní tým, měsíční pak na zcela odděleném disku od sítě.

Posledním opatřením v rámci potlačení tohoto rizika pak navrhuji zavedení správy všech zakoupených licencí, kdy bude přesně zdokumentováno, kolik licencí se zakoupilo, kolik je jich, jakým způsobem a jakými uživatelskými účty využito a kolik licencí je dostupných s předem danou rezervou. Zavedením tohoto opatření by mělo být docíleno zajištění funkčnosti veškerého SW i v případě znehodnocení nějaké z licencí a také eliminace situace, kdy si zaměstnanec volný licenční klíč „vypůjčí“ pro domácí použití.

3.3.4.2. Chyby uživatele

Metoda potlačení rizika: **Retence**

Retence znamená, že na bezpečnostní incidenty vzniklé z těchto rizik nebudou vytvářena bezpečnostní opatření, rizika tak budou akceptována, především pro svůj nízký dopad na společnost a levné odstranění následků. Navíc v případě chyb uživatele se nejedná o velmi častý problém a riziko je částečně potlačeno i pomocí opatření zavedených skrze riziko neoprávněné manipulace s aktivy. Jedná se především o zálohování dat.

3.3.4.3. Poškození aktiv

Metoda potlačení rizika: **Redukce**

V rámci rizika poškození aktiv se jedná především o poškození samotného vybavení, jelikož dokumenty jsou chráněny již pomocí zálohování. Navrhuji zavedení systému osobní zodpovědnosti všech zaměstnanců za předem svěřený majetek, kdy v případě prokázání úmyslného poškození těchto aktiv bude daná osoba penalizována snížením mzdy o celou nebo poměrnou část výše škody. Cílem tohoto opatření je opatrnosti zaměstnanců při používání firemní techniky.

3.3.4.4. Krádež aktiv

Metoda potlačení rizika: **Transfer**

Po zavedení monitorovacího systému do vnitřních prostor společnosti si organizace slibuje rapidní pokles jakýchkoliv krádeží z řad vlastních zaměstnanců. Krádežím a vloupáním z řad externích lidí je však velmi těžké, a mnohdy i příliš nákladné zabránit, proto navrhuji místo instalace senzorů pohybu, alarmů, bezpečnostních dveří, zámků a klíčů spíše pojištění proti krádeži, které by díky instalovanému systému nemělo být příliš nákladné. Toto opatření volím i proto, že z řad lidí mimo společnost k vloupání ještě nedošlo.

3.3.4.5. Ztráta peněžních prostředků

Metody potlačení rizika: **Transfer, redukce**

Po zavedení všech výše zmíněných opatření se toto riziko týká z velké části krachu banky, kdy navrhuji pojistit společnost právě proti krachu banky. Jelikož pravděpodobnost tohoto rizika je minimální, nejedná se o příliš nákladnou variantu.

Dalším způsobem, jak toto riziko potlačit, je rozprostření peněžních prostředků mezi více peněžních ústavů, z aktuálního jednoho, aby v případě krachu jednoho objektu nebyly ohroženy veškeré finanční prostředky společnosti.

3.3.4.6. Přerušení dodávky elektrické energie

Metoda potlačení rizika: **Redukce**

Jedná se o velmi vážné, nicméně nepříliš časté riziko pro společnost. V případě výpadku dodávky elektrické energie je veškerá produktivita společnosti nulová, jelikož stojí veškerá výroba, zpožďují se tak všechny plány výroby a při nedostatečné časové rezervě je společnost za nedodržení termínů penalizována.

Z tohoto důvodu navrhuji zakoupit dieselový agregát o dostatečném výkonu, který společnost po dobu výpadku dodávky elektrické energie bude zásobovat místo distribuční sítě.

3.3.4.7. Odchod klíčových zaměstnanců

Metoda potlačení rizika: **Redukce**

Odchod klíčových zaměstnanců je pro společnost kritický, skrze jejich vysokou specializaci a těžkou nahraditelnost. Navrhuji tedy zavedení zaměstnancům do mzdy variabilní složku, která bude vyplácena na základě výkonnosti a další bonusy, například možnosti školení, příspěvků na dopravu, stravování, firemního automobilu apod. Zavedení těchto bonusů by měl předcházet průzkum mezi zaměstnanci, o které bonusy by měli zájem. Výsledky by pak měly být vyhodnocení vedením společnosti.

