VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

ZAVEDENÍ MANAGEMENTU INFORMAČNÍ BEZPEČNOSTI V MALÉM PODNIKU

THE IMPLEMENTATION OF INFORMATION SECURITY MANAGEMENT SYSTEM IN THE SMALL COMPANY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — RNDr. MARTIN RADVANSKÝ
AUTHOR

VEDOUCÍ PRÁCE — Ing. Petr Sedlák
SUPERVISOR

BRNO 2011

Tato verze diplomové práce je zkrácená (dle Směrnice děkanky č. 1/2010). Neobsahuje identifikaci subjektu, u kterého byla diplomová práce zpracována (dále jen „dotčený subjekt“) a dále informace, které jsou dle rozhodnutí dotčeného subjektu jeho obchodním tajemstvím či utajovanými informacemi.

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2010/2011
Ústav informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Radvanský Martin, RNDr.

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:

Zavedení managementu informační bezpečnosti v malém podniku

v anglickém jazyce:

The Implementation of Information Security Management System in the Small Company

Pokyny pro vypracování:

Úvod
Vymezení problému a cíle práce
Analýza současného stavu
Teoretická východiska řešení
Návrh řešení
Zhodnocení a závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

BROTBY, K. Information Security Governance: Guidance for Information Security Managers, Rolling Meadows (USA): IT Governance Institute, 2008. 78 s. ISBN 978-1-933284-73-6.
DOUCEK, P. NOVÁK, Luděk, SVATÁ, Vlasta. Řízení bezpečnosti informací. 1. vyd. Příbram: PROFESSIONAL PUBLISHING, 2008. 239 s. ISBN 978-80-86946-88-7.
GREGORY, P. Enterprise Information Security for Non-Technical Decision Makers, Harlow (Great Britain): Pearson Education Limited, 2003. 167 s. ISBN 0-273-66157-4.
POŽÁR, J. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2005. 309 s. ISBN 80-86898-38-5.
STRNÁD, O. Systémový prístup k riadeniu informačnej bezpečnosti. 1. vyd. Trnava (Slovensko): SP Synergia, 2008. 233 s. ISBN 978-80-89291-20-5.
TULLOCH, M. Microsoft Encyclopedia of Security, Washington (USA): Microsoft Press, 2003. 480 s. ISBN 0-7356-1877-1.

Vedoucí diplomové práce: Ing. Petr Sedlák

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2010/2011.

L.S.

Ing. Jiří Kříž, Ph.D. Ředitel ústavu	doc. RNDr. Anna Putnová, Ph.D., MBA Děkan fakulty

V Brně, dne 13.05.2011

Abstrakt

Obsahem této diplomové práce je návrh zavedení managementu informační bezpečnosti v malém podniku. Úvodní část práce je zaměřena na shrnutí teoretických poznatků z bezpečnosti informačních systémů a popisuje obsah norem řady ČSN ISO/IEC 27000:2006. Praktická část práce pak tyto teoretické poznatky aplikuje při zavedení ISMS v malém podniku. Celá implementace ISMS je rozdělena do tří částí, přičemž tato práce podrobně popisuje první etapu.

Klíčová slova

Informační bezpečnost, informační bezpečnostní rizika, management informační bezpečnosti, bezpečnostní politika, normy bezpečnosti IT, ISO/IEC 27000.

Abstract

This diploma thesis deals with methods of management of information security in the small company. The thesis is divided into two main parts. The first part of this thesis is focused on theoretical aspects of information security and contains description of standards ČSN ISO/IEC 27000:2006. The practical part of this work is about the project of implementation of the information security management system in the small company. The implementation is divided into three separate parts with the first part of implementation being described in detail.

Keywords

Information security, information security risks, management information security, security policy, standards for IT security, ISO 27000.

BIBLIOGRAFICKÁ CITACE

RADVANSKÝ, M. Zavedení managementu informační bezpečnosti v malém podniku. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2011. 94 s. Vedoucí diplomové práce Ing. Petr Sedlák.

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Dále prohlašuji, že citace použitých pramenů je úplná, že jsem v práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským, ve znění pozdějších předpisů).

V Brně 14.5.2011

……

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu diplomové práce Ing. Petru Sedlákovi, za podmětné připomínky a konzultace této práce, panu Robertovi Gogelovi za konzultace a rady při implementaci.

Obsah

Úvod

Při pohledu do historie můžeme pozorovat, že vládcové a jejich generálové spoléhali na velmi důmyslné komunikační systémy, které byly nezbytné, aby mohli vládnout svým zemím anebo velet armádám. Je zcela nepochybné, že si uvědomovali, jaký význam mají tyto informace a jaký by byl důsledek toho, kdyby se tyto strategické informace dostaly do nepovolaných rukou. V těchto historických dobách se rozvíjely techniky šifrování jako metoda ochrany informací a samozřejmě i techniky pro luštění těchto šifer. Ochrana takových informací byla relativně jednoduchá, protože tyto informace byly soustředěny a dostupné pouze úzkému okruhu lidí. Tato situace ovšem nevydržela věčně.

S rozmachem výpočetní techniky, od poloviny minulého století se stále větší a větší množství informací shromažďuje v informačních systémech a tím se situace radikálně mění a komplikuje. Uložená data jsou dostupná narůstajícímu počtu uživatelů nejen vlastních informačních systémů, ale i v rámci zapojení do globální počítačové sítě. Tento stav vede k velmi vysokým nárokům na jejich zabezpečení. V dnešní době jsou informace tím nejdůležitějším prvkem pro podniky či stát. Toto si uvědomují samozřejmě i lidé, kteří by se rádi k těmto informacím dostali a neváhají využít jakéhokoliv prostředku na jejich získání. Téměř na denním pořádku jsou v médiích informace o tom, jak jsou počítače organizací nebo jen obyčejných lidí napadány útočníky.

Jako nejčastějším cílem takovýchto útoků jsou zejména osobní data, informace o technologiích, obchodní informace podniků, bankovní účty. V případě, že se neoprávnění lidé dostanou k těmto informacím, jsou následky pro podnik fatální a mohou vést i k jeho naprosté likvidaci. Proto, aby se minimalizovaly možné průniky či zneužití informačních systémů, vynakládají podniky, instituce, ale i občané nemalé prostředky na jejich ochranu.

Na bezpečnost informačních systémů a obecně správu informací je třeba nahlížet jako na trvalý a průběžně inovovaný proces, ve kterém je třeba podchytit všechny faktory, které by mohly být příčinou vzniku možných slabých míst v zabezpečení. Je třeba podchytit nejenom vlastní výpočetní techniku, ale i fyzickou ochranu budov, personálu a v neposlední řadě i proaktivně vyhledávat možná rizika. Zde je možné uplatnit postupy, které byly postupem času ověřeny a zaváděny ve formě managementu informační bezpečnosti.

Teoretická část této práce je tvořena dvěma kapitolami. V kapitole 2 jsou uvedeny základní prvky bezpečnosti informačních systémů a je zde uveden popis managementu informační bezpečnosti. Ve třetí kapitole jsou pak shrnuty metodické pokyny pro zavádění managementu informační bezpečnosti v podniku, které vycházení z norem řady ISO/IEC 27000.

V praktické části diplomové práce jsou dříve uvedené postupy aplikovány na příkladu malého podniku. V pěti kapitolách je pak popsána realizace vybraných opatření z norem takovým způsobem, aby se stávající situace v uvedeném podniku vzhledem k bezpečnosti informací zlepšila.

1 Vymezení problému a cíl práce

Práce je zaměřena na problematiku řešení managementu informační bezpečnosti v malém podniku, který v rámci své běžné činnosti přichází do styku s citlivými informacemi a ve svém informačním systému má také důvěrná data uložena. Uvedený podnik musí ze zákona splňovat předpisy pro nakládání s osobními údaji a samozřejmě se snaží řešit i otázku bezpečnosti a ochrany informací. Protože bezpečnost informací není jen o vlastním zabezpečení fyzických zařízení obsahujících tyto informace, je třeba komplexnější pohled zahrnující současně také fyzickou ochranu budov, zařízení a současně také poučení osob, které mohou s chráněnými informacemi přijít do styku.

Cílem této práce je analýza současného stavu bezpečnosti informací v malém podniku a návrh na zlepšení zjištěného stavu za využití metodiky zahrnuté v ISO/IEC 27000. Tato práce si neklade za cíl komplexní řešení problematiky managementu informační bezpečnosti podle normy ISO, ale své návrhy zaměřuje pouze na ty aspekty, které jsou pro danou firmu akceptovatelné při zachování přiměřených nákladů.

V této práci jsem čerpal z veřejně dostupných zdrojů, co se týká zákonných požadavků na práci s osobními údaji, dále pak se zdroji jako jsou normy ISO či v závěru uvedená odborná literatura a z úředních dokumentů jako jsou metodické pokyny, vnitřní opatření či projektové dokumentace budovy.

2 Teoretická východiska

Tato práce se zaměřuje na bezpečnost v oblasti informačních technologií (IT). Ne vždy je ovšem tento pojem správně chápán. Nejčastěji je s pojmem bezpečnosti IT spojována v podnikovém prostředí bezpečnost informačních systémů (IS) a těmito systémy zpracovávanými a uloženými informacemi, řízení přístupu k IS, internetu a citlivým datům. Obecně bývá bezpečnost personifikována na cokoliv, co je možné zpracovávat pomocí výpočetní techniky.

Tento pohled na bezpečnost IT není zcela úplný a může vést k velmi vážným důsledkům pro organizaci. Jednou z velmi opomíjených bezpečnosti je bezpečnost personální, fyzická, komunikační a také je třeba brát v potaz i minimalizaci hrozeb vzniklých z přírodních katastrof. Tyto opomíjené faktory, pak způsobí, že celý systém bezpečnosti IT v podniku je vlastně zranitelný a snadno napadnutelný. Jako příklad takového přístupu lze uvést velmi dobře zabezpečený informační systém pomocí přístupových hesel pro uživatele, ovšem tito si špatně zapamatovatelná hesla klidně přilepí na okraj monitoru. Takováto situace je k vidění zejména v menších firmách a rozhodně není výjimečná.

V dalším textu budou podrobně probrány základní pojmy z oblasti bezpečnosti informačních a komunikačních technologií (ICT) a managementu bezpečnosti informačních systémů.

2.1 Hlavní pojmy z oblasti bezpečnosti IS

2.1.1 Důvody, proč se zabývat informační bezpečností

Pro jakýkoliv podnik, který se chce prosadit na trhu je v dnešním stavu technologického pokroku nevyhnutelné, aby zpracovával velké množství informací, které se tak stávají jeho nejcennějšími aktivy. Metody pro zpracování dat jsou stále zdokonalovány a správné vyhodnocení těchto informací přináší podnikům nemalé konkurenční výhody. Z tohoto plyne, že informace jednoho podniku jsou pro jiného velmi užitečné a to vyvolává potřebu tyto informace zabezpečit.

Informační bezpečností se v minulosti zabývaly organizace spojované se státní bezpečností a utajováním důležitých strategických informací. Postupem času se ovšem obor rozšířil do obecně využívaných metodik a pro spolupráci se státní správou je v mnoha případech dokonce nezbytné, aby organizace, která se chce podílet na státních zakázkách, byla schopna splňovat požadavky na informační bezpečnost a byla i certifikována. (DOUCEK P., 2008)

Problematika informační bezpečnosti je velmi široká, zahrnující všechny faktory, které se mohou podílet na stavu, jež by umožnil nepovolaným osobám dostat se k citlivým informacím. Samotné informace musí být chráněny proti zneužití ve všech etapách jejich vlastního zpracování. Zároveň také ale musí být zabezpečena jejich dostupnost. Je tedy třeba přijímat v organizaci opatření z hlediska bezpečnosti i pro takové běžné činnosti, jako je posílání emailů, faxů, tisk, zálohování dat.

Bohužel smutným faktem je, že samotná problematika informační bezpečnosti je stále v našich končinách velmi podceňována. Mnoho manažerů podniků si myslí, že data organizace a zpracování informací v organizaci není třeba chránit, a tak vynakládají na informační bezpečnost minimální výdaje. Pro případného konkurenta je možnost získání našich dat velmi lákavé a je jisté, že se o to v případě slabé ochrany může pokusit. Zákony v ČR upravují pouze některé aspekty pro ochranu osobních informací, zejména nakládání s osobními údaji a neřeší komplexní problematiku informační bezpečnosti, jelikož vlastně ani nemohou. Každý podnik má svá vlastní specifika a je na něm, aby si bezpečnost řešil ve své režii, protože má dokonalou znalost svého prostředí ICT.

S růstem hodnoty informací se lze na informace dívat jako na další základní zdroje firmy. Tak v podnicích dostáváme výrobní, lidské, kapitálové a informační zdroje. Informační zdroje mohou často tvořit majoritní podíl na aktivech firmy. Aby bylo možné tyto zdroje přiměřeně a ekonomicky chránit, je nutné si tyto informační zdroje ocenit podle jejich významu a případného dopadu na chod podniku.

Z výše uvedeného je tedy patrné, že není stanoveno jedno konkrétní řešení bezpečnosti ICT v organizaci, ale pro každý podnik se toto vytváří tzv. ad hoc. Ovšem jako pro většinu lidských činností, i pro oblast bezpečnosti existují určité mechanismy, návody a doporučení, jakým způsobem tuto problematiku řešit. Je třeba si uvědomit, že samotné řešení problému bezpečnosti přináší nutnost řešit problémy z oblastí fyzické bezpečnosti, počínaje budovami, přístupy do nich, jednotlivými zařízeními, kabelovými propojeními mezi počítači či zařízeními. Řeší se dostupnost dat a chování systému v případě poruchy, zálohování dat, ochrany počítačů pomocí antivirů, antispamů, firewallů, šifrování dat a jejich přenosy. Z jiného úhlu pohledu se řeší dodržování směrnic, proškolování pracovníků, analyzují se možná rizika. (GREGORY P., 2003)

Z uvedeného neúplného výčtu oblastí je zřejmé, že náklady na bezpečnost ICT v podniku budou jistě nemalé. Co je tedy motivačním motorem proto, aby podniky zavedly a následně používaly postupy vedoucí k bezpečným IS a případně si provedly certifikaci svého systému bezpečnosti a řízení bezpečnosti v podniku?

1. V dnešní době jsou běžně podniky certifikovány pro systém managementu jakosti podle normy řady ISO 9000. Tyto podniky se pak v očích jejich zákazníků stávají kvalitnější a důvěryhodnějšími partnery. Stejně jako tato norma pro management jakosti řízení, zavedením managementu bezpečnosti informačních systémů podle normy řady ISO 27000 pro okolí podniku znamená, že ve firmě existuje definovaná bezpečnostní politika. Tato skutečnost dává obchodním partnerům důvěru ve svého dodavatele a mohou si být jisti, že nemůže dojít k zneužití či vyzrazení důvěrných dat.
2. Podnik, který aplikuje ISMS je schopen do bezpečnosti investovat přesně optimální množství nákladů tím, že jsou v rámci zavádění ISMS v podniku prováděna ohodnocení chráněných informací a na tomto základě pak vybrána adekvátní řešení či technologie.

3. V podniku je definována vnitřní bezpečnostní politika, která definuje, jak chránit podnik proti vnějším útokům, jakým způsobem pracovat s elektronickými dokumenty, jak chránit zaměstnance a jejich emailové účty před podvodnými emaily a podobně. Tím pádem se minimalizuje riziko úniku dat či zneužití firemních počítačů nebo i porušení podnikového informačního systému.
4. V podniku je zavedeno dělení pracovníků do jednotlivých skupin s minimálními přístupovými právy, které vyplývají z povahy jejich činnosti. Tím je docíleno stavu, kdy pracovníci oddělení IT jsou v pozici, kdy mají také pouze přístup k nejnutnějším informacím a systémům v rámci jimi vykonávaných činností.
5. Aby byl tento systém funkční a hlavně flexibilní vzhledem k technologickým trendům a inovacím, jsou v rámci ISMS definovány mechanismy, na jejichž základě jsou řešeny neočekávané události, detekovány nově vzniklé rizikové stavy a tyto náležitě dokumentovány a nachystány scénáře jejich řešení. Tímto se celý systém ISMS postupně zpřesňuje a stává se tak více odpovídajícím realitě v podniku.

Tyto zde uvedené důvody mohou být právě tím faktorem, který nakonec rozhoduje, zda podnik získá zakázku, či nikoliv. V dnešní době je jakákoliv konkurenční výhoda, zejména dobře prezentovaná, klíčová pro úspěšné společnosti. (POŽÁR J., 2005)

2.1.2 Obecné pojmy informační bezpečnosti

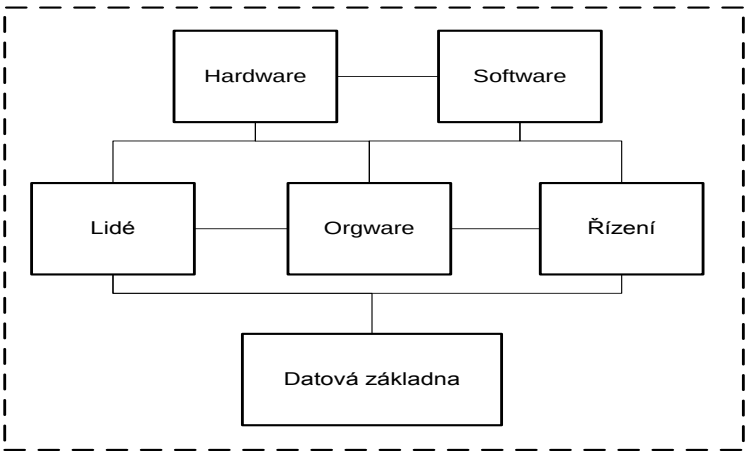
Při řešení informační bezpečnosti se setkáváme s pojmy, které nemusí být úplně zřejmé, a proto v následujících odstavcích budou uvedeny jejich krátká vysvětlení. (TULLOCH M., 2003)

- **Informační aktiva** – jedná se o aktiva, která mají pro organizaci hodnotu a význam, převážně se jedná o vlastní data zpracovávané určitým softwarem na patřičném hardware.
- **Citlivá data** – data, která jsou důležitá pro chod podniku. Pokud tato data jsou zneužita, zničena, či jen zveřejněna, mohou mít nedozírné následky pro chod podniku. Tato data mohou být data o technologiích, osobní informace, nabídky zákazníkům atd.
- **Autorizace** – proces posouzení, zda osoba nebo zařízení je oprávněno provádět požadované činnosti.
- **Autentizace** – proces, při kterém dochází k ověření identity osoby či zařízení. Zde existuje celá řada možností, jak toto provádět, od prostého ověření heslem, čipovou kartou, otiskem prstu či snímačem sítnice nebo jiné technologicky dostupné metody.
- **Autenticita** – vlastnost, která zajišťuje, že identita, původ osoby nebo zdroje je přesně taková, za kterou je prohlašována. Obecně autenticitu vztahujeme na různé entity, jako jsou uživatelé, procesy, systémy nebo informace.

- **Nepopiratelnost** – doplnění autenticity o vlastnost nemožnosti popření původu daného zdroje. (elektronický podpis, datová schránka atd.)
- **Důvěrnost** – zajištění stavu, kdy jsou informace dostupné pouze těm osobám či zařízením, které jsou autentizovány a autorizovány pro přístup k nim.
- **Dostupnost** – vlastnost dat nebo jiného zdroje, být definovaným způsobem po celou nezbytně nutnou dobu pro všechny autentikované a autorizované osoby či systémy přístupná.
- **Integrita** – pro zaručení správnosti dat či informací, musí být povoleno provádět změny v systému či datech pouze osobám nebo procesům, které jsou pro tuto činnost autentikovány a autorizovány.
- **Hrozba** – jedná se o možné zdroje ohrožení informačních aktiv podniku. Může se jednat o možnost vzniku požáru, možnost zaplavení, možnost odposlechu kabelového vedení, možnost útoku na webový server podniku atd.
- **Riziko** – každá potenciální hrozba představuje pro podnik určité riziko, že bude naplněna. Některé hrozby lze eliminovat za použití patřičných opatření, a tím i minimalizovat či úplně vyloučit riziko. Některé hrozby nelze ani omezit či vyloučit (případně s velmi vysokými náklady)

2.1.3 Informační systém

Centrálním místem, kde se v podniku shromažďují a vyhodnocují data je informační systém. Pod pojmem IS je širší veřejností obecně chápán nějaký software, ve kterém se shromažďují informace zejména účetního, personálního či výrobního charakteru. Tento pohled je ovšem silně zjednodušený. Při hlubším zkoumání lze pojem informační systém spíše definovat jako určitou skupinu prvků, jejich vzájemných vazeb a specifického chování.(Koch M.,2010)



Obr. 1 Informační systém (Zdroj: Koch M., 2010)

V případě informačních technologií je sice hlavní částí IS opravdu hardware a software, ovšem neméně důležité jsou i ostatní na první pohled méně viditelné části IS. V podnicích existují pravidla a definované odpovědnosti, kdo, kdy a co má do informačního systému vkládat, případně jiná pravidla či definované odpovědnosti. Tyto postupy lze sdružit do pojmu orgware. Nemalou měrou na správném fungování a využívání informačního systému jsou také schopnosti lidí, kteří se systémem pracují. Zcela jistě zde hraje roli i management firmy, který řídí rozvoj systému a určuje úroveň řízení. Na datovou základnu lze pohlížet jako na množinu požadovaných dat, které proto, aby plnila svou funkci, musí splňovat požadavky na poskytnutí úplných a správných informací, v tom správném čase a na správném místě.(Koch M., 2010)

2.1.4 Informační bezpečnost

Definic informační bezpečnosti je celá řada. Ze zahraniční literatury zde uvádím dvě, které jsou dle mého názoru dostatečně srozumitelné.

- Informační bezpečnost je činnost, jejímž cílem je zabezpečit informační systémy firmy a data v těchto systémech obsažených tak, abychom mohli zajistit jejich integritu dostupnost a důvěrnost. (KAJAVA J., 2006)
- Informační bezpečnost není pouze interní věcí organizace, ale v době rozvinutých elektronických komunikací, také mezi organizacemi a státní správou. Informační bezpečnost podniku také dopadá na jeho obchodní partnery. Je proto běžné, že se požaduje v rámci dobrých obchodních vztahů, aby si obchodní partneři navzájem demonstrovali, jaké mechanismy podniky používají, k zabezpečení informací a informačních systémů. Organizace často toto řeší zavedením bezpečnostních standardů a samozřejmě certifikací. (STRNÁD, O. 2008)

Do informační bezpečnosti se zahrnují oblasti jako je problematika datových přenosů, ochrana počítačových sítí, kabelových i bezdrátových propojení, ochrana před vnějšími i vnitřními útoky, autentizace, autorizace, fyzická ochrana budov, proškolování personálu, definice aktiv podniku a jejich zabezpečení, identifikace a analýza rizik, scénáře obnovy dat při nenadálých událostech, zajištění dostupnosti dat, zálohování, definování a dodržování bezpečnostních směrnic atd.

Z uvedeného je vidět, že řešení informační bezpečnosti na obecné úrovni je velice komplexní problém a každé řešení je v podstatě vytvářeno přesně pro potřeby dané organizace. Pro zavedení informační bezpečnosti nestačí pouze podpora ze strany oddělení informačních technologií, ale musí být dosaženo podpory napříč celou organizací, počínaje výkonnými pracovníky konče u vedení firmy.

Při řešení informační bezpečnosti se tedy snažíme o zamezení informačním incidentům. Tyto incidenty mohou vznikat, ať už úmyslně za účelem získání informací podniku, či neúmyslně. Mezi neúmyslné narušení informační bezpečnosti lze zařadit běžné situace, které potkáváme téměř denně. Sem patří chyby v software či hardware, poruchy napájení, chyby v síťových komunikacích, malá kvalifikace pracovníků, z ní plynoucí chybná obsluha software či zařízení, nedodržování vnitřních směrnic a samozřejmě i vlastní informační systém, který neúplně či vůbec neřeší informační bezpečnost.

Každá společnost, která si je vědoma svých informačních aktiv, by měla ustanovit bezpečnostní politiku. Tato politika musí být základním konceptem, který uvnitř společnosti definuje, jakým způsobem bude podnik chránit své informace. Stanovuje cíle, použité strategie, definuje vyhodnocování a monitorování průběhu, stanovuje nástroje, prostředky a bezpečnostní mechanismy.

2.1.5 Komunikační bezpečnost

Informační technologie jsou založeny na komunikaci a tato tvoří potenciálně velmi rizikovou oblast při řešení bezpečnosti ICT. Cílem v komunikační bezpečnosti je vytvořit a udržovat takovou komunikační infrastrukturu, které bude splňovat základní požadavky na komunikaci mezi systémy.

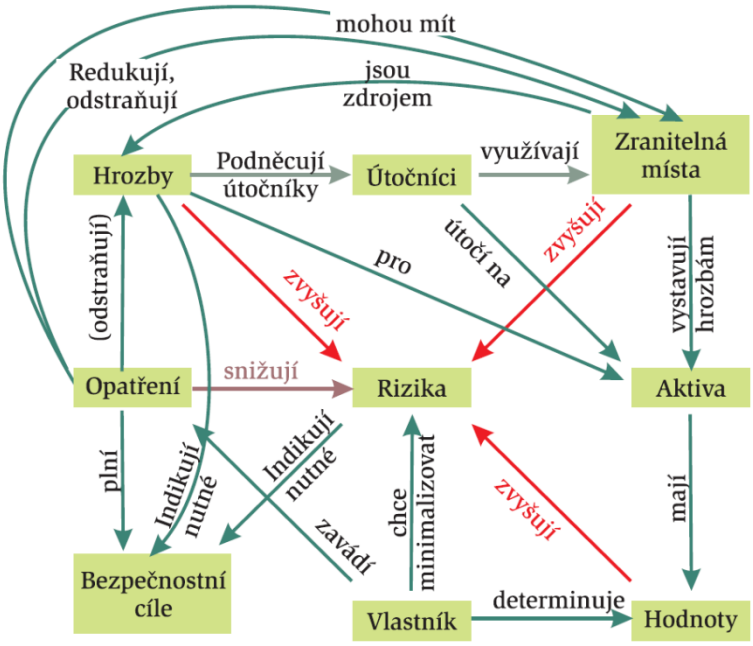
Hlavními faktory, které budeme požadovat, jsou v komunikační infrastruktuře podniku a IS požadavky na zajištění důvěrnosti a autenticity přenášených dat. Tyto požadavky pak musí být zajištěny i v rámci různorodých komunikačních prostředí, jako jsou kabelové instalace, bezdrátové spoje, či jen vzdálené přístupy do firemního prostředí z vnějšku.

