Požiadavky na presadenie zásad kybernetickej bezpečnosti v organizácii

Bc. Rudolf Jelenek

Diplomová práce
2016

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2015/2016

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Rudolf Jelenek**
Osobní číslo:	**A14562**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Požadavky na prosazení zásad kybernetické bezpečnosti v organizaci**
Téma anglicky:	**The Requirements for Enforcing Cyber Security Principles in an Organisation**

Zásady pro vypracování:

1. **Proveďte informační rešerši v oblasti legislativy informační a kybernetické bezpečnosti.**
2. **Popište způsob implementace systému řízení informační bezpečnosti (ISMS).**
3. **Zhodnoťte výchozí stav organizace, kde bude ISMS řešena.**
4. **Vypracujte návrh implementace ISMS ve zvolené organizaci.**
5. **Je-li možné, realizujte navržené změny v prostředí organizace.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **SMEJKAL, Vladimír a Karel RAIS. Řízení rizik ve firmách a jiných organizacích. 2., aktualiz. a rozš. vyd. Praha: Grada, 2006, 296 s. Expert (Grada). ISBN 80-247-1667-4.**
2. **Audit informační bezpečnosti systém řízení informační bezpečnosti (ISMS) [online]. [cit. 2016-01-31]. Dostupné z: http://blog.brichacek.net/audit-informacni-bezpecnosti-system-rizeni-informacni-bezpecnosti-isms/.**
3. **SORIANO, Miguel. Informačná a sieťová bezpečnosť. Vyd. 1. V Praze: České vysoké učení technické, 2014, 1 CD-ROM. ISBN 978-80-01-05299-0.**
4. **Národná stratégia pre informačnú bezpečnosť v SR [online]. [cit. 2016-01-31]. Dostupné z: http://www.informatizacia.sk/narodna-strategia-pre-ib/6783s.**
5. **Zavedení systému řízení bezpečnosti - ISMS [online]. [cit. 2016-01-31]. Dostupné z: http://www.chrantesidata.cz/cs/art/1147-dil-1/.**

Vedoucí diplomové práce: **doc. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **5. února 2016**

Termín odevzdání diplomové práce: **16. května 2016**

Ve Zlíně dne 5. února 2016

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 16.5.2016

.....
podpis diplomanta

ABSTRAKT

Diplomová práca je zameraná na problematiku informačnej bezpečnosti v nami zvolenej organizácii Protherm Production Skalica. Práca pozostáva z dvoch samostatných častí, a to z teoretickej a praktickej.

Teoretická časť tvorí literárny prierez informačnou bezpečnosťou tak ako ju definuje norma ISO/IEC 27001. Konkrétne sme sa zamerali na postup implementácie ISMS a následnú certifikáciu ISMS.

Praktická časť pozostáva z definovania a ohodnotenia aktív spoločnosti a hrozieb, ktorými môžu byť tieto aktíva ohrozené. Na základe týchto údajov sme vytvorili rizikovú analýzu. V nej boli odhalené možné hrozby pre konkrétne aktíva na základe čoho sme definovali nápravné opatrenia. Tieto boli predložené vedeniu spoločnosti, ktoré sa rozhodlo niektoré z nich implementovať.

Kľúčové slova: bezpečnosť informácií, kybernetická bezpečnosť, IT služby, ISMS

ABSTRACT

The diploma thesis is dealing with the topic of information security in the company Protherm Production Skalica. The thesis is divided into two parts; theoretical and practical.

The theoretical part focuses on the literary survey about the information security in the way it is defined by the ISO/IEC 27001 norm. The specific focus is on the approach of implementation of ISMS and consecutive ISMS certification.

The practical part is oriented on the definition and evaluation of the corporative assets and threatments that can consecutively affect the assets. The insecure analysis was created as a result of these data. It revealed possible threats for certain assets which were defined by the corrective actions. These possible corrective measurements were presented and some of them also implemented by the company Protherm Production Skalica.

Keywords: information security, cyber security, IT services, ISMS

Ďakujem vedúcemu práce doc. Mgr. Romanovi Jaškovi, Ph.D. za poskytnuté rady a priateľke Ing. Lucii Konečnej za podporu v mojom štúdiu.

Prehlasujem, že odovzdaná verzia diplomovej práce a verzia elektronická nahraná do IS/STAG sú totožné.