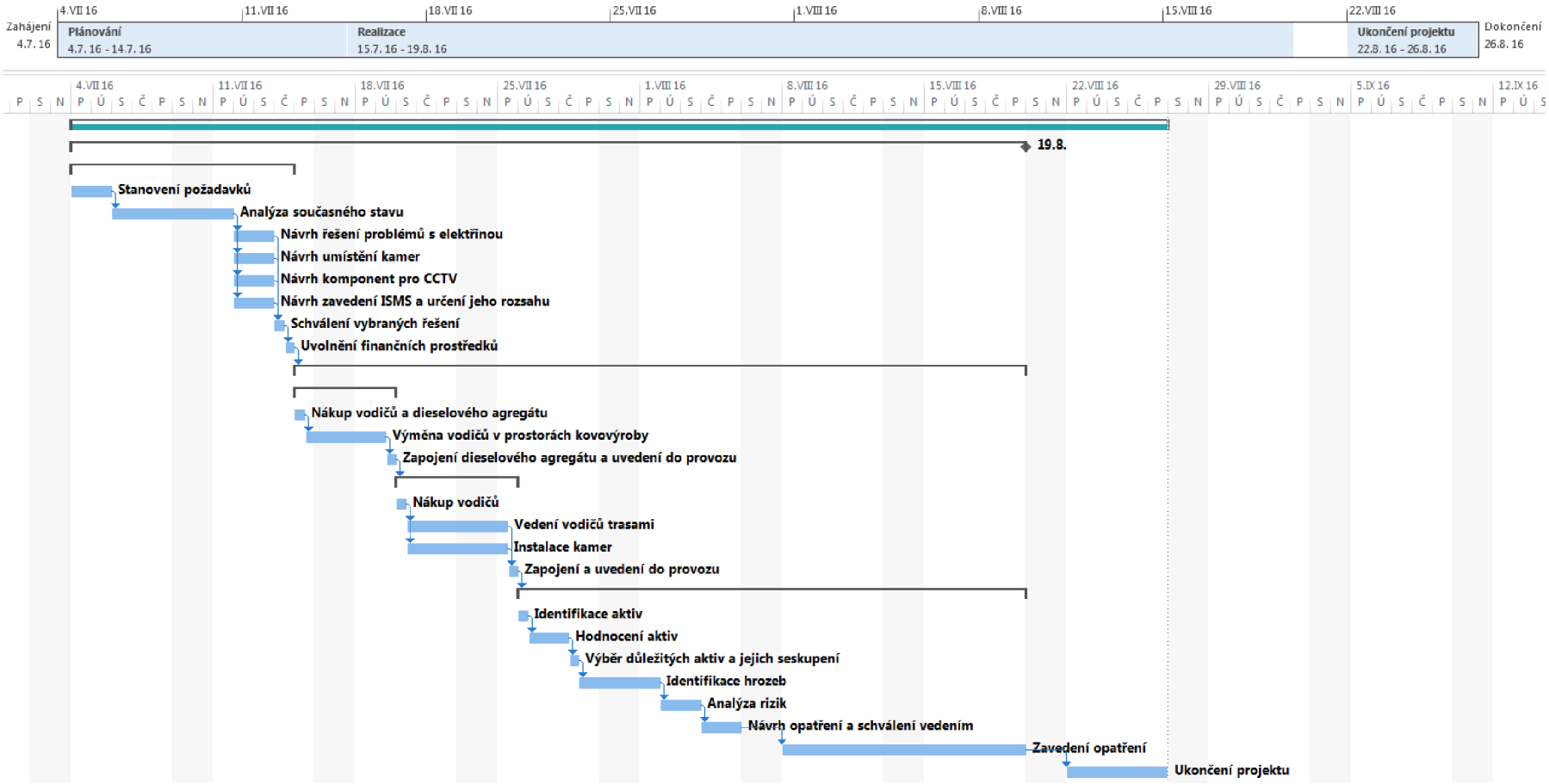
3.4. Management projektu

Celý projekt byl rozdělen na fázi plánování a realizaci, realizace pak na další, menší fáze, kdy na všechny fáze je třeba vyčlenit 40 pracovních dnů. Jednotlivé činnosti projektu lze vidět v tab.12 a obr.25. V části ukončení projektu je počítáno s informováním uživatelů o nově zavedených změnách, jejich školením na nové používání IT prostředků a také s určitou časovou rezervou, do které by mělo být vše hotovo. Kontrola účinnosti zavedených opatření by měla probíhat minimálně jednou za kvartál.