Komunikační kanály se stávají potenciální cestou možného průniku do podnikových sítí, či jen odposlechu a získání citlivých informací. Proto je třeba této oblasti věnovat mimořádnou pozornost a zabezpečení komunikační bezpečnosti vyžaduje většinou vyšší náklady, sledování a zavádění nových ochranných opatření, periodické testování komunikační bezpečnosti. Rozmachem technologií, které umožňují on-line komunikaci se zákazníky či partnery, internetovou telefonii či jen vzdálený přístup do firemní sítě, se zefektivnily a zkvalitnily podnikové IS, čímž inovativní podniky získaly určitou

konkurenční výhodu. Bez důsledného zabezpečení komunikací se ovšem tato výhoda může snadno stát začátkem konce podniku.

2.1.6 Obecný model bezpečnosti ICT

Řešení bezpečnosti informačních systémů je dlouhodobý proces, jehož cílem je neustále se zlepšovat a pružně reagovat na nově vznikající rizika. Následující obrázek zachycuje obecný model bezpečnosti. V tomto modelu jsou zachyceny hlavní požadavky na řešení bezpečnosti, přičemž jsou zde zachyceny vazby mezi komponentami bezpečnosti IS.



Obr. 2 Obecný model bezpečnosti informačních technologií (Zdroj: STAUDEK J., 2007)

Bezpečnost ICT je globálním problémem, a tak je možné nalézt kuchařky, které řeší, jakým způsobem se dá poučit z chyb jiných. Tyto návody a obvyklá oborová řešení jsou shrnuty do světově uznávaných norem. Při jejich aplikování, dodržování a po certifikaci je možné organizaci považovat za bezpečného partnera v obchodním styku.

Při pohledu na schéma modelu bezpečnosti informačních technologií je třeba si všimnout, že zde nefigurují IT technologie. Model využívaný k řešení informační bezpečnosti totiž obsahuje mnohem více a zahrnuje mimo bezpečnost IT, také bezpečnost personální, infrastruktury, budov a prostředí, požární ochranu, poplašné systémy, kontroly přístupu a další.

2.2 Zákony a normy v oblasti bezpečnosti IT

Tak jako v každém oboru lidské činnosti, také pro oblast managementu bezpečnosti informačních systémů, existují mezinárodně uznávané standardy, které vytváří nadnárodní organizace a reflektují specifika jednotlivých národních normalizačních institutů. Protože bezpečnost informačních systémů a její řízení je třeba založit na přesně a jasně definovaných postupech mezinárodní normy vlastní implementaci velmi usnadňují. Přestože normy jsou v rámci České legislativy brány pouze jako doporučení pro řešení určité problematiky, je velmi vhodné se těmito normami řídit, čímž se velmi usnadní případná certifikace podniku management bezpečnosti informačních systémů (ISMS). V legislativě České republiky jsou definovány zákony, které jsou pro podniky závazné a musí být bezpodmínečně a bezodkladně plněny.

Mezinárodní organizace podílející se na tvorbě dále uvedených norem jsou:

- International Organization for Standardization (ISO).
- International Electrotechnical Comission (IEC)
- Internation Telecommunications Union (ITU)
- The Institute of Electrical and Electronics Engineers (IEEE)

2.2.1 Zákony v legislativě České republiky

V legislativě České republiky lze nalézt několik zákonů, které mohou mít vliv na otázku bezpečnosti a zabezpečení informačních systémů. Není náplní této práce komentovat či jinak popisovat zákony, proto jsou v následujících řádcích pouze uvedeny odkazy na jednotlivé zákony a čtenář si může jednotlivé zákony najít v případě zájmu ve sbírce zákonů České republiky. V následujícím textu jsou některé uvedeny. Vzhledem k tomu, že v zákonech naší republiky je velká vzájemná provázanost, jsou zde uvedeny pouze některé zákony, které budou využity v praktické části této práce.

- **Zákon č. 101/2000 Sb. o ochraně osobních údajů.** „*Tento zákon se vztahuje na osobní údaje, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci, jakož i fyzické a právnické osoby a řeší problematiku zpracování osobních údajů*.“
- **Zákon č. 227/2000 Sb. o elektronickém podpisu.** „*Tento zákon upravuje používání elektronického podpisu, poskytování souvisejících služeb, kontrolu povinností stanovených tímto zákonem a sankce za porušení povinností stanovených tímto zákonem.*“
- **Zákon č. 480/2004 Sb. o některých službách informační společnosti**. „*Tento zákon zdůrazňuje povinnost členských států EU zajistit důvěrný charakter sdělení přenášených pomocí veřejné komunikační sítě a veřejně dostupných elektronických služeb*.“

- **Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností (zákon č. 310/2002).** „*Tento zákon vymezuje skutečnosti, které je nutno v zájmu České republiky utajovat způsob jejich ochrany, působnost a pravomoc orgánů státu při výkonu státní správy v oblasti ochrany utajovaných skutečností, povinnosti orgánů státu, práva a povinnosti fyzických a právnických osob a odpovědnost za porušení povinností stanovených tímto zákonem a upravuje postavení Národního bezpečnostního úřadu.*“

(citace z uvedených zákonů)

2.2.2 Normy ISO/IEC řady 27000

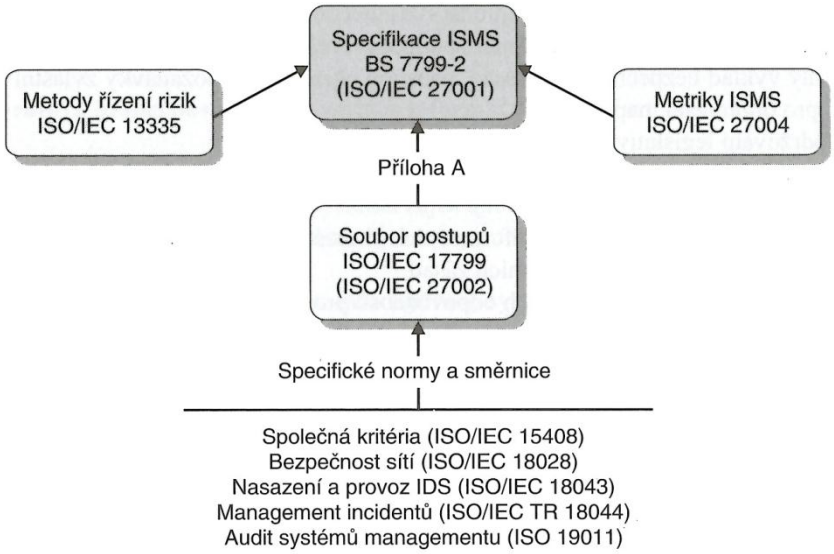
Pro oblast bezpečnosti informačních systémů byla Britským normalizačním institutem uvedena v platnost v roce 1995 norma s označením BS7799. Tato národní norma položila základ pro zavádění a implementaci managementu bezpečnosti informačních systémů. Postupem času se tato norma začala uplatňovat i v jiných zemích a byla označována jako ISMS (Information Security Management System). Při návrhu této normy byl obzvláště kladen důraz na univerzalitu ve vztahu k technologiím, čímž byla tato norma schopna efektivně umožnit podnikům její správnou implementaci.

Tato norma BS7799 je cíleně zaměřena na faktory dostupnosti, důvěrnosti a integrity informací a informačních systémů v podniku. Norma se snaží komplexně řešit obranu proti možným hrozbám a nebezpečím, které byly v podniku identifikovány, oceněny a mohou mít dalekosáhlé dopady. Tuto britskou normu začaly hned po jejím vydání používat podniky ve všech částech světa a postupem času byla tato národní norma v roce 2000 přijata jako nadnárodní norma standardu ISO pod označením ISO 17799.

Mezinárodní organizace pro normalizaci v roce 2005 vydala sérii norem ISO/EIC 27000 zahrnující systém řízení informační bezpečnosti, přičemž tyto normy vychází z normy ISO 17799. Normy řady ISO/IEC 27000 jsou tvořeny následujícími částmi:

- **ISO 27000** – zavádí pojmy, definice a terminologický slovník pro všechny následující normy řady 27000.
- **ISO 27001** – norma byla vydána koncem roku 2005 a jedná se o normu, podle které se systémy řízení bezpečnosti informací certifikují. (původní norma BS7799-2)
- **ISO 27002** – jedná se o aktuální verzi normy od července 2007 je tato norma označována jako ISO/IEC 27002:2005. (nahradila normu ISO/IEC 17799:2005). Obsahuje sbírku nejlepších bezpečnostních praktik a může být využita jako seznam postupů, které je nutno pro bezpečnost informací v organizaci provést.
- **ISO 27003** – poskytuje implementační návody pro ostatní normy řady 27000.

- **ISO 27004** – tato norma poskytuje doporučení pro vývoj a používání metrik a pro měření účinnosti zavedeného systému řízení bezpečnosti informací (ISMS) a účinnosti opatření nebo skupin opatření, jak je uvedeno v ISO/IEC 27001.
- **ISO 27005** – norma se zaměřuje na řízení bezpečnostních rizik informačních technologií.
- **ISO 27006** – obsahuje požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací.



Obr. 3 Normy ze série ISO/IEC 27000 a další normy (Zdroj: SMEJKAL V., 2010)

Z výše uvedeného výčtu je zřejmé, že problematika řízení bezpečnosti informací a informačních technologií je řešena za pomocí postupů definovaných v patřičných normách (nejen v řadě 27000). Tato obsáhlost může odrazovat zejména malé podniky od jejich použití, jelikož v normách uváděné postupy kladou nemalý důraz na vytváření nejrůznějších dokumentů a jejich neustálých revizí. Tato skutečnost sama o sobě by ovšem neměla být pro podniky důvodem, proč metodiku nepoužít. Normy tvoří obvyklé doporučené postupy a podnik, který se rozhodne řešit problematiku ISMS, si může pro zavedení zvolit pouze oblasti, které je schopen zvládnout.

2.2.3 ČSN ISO/IEC 27001:2006

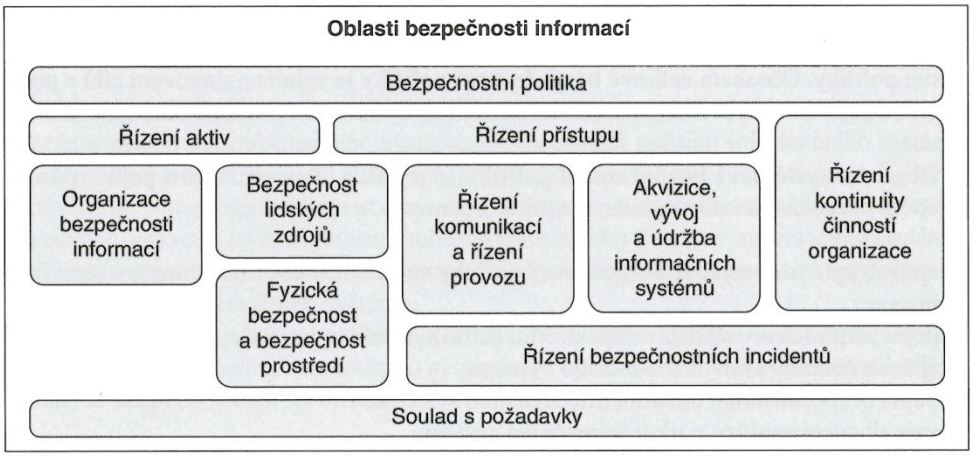
Tato norma definuje oblasti, které je třeba zahrnout při ochraně a řízení informací v podniku. Systém ISMS umožňuje vedení podniku řídit a monitorovat informační bezpečnost, minimalizovat obchodní rizika a zabezpečit, aby byly splněny požadavky bezpečnosti informací na úrovni podniku, zákazníků a byly také splněny případné zákonné požadavky na uchovávaná či zpracovávaná data.

Tato norma, potažmo ISMS může být aplikována v libovolné organizaci. Tento standard je určen pro každou organizaci, která využívá interní či externí počítačové systémy, vlastní či

zpracovává citlivé informace, či je činnost podniku závislá na informačních systémech. Z globálního pohledu je možné tedy říci, že ISMS by mělo tvořit nedílnou součást podnikových strategií.
Základním záměrem ČSN ISO/IEC 27001:2006 je zajištění důvěrnosti, integrity a dostupnosti informací v podniku. Tento standard toto řeší za pomocí rozsáhlého seznamu 134 opatření v 39 kategoriích bezpečnosti a tyto jsou dále seskupeny v 11 oblastech. (ČSN ISO /IEC 27001:2006)

Tab. 1 Oblasti řešení ISMS podle normy ČSN ISO/IEC 27001:2006 (Zdroj: norma ČSN)

ČSN ISO/IEC 270001:2005	**Počet kategorií**	**Počet opatření**
Bezpečnostní politika	1	2
Organizace bezpečnosti informací	2	11
Řízení aktiv	2	5
Bezpečnost lidských zdrojů	3	9
Fyzická bezpečnost a bezpečnost prostředí	2	13
Řízení komunikace a řízení provozu	10	33
Řízení přístupu	7	25
Akvizice, vývoj a údržba informačních systémů	6	16
Zvládání bezpečnostních incidentů	2	5
Řízení kontinuity řízení organizace	1	5
Soulad s požadavky	3	10
	39	**134**



Obr. 4 Rozdělení bezpečnosti informací podle ISO/IEC 17799:2005 (Zdroj: SMEJKAL V., 2010)

Uvedené oblasti pro řešení ISMS v podniku nejsou a ani nemohou být všechna. Tato norma stanovuje určitý minimální rozsah, v rámci kterého, lze systémy ISMS následně certifikovat a vzájemně srovnávat. Současně také není striktně vyžadováno řešení všech zde uvedených oblastí, jelikož ne vždy musí být tyto oblasti pro daný podnik relevantní. Z tohoto plyne, že pro řešení ISMS je třeba identifikovat možné hrozby, a tyto pak následně přiřadit do adekvátních kategorií. V případě, že nebude možné identifikované hrozby zařadit do v normě uvedených kategorií, je nutné zavést do systému ISMS odpovídající novou kategorii.

Je třeba si uvědomit, že v normě definované oblasti informační bezpečnosti mohou být vzájemně závislé, či dokonce se i částečně překrývat svým rozsahem. V normě uvedených 134 opatření také není pevně daný a konečný počet. Každé z těchto opatření ve svém důsledku obsahuje další dílčí opatření a teprve jejich složením je dané opatření naplněno. Normu je třeba brát jako návod na praxí ověřené nejlepší možné řešení daného problému, ovšem není možné postihnout všechna možná specifika všech podniků. Proto je výběr aplikovaných opatření ponechán na podniku a tato si aplikovaná opatření vybírá na základě důkladné analýzy identifikovaných rizik.

2.3 Analýza rizik a bezpečnostní politika

2.3.1 Analýza rizik

Při řešení ISMS je nejdůležitějším krokem, který je prováděn v počátečních fázích procesu analýza rizik. Tato analýza je klíčovým prvkem, který stojí na vrcholu pomyslné pyramidy zavedení systému ISMS. (SMEJKAL V., 2010) Pro analýzu rizik lze nalézt sadu obecných kroků skládající se z:

- **Stanovení hranice analýzy rizik** – je třeba určit, která aktiva budou do vytvářené analýzy rizik zahrnuta a která budou vyloučena. Tímto krokem je jednoznačně dán výsledný rozsah analýzy. Tato hranice je převážně stanovována vedením podniku na základě vytvořené úvodní studie či sledovaná oblast obsahuje aktiva podniku, která se přímo podílejí na jeho činnosti nebo tvoří jeho konkurenční výhodu atd.
- **Identifikace aktiv** – vytváří se soupis všech identifikovaných aktiv uvnitř definované hranice pro analýzu rizik.
- **Stanovení hodnoty a seskupování aktiv** – při stanovení hodnoty aktiv je možné vycházet z různých hledisek. Tato hlediska lze v základě rozdělit na zkoumání nákladových či výnosových charakteristik aktiva. Použijí se vždy ty charakteristiky, které odpovídají vyšší hodnotě pro podnik. Jako charakteristiky pro stanovení hodnoty lze chápat např. pořizovací cenu, zisky z aktiva, ochranná známka, patent, průmyslový vzor, kvalifikace, důvěryhodnost vzhledem k partnerům, know-how, technologie atd. Do hodnoty je třeba započítat, jak podnik je moc závislý na daném aktivu, co se v podniku stane v případě ztráty, nedostupnosti, zničení či výpadku funkce aktiva. Protože aktiv může být v podniku identifikováno velké množství, je vhodné tyto aktiva shlukovat do určitých celků podle jejich povahy a pro tyto celky zavádět opatření s důrazem na zavedení opatření pro všechny jednotlivá aktiva logického celku.
- **Identifikace hrozeb** – v tomto kroku analýzy rizik se vyhledávají hrozby, pro které musí být v dalších krocích následně nalezeno odpovídající protiopatření. Výběr možných hrozeb je třeba provádět tak, aby tyto hrozby ohrožovaly alespoň jedno

z identifikovaných aktiv. Hrozby lze získat z mnoha zdrojů, především z literatury, oborových zkušeností, případně z provedených analýz. Hrozby se často odvíjí od chodu a fungování podniku, lze je také identifikovat za pomocí metod brainstormingu.

- **Analýza hrozeb a zranitelnosti** – každou identifikovanou hrozbu je třeba hodnotit vůči všem skupinám aktiv, které jsme předchozími kroky vytvořili. Je třeba, aby pro aktiva, u kterých se může daná hrozba uplatnit, byla určena úroveň hrozby vůči aktivu a také úroveň zranitelnosti aktiva vůči této hrozbě. Faktory, jako jsou nebezpečnost, motivace a přístup se použijí ke stanovení úrovně hrozby. Naopak z citlivosti a kritičnosti se stanovuje úroveň zranitelnosti. Při této analýze se musí brát v potaz také případná protiopatření, jelikož tato mohou snížit úroveň jak hrozeb, tak zranitelnosti.
- **Pravděpodobnost jevu** – při zkoumání výskytu hrozeb je třeba brát v potaz pravděpodobnost výskytu dané hrozby. Je tedy potřeba při analýze hrozeb tyto identifikované hrozby doplnit pravděpodobností jejich výskytu a tuto hodnotu pak brát v potaz při vytváření adekvátních protiopatření. Při vyjadřování pravděpodobnosti výskytu je třeba také zkoumat, zda se jedná o jevy náhodné či nikoliv, zda leží v určitém námi sledovaném intervalu pravděpodobnosti, či danou hrozbu lze vyloučit z našeho uvažování.
- **Měření rizika** – výše rizika vyplývá z hodnoty aktiva, úrovně hrozby a zranitelnosti aktiva. Stanovení hodnoty rizika je velmi obtížný úkol, protože riziko je často vyjádřeno neměřitelnou veličinou, případně velmi těžce měřitelnou veličinou. Velmi často se měření rizika spíše odvíjí od hodnocení specialisty, na základě jeho zkušeností. Nejčastěji tak lze při měření rizika narazit na pojmy vágní zejména výrazy typu malé, střední vysoké riziko. Při kvantifikaci rizika je také třeba počítat s pravděpodobností výskytu jevu, kdy pravděpodobnější výskyt dostává od hodnotitele vyšší hodnotu rizika. Uvedené vágní pojmy slouží spíše ke srovnání míry rizika a lze říci, že představují měřítko možné ztráty.

2.3.2 Bezpečnostní politika

Na vrcholu pomyslné pyramidy úkonů při zavádění ISMS je vytvoření bezpečnostní politiky. Sama o sobě tato politika je výchozím dokumentem při řešení bezpečnosti a zavádí pravidla, určuje interní směrnice, definuje postupy, jejichž primárním účelem je řízení, ochrana a zacházení s informačními aktivy. Při vytváření bezpečnostní politiky je v ní také zakotvena nezbytná podpora a zájem vedení podniku na řízení bezpečnosti informací.

Bezpečnostní politika by měla minimálně obsahovat:

- Definici bezpečnosti informací, její cíle, rozsah, význam a důležitost.
- Záměr vedení podniku podporovat cíle a principy bezpečnosti informací.
- Stručný výklad bezpečnostních zásad, principů, standardů a případné speciální požadavky.
- Definice obecných a specifických odpovědností pro řízení bezpečnosti informací i pro hlášení případných bezpečnostních incidentů.
- Odkazy na dokumentaci, kde lze nalézt detailnější bezpečnostní politiku, postupy specifické oblasti či bezpečnostní pravidla, která by měla být pracovníky dodržována.

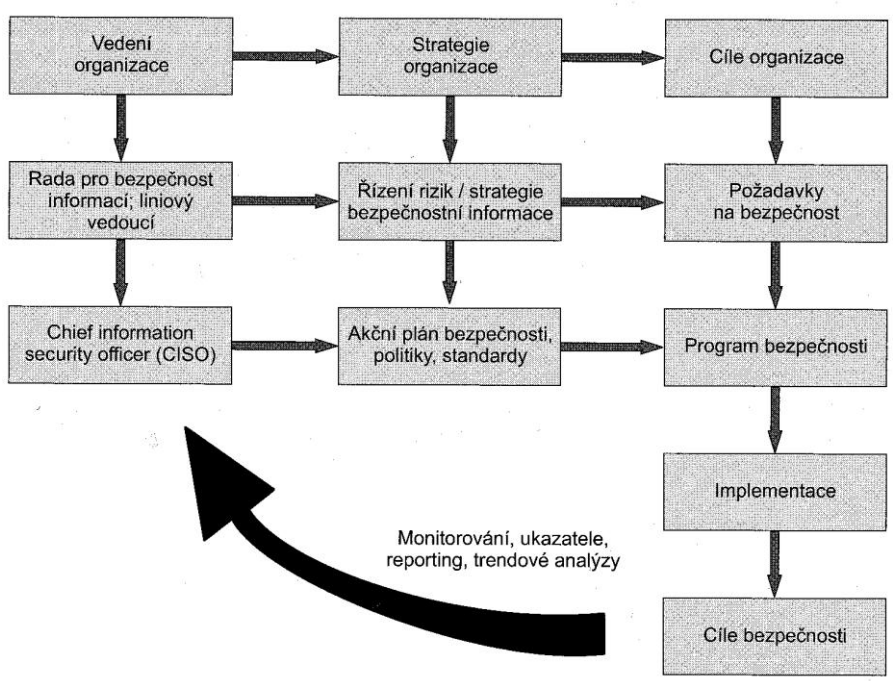
Podle kritérií hodnocení bezpečnosti informačních systémů (ITSEC) je vhodné zpracovat až tři úrovně bezpečnostních politik:

- **Celková bezpečnostní politika** – stanovuje cíle a popis způsobu zajištění celkové bezpečnosti informačního systému ve vztahu k bezpečnosti podniku.
- **Systémová bezpečnostní politika** – popisuje jakým způsobem zajistit bezpečnost informačního systému podniku. Podrobněji se zabývá popisem vnitřních a vnějších vazeb IS podniku, způsobem ochrany aktiv informačního systému, popisem bezpečnostních opatření informačního systému a vyhodnocováním analýzy rizik IS.
- **Technická bezpečnostní politika** – má za cíl popsat jednotlivá konkrétní opatření pro zajištění bezpečnosti při využívání zdrojů a při zpracování informací v organizaci.

V rámci systému ISMS musí v pravidelných časových intervalech docházet k revidování bezpečnostní politiky. Cílem revize je zajištění, aby bezpečnostní politika odpovídala skutečnosti zjištěné revizí, prověrka manažerů bezpečnostní politiky, posouzení adekvátnosti a efektivnosti navržených a používaných opatření a současně upravovat bezpečnostní politiku aktuálním potřebám podniku.

3 Management bezpečnosti informačních systémů (ISMS)

Pro zavedení ISMS neexistuje žádné univerzální řešení, které by bylo možné snadno přizpůsobit podmínkám v podniku. Každý podnik svým zaměřením, zažitými postupy, pracovníky, firemní kulturou je originální. Vytvoření a zavedení ISMS je dlouhodobý a v podstatě nekončící proces. Podnik musí z důvodu neustále se měnících rizik, či ohrožení a probíhajících změn, pružně na tyto změny reagovat a tím zdokonalovat svůj systém. Další odstavce této kapitoly jsou použity z normy ČSN ISO/IEC 27001:2006



Obr. 5 Koncepční model řízení informační bezpečnosti organizace (Zdroj: SMEJKAL V., 2010)

3.1 Všeobecné požadavky

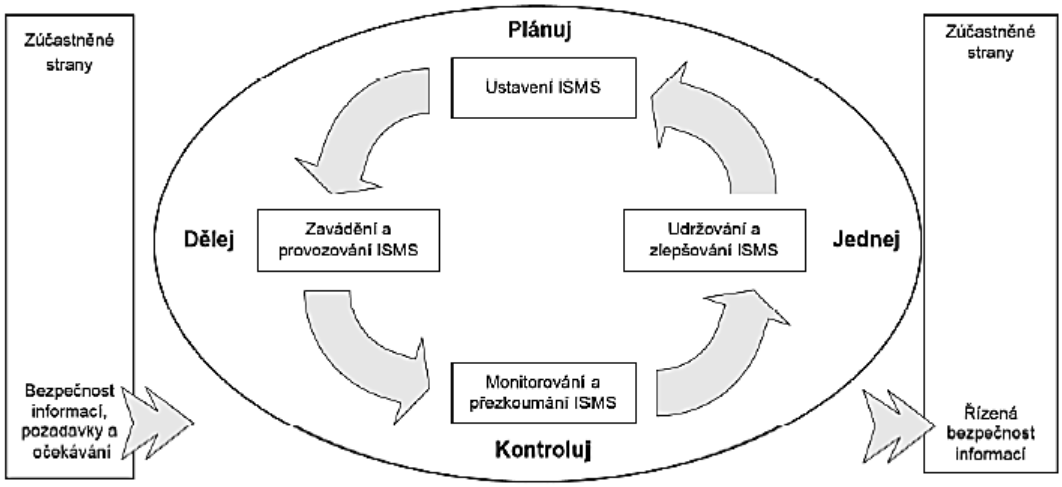
Základní požadavky na ISMS v podniku jsou:

- Ustanovení
- Zavedení
- Provozování
- Monitorování
- Přezkoumávání
- Udržování
- Soustavné zlepšování

Všechny tyto činnosti musí být dokonale dokumentovány a to v kontextu všech činností a identifikovaných rizik. Použitý proces, který je obsažen v normě ČSN ISO/EN 27001:2006 vychází z Demingova modelu PDCA.