OBSAH

ÚVOD

Internet a všeobecne kybernetický priestor majú v posledných dvoch desaťročiach nesmierny vplyv na všetky zložky spoločnosti. Na dokonalom fungovaní informačných komunikačných technológií závisí nielen náš každodenný život, základné práva a sociálne interakcie, ale aj ekonomika a zásady bezpečnosti v organizáciách. Otvorený a slobodný kybernetický priestor pomohol presadzovať politické sociálne začlenenie na celom svete.

Aby zostal kybernetický priestor slobodný, musí Európska Únia na internete uplatňovať rovnaké normy, zásady a hodnoty ako mimo neho. Rovnako ako organizácie, ktoré pracujú prostredníctvom internetu existujú aj skupiny útočníkov. Títo útočníci používajú veľa spôsobov ako napadnúť počítač či celú organizačnú sieť. S rastúcou závislosťou na informačné technológie rastie aj riziko napadnutia alebo zneužitia.

V súvislosti s tým môžeme spomenúť pojem informačná bezpečnosť, ktorý v jednoduchšom zmysle slova znamená ochranu informačno-komunikačných technológií a všetkého čo s nimi súvisí. Ide teda o ochranu informácií pred hrozbami a zraniteľnosťami, ktoré môžu poškodiť aktíva spoločnosti. Cieľom informačnej bezpečnosti je zabezpečiť kontinuálny a úspešný chod činnosti organizácie a maximalizovať využitie investícií a obchodných príležitostí.

Aby bola v organizácii táto bezpečnosť dosiahnutá, je potrebné zabezpečiť implementáciu vhodných opatrení ako sú procesy, postupy, politiky, softvérové a hardvérové funkcie.

Pre zavedenie systému manažérstva informačnej bezpečnosti boli vytvorené medzinárodné normy (štandardy) radu ISO/IEC 27000, ktoré špecifikujú požiadavky na riadenie informačnej bezpečnosti pre všetky typy a veľkosti organizácií. Normy predstavujú akúsi príručku pre podniky, ktoré sa snažia zaviesť systém informačnej bezpečnosti. V rámci noriem sú dopodrobna popísané kroky, ktoré musia byť počas implementácie dodržané.

Treba si však uvedomiť, že informačná bezpečnosť nie je manažérsky proces vytvárajúci zisk, ale v súčasnosti je nevyhnutným nástrojom pre bezproblémový chod procesov, ktoré sa na vytváraní zisku priamo podieľajú. Týmto ziskom sa nemyslí len materiálny prospech pre spoločnosť ale aj nehmotný.

Diplomová práca spracováva tematiku informačnej bezpečnosti a ukazuje praktický príklad jej implementácie v rámci spoločnosti.

I. TEORETICKÁ ČASŤ

1 KYBERNETICKÁ BEZPEČNOSŤ

Kybernetická bezpečnosť (Cyber Security) je pojem 21. storočia, ktorý úzko súvisí s rozvojom informačných technológií a „internetovým“ poňatím spoločnosti. [1]

Kybernetickú bezpečnosť môžeme definovať ako odvetvie výpočtovej techniky známej ako informačná bezpečnosť, ktoré je uplatňované ako u počítačov tak u sietí. Cieľom informačnej bezpečnosti je ochrana informácií a majetku pred krádežou, korupciou alebo prírodnou katastrofou, pričom informácie a majetok musia zostať prístupné a produktívne ich predpokladaným užívateľom. [2]

Investovanie do kybernetickej bezpečnosti znamená investície do budúcnosti a ekonomického rastu. Úroveň kybernetickej bezpečnosti je súhrnom všetkých opatrení, ako národných tak aj medzinárodných, ktoré boli prijaté k ochrane dostupnosti informácií komunikačných technológií a integrity, autenticity a dôvernosti dát v kybernetickom priestore. Kybernetická bezpečnosť musí byť založená na komplexnom prístupe, čo vyžaduje intenzívne zdieľanie informácií a koordináciu aktivít. Pri budovaní kybernetickej bezpečnosti je potrebné presadzovať spoluprácu medzi civilnými a ozbrojenými zložkami, verejným a privátnym sektorom a medzi národnými a medzinárodnými inštitútmi. Len takýmto spôsobom je možné zaistiť spoľahlivú prevádzku informačných a komunikačných infraštruktúr v kritických sektoroch, rýchle a efektívne reakcie na kybernetické útoky a odpovedajúcu legislatívnu ochranu v digitálnom svete. [3]