3.4.1. Časová náročnost

Tabulka 12: Časová náročnost projektu (Vlastní zpracování)

Název úkolu	Doba trvání	Zahájení	Dokončení	Předchůdci
Implementace systému CCTV a management informační bezpečnosti	**40 dny**	**4.7. 16**	**26.8. 16**	
Zahájení projektu	**35 dny**	**4.7. 16**	**19.8. 16**	
Plánování	**9 dny**	**4.7. 16**	**14.7. 16**	
Stanovení požadavků	2 dny	4.7. 16	5.7. 16	
Analýza současného stavu	4 dny	6.7. 16	11.7. 16	4
Návrh řešení problémů s elektřinou	2 dny	12.7. 16	13.7. 16	5
Návrh umístění kamer	2 dny	12.7. 16	13.7. 16	5
Návrh komponent pro CCTV	2 dny	12.7. 16	13.7. 16	5
Návrh zavedení ISMS a určení jeho rozsahu	2 dny	12.7. 16	13.7. 16	5
Schválení vybraných řešení	0,5 dny	14.7. 16	14.7. 16	6;7;8;9
Uvolnění finančních prostředků	0,5 dny	14.7. 16	14.7. 16	10
Realizace	**26 dny**	**15.7. 16**	**19.8. 16**	**11**
Řešení problémů s elektřinou	**3 dny**	**15.7. 16**	**19.7. 16**	
Nákup vodičů a dieselového agregátu	0,5 dny	15.7. 16	15.7. 16	
Výměna vodičů v prostorách kovovýroby	2 dny	15.7. 16	19.7. 16	14
Zapojení agregátu a uvedení do provozu	0,5 dny	19.7. 16	19.7. 16	15
Implementace CCTV	**4 dny**	**20.7. 16**	**25.7. 16**	**16**
Nákup vodičů	0,5 dny	20.7. 16	20.7. 16	
Vedení vodičů trasami	3 dny	20.7. 16	25.7. 16	18
Instalace kamer	3 dny	20.7. 16	25.7. 16	18
Zapojení a uvedení do provozu	0,5 dny	25.7. 16	25.7. 16	20;19
Implementace ISMS	**19 dny**	**26.7. 16**	**19.8. 16**	**21**
Identifikace aktiv	0,5 dny	26.7. 16	26.7. 16	
Hodnocení aktiv	2 dny	26.7. 16	28.7. 16	23
Výběr důležitých aktiv a jejich seskupení	0,5 dny	28.7. 16	28.7. 16	24
Identifikace hrozeb	2 dny	29.7. 16	1.8. 16	25
Analýza rizik	2 dny	2.8. 16	3.8. 16	26
Návrh opatření a schválení vedením	2 dny	4.8. 16	5.8. 16	27
Zavedení opatření	10 dny	8.8. 16	19.8. 16	28
Ukončení projektu	5 dny	22.8. 16	26.8. 16	29



Obrázek 25: Ganttův diagram projektu (Vlastní zpracování)

3.4.2. Rozpočet

Tabulka 13: Rozpočet pořizovaných prvků na projekt (Vlastní zpracování)

Popis	Značka	Označení	M. j.	Počet m.j.	Cena za m.j. [Kč] vč. DPH	Cena celkem [Kč] vč. DPH
Měděný kabel	CYKY	-	m	100	19,80 Kč	1 980,00 Kč
Dieselový agregát	Europower	EP7000TD	ks	1	90 000,00 Kč	90 000,00 Kč
Kroucený pár	OEM	-	m	500	4,00 Kč	2 000,00 Kč
IP kamera	HIKVISION	DS-2CD2622FWD-I(Z)(S)	ks	16	7 800,00 Kč	124 800,00 Kč
NVR zařízení	HIKVISION	DS-7600NI-E2/16P	ks	1	20 000,00 Kč	20 000,00 Kč
Pevný disk pro NVR 4TB	Seagate	ST4000DM000	ks	2	3 589,00 Kč	7 178,00 Kč
Pevný disk pro zálohy 4TB	Lenovo	ThinkServer	ks	1	16 383,00 Kč	16 383,00 Kč
Docházkový terminál	ADI	DT3000 SA	ks	2	20 449,00 Kč	40 898,00 Kč
Celkem						**303 239,00 Kč**