Tento model obsahuje 4 základní procesy:

1. **Plánuj (ustanovení ISMS):** Vytvoření politiky ISMS, definice cílů, procesů a postupů, které souvisí s řízením rizik a zlepšováním vlastní ochrany informací takovým způsobem, aby byly splněny cíle stanovené ve vytvořené politice ISMS a v souladu s cíli organizace.
2. **Dělej (zavádění a provozování ISMS):** Vlastní zavedení a provádění stanovené podnikové politiky ISMS, postupů, opatření a procesů sloužících ke splnění cílů.
3. **Kontroluj (monitorování a přezkoumání ISMS):** Posuzování a případně i měření výkonu vzhledem k politice ISMS, definovaným cílům a praktickým zkušenostem se současným pravidelným hlášením výsledků vedení podniku k přezkoumání postupu plnění ISMS.
4. **Jednej (udržování a zlepšování ISMS):** Přijetí nezbytných opatření k nápravě zjištěných problémů a vytváření preventivních opatření, která jsou založena na výsledcích interního podnikového auditu ISMS, při současném přezkoumání systému řízení ze strany vedení podniku za účelem neustálého zlepšování a zkvalitňování ISMS.

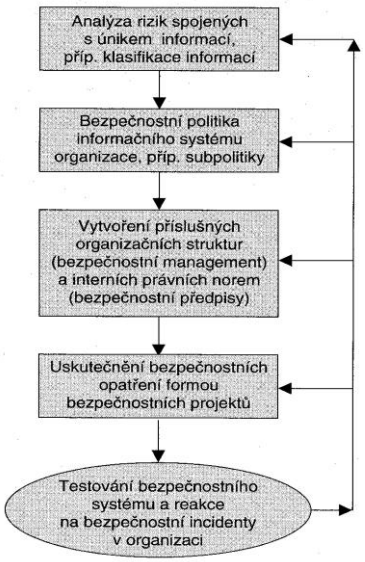


Obr. 6 Demingův model aplikovaný na procesy ISMS (Zdroj: ČSN ISO/IEC 27001:2006)

Procesy ISMS jsou při implementaci navrhovány takovým způsobem, aby byla zajištěna odpovídající a přiměřená bezpečnostní opatření, jejichž cílem je chránit informační aktiva podniku. Současně tyto opatření musí poskytovat odpovídající jistotu i dalším zúčastněným stranám, ovšem při zachování přijatelné míry nákladů s těmito opatřeními spojenými.

3.2 Ustanovení a řízení ISMS

Proces ISMS lze shrnout do následujícího obrázku.



Obr. 7 Budování informační bezpečnosti jako iterační proces (Zdroj: SMEJKAL V., 2010)

3.2.1 Ustanovení ISMS

V rámci ustanovení ISMS v podniku je třeba splnit následující požadavky (ČSN ISE/IEC 27001):

- Na základě analýzy činností v podniku, jejího vnitřního uspořádání, umístění, aktiv a používaných technologií je definován rozsah a hranice pro ISMS. Musí být také zdokumentovány důvody, pro které budou určité aspekty podniku vyjmuty z procesu ISMS.
- Na základě znalosti rozsahu a hranic zaváděného ISMS je třeba co nejpřesněji definovat politiku ISMS v podniku. V politice ISMS musí být zahrnuty cíle a celkový směr řízení činností v rámci bezpečnosti informací. Musí také zahrnout požadavky vyplývající z činnosti podniku či zákonů dané země.
- Je nutno stanovit, jakým způsobem budou v podniku hodnocena rizika. Stanovit kritéria pro akceptaci rizik a jejich akceptační úrovně. Zvolená metodika musí být schopna zajistit, že získané výsledky jsou reprodukovatelné a porovnatelné.
- Identifikace rizik, aktiv a jejich vlastníků, vyhledat hrozby pro tato aktiva, nalézt místa zranitelnosti a v neposlední řadě také identifikovat, jaké dopady na aktiva by mohla mít případná ztráta jejich důvěrnosti, integrity nebo dostupnosti.
- Analýza a vyhodnocení rizik musí řešit možné dopady na podnik v případě, že dojde k bezpečnostnímu incidentu. Musí brát v potaz následky ze ztráty důvěrnosti, integrity či dostupnosti aktiv. Je třeba posoudit reálnou možnost selhání bezpečnosti a dopady s přihlédnutím k zavedeným opatřením. Stanovit úrovně rizik a definovat, zda jsou rizika pro podnik akceptovatelná, či je třeba tato rizika řešit.
- Zvládání rizik, aplikování opatření, které minimalizují rizika či vyhnutí se rizikům. Vědomé akceptování rizik, či přenesením rizik na třetí stranu.
- Stanovení cíle opatření a jednotlivá bezpečnostní opatření pro zvládnutí rizik. Vybraná opatření musí být zdůvodněna na základě hodnocení a zvládání rizik.
- Odsouhlasení zbytkových rizik vedením podniku.
- Souhlas vedení podniku se zavedením a provozu ISMS v podniku.
- Vytvoření Prohlášení o aplikovatelnosti. Toto prohlášení obsahuje cíle, důvody výběru a konkrétní opatření, shrnutí cílů a bezpečnostních opatření, která jsou již v podniku aplikována a vyloučené cíle včetně důvodu jejich vyloučení.

3.2.2 Zavádění a provozování ISMS

Základní kroky organizace:

- Vytvoření plánu pro zvládání rizik, který obsahuje jednotlivé činnosti pro vedení, zdroje, stanovení priority pro řízení rizik bezpečnosti informací.
- Zavedení plánu pro zvládání rizik do podniku takovým způsobem, aby bylo dosaženo cílů opatření, za současného přiřazení rolí a odpovědnosti se zřetelem na dostupné finanční zdroje.
- Zavedení vybraných bezpečnostních opatření pro dosažení stanovených cílů těchto opatření.
- Je třeba stanovit metriky, kterými se budou vybraná opatření, či skupiny opatření vyhodnocovat a následně stanovovat jejich účinnost se zřetelem na porovnatelnost a opakovatelnost při hodnocení závěrů.
- Řízení provozu i zdrojů ISMS.
- Zavedení postupů a opatření pro rychlou detekci a reakci na bezpečnostní události a incidenty.

3.2.3 Monitorování a přezkoumání ISMS

V rámci tohoto kroku ISMS je nutné:

- Monitorování, přezkoumávání a případně zavedení dalších opatření pro včasnou detekci chyb zpracování, včasnou identifikaci úspěšných i neúspěšných pokusů o narušení bezpečnosti a detekci bezpečnostních incidentů. Vedení podniku musí být schopno určit, zda bezpečnostní aktivity prováděné pověřenými osobami a implementované technologie plní svou funkci. Je třeba vyhodnocovat, zda opatření podniknutá při narušení bezpečnosti jsou dostatečně účinná.
- Provádět pravidelné přezkoumávání účinnosti ISMS. Tato přezkoumávání se zaměřují zejména na plnění politiky, cílů a opaření ISMS, přičemž je třeba brát ohled na výsledky bezpečnostních auditů, incidentů a měření účinnosti opatření. Dále je třeba se zabývat případnými návrhy a připomínkami všech zúčastněných stran.
- Na základě měření účinnosti zavedených opatření ověřovat, zda dochází k naplnění stanovených požadavků na bezpečnost.
- V předem stanovených intervalech přezkoumávat hodnocení rizik a revidovat zbytková rizika. Při ověření úrovně akceptovatelných rizik vzhledem ke změnám na úrovni podniku, technologie, cílů činností, či procesů podniku, nalezených hrozeb, účinnosti používaných opatření, právního prostředí, či případných změn, které vznikly v důsledku změny smluvních vztahů či sociálního klimatu.

- V pravidelných intervalech provádět vnitřní audity.
- Vedení podniku musí pravidelně provádět přezkoumání ISMS, pro zajištění odpovídajícího rozsahu opatření a pro nalezení případných možných zlepšení ISMS v podniku.
- Je nezbytné udržovat aktualizované bezpečnostní plány s ohledem na výsledky získané monitorováním a přezkoumáváním.
- Je třeba zaznamenávat všechny činnosti a události s možným dopadem na ISMS, či účinnost opatření.

3.2.4 Udržování a zlepšování ISMS

Za účelem neustálého zlepšování a udržování ISMS se pravidelně provádí zavádění nově identifikovaných zlepšení systému ISMS, provádí odpovídající preventivní a nápravné činnosti s přihlédnutím nejen vlastních získaných zkušeností, ale i zkušeností jiných organizací v oblasti bezpečnosti. Nové činnosti či návrhy na zlepšení je nutné pravidelně konzultovat se všemi zainteresovanými stranami a koordinovat postup při jejich zavádění. Nedílnou součástí procesu zlepšení je i zabezpečit, aby navržená zlepšení dosáhla vytyčených cílů.

3.3 Požadavky na dokumentaci

Všechny záznamy o rozhodnutí vedení, včetně všech činností musí být zpětně identifikovatelné v politikách bezpečnosti a dohledatelné v záznamech. Pro zajištění jejich opakovatelnosti musí být výše uvedené záznamy řádně dokumentovány. Je nutno, aby byl zaznamenán vztah mezi výsledky z procesu hodnocení a zvládání rizik, vybranými opatřeními a jejich vazbou na politiku a cíle ISMS. Velikost a rozsah dokumentace ISMS je přizpůsobena velikosti podniku a jeho činnosti, přičemž je také brán zřetel na rozsah a složitost systému.

Do dokumentace ISMS je nutno zahrnout:

- Prohlášení politiky, cílů a rozsah ISMS.
- Postupy a opatření podporující ISMS.
- Popis metodik hodnocení rizik.
- Zprávu o hodnocení rizik.
- Plán, jakým způsobem budou rizika zvládána.
- Postupy, které jsou nezbytné pro zajištění efektivního plánování, provozu a řízení procesů ISMS a definovat, jakým způsobem je měřena účinnost jednotlivých opatření.
- Záznamy, které jsou vyžadovány normou o výskytech bezpečnostních incidentů a výkonu procesů.
- Prohlášení o aplikovatelnosti.

3.3.1 Řízení dokumentů

Všechny dokumenty vytvářené v rámci ISMS musí být odpovídajícím způsobem chráněny a řízeny. Je nutné, aby byl vytvořen dokumentovaný postup, který vymezuje řídící činnosti, jež jsou nutné pro:

- Schvalováním obsahu dokumentů dříve, než budou vydány.
- Přezkoumání a případnou aktualizaci dokumentů a jejich opakovanému schvalování.
- Zajištění identifikace změn dokumentů a aktuálního stavu revize dokumentů.
- Zajištění čitelnosti a snadné identifikace dokumentů.
- Zajištění dostupnosti a pravidel manipulace s těmito dokumenty, při současném zohlednění klasifikace těchto dokumentů.
- Jednoznačná identifikace původu dokumentů, zejména pocházejících z externích zdrojů.
- Zajištění řízené distribuce dokumentů, zabránění použití zastaralých dokumentů a vytvoření vhodné metody identifikace dokumentů pro případ jejich dalšího použití.

3.3.2 Řízení záznamů

Všechny záznamy musí být vytvořeny, udržovány, chráněny a řízeny tak, aby poskytly důkaz o shodě s požadavky o efektivním fungování ISMS. Záznamy musí zohledňovat právní regulatorní a smluvní závazky. Je třeba zajistit jejich čitelnost, identifikovatelnost a snadnost jejich vyhledání. Opatření navržená ke splnění předchozích požadavků musí být opět dokumentována. Kromě těchto záznamů je třeba také uchovávat a udržovat záznamy o samotném výkonu procesu budování a řízení ISMS a také všechny záznamy o výskytech bezpečnostních incidentů.

3.4 Odpovědnost vedení

Vedení podniku musí být schopno poskytnout důkazy o své vůli k ustanovení, zavedení, provozu, monitorování, přezkoumávání, udržování a zlepšování procesu ISMS. Podpora vedení je přímo vyjádřena v ustanovení politiky ISMS, stanovení cílů ISMS a plánů, jak tyto cíle dosáhnout. Mezi další odpovědnosti vedení patří stanovení rolí, povinností a odpovědností pro úspěšné řešení ISMS. V rámci podniku musí být dostatečně propagován význam plnění cílů, jejich souladu s vytvořenou bezpečnostní politikou, odpovědností plynoucích ze zákona a nutnost soustavného zlepšování.

Povinností vedení je zajistit dostatečné zdroje pro celý proces ISMS a provádění interních auditů. Vedení stanovuje kritéria pro akceptaci rizik, definuje přijatelnou míru zůstatkového rizika, přičemž provádí přezkoumávání ISMS.

3.5 Řízení zdrojů

3.5.1 Zajištění zdrojů

V podniku musí být určeny a zajištěny zdroje, které jsou potřebné pro provozování ISMS v podniku. Tyto zdroje zajišťuje vedení podniku v souladu s politikou bezpečnosti v podniku a prohlášení o aplikovatelnosti. Především se jedná o zdroje nezbytné k ustavení, zavedení, provoz, monitorování, přezkoumání, udržování a zlepšování ISMS v podniku.

3.5.2 Školení, informovanost a odborná způsobilost

Aby bylo možné provádět všechny úkoly související s ISMS, je třeba zajistit odbornou způsobilost zaměstnanců. Je také nutno zajistit odpovídající školení, či nábor již kvalifikovaných zaměstnanců, pravidelně vyhodnocovat účinnosti absolvovaných školení a udržovat záznamy o vzdělání, školení, dovednostech, zkušenostech a jiných kvalifikačních předpokladech. Nezbytnou součástí je informovanost personálu o závažnosti a významu jednotlivých činností, které jsou prováděny v rámci bezpečnosti informací a také o podílu pracovníků na dosažení cílů stanovených v ISMS.

3.6 Interní audity

V podniku musí být prováděny interní audity ISMS, v předem plánovaných intervalech, přičemž se určuje v těchto auditech, zda jsou cíle, opatření, jednotlivá bezpečnostní opatření, procesy a postupy ISMS vyhovující požadavkům normy ČSN ISO/IEC 27001:2006, zákonným, či regulatorním požadavkům. Současně musí být ověřeno, zda postupy ISMS odpovídají identifikovaným požadavkům na bezpečnost informací, jsou zavedeny, vykonávány a udržovány efektivně a splňují očekávání.

Obsah každého auditu musí být naplánován s ohledem na stav a význam auditovaných procesů, přičemž musí zohledňovat stav daného procesu v předcházejících auditech. Pro provádění auditů musí být jasně stanovena kritéria, rozsah, četnost opakování a použité metody s ohledem na zaručení jejich opakovatelnosti. Auditoři musí být schopni zajistit nestranný a objektivní audit a nesmí auditovat svou vlastní práci. Odpovědnosti, požadavky, hlášení výsledků a udržování a zacházení s audity musí být dokumentovány.

Vedoucí pracovníci jsou odpovědní za oblast, která je předmětem auditu a musí zajistit, aby odstranění případných nedostatků a jejich příčin bylo provedeno bez zbytečného odkladu. Tyto prováděné nápravné kroky musí být zpětně zkontrolovány a dokumentovány.

3.7 Přezkoumání ISMS vedením organizace

Přezkoumávání ISMS v podniku je třeba provádět v plánovaných intervalech a to minimálně jednou ročně. Na základě těchto přezkoumávání je třeba zhodnotit a navrhnout možné zlepšení či změny v systému ISMS a to včetně změn týkajících se cílů a politiky bezpečnosti. Veškeré zjištěné, navrhované a provedené skutečnosti musí být řádně dle stanovených pravidel zdokumentovány a musí být o nich udržovány záznamy.

3.7.1 Vstup pro přezkoumání

Přezkoumávání stavu a účinnosti ISMS v podniku zahrnuje minimálně tyto informace:

- Výsledky auditů a přezkoumávání ISMS.
- Informace od zainteresovaných stran na podnikovém ISMS.
- Informace, které by mohly vést ke zlepšení výkonu a účinnosti ISMS.
- Preventivní opatření, včetně stavu opatření nutných k nápravě.
- Možné zranitelnosti či hrozby, které nebyly v odpovídající míře zapracovány do systému ISMS v podniku.
- Hodnocení měření účinnosti zavedených opatření.
- Kroky, které následovaly po předchozím přezkoumávání vedením podniku.
- Změny ovlivňující bezpečnost informací a doporučení pro zlepšení ISMS.

3.7.2 Výstup z přezkoumání

Výstupem z přezkoumávání je jakékoliv rozhodnutí a činnosti, které mají vztah k:

- Zvýšení účinnosti ISMS
- Změnám v hodnocení rizik, či plánu k jejich zvládání.
- Nezbytným změnám postupů v bezpečnosti informací, v reakci na vnitřní nebo vnější události, které mohou mít vliv na ISMS.
- Potřebě nových zdrojů.
- Postupům, které umožní zlepšení měření účinnosti opatření.

3.8 Zlepšování ISMS

Zavedení a provozování systému ISMS v podniku je ze své podstaty nikdy nekončící proces. Možná nová rizika se objevují prakticky denně a je jen na vedení podniku a odpovědných osobách, které v podniku přímo zodpovídají za ISMS, aby na nové situace a rizika adekvátně reagovali. Proto je nedílnou součástí ISMS proces, vedoucí ke zlepšování účinnosti, bezpečnosti informací, analýz monitorovaných událostí, nápravných a preventivních opatření i přezkoumávání prováděných

vedením podniku. Při zlepšování sytému ISMS lze opatření dělit na dvě hlavní skupiny. Opatření vedoucích k nápravě určitého nežádoucího stavu a opatření s preventivním účinkem.

3.8.1 Opatření k nápravě

Aby byla vyloučena možnost opětovného výskytu nedostatků v provozovaném systému ISMS spojených s implementací či provozem, je třeba v organizaci přijmout adekvátní opatření. Zdokumentované postupy nápravných opatření musí být schopny zachytit požadavky na:

- Nalezení nesouladu v zavedení či provozu ISMS.
- Určení příčin nesouladu.
- Zhodnocení potřeby opatření, zda zajistí, že se nesoulad nemůže znovu vyskytnout.
- Zavedení nezbytných opatření k nápravě nesouladu.
- Zaznamenání výsledků z přijatých opatření.
- Opětovné přezkoumání zavedených opatření.

3.8.2 Preventivní opatření

Preventivní opatření se z pohledu finančního jeví méně náročná, než zavádění opatření pro nápravu nesouladu. V podniku by mělo být definováno preventivní opatření, které je přiměřeno povaze a závažnosti možných rizik. Požadavky na preventivní opatření odpovídají požadavkům na opatření nápravná mimo bodu určení příčin nesouladu, jelikož tento nemohl ještě vzniknout. V organizaci je třeba proaktivně vyhledávat možné významné změny v rizicích, na které bude třeba do budoucna reagovat.

V této kapitole byly shrnuty požadavky normy ČSN ISO/IEC 27001:2006. Kapitola 3 této práce je použita z uvedené normy, jelikož tato norma je využívána k certifikaci podniků a jejich systému ISMS. (ČSN ISO/IEC 27001:2006)

4 Současný stav bezpečnosti v podniku

V praktické části této práce bude provedena analýza stávajícího stavu v malém podniku a na základě této analýzy budou navržena odpovídající opatření v souladu s metodikou uvedenou v ČSN ISO/IEC 27001:2006 pro zavedení řízení bezpečnosti informačních systémů v tomto podniku.

4.1 Popis podniku

Dotčený subjekt je softwarovou firmou, která v dané oblasti podniká od roku 1999. V současné době je ve firmě zaměstnáno 11 stálých zaměstnanců a dále využívá více externích specialistů. Firma má sídlo v přízemí budovy, která je v současnosti obývána majitelem firmy.

Hlavní náplní firmy je vývoj a prodej software. V současné době využívá software firmy kolem xxxx aktivních uživatelů. Firma působí převážně na území České republiky, ale software je prodáván i na území Slovenské republiky.

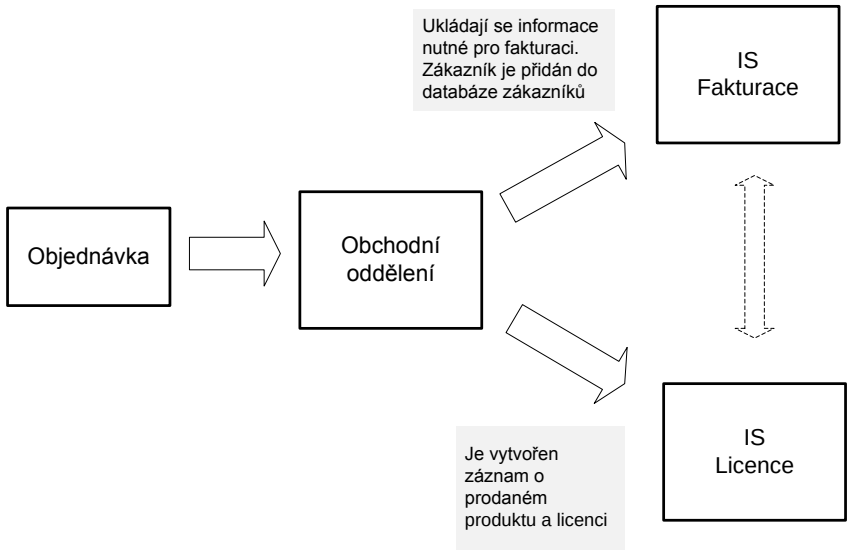
Firmu lze z hlediska vnitřního členění rozdělit do tří základních organizačních částí:

1. Obchodní oddělení a vedení účetnictví
2. Technická podpora uživatelům
3. Vývoj aplikací

4.1.1 Obchodní oddělení, vedení účetnictví

V tomto oddělení se přijímají a vyřizují objednávky produktů, vytváří se marketingové akce a vede se účetnictví firmy. Pracovníci tohoto oddělení využívají firemní IS, jenž je v podniku vyvíjen a také prodáván. Pracovníci jsou náležitě vyškoleni v účetních agendách a postupech, ke své práci používají základní komunikační prostředky, jako jsou email a telefon.

Oddělení se také stará o propagaci produktů. Firemní strategie je zaměřena na využívání moderních komunikačních kanálů, jako je direct marketing a inzerce přes internet. Z oddělení je vyčleněn pracovník, který je v rámci svých ostatních povinností zodpovědný za recepci firmy, kde probíhá prvotní kontakt s případnými návštěvami, poštovními službami atd.



Obr. 8 Diagram hlavního procesu obchodního oddělení (Zdroj: Vlastní analýza)

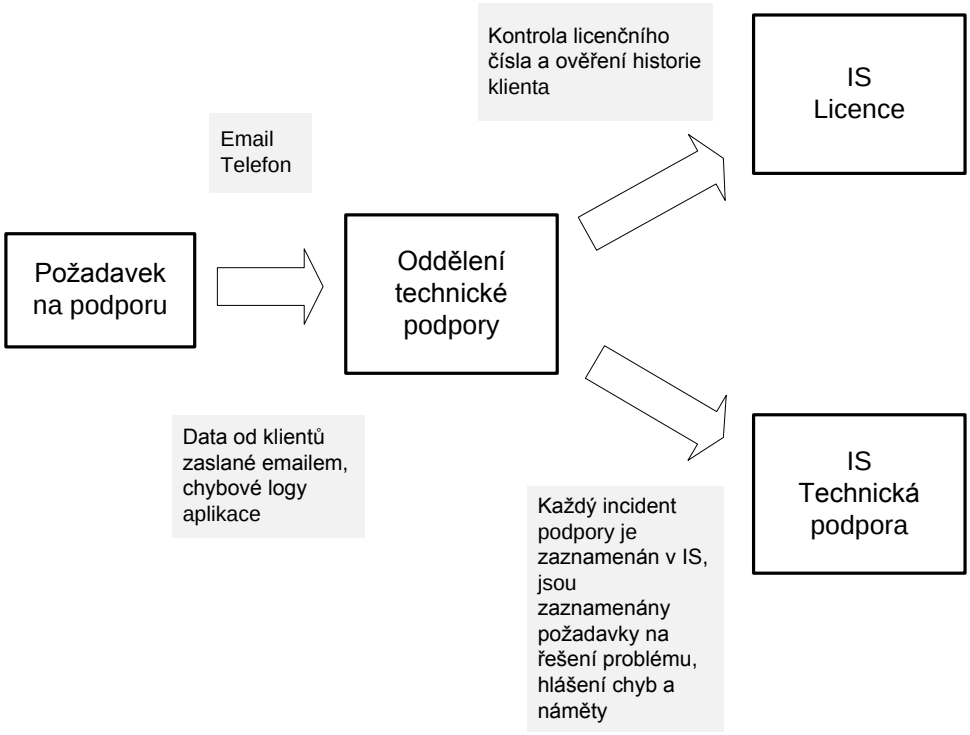
4.1.2 Oddělení technické podpory uživatelů

Pracovníci v tomto oddělení poskytují technickou podporu aktivním uživatelům firmou vyvíjených produktů. Oddělení je vnitřně rozděleno na tři nezávislé části.

- Podpora interní
- Podpora software
- Technická podpora druhé úrovně

Při činnosti technické podpory jsou používány běžné prostředky komunikace se zákazníky a to pomocí telefonu, emailu, případně se některé speciální činnosti provádí za pomocí vzdáleného přístupu na počítače zákazníků. Při poskytování technické podpory zákazníkům je zcela běžné, že se na oddělení technické podpory dostávají velmi citlivá data od klientů, kteří potřebují vyřešit svůj problém a zasláním zálohy svých dat umožní vyřešení daného problému. V takovém případě je se zákazníkem sepsána doložka o mlčenlivosti a neposkytnutí takovýchto dat třetím osobám.

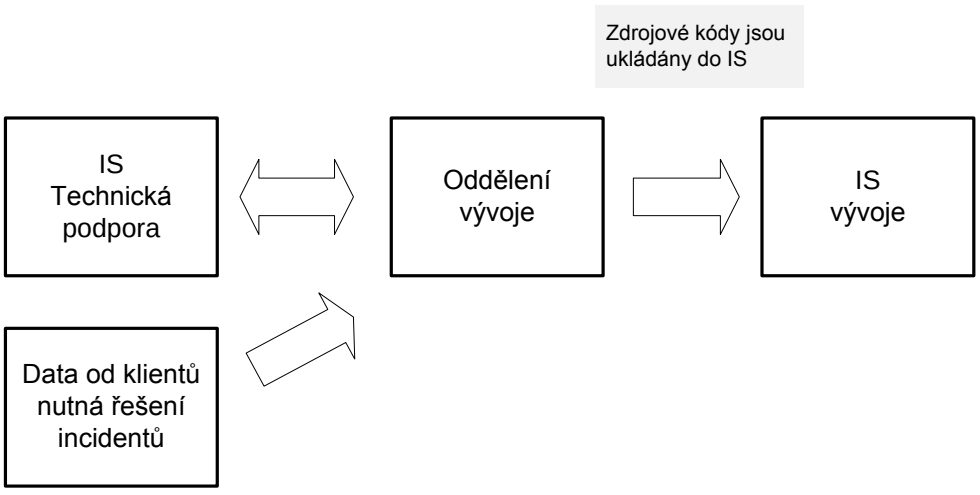
Pracovníci technické podpory druhého stupně se starají o neustálé udržování aktuálnosti software po stránce legislativní, provádí drobné úpravy v software, jako jsou vytváření specifických tiskových sestav, či zavádění a aktualizací do aplikace.