1.1 Kybernetický zákon

Základným cieľom ***Zákona o kybernetickej bezpečnosti*** je zvýšiť bezpečnosť kybernetického priestoru a predovšetkým sa snažiť ochrániť tú časť infraštruktúry, ktorá je pre fungovanie štátu dôležitá a ktorej narušenie by viedlo k poškodeniu alebo ohrozeniu záujmov štátu. [4]

Cieľom Zákona nie je riešiť všetky riziká v kyberpriestore, ako je napr. porušovanie autorských práv, rôzne podvodné aktivity, úniky elektronických dát či šírenie chybného elektronického obsahu. [4]

Samotný Zákon je postavený na dvoch základných zásadách, a to na zásade minimalizácie zásahov do práv súkromnoprávnych subjektov a na zásade individuálnej zodpovednosti za bezpečnosť informačných systémov. [5]

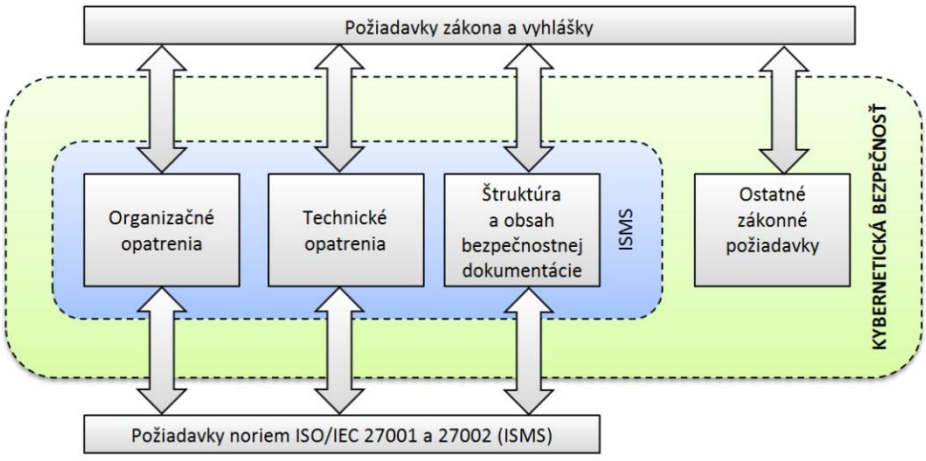
1.1.1 Aktuálny stav v Českej republike

Dlho pripravovaný Zákon o kybernetickej bezpečnosti (ZKB) nadobudol platnosti vyhlásením v Zbierke zákonov dňa 29.09.2014 ako zákon č. 181/2014 Zb., o kybernetickej bezpečnosti a o zmene súvisiacich zákonov. Zákon je účinný od 01.01.2015. [4]

S týmto zákonom súvisia nasledujúce predpisy:

- ***Vyhláška č. 316/2014 Zb.***, o bezpečnostných opatreniach, kybernetických bezpečnostných incidentoch, reaktívnych opatreniach a o stanovení náležitosti podania v oblasti kybernetickej bezpečnosti (vyhláška o kybernetickej bezpečnosti),
- ***Vyhláška č. 317/2014 Zb.***, o významných informačných systémoch a ich určujúcich kritériách,
- ***Nariadenie vlády č. 315/2014 Zb.***, o kritériách pre určenie prvku kritickej infraštruktúry. [4]

Zákon stanovuje, akým spôsobom má byť kybernetická bezpečnosť zaistená a určuje spôsob reakcie na kybernetické hrozby alebo riešenie uskutočneného incidentu. Podrobnosti k spôsobu realizácie bezpečnostných opatrení, ku komunikácii s kontaktnými miestami, vedenie bezpečnosti dokumentácie a kategorizácie kybernetických bezpečnostných incidentov určuje Vyhláška. Povinnosti vyplývajúce zo Zákona sa dotýkajú len vymedzeného okruhu právnických osôb, orgánov a podnikajúcich fyzických osôb. To ale neznamená, že ostatných subjektov sa potreba chrániť svoje informačné a komunikačné systémy pred neustále narastajúcimi kybernetickými hrozbami nijako netýka. Pre tieto subjekty môže Zákon a najmä Vyhláška slúžiť ako vhodná inšpirácia alebo metodika. [4]



Obr. 1. Kybernetická bezpečnosť [4]