V tabulce výše je uveden rozpočet pouze za nově pořizované prvky, především pro první a druhou část návrhu. V rámci ISMS lze velkou část práce provést bez pořizování jakýchkoliv prvků, samotné náklady na vykonanou práci však v tabulce uvedeny nejsou a je jen na společnosti, jestli tuto práci ocení klasickou hodinovou sazbou nebo formou bonusu ke stávající mzdě. Dále není v tabulce zaznamenáno pojištění, ani proti krádeži, ani proti krachu banky. Těchto produktů je na trhu velmi velké množství, s možností nastavení nejrůznějších parametrů pojištění, a proto opět je jen na společnosti, jaký produkt si společnost vybere, dle vlastních preferencí. Skrze dostupnost práce pro širokou veřejnost jsou uvedeny internetové ceny, místo těch, kterých společnost reálně může dosáhnout.

Závěr

Diplomová práce se zabývala otázkami řešení velkého množství problémů společnosti MBG, spol. s r.o., sídlícím ve městě Zábřeh na Moravě. Jelikož má firma v tomto městě 2 objekty, je nutno upřesnit, že se práce zabývala řešením problémů na starším z nich.

Práce při řešení problematiky postupuje práce systematicky od řešení problémů s fungováním společnosti v době výpadku dodávky elektrické energie, přes zvýšení fyzické bezpečnosti v interních prostorách haly, až po zvýšení bezpečnosti informací. Návrh na zvýšení informační bezpečnosti vznikl na základě potřeb dodržet legislativu České republiky, modernizovat pracovní prostředí (digitalizovat velké množství dat) a také potlačit rizika, která stávající řešení obsahují.

Cíle práce se dle výsledků projektu zdají být splněny, především termín vyhotovení všech řešení, který měl být, dle požadavků společnosti, do začátku měsíce září. Termín ukončení projektu je uveden několik dnů před koncem měsíce srpna a je v něm počítáno i s menším zdržením na kterékoliv činnosti v podobě několikadenní časové rezervy. Všechna řešení byla navržena tak, aby byly všechny cíle splněny, společně s maximálním možným ohledem na všechny požadavky společnosti. Při průběhu projektu dle plánu by tohoto mělo být dosaženo. Jediným požadavkem společnosti, který není zcela splněn, je minimalizace nákladů. Ty jsou navýšeny skrze nutnost zakoupit náhradní zdroj elektrické energie a také skrze mé rozhodnutí nevybírat prvky pro implementaci pouze na základě ceny, ale především na základě poměru parametrů kvality, výkonu a ceny.

Jelikož nebyly zcela splněny požadavky společnosti na minimalizaci nákladů za každou cenu, snažil jsem se vykompenzovat tuto ztrátu v návrhu systému řízení bezpečnosti informací. Kompenzace je ve formě volby vlastních zaměstnanců společnosti na zavedení a následnou správu ISMS, místo outsourcingu externí firmou. Náklady na práci v této části projektu by tak měly být výrazně ušetřeny, společně s možností společnosti rozhodnout, zda zaměstnance za zavedení odmění standardní mzdou, či ve formě prémií.

Praktická kontrola ve formě reálných výsledků nyní není možná, jelikož je projekt plánován do budoucna. Jsou však určeny osoby odpovědné za kontrolu účinnosti zavedených opatření, včetně frekvence kontrol a osob pro následné sjednání nápravy.

Seznam použité literatury

(1) BIGELOW, S. Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů. 1. vydání. Brno: Computer Press, 2004. 990 s. ISBN: 80-251-0178-9.

(2) ČSN ISO/IEC 27001. Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky. Praha: Český normalizační institut, 2006.

(3) JANEČKOVÁ, E. a V., BARTÍK. Kamerové systémy v praxi. 1. vydání. Praha: Linde, 2011. 240 s. ISBN 978-80-7201-850-5.

(4) PUŽMANOVÁ, R. Moderní komunikační sítě od A do Z. 2. aktualizované vydání. Brno: Computer Press, 2006. 430 s. ISBN: 80-251-1278-0.