Obr. 9 Hlavní proces technické podpory (Zdroj: Vlastní analýza)

4.1.3 Oddělení vývoje aplikací

Oddělení vývoje aplikací je centrálním prvkem organizace, kde se vytváří softwarové produkty pro další prodej a vlastní potřeby firmy. Pro vlastní vývoj jsou kromě kmenových zaměstnanců firmy také využívání externisté, zejména pro speciální potřeby elektronické komunikace, či řízení projektu a vytváření a udržování architektury. Jelikož převážná většina těchto externistů pochází z blízkého okolí, je těmto zaměstnancům umožněn přístup do prostředí intranetu firmy. V tomto oddělení je také vyčleněn pracovník, který má na starosti technickou podporu uvnitř firmy a řešení případných hardwarových či softwarových požadavků zaměstnanců.



Obr. 10 Hlavní proces oddělení vývoje aplikací (Zdroj: Vlastní analýza)

4.1.4 ICT infrastruktura

Interní síť LAN je vytvořena zčásti svépomocí, strukturovaná kabeláž je vedena v kabelových žlabech, nebo v prostoru nad stropem. Centrálním místem je serverovna, kde jsou soustředěny aktivní prvky firemní sítě, servery, telefonní ústředna. Konektivita směrem do internetu je řešena pomocí dvou nezávislých připojení. V prvé řadě se jedná o bezdrátové připojení s přenosovými vlastnostmi 16/8 MBit a jako druhé – záložní řešení je použita konektivita pomocí ADSL s přenosovými vlastnostmi 4/4 MBit.

V rámci infrastruktury jsou využívány vnější bezdrátové přístupové body pro připojení externích specialistů do firemní sítě a vnitřní přístupový bod pro připojení návštěv, či pro potřeby testování software v podmínkách pomalých sítí. V serverovně jsou všechny aktivní prvky a servery vybaveny záložními zdroji stejně, tak i všechna jednotlivá PC ve firmě. Používaná výpočetní technika je z části nakupována od výrobce PC a z části sestavována ve firmě. Stáří jednotlivých pracovních stanic odpovídá průměrně 3 – 4 roky starým zařízením. Oddělení vývoje aplikací má stanoven cyklus obnovy pracovních stanic na 1,5 roku.

Prostory firmy jsou vybaveny elektronickým signalizačním zařízením pro případ neoprávněného vniknutí spolu s kamerovým systémem napojeným na záznamové zařízení zapojené do sítě LAN s ukládáním na server umístěným na internetu. Pro přístup do firmy je používán systém na bázi RFID. Záznamy příchodů a odchodů jsou dále využívány pro účely vytváření mezd pracovníků.

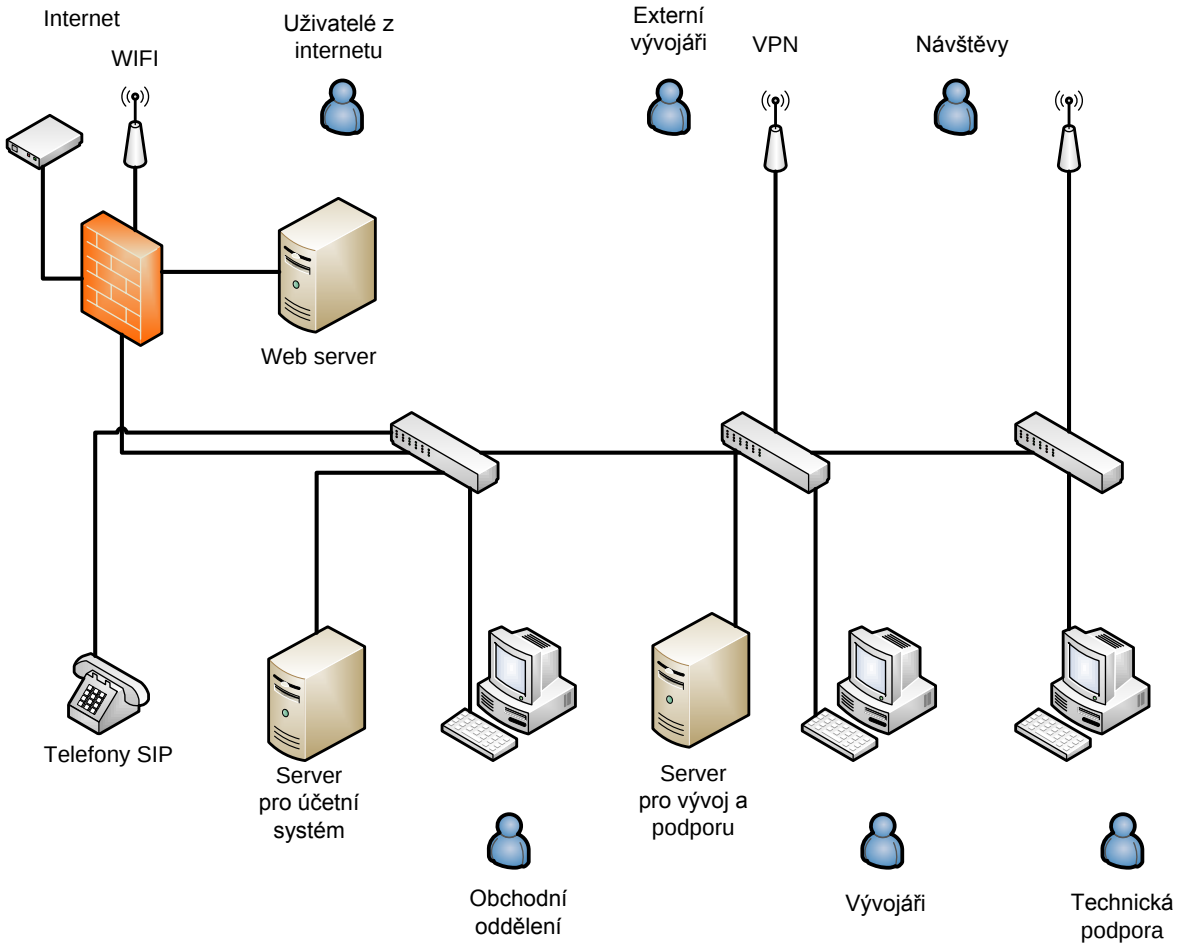
Operační systémy ve firmě jsou výhradně MS Windows 7 Pro na pracovních stanicích a servery jsou vybaveny odpovídajícím serverovým operačním systémem firmy Microsoft Windows Server 2008 R2.

Z aplikačního hlediska lze ve firmě nalézt tři části v podstatě odpovídající logice dělení firmy do oddělení. Informační systém podniku je založen na produktu XXX, který je využíván pro běžné činnosti obchodního oddělení, ovšem proti běžně prodávanému produktu je rozšířen o speciální podpůrné moduly zejména pro generování licencí pro uživatele. Pracovníci linky technické podpory mají dostupný systém s evidencí uživatelů, jejich historií zakoupených produktů a sériových čísel zakoupených produktů. V oddělení technické podpory je využíván software pro řízení helpdesku, do kterého zaznamenávají pracovníci technické podpory informace o řešených problémech, náměty na vylepšení software pro vývojáře a hlášení chyb.

Pracovníci vývoje mají k dispozici přístup do helpdeskového systému, do kterého zapisují provedené úpravy v programu jako reakce na hlášené chyby a náměty. Dalším důležitým softwarem je využívání sdílení zdrojových kódů prostřednictvím týmového serveru. Jako poslední nástroj určený pro vývojáře je speciální aplikace, sloužící pro vytváření a úpravy nových formulářů používaných v programu YYY.

Pro účely kontroly licenčních čísel a aktivace aplikací je ve firmě k dispozici server, obsahující webové služby pro ověření platnosti licenčních čísel a dále webová služba umožňující uživatelům stažení faktury a licenčního čísla k zakoupenému produktu.

Veškerá emailová komunikace linky technické podpory a vývoje aplikací je řešena serverovým řešením mail serveru a sdílena napříč odděleními z důvodu zástupnosti jednotlivých pracovníků a kontroly ze strany vedoucího vývoje a vedení firmy. Došlé datové soubory či hlášení problémů jsou ukládány na souborovém serveru v prostoru s omezenými přístupovými právy na zaměstnance oddělení podpory a vývoje.



Obr. 11 Komponenty ICT infrastruktury podniku (Zdroj: Vlastní analýza)

4.1.5 Poloha objektu a uspořádání prostor podniku

Ráz krajiny je plochého profilu bez výraznějších kopců či údolí. Poslední zaznamenané povodně byly v roce 1976, kdy bylo centrum města zaplaveno náhlým přívalovým deštěm do výše cca 30cm, když bývalý mlýnský náhon vedoucí centrem města nestačil vodu odvádět.

V přízemí dvoupodlažní budovy majitele firmy se nachází prostory, které jsou využívány k podnikání. Budova samotná je z jedné strany napojena na sousední obytný dům a z druhé strany je oddělena zahradou od sousedního domu. Před samotnou budovou se nachází malé parkoviště pro zaměstnance a návštěvy. Za budovou se nachází oplocený dvůr se zahradou a prostory pro skladování materiálu. Vstup do firmy je chráněn vnějším plotem s uzavíratelnou brankou ovládanou z recepce firmy. V těsné blízkosti budovy se nachází dva vzrostlé smrky, každý o výšce cca 15m.

Rozdělení prostor firmy na jednotlivá pracoviště odpovídá jejich organizačnímu členění, kde pracoviště jsou řešena jako tzv. open space kancelář. Firemní zvyklostí je nechávat dveře do kanceláří otevřené, kromě pracoviště technické podpory. Serverovna je volně přístupným prostorem vybaveným klimatizací a bývá také uzavřena, nikoliv však zamčena.

4.2 Řešení bezpečnost v podniku

Firma XXX patří mezi malé podniky, kde je velmi plochá organizační struktura. Majitel firmy je zároveň jedním z pracovníků vývoje a celá firma je postavena na velice neformálních vztazích. Svým způsobem právě tato neformálnost a velmi přátelské vztahy na pracovišti spolu s určitou sounáležitostí zaměstnanců s firmou vedou k velmi dobrým výsledkům firmy. Tyto neformální vztahy a vzájemná důvěra ovšem vede k neřešení bezpečnosti informací ve vztahu k vnitropodnikovému prostředí, což by mohlo mít v budoucnu fatální důsledky a firma tak může na své potenciální odběratele působit nedůvěryhodně.

4.2.1 Bezpečnost fyzická vnější prostory – EZS

Vynecháno – utajované informace.

4.2.2 Bezpečnost fyzická vnitřní prostory

Vynecháno – utajované informace.

4.2.3 Bezpečnost komunikační a softwarová

Vynecháno – utajované informace

4.3 Zhodnocení stávajícího stavu

Z předchozích odstavců je patrné, že ve firmě de facto neexistuje řízení bezpečnosti, nakládání s citlivými informacemi a metodika pro zvládání bezpečnostních incidentů. V případě pracovních stanic zde dokonce hrozí přímé nebezpečí ohrožení zdraví, či majetku z důvodu neprovádění pravidelných kontrol. Zavedení systému bezpečnosti informačních systémů je dle mého názoru jedinou možností, jak tento nepříznivý stav ve firmě napravit. Je zde evidentní riziko možnosti zcizení firemních a důležitých dat zaměstnanci. Tato a další rizika musí být minimalizována vytvořením bezpečného prostředí pro fungování firmy.

Ve firmě je také problém s praktickou neexistencí jakýchkoliv vnitřních směrnic, stanovením odpovědností a toto by mohlo reálně ohrozit fungování firmy. Existuje vysoké riziko zavlečení různých virů či špionážního software do prostředí firmy. Ačkoliv firma spolupracuje s externím subjektem pro správu a nastavení firewalu pro přístup k internetu, neexistuje zde žádná smlouva s externími vývojáři, která by stanovovala, jaké bezpečnostní opatření musí tyto externí subjekty provádět. Samotné připojení VPN neřeší problém přístupu z napadené sítě externího vývojáře.

V dalších odstavcích této práce bude provedena analýza rizik a návrh řešení ke snížení identifikovaných rizik. Ačkoliv firma neuvažuje o certifikaci ISMS, budu při řešení bezpečnosti vycházet právě z norem řady ISO 27000. Případná certifikace je dle mého názoru nezbytná a otevřela by tak podniku prostor pro další trhy, jelikož produkt, který vyvíjí je velmi kvalitní a je využíván ve velké míře v oblasti vyplňování daňových přiznání a elektronické komunikace se státní správou.

V analyzovaném podniku je zcela nedostatečná úroveň dokumentace většiny procesů a ve své podstatě jsou určité procesy a postupy známy je odpovědné osobě, která tyto činnosti provádí. I když se na první pohled zdá, že firma neřeší bezpečnost, opak je pravdou. V podniku se odpovědní zaměstnanci o bezpečnost starají a snaží se ji vylepšovat. To, že v podniku neexistují dokumentované postupy je dáno charakterem firemní kultury, která je více zaměřená na osobní kvality a odpovědnosti osob, než na dokumentace postupů. Tento přístup se podniku ovšem může zcela vymknout z kontroly, kdy stačí, aby se odpovědný a „všeho znalý“ zaměstnanec rozhodl opustit firmu. Dalším problémem, který zde lze spatřit je zastupitelnost takového pracovníka. Některé otázky bezpečnosti jsou v podniku řešeny za pomoci externích firem, což je jistě pro podnik přínosné.

5 Kroky před zavedením ISMS v podniku

Před vlastní implementaci ISMS v podniku je třeba vyjádřit podporu vedení se zavedením ISMS, stanovit rozsah ISMS a také, jakým způsobem se budou hodnotit rizika.

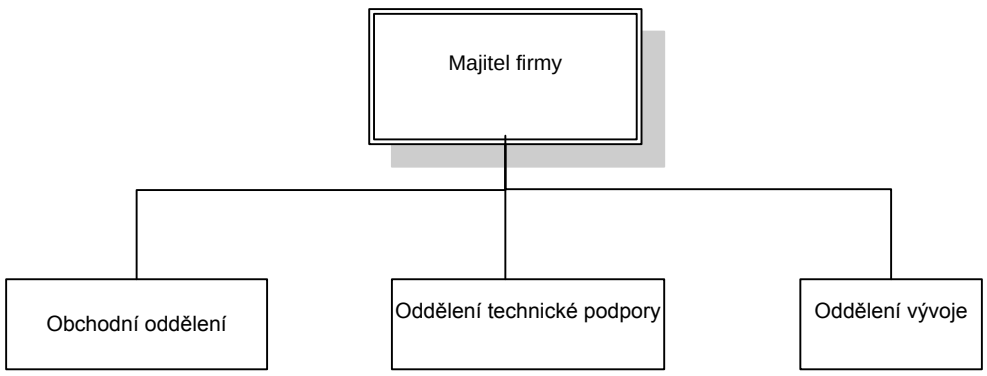
5.1 Ustanovení ISMS

Ustanovení ISMS je první etapa pro zavedení ISMS v podniku. V ustanovení ISMS jsou definovány klíčové prvky mající vliv na výslednou realizaci ISMS. V tomto ustanovení je nadefinován rozsah ISMS, politika ISMS, plán zvládání rizik a metodika hodnocení rizik.

5.1.1 Rozsah ISMS

Přestože podnik neplánuje v nejbližší době certifikaci systému ISMS, je základní rozsah ISMS, který bude zaváděn v podniku totožný s doporučením a vycházející z normy řady ISO 27000. Systém ISMS bude aplikován na celý podnik.

Aplikace na celý podnik a v rozsahu doporučeného normou byla zvolena z důvodu, že je ve stávajícím stavu příliš nedostatků a je třeba tento stav v co nejkratší době napravit. Největší důraz při zavádění ISMS je kladen na ICT a činnosti spojené s fungováním podniku. Zaváděné ISMS musí řešit zpracování informací v jednotlivých odděleních podniku a je nutné vytvořit zdokumentované postupy prakticky pro veškeré procesy v podniku.



Obr. 122 Organizační struktura v podniku (Zdroj: Vlastní analýza)

Všechny oddělení a zařízení podniku se nachází v budově podniku. Externí spolupracovníci, kteří využívají firemní infrastruktury za pomoci bezdrátového připojení, používají svých vlastních zařízení. Pro specifické činnosti řešící bezpečný přístup na internet a správu vnějších i vnitřních připojení pomocí VPN či Wi–Fi je využíván externí subjekt firma. S touto firmou jsou řešeny všechny specifické požadavky na připojení externích subjektů a konzultována patřičná bezpečnostní opatření.

5.1.1.1 Identifikace informačních aktiv

V podniku lze identifikovat tyto informační aktiva:

1. Zdrojové kódy prodávaných aplikací.
2. Databáze klientů podniku.
3. Databáze formulářů dodávaných v rámci produktů.
4. Znalostní databáze problémů a jejich řešení.
5. Systém pro správu námětů a připomínek.
6. Firemní účetnictví.
7. Data od klientů, která jsou využívána k opravám problémů.
8. Servery a aktivní síťové prvky.
9. Pracovní stanice jednotlivých uživatelů.
10. Komunikační služby třetích stran.

Všechna tato informační aktiva musí být obsažena v ISMS.
Tato identifikovaná aktiva jsou rozložena mezi všechna oddělení podniku. Za aktiva 1, 3, 7, 8, 9, 10 je zodpovědné oddělení vývoje. Aktiva 2, 6, náleží do obchodního oddělení a aktiva 4, 5 spadají pod oddělení technické podpory.

5.1.1.2 Rozhraní ISMS

Pro komunikaci s externími pracovníky existuje technické rozhraní Wi–Fi sítě, které společně s firewalem slouží k bezpečnému přístupu z vnějšího prostředí do vnitřní sítě.

5.1.2 Politika ISMS

Obsahuje vize a filozofii podniku v oblasti zajištění bezpečnosti informací a vedení podniku dává najevo svůj zájem a plnění bezpečnostní politiky. Tento dokument musí vydat vedení podniku a měl by obsahovat například následují obsah, se kterým se seznámí všichni pracovníci podniku a dokument bude volně přístupný. V dokumentu se podnik zavazuje k tomu, že:

- Bude trvale vytvářet podmínky k zajišťování všech zdrojů potřebných k zavedení, udržování a soustavnému zlepšování systému managementu bezpečnosti informací v celé organizaci.

- Bude uplatňovat politiku založenou na principech důvěrnosti, dostupnosti a úplnosti informací, na požadavcích právních a normativních předpisů a na požadavcích zainteresovaných stran.
- Bude pravidelně hodnotit plnění cílů a cílových hodnot vycházejících z analýzy rizik a této politiky.
- Bude soustavným prosazováním programu zvyšování informovanosti a právního povědomí zaměstnanců udržovat vysokou úroveň informační bezpečnosti.
- Bude pevně a přesvědčivě prosazovat uplatňování zásad informační bezpečnosti vůči smluvním partnerům a třetím stranám prezentovat profesionální přístup a postavení organizace na současném trhu.
- Bude zavedeným systémem managementu informační bezpečnosti informací poskytovat zákazníkům a smluvním partnerům, ale i svým zaměstnancům dostatečnou míru podpory a jistoty při nakládání s jejich informacemi a daty.

Součástí politiky ISMS je stanovení sponzora projektu, který bude vzhledem k velikosti podniku jeho majitel. Jako nositel změny (bezpečnostní manager) je v tomto případě nejvhodnějším kandidátem vedoucí oddělení vývoje, který má ze své pozice nejlepší přehled o používaných technologiích, používaných zabezpečeních v podniku a požadavcích na bezpečnost.

5.1.3 Plán zvládání rizik

V podniku je třeba vytvořit plán na zvládání rizik. V tomto plánu budou obsaženy krátkodobé cíle (maximálně v období jednoho roku), při zavádění a zlepšování opatření ISMS podle přílohy A normy ČSN ISO/IEC 27001. Součástí plánu musí být písemné jmenování zaměstnanců odpovědných za identifikaci rizik a realizaci opatření v oblastech:

- Bezpečnosti lidských zdrojů.
- Fyzické bezpečnosti a bezpečnosti prostředí.
- Bezpečnosti provozu ICT a informačních systémů.
- Zvládání incidentů a kontinuity činností.
- Souladu s právními požadavky (zákonnými i smluvními).

Vlastníci informačních aktiv budou stanoveni vedoucí jednotlivých oddělení, do kterých identifikované aktivum patří. Tito vlastníci jsou odpovědní za realizaci jednotlivých opatření podle přílohy A normy ČSN ISO/IEC 27001. Tyto úkoly budou uvedeny v kapitole Zavádění a provozování ISMS, případně v přílohách této práce.

Ke každému opatření je třeba uvést:

- Odpovědnou osobu (útvar, funkce).
- Stručný popis, jakým způsobem bylo realizováno.
- Odkazy na případnou další dokumentaci.
- Odhad množství užitých zdrojů (personálních, finančních).
- Termín realizace daného kroku.

5.1.4 Metodika hodnocení rizik

Metodika, jakým způsobem se budou hodnotit rizika, vychází z doporučení uvedených v normě ČSN ISO/IEC 27005:2006.

5.1.4.1 Definice hodnocení aktiv

Aby byly zajištěny základní požadavky na aktiva (dostupnost, důvěrnost a integrita), musí se při hodnocení aktiv brát v potaz závažnost možného dopadu na ně, v případě porušení bezpečnosti informačních aktiv. V podniku je třeba stanovit stupnici pro hodnocení aktiv.

Tab. 2 Stupnice pro hodnocení aktiv v podniku

Hodnota aktiva	Hodnocení dopadu na aktivum
1 – zanedbatelná	Dopad na aktivum je **zanedbatelný** • Případná škoda se neprojevuje do okolí podniku. • Náklady na odstranění či nápravu nepřesahuje částku 50 000 Kč. • Nedošlo k porušení právních norem.
2 – malá	Dopad na aktivum je **malý** • Má negativní vliv na organizační celky, ale neprojeví se ve službách poskytovaných navenek. • Mohlo dojít k porušení právních norem a případné správní řízení nebo soudní pře mohou vést k finančnímu postihu do částky 50 000 Kč.
3 – významná	Dopad na aktiva je **vážný** • Má negativní vliv na oddělení podniku a dopad je promítnut do poskytovaných služeb. • Může způsobit negativní publicitu v rámci oboru podnikání. • Újma způsobená jedné či více osobám mimo ohrožení zdraví či života. • Správní řízení či soudní pře s postihem přesahujícím 50 000 Kč.
4 – velmi cenná	Dopad na aktiva je **velmi vážný** • Veřejná negativní publicita. • Ztráta důvěry jednoho nebo více obchodních partnerů. • Potenciální nebezpečí zachování kontinuity podnikání. • Citelná finanční ztráta • Ohrožení života či vážná zranění.

5.1.4.2 Definice hodnocení úrovně hrozeb

Pro stanovení adekvátních opatření pro jednotlivá aktiva je třeba definovat úroveň hrozby, která je daná velikostí možného dopadu na aktivum a pravděpodobností, že bude hrozba uskutečněna. Současně s definicí hodnocení aktiv je stanoveno, které úrovně hrozby mohou být z hlediska jejich pravděpodobnosti výskytu akceptovatelné (retence), či nikoliv (redukce).

Tab. 3 Definice úrovně hrozeb

Úroveň hrozby	Hodnocení úrovně hrozby
VN – Velmi nízká	• S velmi malou pravděpodobností může dojít k **zanedbatelnému** dopadu na činnost podniku nebo oddělení. • **Riziko je možné akceptovat.**
N – Nízká	• Může dojít nízkou pravděpodobností k **zanedbatelnému** dopadu na činnost podniku či oddělení. • Může dojít k **malému** dopadu na činnost podniku či oddělení, ale s velmi malou pravděpodobností. • **Riziko je možné akceptovat.**
S – Střední	• Může dojít k **malému** dopadu na činnost podniku či oddělení. • **Riziko musí být řešeno.**
V – Vysoká	• Je velmi pravděpodobné, že může dojít k **vážnému** dopadu na činnost podniku či oddělení. • **Riziko musí být řešeno s vysokou prioritou.**
VV – Velmi vysoká	• Téměř jistě může dojít k **velmi vážnému** dopadu na činnost podniku či oddělení. • Riziko se musí řešit s největší prioritou.

5.1.4.3 Definice výpočtu míry rizika

Míru rizika je možné stanovit na základě výpočtu, který zahrnuje hodnotu aktiva a úroveň hrozby. Hodnota aktiva a úroveň hrozby byly nadefinovány v předchozích odstavcích. Z nich je vytvořena tabulka výsledné míry rizika, která je klíčová pro další postup zavádění ISMS a zejména opatření nutných pro odstranění hrozeb a rizik.