1.1.2 Aktuálny stav v Slovenskej republike

Až donedávna nemala kybernetická bezpečnosť na Slovensku jasne stanovených zodpovedných aktérov. V oblasti sa prelínala činnosť Ministerstva financií SR, Ministerstva obrany a Národného bezpečnostného úradu. Niektoré činnosti boli dvojité, iné sa podceňovali. Situáciu dobre ilustruje aj to, že doteraz pre túto oblasť chýba jednotná terminológia. ***Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020***, ktorú vláda schválila v polovici júna 2015, už obsahuje jasnú organizačnú štruktúru. Samotný návrh zákona o kybernetickej bezpečnosti sa má objaviť vo februári 2016. [6]

Cieľom Koncepcie kybernetickej bezpečnosti Slovenskej republiky je dosiahnutie nasledujúcich stavov:

- Ochrana národného kybernetického priestoru je systémom fungujúcim koncepčne, koordinovane, efektívne, účinne a na právnom základe.
- Bezpečnostné vedomie všetkých zložiek spoločnosti sa systematicky zvyšuje.
- Súkromný a akademický sektor, ako aj občianska spoločnosť sa aktívne zúčastňuje na formovaní a realizácii politiky Slovenskej republiky v oblasti kybernetickej bezpečnosti.
- Efektívna spolupráca je zabezpečená na národnej, ako aj medzinárodnej úrovni.
- Prijaté opatrenia sú primerané, uznávajú ochranu súkromia a základné ľudské práva a slobody. [7]

Na Slovensku je kybernetická bezpečnosť zastrešená prostredníctvom ***CSIRT (Computer Security Incident Response Team)***. Ide o špecializovanú jednotku, ktorá je určená pre riešenie počítačových incidentov. Zabezpečuje služby spojené so zvládaním bezpečnostných incidentov, odstraňovaním ich dôsledkov s následným obnovením činnosti informačných systémov. [7]

1.2 Štandardy kybernetickej bezpečnosti

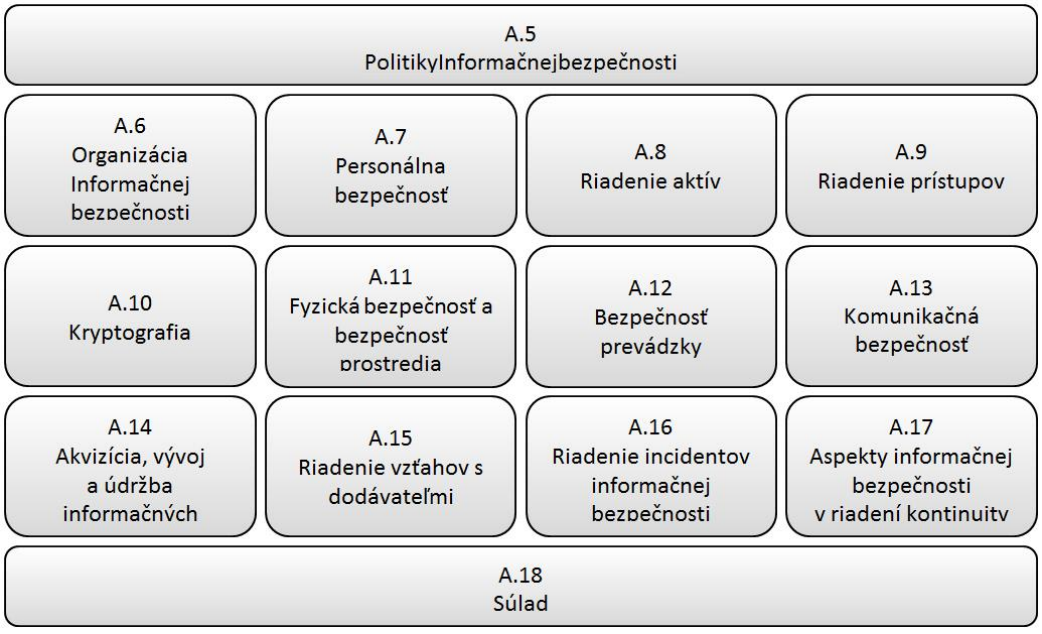
Štandardy kybernetickej bezpečnosti boli vytvorené relatívne nedávno, pretože práve v posledných rokoch pribúda citlivých informácií uložených v počítačoch, ktoré sú pripojené k internetu. Tiež mnoho úloh, ktoré boli pôvodne spracovávané v papierovej forme sú dnes uskutočňované na počítačoch. Preto sa zvyšuje potreba pre informačnú vierohodnosť a bezpečnosť. Dôležitým aspektom kybernetickej bezpečnosti je ochrana pred krádežou identity. [2]