(5) TVRDÍKOVÁ, M. Aplikace moderních informačních technologií v řízení firmy. 1. vydání. Praha: Grada Publishing, 2008. 176 s. ISBN 978-80-247-2728-8

(6) ONDRÁK, V. *Přednášky – počítačové sítě*. Brno: VUT Fakulta Podnikatelská, 2010.

(7) ONDRÁK, Viktor. *Problematika ISMS v manažerské informatice*. Vyd. 1. Brno: CERM, 2013, 377 s. ISBN 978-80-7204-872-4.

(8) POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005, 309 s. Vysokoškolské učebnice (Aleš Čeněk). ISBN 80-868-9838-5.

(9) GITY - Bezpečnost v kostce. *Seriál o ISMS* [online]. © 2008 [cit. 2016-05-10]. Dostupné z: http://www.chrantesidata.cz/cs/art/1146-isms/

(10) ČSN ISO/IEC 27002. *Informační technologie - Bezpečnostní techniky – Systémy managementu bezpečnosti informací - Soubor postupů*. Praha: Český normalizační institut, 2011.

(11) ČSN ISO/IEC 27004. *Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Měření*. Praha: Český normalizační institut, 2011.

(12) ČSN ISO/IEC 27005. *Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací*. Praha: Český normalizační institut, 2013.

(13) ČSN EN 50110-1 ed.3. *Obsluha a práce na elektrických zařízeních – Část 1: Obecné požadavky.* Praha: Český normalizační institut, 2015

(14) DOUCEK, Petr, Luděk NOVÁK a Vlasta SVATÁ. *Řízení bezpečnosti informací.* 1. vyd. Praha: Professional Publishing, 2008. Vysokoškolské učebnice (Aleš Černík). ISBN 978-80-86946-88-7.

(15) BEZPLATNÁ PRÁVNÍ PORADNA. *Maximální doba uchovávání kamerových záznamů na pracovišti* [online]. © 2012 [cit. 2016-05-10]. Dostupné z: http://www.bezplatnapravniporadna.cz/online-zdarma/pracovni-pravo/nezarazene/13815-maximalni-doba-uchovavani-kamerovych-zaznamu-na-pracovisti.html

(16) MBG. *O firmě MBG* [online]. © 2016 [cit. 2016-05-11]. Dostupné z: http://www.mbg.cz/cs/clanek/mbg-o-firme-kdo-jsme-cesky-vyrobce-realizace-na-klic

(17) MAPY.CZ. *MBG spol, s.r.o.* [online]. © 2016 [cit. 2016-05-04]. Dostupné z: https://mapy.cz/letecka?x=16.8597081&y=49.8884778&z=19&source=firm&id=144630

(18) GOOGLE.CZ. *MBG spol, s r.o.* [online]. © 2016 [cit. 2016-05-04]. Dostupné z: https://www.google.cz/maps/@49.8764599,16.8918954,3a,75y,319.75h,87.02t/data=!3m6!1e1!3m4!1seY7kIj07rsJXz3jQZNOYew!2e0!7i13312!8i6656?hl=cs

(19) ČSN EN 50132-1. *Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích: Část 1: Systémové požadavky.* Praha: Český normalizační institut, 2010

(20) ADIGLOBAL. *2MP WDR Vari-focal Bullet Networ Camera HIKVISION DS-2CD2622FWD-I(Z)(S)* [online]. © 2016 [cit. 2016-05-17]. Dostupné z: http://www.adiglobal.cz/iiWWW/docs.nsf/all/95CEBAFE9962BFD4C1257ED70026D6F8/$FILE/kl_ds-2cd2622fwd-i(z)(s)_en.pdf

(21) ADIGLOBAL. *HIKVISION DS-7604NI-E1/4P and DS-7600NI-E2/8P (16P) series NVR* [online]. © 2016 [cit. 2016-05-18]. Dostupné z: http://www.adiglobal.cz/iiWWW/docs.nsf/all/82BD41B790826549C1257EEE00456715/$FILE/kl_ds-7616ni-e2_16p_a_en.pdf

(22) ADIGLOBAL. *DT3000 SA – Docházkový terminál s vestavěnou bezkontaktní čtečkou* [online]. © 2016 [cit. 2016-05-18]. Dostupné z: http://www.adiglobal.cz/iiWWW/docs.nsf/all/B3EB18742669ECF3C1257795008177B5/$FILE/DT3000%20SA%20-%20KL_CZ.pdf

Seznam obrázků

Seznam tabulek