Tab. 4 Výsledná míra rizika

		Úroveň hrozby				
		VN	**N**	**S**	**V**	**VV**
Hodnota aktiva	**1**	N (1)	N (2)	S (3)	S (4)	S (5)
	2	N (2)	S (3)	S (4)	S (5)	V (6)
	3	S (3)	S (4)	S (5)	V (6)	V (7)
	4	S (4)	S (5)	V (6)	V (7)	V (8)

5.1.4.4 Dopad hrozeb na informační aktiva

Tab. 5 Dopad hrozeb na informační aktiva

Aktivum	Dopad na		
	Dostupnost	Důvěrnost	Integritu
Zdrojové kódy aplikací	4	4	4
Databáze klientů podniku	4	4	2
Databáze formulářů	4	3	2
Znalostní báze problémů a řešení	3	2	2
Systém pro správu námětů a připomínek	2	3	3
Firemní účetnictví	3	3	4
Data od klientů	2	4	1
Servery a aktivní síťové prvky	4	3	2
Pracovní stanice uživatelů	3	2	2
Komunikační služby třetích stran	4	3	4

5.1.4.5 Identifikované a uvažované hrozby a jejich dopad

Tab. 6 Identifikované hrozby a jejich dopad na dostupnost, spolehlivost a integritu

	Hrozba	Úroveň dopadu hrozby na		
		Dostupnost	Důvěrnost	Integritu
	Fyzické poškození			
1	Požár	4	1	1
2	Poškození vodou	4	1	1
3	Přehřátí po výpadku klimatizace	4	1	1
4	Poničení budovy okolními stromy	2	1	1
	Ztráta služeb			
5	Výpadek elektrické energie	3	1	3
6	Výpadek klimatizace	2	1	2
7	Výpadek sítě WAN	3	1	2
8	Výpadek sítě LAN	3	1	3
9	Výpadek IS	3	1	3
10	Výpadek IS technické podpory	2	1	1
11	Výpadek serveru se zdrojovými kódy	2	1	3
12	Výpadek hlasových služeb	4	1	1
	Ohrožení důvěrnosti			
13	Neoprávněné získání přístupových údajů	2	3	3
14	Neoprávněné získání informací	2	4	3
15	Chyba v nastavení přístupových práv	1	2	3
16	Slabiny v zabezpečení síťových služeb	2	3	2
17	Zranitelnosti webových služeb	2	3	2
18	Slabiny v architektuře IT infrastruktury	2	3	3
19	Získání dat z vyřazených médií	1	3	1

	Hrozba	Úroveň dopadu hrozby na		
		Dostupnost	**Důvěrnost**	**Integritu**
20	Krádež technického vybavení	3	3	2
21	Zneužití, ztráta nebo krádež USB disků	1	3	1
22	Záměrná škodlivá činnost v síti	1	2	2
23	Škodlivý software	2	3	3
	Technická selhání			
24	Selhání serveru	4	1	3
25	Selhání pracovní stanice	3	1	2
26	Chybné fungování systému	2	1	3
27	Nedostatek zdrojů pro provoz aplikace	3	1	2
	Neoprávněné činnosti			
28	Neoprávněné zkopírování informací	1	4	1
29	Neoprávněný přístup centrální správy systému	1	3	2
30	Zneužití administrátorských oprávnění	2	3	3
31	Zneužití uživatelských oprávnění	2	2	4
32	Porušení mlčenlivosti zaměstnance	1	4	1
33	Neoprávněný přístup do prostor	2	3	2
34	Neoprávněný přístup do aplikace	1	3	3
	Lidská selhání			
35	Nedbalost při údržbě zařízení	2	1	3
36	Nedostatek personálu správy IT služeb	3	1	2
37	Chyby personálu správy IT služeb	4	3	3
38	Nedostatečná dokumentace systému	3	1	4
39	Nedodržování předpisů pro práci s informacemi	2	3	2
40	Chyby obsluhy aplikace	1	2	3
41	Zneužití oprávnění při sdělení hesla	1	3	2

5.1.4.6 Míry identifikovaných rizik

Tab. 7 Míry identifikovaných rizik a jejich dopad na dostupnost, spolehlivost a integritu

	Zdrojové kódy aplikací			Databáze klientů podniku			Databáze formulářů			Znalostní báze problémů a řešení			Systém pro správu námětů a připomínek			Firemní účetnictví			Data od klientů			Servery a aktivní síťové prvky			Pracovní stanice uživatelů			Komunikační služby třetích stran		
	D	D	I	D	D	I	D	D	I	D	D	I	D	D	I	D	D	I	D	D	I	D	D	I	D	D	I	D	D	I
Fyzické poškození																														
Požár	8	5	5	8	5	5	8	4	3	7	3	3	6	4	4	7	4	5	6	5	2	8	4	3	7	3	3	8	4	5
Poškození vodou	8	5	5	8	5	5	8	4	3	7	3	3	6	4	4	7	4	5	6	5	2	8	4	3	7	3	3	8	4	5
Přehřátí po výpadku klimatizace	8	5	5	8	5	5	8	4	3	7	3	3	6	4	4	7	4	5	6	5	2	8	4	3	7	3	3	8	4	5
Poničení budovy okolními stromy	6	5	5	6	5	5	6	4	3	5	3	3	4	4	4	5	4	5	4	5	2	6	4	3	5	3	3	6	4	5
Ztráta služeb																														
Výpadek elektrické energie	7	5	7	7	5	7	7	4	5	6	3	5	5	4	6	6	4	7	5	5	4	7	4	5	6	3	5	7	4	7
Výpadek klimatizace	6	5	6	6	5	6	6	4	4	5	3	4	4	4	5	5	4	6	4	5	3	6	4	4	5	3	4	6	4	6
Výpadek sítě WAN	7	5	6	7	5	6	7	4	4	6	3	4	5	4	5	6	4	6	5	5	3	7	4	4	6	3	4	7	4	6
Výpadek sítě LAN	7	5	7	7	5	7	7	4	5	6	3	5	5	4	6	6	4	7	5	5	4	7	4	5	6	3	5	7	4	7
Výpadek IS	7	5	7	7	5	7	7	4	5	6	3	5	5	4	6	6	4	7	5	5	4	7	4	5	6	3	5	7	4	7
Výpadek IS technické podpory	6	5	5	6	5	5	6	4	3	5	3	3	4	4	4	5	4	5	4	5	2	6	4	3	5	3	3	6	4	5
Výpadek serveru se zdrojovými kódy	6	5	7	6	5	7	6	4	5	5	3	5	4	4	6	5	4	7	4	5	4	6	4	5	5	3	5	6	4	7
Výpadek hlasových služeb	8	5	5	8	5	5	8	4	3	7	3	3	6	4	4	7	4	5	6	5	2	8	4	3	7	3	3	8	4	5
Ohrožení důvěrnosti																														
Neoprávněné získání přístupových údajů	6	7	7	6	7	7	6	6	5	5	5	5	4	6	6	5	6	7	4	7	4	6	6	5	5	5	5	6	6	7
Neoprávněné získání informací	6	8	7	6	8	7	6	7	5	5	6	5	4	7	6	5	7	7	4	8	4	6	7	5	5	6	5	6	7	7
Chyba v nastavení přístupových práv	5	6	7	5	6	7	5	5	5	4	4	5	3	5	6	4	5	7	3	6	4	5	5	5	4	4	5	5	5	7
Slabiny v zabezpečení síťových služeb	6	7	6	6	7	6	6	6	4	5	5	4	4	6	5	5	6	6	4	7	3	6	6	4	5	5	4	6	6	6
Zranitelnosti webových služeb	6	7	6	6	7	6	6	6	4	5	5	4	4	6	5	5	6	6	4	7	3	6	6	4	5	5	4	6	6	6
Slabiny v architektuře IT infrastruktury	6	7	7	6	7	7	6	6	5	5	5	5	4	6	6	5	6	7	4	7	4	6	6	5	5	5	5	6	6	7
Získání dat z vyřazených médií	5	7	5	5	7	5	5	6	3	4	5	3	3	6	4	4	6	5	3	7	2	5	6	3	4	5	3	5	6	5
Krádež technického vybavení	7	7	6	7	7	6	7	6	4	6	5	4	5	6	5	6	6	6	5	7	3	7	6	4	6	5	4	7	6	6
Zneužití, ztráta nebo krádež USB disků	5	7	5	5	7	5	5	6	3	4	5	3	3	6	4	4	6	5	3	7	2	5	6	3	4	5	3	5	6	5
Záměrná škodlivá činnost v síti	5	6	6	5	6	6	5	5	4	4	4	4	3	5	5	4	5	6	3	6	3	5	5	4	4	4	4	5	5	6
Škodlivý software	6	7	7	6	7	7	6	6	5	5	5	5	4	6	6	5	6	7	4	7	4	6	6	5	5	5	5	6	6	7
Technická selhání																														
Selhání serveru	8	5	7	8	5	7	8	4	5	7	3	5	6	4	6	7	4	7	6	5	4	8	4	5	7	3	5	8	4	7
Selhání pracovní stanice	7	5	6	7	5	6	7	4	4	6	3	4	5	4	5	6	4	6	5	5	3	7	4	4	6	3	4	7	4	6
Chybné fungování systému	6	5	7	6	5	7	6	4	5	5	3	5	4	4	6	5	4	7	4	5	4	6	4	5	5	3	5	6	4	7
Nedostatek zdrojů pro provoz aplikace	7	5	6	7	5	6	7	4	4	6	3	4	5	4	5	6	4	6	5	5	3	7	4	4	6	3	4	7	4	6
Neoprávněné činnosti																														
Neoprávněné zkopírování informací	5	8	5	5	8	5	5	7	3	4	6	3	3	7	4	4	7	5	3	8	2	5	7	3	4	6	3	5	7	5
Neoprávněný přístup centrální správy systému	5	7	6	5	7	6	5	6	4	4	5	4	3	6	5	4	6	6	3	7	3	5	6	4	4	5	4	5	6	6
Zneužití admin. oprávnění	6	7	7	6	7	7	6	6	5	5	5	5	4	6	6	5	6	7	4	7	4	6	6	5	5	5	5	6	6	7

	Zdrojové kódy aplikací			Databáze klientů podniku			Databáze formulářů			Znalostní báze problémů a řešení			Systém pro správu námětů a připomínek			Firemní účetnictví			Data od klientů			Servery a aktivní síťové prvky			Pracovní stanice uživatelů			Komunikační služby třetích stran		
	D	D	I	D	D	I	D	D	I	D	D	I	D	D	I	D	D	I	D	D	I	D	D	I	D	D	I	D	D	I
Zneužití uživatelských oprávnění	6	6	8	6	6	8	6	5	6	5	4	6	4	5	7	5	5	8	4	6	5	6	5	6	5	4	6	6	5	8
Porušení mlčenlivosti zaměstnance	5	8	5	5	8	5	5	7	3	4	6	3	3	7	4	4	7	5	3	8	2	5	7	3	4	6	3	5	7	5
Neoprávněný přístup do prostor	6	7	6	6	7	6	6	6	4	5	5	4	4	6	5	5	6	6	4	7	3	6	6	4	5	5	4	6	6	6
Neoprávněný přístup do aplikace	5	7	7	5	7	7	5	6	5	4	5	5	3	6	6	4	6	7	3	7	4	5	6	5	4	5	5	5	6	7
Lidská selhání																														
Nedbalost při údržbě zařízení	6	5	7	6	5	7	6	4	5	5	3	5	4	4	6	5	4	7	4	5	4	6	4	5	5	3	5	6	4	7
Nedostatek personálu správy IT služeb	7	5	6	7	5	6	7	4	4	6	3	4	5	4	5	6	4	6	5	5	3	7	4	4	6	3	4	7	4	6
Chyby personálu správy IT služeb	8	7	7	8	7	7	8	6	5	7	5	5	6	6	6	7	6	7	6	7	4	8	6	5	7	5	5	8	6	7
Nedostatečná dokumentace systému	7	5	8	7	5	8	7	4	6	6	3	6	5	4	7	6	4	8	5	5	5	7	4	6	6	3	6	7	4	8
Nedodržování předpisů pro práci s informacemi	6	7	6	6	7	6	6	6	4	5	5	4	4	6	5	5	6	6	4	7	3	6	6	4	5	5	4	6	6	6
Chyby obsluhy aplikace	5	6	7	5	6	7	5	5	5	4	4	5	3	5	6	4	5	7	3	6	4	5	5	5	4	4	5	5	5	7
Zneužití oprávnění při sdělení hesla	5	7	6	5	7	6	5	6	4	4	5	4	3	6	5	4	6	6	3	7	3	5	6	4	4	5	4	5	6	6

Tab. 8 Hodnota rizika vůči informačnímu aktivu

	1	2	3	4	5	6	7	8	9	10
	Zdrojové kódy aplikací	Databáze klientů podniku	Databáze formulářů	Znalostní báze problémů a řešení	Systém pro správu námětů a připomínek	Firemní účetnictví	Data od klientů	Servery a aktivní síťové prvky	Pracovní stanice uživatelů	Komunikační služby třetích stran
Fyzické poškození										
Požár	8	8	8	7	6	7	6	8	7	8
Poškození vodou	8	8	8	7	6	7	6	8	7	8
Přehřátí po výpadku klimatizace	8	8	8	7	6	7	6	8	7	8
Poničení budovy okolními stromy	6	6	6	5	4	5	5	6	5	6
Ztráta služeb										
Výpadek elektrické energie	7	7	7	6	6	7	5	7	6	7
Výpadek klimatizace	6	6	6	5	5	6	5	6	5	6
Výpadek sítě WAN	7	7	7	6	5	6	5	7	6	7
Výpadek sítě LAN	7	7	7	6	6	7	5	7	6	7
Výpadek IS	7	7	7	6	6	7	5	7	6	7
Výpadek IS technické podpory	6	6	6	5	4	5	5	6	5	6
Výpadek serveru se zdrojovými kódy	7	7	6	5	6	7	5	6	5	7
Výpadek hlasových služeb	8	8	8	7	6	7	6	8	7	8
Ohrožení důvěrnosti										
Neoprávněné získání přístupových údajů	7	7	6	5	6	7	7	6	5	7

	1	2	3	4	5	6	7	8	9	10
	Zdrojové kódy aplikací	Databáze klientů podniku	Databáze formulářů	Znalostní báze problémů a řešení	Systém pro správu námětů a připomínek	Firemní účetnictví	Data od klientů	Servery a aktivní síťové prvky	Pracovní stanice uživatelů	Komunikační služby třetích stran
Neoprávněné získání informací	8	8	7	6	7	7	8	7	6	7
Chyba v nastavení přístupových práv	7	7	5	5	6	7	6	5	5	7
Slabiny v zabezpečení síťových služeb	7	7	6	5	6	6	7	6	5	6
Zranitelnosti webových služeb	7	7	6	5	6	6	7	6	5	6
Slabiny v architektuře IT infrastruktury	7	7	6	5	6	7	7	6	5	7
Získání dat z vyřazených médií	7	7	6	5	6	6	7	6	5	6
Krádež technického vybavení	7	7	7	6	6	6	7	7	6	7
Zneužití, ztráta nebo krádež USB disků	7	7	6	5	6	6	7	6	5	6
Záměrná škodlivá činnost v síti	6	6	5	4	5	6	6	5	4	6
Škodlivý software	7	7	6	5	6	7	7	6	5	7
Technická selhání										
Selhání serveru	8	8	8	7	6	7	6	8	7	8
Selhání pracovní stanice	7	7	7	6	5	6	5	7	6	7
Chybné fungování systému	7	7	6	5	6	7	5	6	5	7
Nedostatek zdrojů pro provoz aplikace	7	7	7	6	5	6	5	7	6	7
Neoprávněné činnosti										
Neoprávněné zkopírování informací	8	8	7	6	7	7	8	7	6	7
Neoprávněný přístup centrální správy systému	7	7	6	5	6	6	7	6	5	6
Zneužití administrátorských oprávnění	7	7	6	5	6	7	7	6	5	7
Zneužití uživatelských oprávnění	8	8	6	6	7	8	6	6	6	8
Porušení mlčenlivosti zaměstnance	8	8	7	6	7	7	8	7	6	7
Neoprávněný přístup do prostor	7	7	6	5	6	6	7	6	5	6
Neoprávněný přístup do aplikace	7	7	6	5	6	7	7	6	5	7
Lidská selhání										
Nedbalost při údržbě zařízení	7	7	6	5	6	7	5	6	5	7
Nedostatek personálu správy IT služeb	7	7	7	6	5	6	5	7	6	7
Chyby personálu správy IT služeb	8	8	8	7	6	7	7	8	7	8
Nedostatečná dokumentace systému	8	8	7	6	7	8	5	7	6	8
Nedodržování předpisů pro práci s informacemi	7	7	6	5	6	6	7	6	5	6
Chyby obsluhy aplikace	7	7	5	5	6	7	6	5	5	7
Zneužití oprávnění při sdělení hesla	7	7	6	5	6	6	7	6	5	6

6 Zavedení ISMS v podniku

V dalším textu budou popsána opatření, které je nutné zavést či revidovat tak, aby byla všechna identifikovaná rizika pokud možno eliminována nebo alespoň minimalizován dopad na informační aktiva podniku. Jako soubor opatření bude použit seznam opatření, který je definován v příloze A normy ČSN ISO/IEC 27001:2006. U jednotlivých opatření je uveden důvod jejich výběru nebo vyloučení, praktické provedení opatření bude uvedeno v dalších kapitolách.

6.1 Soubor opatření podle normy ČSN ISO/IEC 27001:2006

Jak bylo uvedeno dříve, norma obsahuje 11 hlavních oblastí, 34 kategorií a celkem 139 opatření. Cílem těchto opatření je minimalizovat výskyt hrozeb a následně rizik. Pro každé opatření je třeba rozhodnout na základě bezpečnostní analýzy a hodnocení rizik, zda bude dané opatření zavedeno, či revidováno, pokud opatření je již aplikováno. Pokud opatření nebude zavedeno, je doplněn komentář, z jakého důvodu.

Tab. 9 Soubor opatření podle normy a požadovaný stav v organizaci

	Opatření normy ISO/IEC 27001	Stav	Zdůvodnění výběru/výluky
5	Bezpečnostní politika		
5.1.1	Dokument bezpečnostní politiky informací	zavést	podpora procesů ISMS
5.1.2	Přezkoumání bezpečnostní politiky informací	revidovat	podpora procesů ISMS
6	Organizace bezpečnosti informací		
6.1.1	Závazek vedení směrem k bezpečnosti informací	zavést	podpora procesů ISMS
6.1.2	Koordinace bezpečnosti informací	zavést	podpora procesů ISMS
6.1.3	Přidělení odpovědnosti v oblasti informační bezpečnosti	revidovat	podpora procesů ISMS
6.1.4	Schvalovací proces prostředků zpracování informací	zavést	ohrožení důvěrnosti, technická selhání
6.1.5	Dohody o ochraně důvěrných informací	revidovat	ohrožení důvěrnosti, neoprávněné činnosti
6.1.6	Kontakt s orgány veřejné správy	zavedeno	podpora procesů ISMS
6.1.7	Kontakt se zájmovými skupinami		Nejsou prováděny žádné kontakty
6.1.8	Nezávislá přezkoumání bezpečnosti informací		Nezávislé přezkoumávání bezpečnosti se neprovádí.
6.2.1	Identifikace rizik vyplývajících z přístupu externích subjektů	zavést	ohrožení důvěrnosti, neoprávněné činnosti
6.2.2	Bezpečnostní požadavky pro přístup klientů		Klienti nemají přístup k aktivům organizace
6.2.3	Bezpečnostní požadavky v dohodách se třetí stranou	revidovat	ohrožení důvěrnosti, neoprávněné činnosti

	Opatření normy ISO/IEC 27001	Stav	Zdůvodnění výběru/výluky
7	Řízení aktiv		
7.1.1	Evidence aktiv	zavést	podpora procesů ISMS
7.1.2	Vlastnictví aktiv	zavést	podpora procesů ISMS
7.1.3	Přípustné použití aktiv	revidovat	ohrožení důvěrnosti, neoprávněné činnosti
7.2.1	Doporučení pro klasifikaci	zavést	ohrožení důvěrnosti, neoprávněné činnosti
7.2.2	Označování a zacházení s informacemi	zavést	ohrožení důvěrnosti, neoprávněné činnosti
8	Bezpečnost lidských zdrojů		
8.1.1	Role a odpovědností	revidovat	neoprávněné činnosti
8.1.2	Prověřování	zavést	ohrožení důvěrnosti
8.1.3	Podmínky výkonu pracovní činnosti	revidovat	neoprávněné činnosti
8.2.1	Odpovědnosti vedoucích zaměstnanců	zavedeno	neoprávněné činnosti, lidská selhání
8.2.2	Bezpečnostní povědomí, vzdělávání a školení v oblasti bezpečnosti informací	zavést	neoprávněné činnosti, lidská selhání
8.2.3	Disciplinární řízení	zavést	neoprávněné činnosti
8.3.1	Odpovědnosti při ukončení prac. vztahu	zavést	ohrožení důvěrnosti, neoprávněné činnosti
8.3.2	Navrácení zapůjčených prostředků	zavedeno	
8.3.3	Odebrání přístupových práv	revidovat	ohrožení důvěrnosti, neoprávněné činnosti
9	Fyzická bezpečnost a bezpečnost prostředí		
9.1.1	Fyzický bezpečnostní perimetr	zavést	ztráta služeb, ohrožení důvěrnosti
9.1.2	Fyzické kontroly vstupu osob	revidovat	ztráta služeb, ohrožení důvěrnosti, neoprávněné činnosti
9.1.3	Zabezpečení kanceláří, místností a prostředků	zavést	ohrožení důvěrnosti, neoprávněné činnosti
9.1.4	Ochrana před hrozbami vnějšku a prostředí	revidovat	fyzické poškození
9.1.5	Práce v zabezpečených oblastech	zavést	ztráta služeb, lidská selhání
9.1.6	Veřejný přístup, prostory pro nakládku a vykládku	revidovat	ohrožení důvěrnosti, neoprávněné činnosti
9.2.1	Umístění zařízení a jeho ochrana	revidovat	fyzické poškození, ztráta služeb, ohrožení důvěrnosti
9.2.2	Podpůrná zařízení	revidovat	ztráta služeb
9.2.3	Bezpečnost kabelových rozvodů		kabelové vedení je umístěno uvnitř budovy s trvalým obýváním, není přístup pro narušení bezpečnosti
9.2.4	Údržba zařízení	revidovat	ztráta služeb, technická selhání
9.2.5	Bezpečnost zařízení mimo prostory organizace	zavést	ohrožení důvěrnosti, neoprávněné činnosti
9.2.6	Bezpečná likvidace nebo opakované použití zařízení	zavést	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
9.2.7	Přemístění majetku	revidovat	neoprávněné činnosti
10	Řízení komunikací a řízení provozu		
10.1.1	Dokumentace provozních postupů	zavést	ztráta služeb, technická selhání, lidská selhání
10.1.2	Řízení změn	zavést	ztráta služeb, ohrožení důvěrnosti, technická selhání
10.1.3	Oddělení povinností	zavést	ohrožení důvěrnosti, neoprávněné činnosti
10.1.4	Oddělení vývoje, testování a provozu	revidovat	ohrožení důvěrnosti, neoprávněné činnosti
10.2.1	Dodávky služeb	zavést	ztráta služeb, ohrožení důvěrnosti, technická selhání
10.2.2	Monitorování a přezkoumávání služeb třetích stran	revidovat	ohrožení důvěrnosti, technická selhání, lidská selhání

	Opatření normy ISO/IEC 27001	Stav	Zdůvodnění výběru/výluky
10.2.3	Řízení změn služeb poskytovaných třetími stranami	revidovat	ztráta služeb, ohrožení důvěrnosti, technická selhání
10.3.1	Řízení kapacit	revidovat	technická selhání
10.3.2	Přejímání systémů		systémy nejsou přejímány
10.4.1	Opatření na ochranu proti škodlivým programům	zavedeno	ztráta služeb, ohrožení důvěrnosti, technická selhání
10.4.2	Opatření na ochranu proti mobilním kódům		nejsou používána mobilní zařízení
10.5.1	Zálohování informací	revidovat	fyzické poškození, technická selhání, neoprávněné činnosti, lidská selhání
10.6.1	Síťová opatření	zavést	ztráta služeb, ohrožení důvěrnosti, neoprávněné činnosti
10.6.2	Bezpečnost síťových služeb	zavést	ztráta služeb, ohrožení důvěrnosti, neoprávněné činnosti
10.7.1	Správa výměnných počítačových médií	revidovat	fyzické poškození, ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
10.7.2	Likvidace médií	revidovat	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
10.7.3	Postupy pro manipulaci s informacemi	zavést	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
10.7.4	Bezpečnost systémové dokumentace	zavést	ohrožení důvěrnosti, neoprávněné činnosti
10.8.1	Postupy a politiky při výměně informací a programů	zavést	ohrožení důvěrnosti, neoprávněné činnosti
10.8.2	Dohody o výměně informací a programů	zavést	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
10.8.3	Bezpečnost médií při přepravě		média nejsou přepravována
10.8.4	Elektronické zasílání zpráv	zavedeno	ohrožení důvěrnosti
10.8.5	Informační systémy organizace	revidovat	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
10.9.1	Elektronický obchod		nepoužívá se
10.9.2	On-line transakce		nejsou provozovány systémy elektronického obchodu
10.9.3	Veřejně přístupné informace	zavedeno	neoprávněné činnosti
10.10.1	Pořizování auditních záznamů	revidovat	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
10.10.2	Monitorování používání systému	revidovat	ohrožení důvěrnosti, technická selhání, neoprávněné činnosti, lidská selhání
10.10.3	Ochrana vytvořených záznamů	zavést	neoprávněné činnosti
10.10.4	Administrátorský a operátorský deník	zavést	ohrožení důvěrnosti, technická selhání, neoprávněné činnosti
10.10.5	Záznam selhání	zavést	technická selhání, lidská selhání
10.10.6	Synchronizace času	zavést	neoprávněné činnosti
11	Řízení přístupu		
11.1.1	Politika řízení přístupu	zavést	ohrožení důvěrnosti, neoprávněné činnosti
11.2.1	Registrace uživatele	zavést	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
11.2.2	Řízení privilegovaného přístupu	zavést	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
11.2.3	Správa uživatelských hesel	zavedeno	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
11.2.4	Přezkoumání přístupových práv uživatelů	zavést	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání

	Opatření normy ISO/IEC 27001	Stav	Zdůvodnění výběru/výluky
11.3.1	Používání hesel	zavedeno	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
11.3.2	Neobsluhovaná uživatelská zařízení	zavést	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
11.3.3	Zásada prázdného stolu a prázdné obrazovky monitoru	zavést	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
11.4.1	Politika užívání síťových služeb	zavést	ohrožení důvěrnosti, neoprávněné činnosti
11.4.2	Autentizace uživatele pro externí připojení		přeneseno na externího dodavatele služeb
11.4.3	Identifikace zařízení v sítích	revidovat	ohrožení důvěrnosti, neoprávněné činnosti
11.4.4	Ochrana portů pro vzdálenou diagnostiku a konfiguraci		přeneseno na externího dodavatele služeb
11.4.5	Princip oddělení v sítích		přeneseno na externího dodavatele služeb
11.4.6	Řízení síťových spojení		přeneseno na externího dodavatele služeb
11.4.7	Řízení směrování sítě		přeneseno na externího dodavatele služeb
11.5.1	Bezpečné postupy přihlášení	zavedeno	ohrožení důvěrnosti, neoprávněné činnosti
11.5.2	Identifikace a autentizace uživatelů	zavedeno	ohrožení důvěrnosti, neoprávněné činnosti
11.5.3	Systém správy hesel	zavedeno	ohrožení důvěrnosti, neoprávněné činnosti
11.5.4	Použití systémových nástrojů	revidovat	ohrožení důvěrnosti, neoprávněné činnosti
11.5.5	Časové omezení relace		Nelze aplikovat na vývoj SW.
11.5.6	Časové omezení spojení		Nejsou identifikovány vysoce rizikové aplikace.
11.6.1	Omezení přístupu k informacím	revidovat	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
11.6.2	Oddělení citlivých systémů	revidovat	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
11.7.1	Mobilní výpočetní zařízení a sdělovací technika		není v podniku využívána
11.7.2	Práce na dálku	revidovat	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
12	Akvizice, vývoj a údržba informačních systémů		
12.1.1	Analýza a specifikace bezpečnostních požadavků	revidovat	ohrožení důvěrnosti, technická selhání, neoprávněné činnosti, lidská selhání
12.2.1	Validace vstupních dat	zavedeno	technická selhání, lidská selhání
12.2.2	Kontrola vnitřního zpracování	zavedeno	technická selhání, lidská selhání
12.2.3	Integrita zpráv	zavedeno	technická selhání, lidská selhání
12.2.4	Validace výstupních dat	zavedeno	technická selhání, lidská selhání
12.3.1	Politika pro použití kryptografických kontrol		nepoužívají se
12.3.2	Správa klíčů		nepoužívají se
12.4.1	Správa provozního programového vybavení	zavedeno	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
12.4.2	Ochrana dat pro testování systému	revidovat	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
12.4.3	Řízení přístupu ke knihovně zdrojových kódů	zavedeno	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
12.5.1	Postupy řízení změn	revidovat	ztráta služeb, ohrožení důvěrnosti, technická selhání, lidská selhání
12.5.2	Technické přezkoumání aplikací po změnách operačního systému	revidovat	ztráta služeb, ohrožení důvěrnosti, technická selhání
12.5.3	Omezení změn programových balíků	revidovat	ztráta služeb, ohrožení důvěrnosti, technická selhání

	Opatření normy ISO/IEC 27001	Stav	Zdůvodnění výběru/výluky
12.5.4	Únik informací	zavést	ohrožení důvěrnosti, lidská selhání
12.5.5	Programové vybavení vyvíjené externím dodavatelem	revidovat	ohrožení důvěrnosti, neoprávněné činnosti
12.6.1	Řízení, správa a kontrola technických zranitelností	revidovat	ztráta služeb, ohrožení důvěrnosti, neoprávněné činnosti, technická selhání
13	Zvládání bezpečnostních incidentů		
13.1.1	Hlášení bezpečnostních událostí	zavést	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
13.1.2	Hlášení bezpečnostních slabin	zavést	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
13.2.1	Odpovědnosti a postupy reakce na incidenty	zavést	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
13.2.2	Ponaučení z bezpečnostních incidentů	zavést	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
13.2.2	Shromažďování důkazů		V ČR platí zásada volného řízení důkazů a nejsou vydány normy specifikující požadavky na sílu důkazů.
14	Řízení kontinuity činností organizace		
14.1.1	Zařazení informační bezpečnosti do procesu řízení kontinuity činností organizace	zavést	podpora procesů ISMS
14.1.2	Kontinuita činností organizace a hodnocení rizik	zavést	podpora procesů ISMS
14.1.3	Vytváření a implementace plánů kontinuity	zavést	fyzické poškození, ztráta služeb, technická selhání, neoprávněné činnosti, lidská selhání
14.1.4	Systém plánování kontinuity činností organizace	zavést	fyzické poškození, ztráta služeb, technická selhání, neoprávněné činnosti, lidská selhání
14.1.5	Testování, udržování a přezkoumávání plánů kontinuity	zavést	technická selhání, lidská selhání
15	Soulad s požadavky		
15.1.1	Identifikace odpovídajících předpisů	revidovat	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
15.1.2	Ochrana duševního vlastnictví	revidovat	ohrožení důvěrnosti, neoprávněné činnosti
15.1.3	Ochrana záznamů organizace	revidovat	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
15.1.4	Ochrana dat a soukromí osobních údajů	zavedeno	ohrožení důvěrnosti, neoprávněné činnosti
15.1.5	Prevence zneužití prostředků pro zpracování informací	revidovat	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
15.1.6	Regulace kryptografických opatření		nepoužívá se
15.2.1	Shoda s bezpečnostními politikami a normami	zavést	podpora procesů ISMS
15.2.2	Kontrola technické shody	revidovat	podpora procesů ISMS
15.3.1	Opatření k auditu		nepoužívá se
15.3.2	Ochrana nástrojů pro audit		nepoužívá se

6.2 Plán zavedení opatření

Vzhledem k tomu, že podnik je svým personálním obsazením relativně malý, tím pádem jsou omezené zdroje na provádění zejména administrativních opatření, jako je dokumentace či vytváření plánů. Z tohoto úhlu pohledu je vhodné rozdělit opatření, která mají být zavedena a revidována do delšího časového období a několika fází. Protože podnik neusiluje o certifikaci systému ISMS a není tedy časově omezen, lze zavedení systému ISMS brát jako pozitivní krok managementu podniku a celkové řešení současného stavu může být provedeno v průběhu delšího období.

Na podnik čeká několik úkolů:

- Je třeba zavést taková opatření, která by vedla ke snížení identifikovaných rizik.
- Zavedení opatření, která lze svou povahou zavést rychle bez větších nároků na zaměstnance (obecně zdroje) nebo zvolit externího dodavatele na zavedení opatření.
- Zavést zbývající opatření z výše uvedeného seznamu opatření.

Obecně lze snížení rizik provádět za pomocí metod:

- **Akceptace (Retence) rizika** – proti riziku se neprovádí žádné akce na jeho snížení. Podnik dané riziko identifikoval, ale vyhodnotil ho jako akceptovatelné, včetně případné ztráty finanční či jiné. Na základě analýzy rizik se vyberou rizika, s nízkým hodnocením (0-2).
- **Redukce rizika** – odstraňují se příčiny vzniku rizika nebo dopady rizika. Zde lze uvažovat o přesunu rizika na jiné subjekty, zavedení adekvátních opatření pro odstranění či snížení rizika nebo pojištění proti případným následkům.

Protože při analýze rizik prakticky nebyly identifikovány rizika s nízkým hodnocením, je třeba při řešení snižování rizik v podniku provádět redukci rizika výše zmíněnými možnostmi. Podnik při vykonávání své činnosti rozlišuje dvě období. Březen až září je období relativního klidu, kdy je minimálně firma vytížena vzhledem k předmětu podnikání. Zaměstnanci mohou pracovat na více úkolech. V období říjen až únor je vytížení zaměstnanců značné, neboť jsou chystány nové verze produktů atd.

Rozdělení bych díky znalosti vnitřního fungování podniku navrhoval, jako následující:

1. **Etapa I. Červen 2011 – Prosinec 2011**: Podnik v tomto období plánuje stavební práce pro úpravy kanceláří. Část zaměstnanců se tedy může podílet na zavedení opatření týkající se skupiny A.9 Fyzická bezpečnost a bezpečnost prostředí. Druhá část zaměstnanců pak bude řešit oblasti zaměřené více na administrativní činnosti: A.5 Bezpečnostní politika, A.6 Organizace bezpečnosti informací a A.7 Řízení aktiv.

2. **Etapa II. Leden 2012 – Květen 2012**: Technický personál v tomto období má možnost řešit opatření A.10 Řízení komunikace a řízení provozu, A.11 řízení přístupu, A.13 zvládání bezpečnostních incidentů a oblast A.14 řízení kontinuity činností organizace.
3. **Etapa III. Červen 2012 – Prosinec 2012**: Řešené oblasti v tomto období jsou A.12 Akvizice, vývoj a údržba informačních systémů, A.8 Bezpečnost lidských zdrojů a A.15 Soulad s požadavky.

Jednotlivé etapy zavádění byly stanoveny podle vytíženosti jednotlivých oddělení v rámci daného období. V průběhu etapy I. jsou omezeny obchodní aktivity a četnost incidentů na lince technické podpory je minimální. V této době je nejvytíženějším oddělením vývoje, které připravuje vydání nové verze software. V této době lze bez větších problémů zavádět opatření z oblasti fyzické bezpečnosti a opatření, které jsou zaměřeny na administrativní činnost. Zde mohou v rámci podniku být využiti i zaměstnanci obchodního oddělení a technické podpory.

Etapa II. je prováděna v období, kdy jsou obchodní a technické oddělení velmi vytížené. Zde lze naplno využít pracovníků oddělení vývoje na zavedení opatření týkajících se požadavků na komunikační systémy podniku, zvládání bezpečnostních incidentů a řízení kontinuity. V těchto oblastech lze s výhodou využít znalostí vývojových pracovníků.

Poslední etapa je realizována především obchodním oddělením, kde jsou řešeny otázky personálního obsazení podniku a převážně oddělením technické podpory za využití pracovníků z oddělení vývoje.

Takto nastavený plán zavádění ISMS v podniku je realizovatelný, jak z pohledu dostupných zdrojů, tak z pohledu prováděných činností v podniku. Rozdělením do jednotlivých období je řešením, jak provádět postupnou adaptabilitu zaměstnanců na nový systém způsobu jejich práce a rozšíření zaměstnaneckých povinností.

7 Etapa I. zavedení opatření ISMS

Po splnění požadavků z kapitoly 5, tj. ustanovení ISMS v podniku a vytvoření bezpečnostní politiky je dalším krokem řízení bezpečnosti informací v organizaci za pomoci pravidel a postupů pro procesy uvnitř podniku, tak i pro případné externí subjekty. Součástí řízené bezpečnosti je i vlastní řízení aktiv. Bez zavedení těchto základních opatření není možné dále pokračovat při plnění dalších požadavků normy. Tyto zmíněné oblasti jsou řešeny v oblastech A.5, A.6 a A.7. Pro zavedení všech opatření je datum jejich nejzazšího zavedení poslední den období dané fáze. Jednotlivá opatření se budou ovšem zavádět průběžně.

7.1.1 A.5 Bezpečnostní politika informací

Cílem opatření je určení směru a vyjádření podpory bezpečnosti informací vedením podniku, aby byly naplněny požadavky podniku, příslušné zákony a směrnice.

7.1.1.1 A.5.1.1 Dokument bezpečnostní politiky informací

Odpovědná osoba: Sponzor projektu (majitel podniku)

Opatření: Vedení podniku vytvoří bezpečnostní politiku podniku. S touto politikou musí být prokazatelně seznámeni všichni zaměstnanci podniku a případným externím dodavatelům či odběratelům. Obsah tohoto dokumentu je podrobně popsán v kapitole 5.

Zdroje opatření:

Vytvoření dokumentu bezpečnostní politiky	24h
Seznámení zaměstnanců s touto politikou	3h
Informování dodavatelů a odběratelů o této politice	3h

7.1.1.2 A.5.1.2 Přezkoumání bezpečnostní politiky informací

Odpovědná osoba: Bezpečnostní manager

Opatření: V plánu pravidelného přezkoumávání bezpečnostní politiky je obsažen interval pro přezkoumávání účinnosti bezpečnostní politiky. Vzhledem k velikosti podniku a vcelku jeho úzké specializaci tento interval nemá smysl nastavit u počáteční fáze zavádění, na dobu kratší než 1 rok. Období 1 roku je vzhledem k rozdělení činností v rámci podniku odpovídající doba, po které je možné jednotlivá opatření považovat za dostatečně sžité s činnostmi na jednotlivých odděleních. V dalších obdobích je vhodné tento interval zkrátit na polovinu či méně, protože nové hrozby se mohou prakticky objevit v rámci týdnů. Použitelnosti bezpečnostní politiky a její případné úpravy by tak mohly být zavedeny v co nejkratším období po objevení nové hrozby.

Zdroje opatření:

Vytvoření plánu přezkoumávání bezpečnostní politiky	3h
Přezkoumání politiky a její případné úpravy	48h/přezkoumání

7.1.2 A.6 Organizace bezpečnosti informací

Opatření jsou prováděna na podporu řízení bezpečnosti opatření a zachování bezpečnosti informací v podniku a jejích prostředků pro zpracování informací, které jsou dostupné externím subjektům.

7.1.2.1 A.6.1.1 Závazek vedení směrem k bezpečnosti informací

Odpovědná osoba: Sponzor projektu

Opatření: Vedení organizace dává najevo svůj závazek podporovat řešení bezpečnosti informací v podniku. Tato vůle je uvedena v bezpečnostní politice podniku. V dokumentu bezpečnostní politiky jsou uvedeny role v oblasti bezpečnosti informací.

Zdroje opatření:

Sponzor projektu vytváří dokument bezpečnostní politiky a stanoví role	24h

7.1.2.2 A.6.1.2 Koordinace bezpečnosti informací, A.6.1.3 Přidělení odpovědností

Odpovědná osoba: Sponzor projektu, bezpečnostní manager a vedoucí jednotlivých oddělení v podniku.

Opatření: V podniku je třeba zavést směrnici, ve které bude stanoveno, jakým způsobem je v podniku koordinována bezpečnost informací mezi jednotlivými odděleními. Současně se ve směrnici stanoví odpovědnosti v oblasti bezpečnosti informací. Vedoucích jednotlivých oddělení se v těchto směrnicích stávají prostředníky a spoluodpovědní za vzájemnou koordinaci při řešení bezpečnostních incidentů. Při nahlášení bezpečnostního incidentu je třeba postupovat podle předem daného postupu eskalace problému. Podřízení pracovníci hlásí problém svému vedoucímu oddělení a ten pak předává zjištěné skutečnosti bezpečnostnímu managerovi, který zabezpečí vyřešení bezpečnostního incidentu. Všechny skutečnosti musí být náležitě dokumentovány a všichni zaměstnanci musí být seznámeni s těmito postupy. Samotní vedoucí pracovníci mají povinnost se proaktivně věnovat vyhledávání a kontrole bezpečnosti v rámci jejich oddělení.

Zdroje opatření:

Vytvoření směrnice koordinace bezpečnosti	10h
Vyčlenění odpovědných osob na řešení bezpečnosti	2h/týden
Eskalace zjištěného problému managerovi bezpečnosti	1h/incident

7.1.2.3 A.6.1.4 Schvalovací proces prostředků pro zpracování informací

Odpovědná osoba: vedoucí jednotlivých oddělení v podniku, osoba odpovědná za technické či programové vybavení.

Opatření: Každý nový prostředek pro zpracování informací musí být schválen vedoucím patřičného oddělení. V podniku je vytvořen schvalovací proces, se kterým jsou seznámeni všichni pracovníci. Vedoucí pracovníci v případě nutnosti konzultují nezbytnost zavedení nového prostředku s pracovníkem odpovědným za technické nebo programové vybavení podniku. O každém nově zavedeném zařízení musí být proveden záznam a určená odpovědná osoba za toto technické zařízení.

Zdroje opatření:

Vytvoření schvalovacího procesu	2h
Schvalování nových prostředků vedoucími pracovníky	1h/týden

7.1.2.4 A.6.1.5 Dohody o ochraně důvěrných informací

Odpovědná osoba: vedoucí jednotlivých oddělení v podniku

Opatření: V podniku jsou stanoveny dohody, jakým způsobem chránit důvěrné informace. Je v nich uvedeno, kteří pracovníci mají ke kterým důvěrným informacím přístup, jaké operace s nimi mohou provádět a povinnost zachovat mlčenlivost o těchto důvěrných informacích. V dohodách jsou stanoveny sankce za porušení a všichni zaměstnanci jsou s těmito dohodami prokazatelně seznámeni. Současně se vytvoří plán pro přezkoumání existujících dohod o ochraně důvěrných informací, ve kterém se zkoumá, zda stále existuje důvod, aby pracovníci měli přístup k těmto informacím. Pracovníci jednotlivých oddělení by měli mít přístup pouze k těm informacím odpovídajícím povaze jejich práce. Interval pro toto přezkoumávání je podle jednotlivých oddělení individuální a v případě oddělení technické podpory se jedná o týdenní interval, v případě obchodního oddělení je interval měsíční. U pracovníků oddělení vývoje není interval stanoven obdobím, ale změnou zařazení či vyřazení zaměstnance z tohoto oddělení.

Zdroje opatření:

Vytvoření plánu přezkoumávání dohod o ochraně informací	1h
Vyčlenění odpovědné osoby za přezkoumání dohod	1h/týden, měsíc, individuálně

7.1.2.5 A.6.2.1 Identifikace rizik plynoucích z přístupu externích subjektů a A.6.2.3 Bezpečností požadavky v dohodách se třetí stranou

Odpovědná osoba: bezpečnostní manager, externí dodavatel služeb

Opatření: Před povolením externích subjektů k přístupu k aktivům podniku je třeba provést bezpečnostní analýzu pro identifikaci rizik plynoucích z tohoto přístupu. Pro analýzu technického prostředí a způsobů připojení je vyžádán posudek od externího dodavatel služeb v oblasti zabezpečení a správy počítačové sítě. Na základě tohoto posudku a po odstranění případných zjištěných nedostatků je externímu subjektu poskytnuta možnost připojení do firemní sítě a jejího využívání.

Takto se řeší především externí pracovníci vývoje, kteří přistupují do firemní sítě přes VPN a to prostřednictvím Wi–Fi přístupového bodu. S externím subjektem je následně sepsána smlouva o povinnostech subjektu při práci v podnikové síti. V této smlouvě jsou obsaženy klausule o neposkytnutí informací třetím stranám, síle používaných hesel, zásady uzamykání počítačů bez dozoru, používání aktualizovaného systému a antivirového programu. Ve smlouvě jsou stanoveny také sankce za porušení některého ustanovení smlouvy. Je stanovena možnost kontroly používaného zařízení k přístupu do podnikové sítě.

Zdroje opatření:

Posouzení možnosti připojení externího subjektu	24h/požadavek
Vytvoření analýzy rizik přístupu externího subjektu	4h/požadavek
Kontrola dodržování smlouvy	2h/měsíčně

7.1.3 A.7 Řízení aktiv

Sada opatření, pro podporu řízení aktiv, stanovení odpovědnosti za jednotlivá aktiva a nastavení a udržování přiměřené ochrany aktiv podniku. Současně tato opatření zajišťují odpovídající úroveň ochrany informací

7.1.3.1 A.7.1.1 Evidence aktiv

Odpovědná osoba: bezpečnostní manager

Opatření: V etapě ustanovení ISMS byla identifikována všechna informační aktiva podniku. Tato aktiva je třeba evidovat, což je splněno jejich vyjmenováním při ustanovení ISMS. Dalším požadavkem tohoto opatření je pravidelná revize těchto aktiv. Protože identifikovaná aktiva podniku jsou v čase neměnná, lze interval jejich revize stanovit na 1 rok. V průběhu období 1 roku nedochází k významným změnám informační aktiv, ve smyslu jejich struktury. Obsahově dochází ke změnám ve všech těchto aktivech. V okamžiku revize je třeba posoudit stav podniku na existenci případných nových aktiv, či přezkoumávat oprávněnost stávajících aktiv. Pro zachování časové kontinuity evidence aktiv je třeba zaznamenávat změny v aktivech a udržovat seznam aktiv ve skutečnosti odpovídajícím stavu.

Zdroje opatření:

Přezkoumání informačních aktiv podniku	2h/rok

7.1.3.2 A.7.1.2 Vlastnictví aktiv

Odpovědná osoba: bezpečnostní manager

Opatření: Každé identifikované aktivum je třeba přidělit odpovědné osobě. V tomto případě je vhodné za vlastníka aktiva stanovit vedoucího oddělení, ke kterému dané aktivum logicky náleží. O tomto přidělení odpovědnosti aktiva je třeba průkazně jeho vlastníka informovat a případné změny vlastníků, zaznamenat. Protože aktiva odpovídají svou strukturou jednotlivým oddělením, každému

aktivu lze přidělit jako vlastníka vedoucího odpovídajícího oddělení. Nedílnou součástí tohoto opatření je stanovení revize přidělení aktiv, přičemž lze interval revize ponechat stejný jako v opatření A.7.1.1 tj. 1 rok případně revidovat přidělení aktiv v okamžiku změny postu vedoucího oddělení.

Tab. 10 Přiřazení aktiv vlastníkům

Aktivum	Vlastník aktiva
Zdrojové kódy aplikací	vedoucí oddělení vývoje
Databáze klientů podniku	vedoucí obchodního oddělení
Databáze formulářů	vedoucí oddělení vývoje
Znalostní báze problémů a řešení	vedoucí oddělení technické podpory
Systém pro správu námětů a připomínek	vedoucí oddělení technické podpory
Firemní účetnictví	vedoucí obchodního oddělení
Data od klientů	vedoucí oddělení technické podpory
Servery a aktivní síťové prvky	vedoucí oddělení vývoje
Pracovní stanice uživatelů	vedoucí oddělení vývoje
Komunikační služby třetích stran	vedoucí oddělení vývoje

Zdroje opatření:

Přiřazení a případné revize vlastníků informačních aktiv 1h/interval revize

7.1.3.3 A.7.1.3 Přípustné použití aktiv

Odpovědná osoba: vlastníci aktiv

Opatření: V podniku je třeba sestavit pravidla, jakým způsobem lze využívat informace v informačních aktivech firmy, jakým způsobem mohou být využívány technické prostředky v podniku. V tomto kroku je třeba sestavit množinu používaných a povolených aplikací na pracovních stanicích a nastavit odpovědnost jednotlivých pracovníků za obsah pracovních stanic. O všech těchto pravidlech musí být vedena dokumentace a všichni pracovníci musí být s těmito pravidly prokazatelným způsobem seznámeni. Pravidla pro obchodní oddělení jsou stanovena povahou používaných aktiv.

Pravidla pro účetní data a data klientů platí, že jakékoliv jejich použití mimo IS podniku je nepřípustné. Je zakázáno jejich kopírování, přenášení, tisk či jiné akce, které nejsou přímo spojeny s pracovními povinnostmi. Pracovníci technické podpory a vývojoví pracovníci jsou v rámci výkonu své činnosti konfrontováni s daty v jejich binární podobě, i zde platí stejná omezení jako u obchodního oddělení, ale je třeba zabezpečit nemožnost manipulace s těmito daty tak, aby mohla být z podniku jakýmkoliv způsobem vynesena. Tato sestavená pravidla je třeba v pravidelných intervalech revidovat. Interval revize je 1 rok.

Zdroje opatření:

Vytvoření pravidel pro jednotlivé skupiny uživatelů v podniku	5h
Pravidelná revize pravidel	1h/interval revize

7.1.3.4 A.7.2.1 Doporučení pro klasifikaci

Odpovědná osoba: bezpečnostní manager

Opatření: V podniku lze identifikovat 3 druhy informací vzhledem k jejich povaze. Mezi nejcitlivější informace patří zdrojové kódy prodávaných aplikací a data z technické podpory. Zdrojové kódy obsahují podstatu know-how podniku, data technické podpory by svým únikem ohrozily podstatným způsobem důvěryhodnost podniku. Dalším druhem informací jsou informace o klientech. Tyto informace musí být chráněny před zneužitím a zcizením a to z pohledu zákona 101 sb. o ochraně osobních údajů, tak z pohledu konkurenčního boje. Třetím typem informací jsou informace účetní, které jsou vedením podniku utajované, ovšem jejich případné zneužití by nemělo zásadní dopad na chod firmy. Kromě tohoto rozdělení informací lze je také klasifikovat do kategorií podle dopadu na podnik, při jejich kompromitaci či porušení. V kapitole 5.1.4.1 je uvedena tabulka s dělením aktiv podle dopadu na podnik a jeho okolí, v případě porušení informačních aktiv.

Zdroje opatření:

Pravidelná revize klasifikací informací	1h/rok

7.1.3.5 A.7.2.2 Označování a nakládání s informacemi

Odpovědná osoba: vedoucí oddělení vývoje

Opatření: Pro každou skupinu klasifikovaných informací z předcházejícího opatření se zavedou postupy s nakládáním takových informací a v případě jejich tisku, je každá takováto skupina informací opatřena vodoznakem s klasifikací. Oddělení vývoje zajistí, aby tištěné výstupy byly označeny odpovídajícími vodoznaky. Uživatelské skupiny systémových oprávnění musí zajistit pro citlivé informace skupiny 1 a 2 jejich nemožnost kopírování v rámci podniku.

Zdroje opatření:

Nastavení uživatelských práv	2h
Doplnění tiskových výstupů o klasifikace obsažených informací	10h

7.1.4 A.9 Fyzická bezpečnost a bezpečnost prostředí

Cílem těchto navržených opatření je předcházet neautorizovanému fyzickému přístupu do vymezených prostor, předcházet poškození a zásahům do provozních budov a informací podniku.

7.1.4.1 A.9.1.1 Fyzický bezpečnostní perimetr

Odpovědná osoba: bezpečnostní manager

Opatření: V organizaci existuje v podstatě jeden fyzický perimetr a ten je tvořen celým prostorem firmy. Je nutné provedení rozdělení prostoru firmy do jednotlivých zabezpečených oblastí. Podle struktury firmy by odpovídající rozdělení mohlo být podle jednotlivých oddělení. Je tedy třeba vytvořit a zdokumentovat tyto jednotlivé bezpečnostní perimetry. Je vhodné současně přiřadit pracovníkovi z obchodního oddělení činnosti, které zahrnují odpovědnost recepce podniku. V současné době jsou tyto činnosti vykonávány, ovšem nejsou stanoveny odpovědnosti a povinnosti pracovníků, kteří tuto činnost vykonávají. V podniku je používán kartový systém pro přístup do prostor podniku, ovšem není provedeno zabezpečení jednotlivých vstupů do prostor oddělení podniku. Jednotlivé perimetry je vhodné doplnit vstupním systémem na bázi karet, který by umožňoval sledování a omezení vstupu zaměstnancům. Tímto opatřením by bylo dosaženo omezení přístupů nepovolaných osob do jednotlivých prostor a současně by bylo možno tímto systémem monitorovat pracovní dobu zaměstnanců, dodržování přestávek a pauzy na oběd. V návaznosti na tento systém je třeba stanovit odpovědné osoby pro monitorování dat získaných z tohoto systému. Je možné v rámci podniku nechat vyvinout software, který by přístupy analyzoval a na základě kritérií zpracovával týdenní zprávu o pracovní době a přístupech osob do zabezpečených prostor. Důraz na zabezpečení je třeba věnovat zejména serverovně, kterou je třeba tímto systémem vybavit co nejdříve.