Inštitúcie a firmy majú zvýšenú potrebu k zaisteniu informačnej (počítačovej bezpečnosti), pretože potrebujú chrániť svoje obchodné tajomstvá, dôverné informácie a osobné údaje o ich partneroch, zákazníkoch alebo zamestnancoch. [2]

V rámci kybernetickej bezpečnosti sú využívané dve základné normy, ktoré boli odvodené od štandardov BS 7799 vytvorených Britským štandardizačným inštitútom (BSI). Prvou je norma ISO/IEC 27001, ktorá poskytuje model pre zavedenie efektívneho systému riadenia bezpečnosti informácií (ISMS) v organizácii a dopĺňa tak normu ISO/IEC 27002. [2]

1.2.1 ISO/IEC 27002:2013

ISO/IEC 27002:2013 je ***zbierka najlepších bezpečnostných praktík*** a môže byť využitá ako kontrolný zoznam všetkého správneho, čo je nutné pre bezpečnosť informácií v organizácii uskutočniť. 14 hlavných oddielov tejto normy definuje 35 cieľov (kontrolných) opatrení pre ochranu informačných aktív proti narušeniu ich dôvernosti, dostupnosti a integrity. V podstate tieto ciele opatrení zahŕňajú funkčné požiadavky pre architektúru bezpečnosti informácií organizácie. [8]



Obr. 2. Norma ISO/IEC:2013 katalóg opatrení ISMS [8]

Ciele opatrení poskytujú kvalitný základ pre definíciu sady „axiómov“ pre bezpečnostnú politiku. Nie všetky sú aplikovateľné v každej organizácii a môžu sa objaviť požiadavky na ich preformulovanie či prispôsobenie podľa aktuálnych potrieb organizácie. Väčšina z nich je však obecne použiteľná. [8]

ISO/IEC27002 tiež popisuje najlepšie praktiky pre zaistenie bezpečnosti informácií, ktoré by organizácia mala brať do úvahy pre zaistenie kontrolných cieľov. Nová verzia normy obsahuje 113 „základných“ opatrení, ktoré sa v skutočnosti ďalej rozpadajú na stovky špecifických bezpečnostných opatrení. [8]

Norma neprikazuje, ktoré opatrenia musia byť bezpodmienečne aplikované, ale ponecháva rozhodnutie na organizácii. Vhodné opatrenia sú vyberané na základe hodnotenia rizík a ich implementácia je závislá na konkrétnej situácii. Cieľom nie je implementovať všetko, čo norma popisuje, ale skôr naplniť všetky aplikovateľné ciele opatrení. [8]

1.2.2 ISO/IEC 27001:2013

Norma ISO/IEC 27001 si kladie za ciel poskytnúť ***odporúčanie ako aplikovať ISO/IEC 27002*** v rámci procesu ustanovenia, prevádzky, údržby a zlepšovania systému riadenia bezpečnosti informácií v organizácii v súlade so systémami riadenia kvality alebo bezpečnosti prostredia. Norma popisuje vhodný systém riadenia, štruktúru a procesy pre riadenie bezpečnosti informácií podľa opatrení definovaných v ISO/IEC 27002. [9]

Systém manažérstva informačnej bezpečnosti podľa ISO 27001 je určený k ochrane informácií, čiže k zvládnutiu rizík, ktoré tieto informácie môžu eventuálne ohrozovať.

Dôležitou súčasťou normy ISO 27001 je popis pre vybudovanie prevádzky systému riadenia bezpečnosti informácií. Pod čím môžeme rozumieť, že organizácie musia realizovať analýzu rizík, aby bolo možné určiť špecificky optimálne bezpečnostné ciele a opatrenia, zaviesť ich a použiť podľa vlastných požiadaviek. Po identifikácii bezpečnostných cieľov je potrebné ich zrozumiteľne zdokumentovať pre všetky osoby v organizácii. Tieto podklady musia byť dostupné pre manažérov, zamestnancov a rovnako vybraným nezávislým stranám (interný audítori, certifikačný audítor, atď.). [9]