Zdroje opatření:

Vytvoření dokumentace perimetrů	10h
Stanovení pravidel a odpovědností na recepci podniku	5h
Práce pracovníka obchodního oddělení na recepci	2h/den
Kartový otvírací systém v jednotlivých perimetrech	57000,-Kč
Práce programátora pro začlenění systému oprávnění do IS	24h
Dohled a monitorování přístupů do perimetrů	1h/týden

7.1.4.2 A.9.1.2 Fyzické kontroly vstupu osob

Odpovědná osoba: bezpečnostní manager, pracovník recepce

Opatření: Aplikací kartového systému, navrženého v předchozím opatření pro přístup do jednotlivých perimetrů bude splněn tento bod ve vztahu přístupu osob uvnitř firmy. Vzhledem k řešení přístupu osob z vnějšku je třeba, aby pověřená osoba na recepci zaznamenala identifikaci příchozí osoby, dobu a pracovníka, se kterým bude jednat a při jeho odchodu opět zaznamenala čas odchodu. Musí být zajištěno, aby se osoba návštěvy nemohla sama pohybovat po prostorách firmy. Návštěvní kniha, obsahující předchozí údaje musí být umístěna na recepci, je také třeba viditelně na recepci vyvěsit pokyny pro chování návštěv v podniku. Tyto pravidla upozorní návštěvy na zákaz volného pohybu a zákaz připojení svých zařízení do počítačové sítě mimo vyhrazenou Wi-Fi pro návštěvníky.

Zdroje opatření:

Stanovení a dokumentace pravidel pro pohyb návštěv	5h
Práce pracovníka recepce	2/den
Kontroly výkazů recepce	1h/týden

7.1.4.3 A.9.1.3 Zabezpečení kanceláří místností a prostředků

Odpovědná osoba: bezpečnostní manager

Opatření: Pro fyzické zabezpečení kanceláří je vhodné změnit stávající uzavírání dveří kanceláří na systém s otevíráním pouze pomocí karty, alternativně i klíče. Počítače je třeba připevnit pomocí zámků k pevným konzolám stolů. Všechny klíče je třeba umístit do firemního trezoru a vytvořit dokumentaci a záznamový arch pro vypůjčení a vrácení klíčů. Je třeba stanovit pravidla a odpovědnosti za uzavírání a otvírání vstupu do firmy na počátku a konci pracovní doby společně s aktivací bezpečnostního zařízení. Uvedené úpravy vstupů do kanceláří jsou spojeny se stavebními pracemi prováděnými v podniku.

Zdroje opatření:

Zámky pro počítače cca 10 ks	300,-Kč/kus
Vytvoření dokumentace a evidence a výpůjček	3h
Stanovení pravidel a odpovědností pro vstup do firmy	3h
Kontrola plnění povinností a evidence	1h/týden

7.1.4.4 A.9.1.4 Ochrana před hrozbami vnějšku a prostředí

Odpovědná osoba: bezpečnostní manager

Opatření: Z rizik, které by mohly ohrozit chod firmy v dané lokalitě je třeba ošetřit stav kdy by došlo k zatopení firmy přívalovými dešti. Toto lze řešit tak, že počítače, zásuvky sítě a elektrické rozvody budou umístěny minimálně ve výšce 30 cm nad zemí, zařízení v serverovně taktéž. Je vhodné sestavit postup přemístění kritických zařízení do bezpečí.

Dalším hrozbou identifikovanou v úvodní části zavádění ISMS je hrozba požáru. Tato hrozba je vzhledem k množství elektrických zařízení koncentrovaných na jednom místě velmi vysoká. Ve firmě jsou zavedena opatření vyžadovaná legislativou, jako je umístění, počet a typ hasicích přístrojů. Vhodným doplňkovým opatřením je instalace požární signalizace, která je napojena na ústřednu bezpečnostního zařízení s možností signalizace požáru na mobil majitele firmy. Do každé místnosti s výjimkou toalet je vhodné nainstalovat čidlo EPS.

Poslední hrozbou z vnějšího prostředí je možnost fyzického poškození budovy podniku pádem dvou stromů, které se nachází v těsné blízkosti budovy. Riziko z této události je poměrně vysoké, protože stromy jsou již starší a mohou být narušeny jejich kořenové systémy. Opatření, které by omezilo tuto hrozbu, spočívá v prevenci a pravidelném ošetřování stromů (sestřih uschlých větví) a

jedenkrát ročně kontrola stavu stromů odborníkem, pravidelné kontroly je vhodné zaznamenávat do kontrolního deníku.

Jako opatření na snížení rizika všech uvedených hrozeb je vhodné provést pojištění budovy a vnitřního vybavení budovy proti uvedeným hrozbám.

Zdroje opatření:

Sestavení krizového plánu přesunu zařízení	5h
Přesun zařízení do polohy 30cm nad podlahou	30 000,- Kč
Stavební úpravy posunutí zásuvek a rozvodů	50 000,- Kč
Instalace EPS s napojením na stávající EZS	12 000,- Kč
Pravidelná kontrola stavu stromů a ořez	2 500,- Kč/rok

7.1.4.5 A.9.1.5 Práce v zabezpečených oblastech

Odpovědná osoba: bezpečnostní manager, pracovník recepce

Opatření: Pro vstupy do zabezpečených oblastí bude používán přístupový systém na bázi karet a informační systém bude řídit přístupová oprávnění a logovat přístup zaměstnanců. Zabezpečené oblasti budou dále přístupny pomocí klíčů, které jsou umístěny v trezoru firmy. Opatření je plněno opatřeními navrženými v A.9.1.2 a A.9.1.3

Zdroje opatření:

Zdroje jsou zahrnuty v opatřeních A.9.1.2 a A.9.1.3

7.1.4.6 A.9.1.6 Veřejný přístup, prostory pro nakládku a vykládku

Odpovědná osoba: bezpečnostní manager, pracovník recepce

Opatření: Do prostor organizace se lze dostat pouze přes hlavní vstup, který obsluhuje pracovník recepce. Do ostatních chráněných prostor se neoprávněné osoby nemohou dostat bez dozoru. Je třeba vytvořit a zdokumentovat pravidla chování návštěvníků v prostoru firmy. Tato pravidla jsou realizována v opatření A.9.1.2

Zdroje opatření:

Zdroje jsou zahrnuty v opatření A.9.1.2

7.1.4.7 A.9.2.1 Umístění zařízení a jeho ochrana

Odpovědná osoba: vedoucí oddělení vývoje

Opatření: Zařízení pro zpracování dat jsou umístěna v zabezpečených oblastech, do kterých není umožněn přístup neoprávněným osobám bez doprovodu oprávněné osoby. Jednotlivá zařízení jsou chráněna před rizikem zatopení výše 30 cm, jejich polohou. Dále jsou všechny pracovní stanice a monitory připevněny zámkem ke konstrukci stolu, což omezuje riziko jejich náhodného pádu. Do

jednotlivých prostor má přístup pouze omezený okruh zaměstnanců, dle jejich přístupových oprávnění a pracovního zařazení. Toto opatření je splněno aplikací opatření A.9.1.4 a A.9.1.5

Zdroje opatření:

Zdroje jsou zahrnuty v opatřeních A.9.1.4 a A.9.1.5

7.1.4.8 A.9.2.2 Podpůrná zařízení

Odpovědná osoba: vedoucí oddělení vývoje

Opatření: Všechny počítače, aktivní prvky a servery musí být vybaveny nepřerušitelným zdrojem napájení, včetně ochrany před přepětím v elektrické síti. Každý nepřerušitelný zdroj napájení pro pracovní stanice a servery je třeba použít s možností softwarového ovládání a na počítačích mít nainstalovaný software pro automatické ukončení OS počítače, či serveru v případě výpadku napájení delším než 3 min. Pro ostatní zařízení jako jsou aktivní prvky je dostačující nepřerušitelný zdroj napájení, který umožňuje udržet zařízení v provozu po dobu minimálně 20 minut. Tyto záložní zdroje lze použít pro více aktivních zařízení. Vnější konektivita na internet je třeba vybavit přepěťovými ochranami. Externí přístupový bod Wi–Fi musí být na anténní části chráněn bleskojistkou a instalován v souladu s požadavky na vysílací zařízení s anténou.

Zdroje opatření:

Samostatná přepěťová ochrana cca 10ks	350,-/ks
Zdroj UPS s ovládacím připojením k počítači 750VA cca 10 ks	3 500,-/ks
Zdroj UPS bez připojení k PC 500VA cca 5 ks	2 500,-/ks

7.1.4.9 A.9.2.4 Údržba zařízení

Odpovědná osoba: vedoucí oddělení vývoje

Opatření: V podniku je třeba zavést vytvoření plánu pro pravidelné revize pracovních stanic serverů a pomocných aktivních zařízení. Pro tyto zařízení je stanoven odpovědný pracovník oddělení vývoje s patřičným vzděláním podle vyhlášky 50/1978 Sb. Tento pracovník je zodpovědný za fyzické provádění kontrol a revizí zařízení používaných v podniku. O každé provedené revizi vede záznamy a v případě nalezení nedostatků je propaguje vedoucímu oddělení vývoje, který zabezpečí odbornou opravu zařízení. Pro každý zdroj nepřerušitelného napájení je třeba vytvořit plán testování funkčnosti a pravidelně provádět test těchto zařízení na překlenutou délku výpadku napájení. Tyto revize je třeba provádět v intervalu 1 měsíc a o výsledku testu podávat zprávu vedoucímu oddělení. Pravidelné revize výpočetní techniky musí zahrnovat čištění pracovních stanic a serverů od prachu, výměny vadných ventilátorů.

Pro všechny klimatizační jednotky v podniku je zaveden plán jejich pravidelné údržby, zahrnující čištění vstupních filtrů, zbavení prachu externích jednotek. Jednou ročně je vhodné kontaktovat externí firmu pro kontrolu stavu chladícího média v klimatizačních jednotkách. O provedených úkonech je třeba vést záznamy.

Zdroje opatření:

Sestavení plánu kontrol a evidenčního systému	10h
Pravidelné kontroly počítačů a aktivních prvků sítě	3h/týden
Testování a kontroly nepřerušitelných zdrojů napájení	6h/měsíc
Čištění pracovních stanic a serverů	10h/měsíc
Čištění klimatizací	3h/měsíc
Roční kontrola klimatizací	2 500,-/rok

7.1.4.10 A.9.2.5 Bezpečnost zařízení mimo prostory organizace

Odpovědná osoba: vedoucí oddělení vývoje, pracovník odpovědný za kontrolu logů, externí firma řešící správu a nastavení vnějších komunikací.

Opatření: Pro pracovníky používající zařízení mimo prostory organizace musí být vytvořeny předpisy používání zařízení, způsob jejich ochrany a stanovení odpovědnosti za případné bezpečnostní problémy. S těmito předpisy musí být externí spolupracovníci prokazatelně seznámeni a musí o tom existovat záznam uložený na bezpečném místě v podniku. Musí být nastavena politika připojování zařízení mimo prostor firmy a logování jejich činnosti. Dále musí být stanovena kritéria pro nastavení připojení, operačního systému, antivirového software. Ve spolupráci s externím dodavatelem služeb je prováděno monitorování a zpráva vzdálených připojení s jejich monitorováním. Získaná logovací data jsou předávána v pravidelných intervalech vedoucímu oddělení vývoje. Pro kontrolu takto získaných logovacích dat (týdně) je stanovena odpovědná osoba, která v pravidelných intervalech jednou měsíčně vyhotovuje zprávu o bezpečné komunikaci a tuto předává vedoucímu oddělení, který ji eskaluje dále managerovi bezpečnosti.

Zdroje opatření:

Sestavení předpisů a politiky používání externích zařízení	10h
Pravidelná kontrola bezpečnostních logů	2h/týden

7.1.4.11 A.9.2.6 Bezpečná likvidace nebo opakované použití zařízení

Odpovědná osoba: vedoucí oddělení vývoje, pracovník odpovědný za likvidaci

Opatření: Jsou stanoveny postupy pro případ likvidace zařízení obsahující interní či důvěrné informace. Musí být stanovena osoba odpovědná za provádění a kontrolu těchto postupů. O každém likvidovaném zařízení bude vedena evidence. Je třeba vnitřním předpisem stanovit software používaný k bezpečnému odstranění dat z paměťových médií nebo způsob jejich likvidace. Každé médium, či jiné zařízení musí být likvidováno takovým způsobem, aby bylo vyloučeno získání jakýchkoliv informací z tohoto zařízení poté, co opustí perimetr podniku.

Zdroje opatření:

Zakoupení software na bezpečné odstranění dat z paměťových médií	5 000,- Kč
Vytvoření postupů a evidence likvidovaných zařízení	5h

7.1.4.12 A.9.2.7 Přemístění majetku

Odpovědná osoba: vlastník aktiva

Opatření: V podniku jsou stanoveny postupy, jak lze přemisťovat majetek firmy související s informační bezpečností. Každé zařízení nebo informace přemisťované mimo jejich stávající polohu či úložiště může být přemístěno pouze na základě písemného odsouhlasení vlastníkem aktiva do jehož působnosti patří. Vlastník aktiva zaznamená účel a datum přemístění aktiva v evidenci určené pro sledování přemístění majetku či informací. S postupy a povinnostmi pro osoby přemísťující majetek musí být seznámeni všichni pracovníci firmy.

Zdroje opatření:

Vytvoření postupů a evidence přemísťování majetku	5h
Evidence přemístění aktiva	1h/požadavek

7.1.5 Zdroje a náklady na I. etapu

V etapě I. jsou zavedeny požadavky normy ČSN ISO/IEC 27001:2006. Zaváděná opatření v této etapě patří do kategorie spíše administrativních činností v rámci procesu ISMS. Pokrývají opatření definice bezpečnostní politiky, organizace bezpečnosti informací a řízení informačních aktiv podniku. Tyto opatření jsou nezbytným předpokladem pro úspěšné zavádění ISMS v podniku. V průběhu zavádění opatření budou v podniku prováděny stavební práce. Je tedy v této etapě možno bez zásadních omezení fungování podniku do zaváděných opatření přidat i opatření týkající se fyzické bezpečnosti a bezpečnosti prostředí. Všechna opatření, ať ze skupiny administrativních nebo fyzické bezpečnosti mají stanovené požadavky na přidělení zdrojů a to finančních či personálních. Z těchto požadavků na zdroje lze přibližně stanovit i vlastní náklady na zavedení dané etapy projektu.

Tab. 11 Tabulka nákladů etapy I. zavedení ISMS

		jednorázově	opakovaně dle revize	denně	týdně	ročně	incident	jednorázově	ročně
Opatření		h	h	h	h	h	h	Kč	Kč
A.5.1.1	Vytvoření dokumentu bezpečnostní politiky	24							
	Seznámení zaměstnanců s touto politikou	3							
	Informování dodavatelů a odběratelů o této politice	3							
A.5.1.2	Vytvoření plánu přezkoumávání bezpečnostní politiky	3							
	Přezkoumání politiky a její případné úpravy					48			
A.6.1.1	Sponzor projektu vytváří dokument bezpečnostní politiky a stanoví role	24							
A.6.1.2	Vytvoření směrnice koordinace bezpečnosti	10							

		jednorázově	opakovaně dle revize	denně	týdně	ročně	incident	jednorázově	ročně
Opatření		h	h	h	h	h	h	Kč	Kč
	Vyčlenění odpovědných osob na řešení bezpečnosti				2				
	Eskalace zjištěného problému managerovi bezpečnosti						1		
A.6.1.4	Vytvoření schvalovacího procesu	2			1				
	Schvalování nových prostředků vedoucími pracovníky								
A.1.6.5	Vytvoření plánu přezkoumávání dohod o ochraně informací	1							
	Vyčlenění odpovědné osoby za přezkoumání dohod		1						
A.6.2.1	Posouzení možnosti připojení externího subjektu						24		
	Vytvoření analýzy rizik přístupu externího subjektu						4		
	Kontrola dodržování smlouvy		2						
A.7.1.1	Přezkoumání informačních aktiv podniku		2						
A.7.1.3	Vytvoření pravidel pro jednotlivé skupiny uživatelů v podniku	5							
	Pravidelná revize pravidel						1		
A.7.2.1	Pravidelná revize klasifikací informací					1			
A.7.2.2	Nastavení uživatelských práv	2							
	Doplnění tiskových výstupů o klasifikace obsažených informací	10							
A.9.1.1	Vytvoření dokumentace perimetrů	10							
	Stanovení pravidel a odpovědností na recepci podniku	5							
	Práce pracovníka obchodního oddělení na recepci			2					
	Kartový otvírací systém v jednotlivých perimetrech							57000	
	Práce programátora pro začlenění systému oprávnění do IS	24							
	Dohled a monitorování přístupů do perimetrů				1				
A.9.1.2	Stanovení a dokumentace pravidel pro pohyb návštěv	5							
	Práce pracovníka recepce			2					
	Kontroly výkazů recepce				1				
A.9.1.3	Zámky pro počítače cca 10 ks							3000	
	Vytvoření dokumentace a evidence a výpůjček	3							
	Stanovení pravidel a odpovědností pro vstup do firmy	3							

		jednorázově	opakovaně dle revize	denně	týdně	ročně	incident	jednorázově	ročně
Opatření		h	h	h	h	h	h	Kč	Kč
	Kontrola plnění povinností a evidence				1				
A.9.1.4	Sestavení krizového plánu přesunu zařízení	5							
	Přesun zařízení do polohy 30cm nad podlahou							30000	
	Stavební úpravy posunutí zásuvek a rozvodů							50000	
	Instalace EPS s napojením na stávající EZS							12000	
	Pravidelná kontrola stavu stromů a ořez								2500
A.9.2.2	Samostatná přepěťová ochrana cca 10 ks							3500	
	Zdroj UPS s ovládacím připojením k počítači 750VA cca 10 ks							35000	
	Zdroj UPS bez připojení k PC 500VA cca 5 ks							12500	
A.9.2.4	Sestavení plánu kontrol a evidenčního systému	10							
	Pravidelné kontroly počítačů a aktivních prvků sítě				3				
	Testování a kontroly nepřerušitelných zdrojů napájení		6						
	Čištění pracovních stanic a serverů		10						
	Čištění klimatizací		3						
	Roční kontrola klimatizací								2500
A.9.2.5	Sestavení předpisů a politiky používání externích zařízení	10							
	Pravidelná kontrola bezpečnostních logů				2				
A.9.2.6	Zakoupení software na bezpečné odstranění dat z paměťových médií							5000	
	Vytvoření postupů a evidence likvidovaných zařízení	5							
A.9.2.7	Vytvoření postupů a evidence přemísťování majetku	5							
	Evidence přemístění aktiva						1		
		172	**24**	**4**	**11**	**49**	**31**	**208000**	**5000**

Tab. 12 Sumarizace nákladů pro etapu I.

Jednorázové náklady 172 hodin á 450,- Kč	77 400,- Kč
Jednorázové náklady finanční	208 000,- Kč
Náklady denní 4 hodiny á 450,- Kč	1 800,- Kč
Náklady týdenní 11 hodin á 450,- Kč	4 950,- Kč
Náklady roční 49 hodin á 450,- Kč	22 050,- Kč
Náklady na incident 31 hodin á 450,- Kč	13 950,- Kč
Náklady opakované dle četnosti revize 24 hodin á 450,- Kč	10 800,- Kč

Jednorázové přímé náklady činí 208 000,- Kč

Jednorázové přímé náklady na mzdy činí 77 400,- Kč.

Ostatní náklady jsou variabilní a záleží na tom, zda je činnost prováděna a v jaké četnosti.

8 Podíl zavedených opatření etapy I. na snížení či eliminaci rizika hrozeb

Tab. 13 Opatření pro omezení rizika z hrozeb

	Hrozba	Zavést opatření
	Fyzické poškození	
1	Požár	Řeší opatření A.9.1.4
2	Poškození vodou	Řeší opatření A.9.1.4
3	Přehřátí po výpadku klimatizace	Částečně řešeno opatřením A.9.2.4. Snížení teploty provést za pomocí záložních ventilátorů a odvětrání prostor.
4	Poničení budovy okolními stromy	Řeší opatření A.9.1.4
	Ztráta služeb	
5	Výpadek elektrické energie	Řeší opatření A.9.2.2 a A.9.2.4
6	Výpadek klimatizace	Částečně řeší A.9.2.4. Vytvořit plán na řešení náhradního chlazení serverovny za použití záložních ventilátorů a snížení počtu aktivních prvků na minimum.
7	Výpadek sítě WAN	WAN (internet) připojení je realizovat jednou hlavní a jednou záložní linkou, riziko z dané hrozby v případku obou nezávislých připojení současně je akceptovatelné.
8	Výpadek sítě LAN	Částečně řeší A.9.2.4 Sestavit plán pro řešení co nejrychlejšího obnovení činnosti sítě LAN. Pro klíčové aktivní prvky mít záložní funkční prvky k dispozici.
9	Výpadek IS	Sestavit plánu obnovení IS podniku ze zálohy, vytvářet pravidelné provádění zálohy celého IS podniku.
10	Výpadek IS technické podpory	Částečně řeší A.9.2.4. Sestavení plánu obnovení IS technické podpory podniku a pravidelné provádění zálohy celého IS technické podpory.
11	Výpadek serveru se zdrojovými kódy	Částečně řeší A.9.2.4. Sestavení plánu obnovení serveru se zdrojovými kódy podniku a pravidelné provádění zálohy celého serveru se zdrojovými kódy. Zdrojové kódy jsou umístěny také na pracovních stanicích vývojářů jako případná záloha.
12	Výpadek hlasových služeb	Pro hlasové služby používat minimálně dva různé poskytovatele hlasových služeb. Sestavit plán na nejrychlejší odstranění poruchy hlasových služeb. Poskytovat informace zákazníkům o možnosti využití více komunikačních cest s podnikem.
	Ohrožení důvěrnosti	
13	Neoprávněné získání přístupových údajů	Provádět pravidelná proškolování pracovníků na dodržování interních pravidel zacházení s přístupovými údaji. Pravidelné změny přístupových údajů, monitorovat pokusy o neoprávněný přístup do podniku.
14	Neoprávněné získání informací	Zamezit přístup neoprávněným osobám do podnikového IS. Kontrola dodržování stanovených pravidel v bezpečnostní politice podniku.
15	Chyba v nastavení přístupových práv	Přístupová práva nastavovat na základě písemného podkladu ověřeného vedoucím oddělení, pro které se mají přístupová práva přidělovat. Dodržovat pravidlo přidělování nezbytně nutných minimálních přístupových. O přidělených přístupových právech vést záznamy.
16	Slabiny v zabezpečení síťových služeb	Částečně řeší A.6.2.1. Pravidelně provádět přezkoušení zabezpečení síťových služeb s ohledem na nově získané poznatky. Postupovat podle stanoveného a pravidelně aktualizovaného plánu vytvořených testů bezpečnosti síťových služeb.

	Hrozba	Zavést opatření
17	Zranitelnosti webových služeb	Pro návrh webových služeb využívat doporučované postupy pro zajištění bezpečnosti webových služeb. Aktivně vyhledávat možné zranitelnosti a o opatřeních vytvářet záznamy.
18	Slabiny v architektuře IT infrastruktury	Řeší opatření A.6.2.1.
19	Získání dat z vyřazených médií	Řeší opatření A.9.2.6.
20	Krádež technického vybavení	Řeší opatření A.9.2.1.
21	Zneužití, ztráta nebo krádež USB disků	Částečně řeší A.9.2.7. V podniku zavést směrnici o zákazu používání soukromých USB zařízení připojitelných k počítači a s touto směrnicí prokazatelně seznámit všechny zaměstnance. Použití USB disků je možné pouze firemních a tyto vydávat na základě žádosti a neumožnit tato firemní zařízení vynášet mimo objekt podniku.
22	Záměrná škodlivá činnost v síti	Zavedenými přístupovými právy omezit možnost škodlivé činnosti v síti. Deklarovat zákaz využívání jakýchkoliv jiných aplikací než těch, které schválil vedoucí oddělení a s tímto prokazatelně seznámit všechny zaměstnance. Vedoucí oddělení evidují požadavky na specifický software. Provádět pravidelné kontroly obsahu pracovních stanic zaměstnanců.
23	Škodlivý software	Prováděná opatření jsou společná s hrozbou 22. Na všech počítačích podniku je udržován aktualizovaná verze antivirového software.
	Technická selhání	
24	Selhání serveru	Částečně řešeno opatřením A.9.2.4. Sestavit plán obnovení činnosti serveru při jeho selhání. Provádět pravidelné zálohování obrazů celého serveru. V serverech používat pole disků s mechanismem překonání výpadku minimálně jednoho disku.
25	Selhání pracovní stanice	Částečně řeší opatření A.9.2.4. V podniku udržovat minimálně jednu pracovní stanici jako případnou zálohu pro případ selhání pracovní stanice.
26	Chybné fungování systému	Částečně řešeno v opatření A.9.2.4. Pravidelně a plánovaně provádět kontroly kabelových vedení, zásuvek, kabelových koncovek, kontroly chybových logů na serverech a jejich vyhodnocení. Sledovat parametry pevných disků a proaktivně odstraňovat prvotní příčiny možné chybné funkce systému.
27	Nedostatek zdrojů pro provoz aplikace	Všechny požadavky na provoz aplikace hlásit v dostatečně dlouhém předstihu před realizací a zadat požadavky na zdroje finanční či personální. Management tyto požadavky musí odsouhlasit či zamítnout.
	Neoprávněné činnosti	
28	Neoprávněné zkopírování informací	Částečně řešeno v opatření A.7.2.2. Zamezit možnost neoprávněného kopírování informací. V bodě 21 je provedeno opatření zákaz používání přenosných disků v organizaci. V bodě 15 je zavedeno opatření na přidělení nejmenšího možného přístupu k sdíleným zdrojům. Tyto opatření omezují či zabraňují neoprávněnému kopírování informací.
29	Neoprávněný přístup centrální správy systému	Do centrální správy systému přidělit přístup pouze úzkému okruhu pracovníků. Další řešeno opatřením 13.
30	Zneužití administrátorských oprávnění	Administrátorská oprávnění nastavit pouze pro zaměstnance s prokazatelným důvodem potřeby administrátorského oprávnění. Administrátorská oprávnění přidělená k serverům přiřadit pouze minimální skupině uživatelů.
31	Zneužití uživatelských oprávnění	Uživatelská oprávnění jsou nastavit na minimální nutná a zavést omezení pohybu nepovolaných osob v rámci oddělení a přístupu k pracovním stanicím.
32	Porušení mlčenlivosti zaměstnance	Zavést programy motivující pracovníky dodržovat mlčenlivost a loajalitu. Pro nově přijaté pracovníky zavést práci pod dohledem jiného zkušeného pracovníka a zabránit pokud možno přístupu k citlivým informacím.
33	Neoprávněný přístup do prostor	Řeší opatření A.9.1.2
34	Neoprávněný přístup do aplikace	Zavést směrnice, stanovující za jakých podmínek lze opustit rozpracovanou práci a pracovní stanici zaměstnance. Kontrolovat dodržování uzamčení

	Hrozba	Zavést opatření
		pracovní stanice při opuštění pracovního místa.
	Lidská selhání	
35	Nedbalost při údržbě zařízení	Částečně řešeno v opatření A.9.2.4. Písemně stanovit odpovědnosti a postihy všem osobám, které se podílejí na údržbě zařízení. Provádět namátkové kontroly provedené údržby. O každé údržbě vést záznamy a tyto budou odsouhlaseny vedoucím pracovníkem.
36	Nedostatek personálu správy IT služeb	Pro správu IT služeb vyhradit vždy v každém okamžiku 2 odpovědné pracovníky. Tyto pracovníky současně proškolovat. V běžném provozu budou tito pracovníci plnit vzájemnou zástupnost.
37	Chyby personálu správy IT služeb	Každou činnost, která bude prováděna pečlivě kontrolovat a provádět dokumentaci provedených úkonů. Vedoucí IT oddělení potvrzuje provedené úkony.
38	Nedostatečná dokumentace systému	Vytvoření počáteční dokumentace systému a tuto dokumentaci pravidelně revidovat. Intervaly revidování dokumentace zavést ve vnitropodnikovém předpise.
39	Nedodržování předpisů pro práci s informacemi	Stanovit postihy pracovníků za nedodržování předpisů pro práci s informacemi s přenesením zodpovědnosti na vedoucí oddělení. S těmito postihy prokazatelně seznámit pracovníky. Vytvořit plán pro namátkové kontroly dodržování předpisů pro práci s informacemi.
40	Chyby obsluhy aplikace	Provádět v pravidelných intervalech školení pracovníků na obsluhu používaných systémů. Sledovat účast všech pracovníků podniku na těchto školeních.
41	Zneužití oprávnění při sdělení hesla	Provádět monitorování přístupu pracovníků do IS v pracovní době a mimo tuto dobu. Stanovit směrnici odpovědnosti pracovníků za přístup do IS a prokazatelně seznámit pracovníky s postihy za zneužití přístupových informací do systému.

Z identifikovaných 41 hrozeb je po zavedení etapy I. sníženo riziko z identifikovaných hrozeb na akceptovatelnou úroveň celkem v 8 případech a snížena úroveň rizika plynoucí z hrozby v 13 případech. Zbývající hrozby nejsou zavedenými opatřeními ovlivněny. V dalších etapách II. a III. budou zavedeny opatření pro snížení všech rizika všech hrozeb na akceptovatelnou úroveň.

9 Monitorování, přezkoumávání, udržování a zlepšování

Zavedení systému ISMS v podniku je soustavný proces, který má jasně definován svůj začátek a to okamžik vytvoření bezpečnostní politiky v podniku a vyjádřením podpory vedení podniku s cílem řešit bezpečnost informací. Konec procesu ISMS není nikde definován a ani nemůže být stanoven. V rámci postupu podle cyklu PDCA se jedná o neustále se opakující sekvence kroků, jejímž cílem je neustále zdokonalování, zlepšování a řešení nově se objevujících hrozeb.

V rámci opatření zavedených podle normy ČSN ISO/IEC 27001:2006 se stanovují u většiny opatření plány pravidelného revidování opatření, monitorování bezpečnostních incidentů a je vhodné doplnit povinnosti odpovědných pracovníků zejména o proaktivní vyhledávání možných hrozeb a z nich plynoucích rizik. Oblast ICT je charakteristická tím, že vývojem nových technologií a obecně nárůstem znalostí a zkušeností osob, které se snaží z nejrůznějších příčin proniknout do systémů jiných subjektů, je stále těžší se chránit proti nově vznikajícím hrozbám. Proaktivní přístup, v rámci něhož je vhodné proškolovat firemní specialisty na novinky v oblasti zabezpečení, je tak nezbytným doplňkem elementárních opatření zavedených systém ISMS.

Závěr

Tato práce je rozdělena na dvě základní oblasti. V první teoretické části práce je popsána metodika řešení bezpečnosti informačních technologií v podniku. V úvodní části jsou soustředěny informace z oblasti základních pojmů a procesů z bezpečnosti informací, včetně zákonů a analýzy rizik. V dalších kapitolách jsou představeny normy řady ČSN ISO/IEC 27000:2006, přičemž hlavní důraz je kladen na politiku bezpečnosti informací v podniku a opatření při zavádění ISMS podle ČSN ISO/IEC 27001:2006. Tato úvodní část tvoří shrnutí pro management malého podniku a slouží k rychlému přehledu managerů, jaký je princip zavedení ISMS v podniku.

Praktická část práce je tvořena vlastním zavedením ISMS v malém podniku. Klíčovým prvkem této praktické části je identifikace hrozeb v podniku, analýza možných rizik z těchto hrozeb na návrh, jakým způsobem nalezená rizika snížit, či úplně odstranit. Při vlastním návrhu jsem vycházel z dokonalé znalosti podniku, jehož jsem externím spolupracovníkem, a kde jsem byl dříve zaměstnán. Vzhledem k velikosti podniku a charakteru podnikatelské činnosti jsem při návrhu opatření vycházel z personálních a časových možností daného podniku. Samotný zde uvedený návrh opatření je rozdělen do 3 etap postupného zavádění opatření podle normy a podrobně se v této práci věnuji první etapě. V první etapě jsou vypracovány postupy zejména administrativního charakteru odpovídající první fázi zavádění ISMS. Současně jsem do této fáze připojil i opatření týkající se fyzické bezpečnosti a bezpečnosti prostředí, protože v rámci minimalizace nákladů na zavádění opatření budou tyto některé požadavky vyžadovat dodatečné stavební úpravy.

Celá první navržená fáze zavedení ISMS je zakončena požadavky na zdroje. Tyto slouží vedení podniku k zhodnocení nákladů a plánování výdajů a dalších zdrojů podniku, protože pro zavedení kompletního ISMS v podniku je třeba zavést velké množství opatření. Popisem aplikace v prostředí podniku by tato práce značně překročila svůj povolený rozsah, jsou opatření určená k zavedení v dalších etapách stručné popsána v příloze této práce.

Tento projekt vzniknul z požadavku řešení nepříznivé situace v podniku a jeho budoucí rozvoj spočívá v dopracování všech opatření uvedených v přílohách této práce. Tento projekt, ač praktického charakteru je významným zdrojem zkušeností zejména z pohledu analýzy rizik a jejich hodnocení dopadu na podnik. Při této analýze se dostávají do popředí málo zřetelné detaily, jako je například možná hrozba pádu blízko stojících stromů a tím narušení funkčnosti celého podniku z důvodu přerušení dodávky elektrické energie a externích datových služeb. V rámci zaváděných opatření vyplynulo, že v podniku nejsou plněny základní požadavky na bezpečnost práce ve vztahu k elektrickým zařízením, jak je stanoveno ve vyhlášce 50/1978 Sb. Zejména v oblasti bezpečnosti zařízení informačních technologií podle ČSN EN 60950–1. Což bude v rámci zavedených opatření vyřešeno a bude zajištěna vyšší bezpečnost zaměstnanců a omezena možnost případného postihu.

Literatura

[1] BROTBY, K. *Information Security Governance: Guidance for Information Security Managers*. Rolling Meadows (USA): IT Governance Institute, 2008. 78 s. ISBN 978-1-933284-73-6.

[2] ČESKÝ NORMALIZAČNÍ INSTITUT. ČSN ISO/IEC 27001:2006. *Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky*. Praha: Český normalizační institut 2006.

[3] DOUCEK, P., NOVÁK, L., SVATÁ, V. *Řízení bezpečnosti informací*. 1. vyd. Příbram: PROFESSIONAL PUBLISHING, 2008. 239 s. ISBN 978-80-86946-88-7.

[4] GREGORY, P. *Enterprise Information Security for Non-Technical Decision Makers.* Harlow (Great Britain): Pearson Education Limited, 2003. 167 s. ISBN 0-273-66157-4.

[5] KAJAVA, J., ANTTILA, J., et al. *Senior Executives Commitment to Information Security – from Motivation to Responsibility*. Guangzhou (China): 2006. Computational Intelligence and Security CIS2006. s. 34-46.

[6] KOCH, M., et al. *Management informačních systémů.* 3. vyd. Brno: Akademické nakladatelství CERM, s.r.o., 2010. 171 s. ISBN 97880-214-4157-6.

[7] POŽÁR, J. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2005. 309 s. ISBN 80-86898-38-5.

[8] SMEJKAL, V., RAIS, K. *Řízení rizik ve firmách a jiných organizacích*. 3. Vyd. Praha: Grada Publishing, a.s., 2010. 360 s. ISBN 978-80-247-3051-6.

[9] STAUDEK, J. *Úvod do problematiky bezpečnosti IT. 3* [online]. FI MU Brno, verze podzim 2007. [cit. 2011-05-12]. URL: http://www.fi.muni.cz/usr/staudek/vyuka.

[10] STRNÁD, O. *Systémový prístup k riadeniu informačnej bezpečnosti*. 1. vyd. Trnava (Slovensko): SP Synergia, 2008. 233 s. ISBN 978-80-89291-20-5.

[11] TULLOCH, M. *Microsoft Encyclopedia of Security.* Washington (USA): Microsoft Press, 2003. 480 s. ISBN 0-7356-1877-1.

Seznam použitých zkratek

AD	Active Directory je implementace adresářových služeb
ČSN	Česká technická norma
EPS	Elektronická požární signalizace
EZS	Elektronické zabezpečovací zařízení
ICT	Informační a komunikační technologie
IEC	Mezinárodní úřad pro elektrotechniku
IEEE	Společnost pracovníků v elektrotechnice a elektronice v USA
IS	Informační systém
ISO	Mezinárodní organizace pro normalizaci
IT	Informační technologie
ITU	Mezinárodní telekomunikační unie
PDCA	Demingův cyklus (Plánuj, dělej, kontroluj, jednej)
UPS	Nepřerušitelný zdroj napájení
VPN	Virtuální privátní síť
Wi–Fi	Spolehlivá bezdrátová komunikace

Seznam obrázků

Seznam tabulek

Seznam příloh

Seznam opatření k zavedení ISMS fáze II.

	Opatření normy ISO/IEC 27001	Zavést opatření
10	Řízení komunikací a řízení provozu	
10.1.1	Dokumentace provozních postupů	Je třeba zavést a zdokumentovat provozní postupy na všech odděleních podniku a tyto dokumenty uložit na místě, kde jsou dostupné zaměstnancům. Pro každé oddělení tyto postupy vytvořit a uchovávat odděleně.
10.1.2	Řízení změn	V podniku je třeba zavést změnové řízení pro všechny požadavky na změny v podniku. Musí být identifikovány a zaznamenány důležité změny, prováděno hodnocení dopadů změn.
10.1.3	Oddělení povinností	Pro každého zaměstnance specifikovat jeho povinnosti v rámci jednoho oddělení, do kterého je přidělen.
10.1.4	Oddělení vývoje, testování a provozu	Stanovit scénáře pro zavedení testovacích verzí do provozních. Provádět testy a simulace před nasazením do ostrého provozu.
10.2.1	Dodávky služeb	Před dodávkou služeb třetí stranou je třeba ověřit úroveň bezpečnosti, kvalitu služeb a dostatečné kapacity pro naplnění dodávky.
10.2.2	Monitorování a přezkoumávání služeb třetích stran	Monitorovat funkčnost a spolehlivost služeb třetích stran. Vyžadovat hlášení o případných bezpečnostních incidentech.
10.2.3	Řízení změn služeb poskytovaných třetími stranami	Na základě důvodu změny v síťových službách identifikovat možná rizika či přínosy plynoucí podniku ze změny služeb.
10.3.1	Řízení kapacit	Pro každou činnost by měly být identifikovány a vyhrazeny odpovídající kapacity. Jejich využití je třeba monitorovat a pravidelně vyhodnocovat.
10.5.1	Zálohování informací	Podle stanoveného plánu provádět zálohování v takovém rozsahu, aby byla zajištěna kontinuita podniku v případě poruchy. Je třeba stávající postupy a zařízení doplnit o možnost zálohování na magnetické pásky a tyto udržovat mimo objekt podniku. Dalším vhodným opatřením je pronajmutí služby pro bezpečné zálohování do internetového zálohovacího úložiště.
10.6.1	Síťová opatření	Převést odpovědnost na externího dodavatele služeb a tyto služby pravidelně monitorovat a přezkoumávat.
10.6.2	Bezpečnost síťových služeb	Převést odpovědnost na externího dodavatele služeb a tyto služby pravidelně monitorovat a přezkoumávat.
10.7.1	Správa výměnných počítačových médií	Výměnná média před dalším použitím bezpečně vymazat, pokud nejsou znovu použít tak tato média bezpečně zlikvidovat.
10.7.2	Likvidace médií	Zabezpečit, aby média byla likvidována odpovídajícím způsobem bez možnosti získání informace z těchto médií nepovolaným osobám.
10.7.3	Postupy pro manipulaci s informacemi	Podle klasifikace jednotlivých informací, zajistit omezení přístupu k těmto informacím, zachování záznamů, označování kopií.
10.7.4	Bezpečnost systémové dokumentace	Stanovit bezpečné uložení systémové dokumentace a stanovení pravidel jejího používání.
10.8.1	Postupy a politiky při výměně informací a programů	Definovat pro zaměstnance směrnice pro elektronickou komunikaci, dodržovat pravidla likvidace obchodní korespondence, zákaz přesměrování emailů do externích schránek mimo podnik.
10.8.2	Dohody o výměně informací a programů	S externími dodavateli služeb smluvně stanovit rozsah a obsah a způsob vyměňovaných dat. Ve smlouvě také definovat sankce za porušení dohody.
10.8.5	Informační systémy organizace	Zavedení směrnic o používání IS podniku a na něj navázaných systémů jako třeba IS pro technickou podporu.
10.10.1	Pořizování auditních záznamů	Pokud to používaný systém umožňuje, je třeba zavést auditní záznamy obsahující chybové hlášení a významné bezpečnostní události.
10.10.2	Monitorování používání systému	Je třeba zavést pravidelné přezkoumání použití výpočetní techniky a kontrolovat neautorizované přístupy, speciální operace systémové chyby,

	Opatření normy ISO/IEC 27001	Zavést opatření
		pokusy o změnu v nastavení systému.
10.10.3	Ochrana vytvořených záznamů	Všechny systémové záznamy na pracovních stanicích a serverech musí být chráněny proti jejich úpravám či smazání.
10.10.4	Administrátorský a operátorský deník	Aktivity administrátora systému musí být zaznamenávány v míře dané prováděnými úkony a pravidelně analyzovány.
10.10.5	Záznam selhání	Každé selhání, či chyba systému musí být zaznamenána a odpovědná osoba musí tyto záznamy přezkoumat a přijmout adekvátní opatření.
10.10.6	Synchronizace času	Všechny výpočetní prostředky nastavit na synchronizaci časových informací z externího časového serveru. Pravidelně kontrolovat dostupnost tohoto serveru.
11	Řízení přístupu	
11.1.1	Politika řízení přístupu	Pro každý software, který je využíván v podniku je třeba stanovit bezpečnostní požadavky vzhledem ke klasifikaci zpracovávaných informací. Tyto požadavky evidovat a pravidelně revidovat. Je třeba stanovit postup schvalování žádostí o přístup do systému.
11.2.1	Registrace uživatele	Vytvoření evidence s použitím uživatelského identifikátoru pro přístup do systému. Zde jde využít toho, že zaměstnanci jsou zavedeni v active directory (AD) podniku a při zavádění do AD je třeba definovat požadavky na přístup k aplikacím.
11.2.2	Řízení privilegovaného přístupu	V souladu s politikou řízení přístupu je přidělování privilegovaných přístupů třeba dokumentovat a zdůvodnit. Každé povolení přístupu musí být hodnoceno z hlediska nezbytnosti přidělení privilegií a možným rizikem ze ztráty či poškození dat.
11.2.4	Přezkoumání přístupových práv uživatelů	Správce AD musí v pravidelném časovém intervalu provádět přezkoumávání přístupových práv jednotlivých uživatelů. Každou případnou změnu je třeba zaznamenat v dokumentaci řízení přístupových práv.
11.3.2	Neobsluhovaná uživatelská zařízení	Vytvoření podnikové směrnice, která stanoví zaměstnancům, jak se zachovat v případě, že opustí počítač, rozpracovanou práci na kopírce. Je vhodné zavést a kontrolovat uzamčení pracovních stanic při opuštění pracovního místa.
11.3.3	Zásada prázdného stolu a prázdné obrazovky monitoru	Zavedení interních předpisů pro práci s papírovými dokumenty vzhledem k jejich bezpečnostní klasifikaci. Při odchodu ze zaměstnání vyžadovat prázdné stoly a přihrádky ve vztahu k citlivým dokumentům. Pokud dokumenty už není třeba, je nutné je bezodkladně zlikvidovat bezpečným způsobem. Před odchodem je třeba kontrolovat, zda v kopírce či skeneru nejsou zapomenuty dokumenty z předchozího používání.
11.4.1	Politika užívání síťových služeb	V rámci podniku je třeba definovat, jaké jsou dostupné síťové služby. Jejich přidělení jednotlivým pracovníkům je navázáno na AD. Je třeba provádět pravidelné kontroly logů s informacemi o přístupu k síťovým službám.
11.4.3	Identifikace zařízení v sítích	Každé zařízení zapojené do sítě musí být možno jednoznačně identifikovat. V podniku jsou všechna zařízení monitorována pomocí SMNP a jsou definovány odpovědné osoby za tyto zařízení.
11.5.4	Použití systémových nástrojů	Pro uživatele bez privilegovaných oprávnění je třeba zakázat použití nástrojů, které by mohly vést k narušení činnosti systému. V rámci směrnice o používání software na pracovních stanicích je třeba definovat skupiny zakázaných programů, které by mohly vést k narušení systému či bezpečnosti.
11.6.1	Omezení přístupu k informacím	Každý pracovník musí mít přístup k informacím, které jsou nezbytné pro vykonávání jeho činnosti. Ostatní informace musí být dostatečně chráněny před přístupem nepovolaných pracovníků a pokusy o přístup monitorovány. Pokud to charakter aplikace dovoluje, je třeba zavést omezení přístupu i na aplikační úrovni.
11.6.2	Oddělení citlivých systémů	V podniku jsou citlivé informace využívány vzhledem k povaze činností jednotlivých oddělení a tyto informace jsou separovány do oddělených

	Opatření normy ISO/IEC 27001	Zavést opatření
		fyzických míst. K tomuto opatření je třeba zavést dokumentaci s popisem charakteru uložených informací a přístupová oprávnění.
11.7.2	Práce na dálku	Je nutné zavést postupy a požadavky, které ošetřují práci na dálku. S těmito postupy seznámit pracovníky, kteří tento způsob práce využívají. Je třeba stanovit sankce za nedodržení bezpečnostních opatření. Vzdálený přístup do podniku je třeba omezit na dobu odpovídající smluvním požadavkům a kontrolovat pokusy o neautorizovaný přístup či neoprávněné využití podnikových síťových prostředků.
13	Zvládání bezpečnostních incidentů	
13.1.1	Hlášení bezpečnostních událostí	Zavést formalizovaný postup pro hlášení, reakci a eskalaci na bezpečnostní incident. Seznámit pracovníky s těmito postupy.
13.1.2	Hlášení bezpečnostních slabin	Vytvoření postupů pro zaměstnance a externí dodavatele pro hlášení případných bezpečnostních slabin v systémech či službách.
13.2.1	Odpovědnosti a postupy reakce na incidenty	Stanovení odpovědností za hlášení bezpečnostních incidentů, monitorování systémů a sledování varovných signálů a zranitelností.
13.2.2	Ponaučení z bezpečnostních incidentů	Pravidelně analyzovat bezpečnostní incidenty a zkoumat jejich příčiny. V případě objevení možné zranitelnosti tuto zahrnout do systému ISMS pro minimalizaci budoucích nákladů.
14	Řízení kontinuity činností organizace	
14.1.1	Zařazení informační bezpečnosti do procesu řízení kontinuity činností organizace	Identifikace a zvážení implementace možných dodatečných preventivních opatření. Zajištění bezpečnosti zaměstnanců v podniku. Ostatní činnosti zahrnuté v této oblasti jsou již zavedeny v rámci identifikace rizik.
14.1.2	Kontinuita činností organizace a hodnocení rizik	
14.1.3	Vytváření a implementace plánů kontinuity	Vytvoření plánů obsahujících přijatelné úrovně pro ztrátu služeb nebo informací. Vytvoření provozní dokumentace s odsouhlasenými procedurami a postupy, školení zaměstnanců v havarijních procedurách.
14.1.4	Systém plánování kontinuity činností organizace	Stanovit odpovědnou osobu, která vyhodnotí nutnost spuštění havarijních plánů. Vytvoření plánů na dočasné provozní činnosti do okamžiku obnovení plné činnosti podniku.
14.1.5	Testování, udržování a přezkoumávání plánů kontinuity	Pravidelně ověřovat, zda lze systémy podniku obnovit ze záloh, kontrolovat úplnost scénářů realizovatelnosti navržených plánů. Testování externích služeb.

Seznam opatření k zavedení ISMS fáze III.

	Opatření normy ISO/IEC 27001	Zavést opatření
8	Bezpečnost lidských zdrojů	
8.1.1	Role a odpovědností	Pro každou zaměstnaneckou pozici definovat role a odpovědnost v rámci podniku.
8.1.2	Prověřování	Při pracovním pohovoru zjišťovat, zda osoba nepatří do rizikových skupin z hlediska bezpečnosti a prověřit dodané údaje od uchazeče.
8.1.3	Podmínky výkonu pracovní činnosti	Pro každou pracovní činnost definovat požadavky a povinnosti zaměstnance vzhledem k bezpečnosti informací.
8.2.2	Bezpečnostní povědomí, vzdělávání a školení v oblasti bezpečnosti informací	Určený pracovník technického oddělení provádí pravidelné proškolení ostatních zaměstnanců na bezpečnostní opatření.
8.2.3	Disciplinární řízení	V rámci podniku revidovat existující disciplinární opatření a seznámit s nimi všechny zaměstnance.
8.3.1	Odpovědnosti při ukončení pracovního vztahu	Vypracovat plán činností, které je třeba provést po ukončení pracovního poměru zaměstnance. Je třeba zahrnout převod odpovědností, kontaktovat externí dodavatele, seznámit pracovníky s odchodem zaměstnance.
8.3.3	Odebrání přístupových práv	Je třeba definovat postupy, jakými lze zaměstnanci odebrat či změnit přístupová práva. V těchto postupech je třeba brát do úvahy hodnoty aktiv, důvod změny práv a jejich dopad.
12	Akvizice, vývoj a údržba informačních systémů	
12.1.1	Analýza a specifikace bezpečnostních požadavků	Pro všechny nové informační systémy nebo úpravy stávajících systémů je třeba pamatovat na splnění bezpečnostních požadavků stanovených v podniku. Je vhodné provést analýzu rizik.
12.4.2	Ochrana dat pro testování systému	Je třeba zabezpečit, aby každá data použitá při testování systému byla anonymní. O provádění testování a jeho ukončení musí být vedeny záznamy.
12.5.1	Postupy řízení změn	Je třeba revidovat postupy změnového řízení. Každý návrh změny musí být kontrolován na jeho oprávněnost, omezení funkčnosti systému. Po změně je nutno revidovat dokumentaci.
12.5.2	Technické přezkoumání aplikací po změnách operačního systému	Při potřebě změny operačních systémů všechny kritické aplikace podniku otestovat na jejich bezchybnou funkčnost pomocí virtuálních počítačů s požadovaným OS. Tyto testy vyhodnotit a doporučit či zamítnout změnu OS.
12.5.3	Omezení změn programových balíků	Změny v použitém IS prováděné oddělením vývoje musí být dokumentovány ve speciální dokumentaci pro interní použití. Je třeba zamezit, aby se tyto změny dostaly do prodejních verzí IS.
12.5.4	Únik informací	Před instalací nového software odpovědná osoba prověří, zda nedochází k nežádoucí komunikaci software s externími zdroji.
12.5.5	Programové vybavení vyvíjené externím dodavatelem	Pro každého externího dodavatele kontrolovat správnost licenčního ujednání, ukládat zdrojové kódy na bezpečné místo v rámci podniku a porovnat dokumentaci s realitou.
12.6.1	Řízení, správa a kontrola technických zranitelností	Je třeba kontrolovat dodržování pravidelné revidování technické zranitelnosti. Odpovědná osoba vypracovává měsíční správu technické zranitelnosti. Nalezené zranitelnosti je třeba zahrnout do rizik a adekvátně na tyto rizika reagovat.
15	Soulad s požadavky	
15.1.1	Identifikace odpovídajících předpisů	Je třeba stanovit odpovědnou osobu za pravidelné sledování změn v předpisech týkajících se činnosti podniku, případně vyvíjeného software.
15.1.2	Ochrana duševního vlastnictví	Je třeba zajistit dodržování autorských práv, nákupy software či komponent provádět výhradně přes ověřené dodavatele. V rámci podniku kontrolovat využití pracovních stanic zaměstnanců.

	Opatření normy ISO/IEC 27001	Zavést opatření
15.1.3	Ochrana záznamů organizace	Vytvoření směrnice pro ukládání, zpracování a likvidaci záznamů a informací. Je nutné definovat a uchovávat soupis klíčových zdrojů informací.
15.1.5	Prevence zneužití prostředků pro zpracování informací	Prokazatelně seznámit zaměstnance s použitím systému a monitorování neautorizovaných přístupů.
15.2.1	Shoda s bezpečnostními politikami a normami	Stanovit intervaly pravidelné kontroly na shodu používaných prostředků s bezpečnostní politikou a normami. V případě nesouladu tyto zjištěné nedostatky zaznamenat a co nejdříve odstranit.
15.2.2	Kontrola technické shody	Sestavení plánů testů, pro prověřování bezpečnostních opatření. Použité testy musí být dokumentovány a stanoveny pro ně takové podmínky, aby byly snadno reprodukovatelné.

Navržená opatření etapy II A III je třeba doplnit o opatření, která budou při realizaci dané etapy nutná k splnění odpovídajícího opatření normy. Vzhledem k tomu, že při zavádění některých opatření se jejich důsledek promítá do více oblastí. Všechna opatření uvedená v tabulce však nebude nezbytně nutno zavést, protože budou již splněna opatřeními z jiné etapy zavádění ISMS.