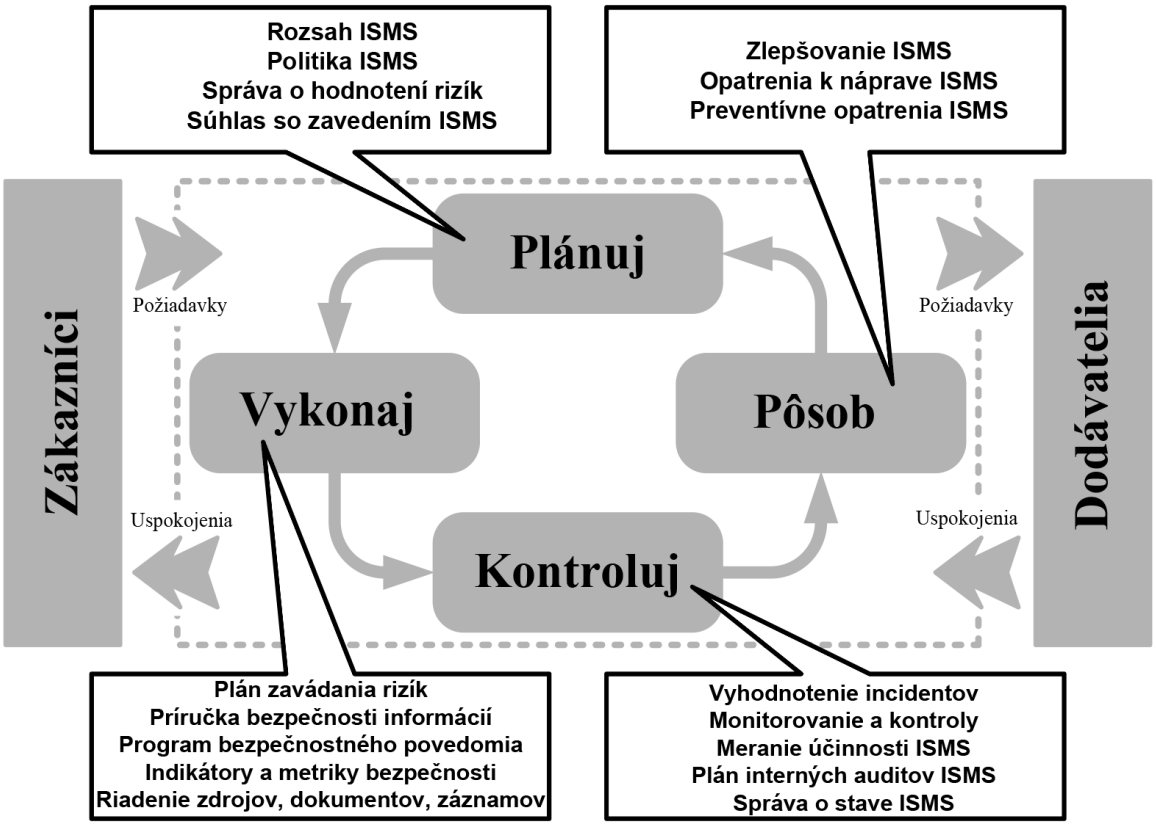
Norma ISO 27001 je takisto ako všetky ISO štandardy medzinárodne platným štandardom. Spoločnosť, ktorá získa certifikát v jednej krajine, nemusí opäť preukazovať splnenie požiadaviek v inej krajine. [10]

2 POSTUP IMPLEMENTÁCIE ISMS

Norma ISO/IEC 27001 v najnovšom vydaní ISO/IEC 27001:2013 je medzinárodný štandard, ktorý špecifikuje požiadavky na riadenie informačnej bezpečnosti v organizácii. Norma bola vyvinutá tak, aby spĺňala požiadavky na informačnú bezpečnosť pre všetky typy a veľkosti organizácií. Systém je možné aplikovať a certifikovať do výrobných, obchodných, servisných, montážnych, zdravotných poradenských či vzdelávacích organizácií zo všetkých oblastí priemyslu a služieb. [11]

Systém riadenia bezpečnosti informácií je jeden, rozdielne môžu byt výklady jednotlivých doporučení a postupy ako dosiahnuť stanovené ciele. Princípom celého ISMS je tzv. ***PDCA model (Demingov model)***, ktorý je zobrazený na obrázku č. 3. [12]

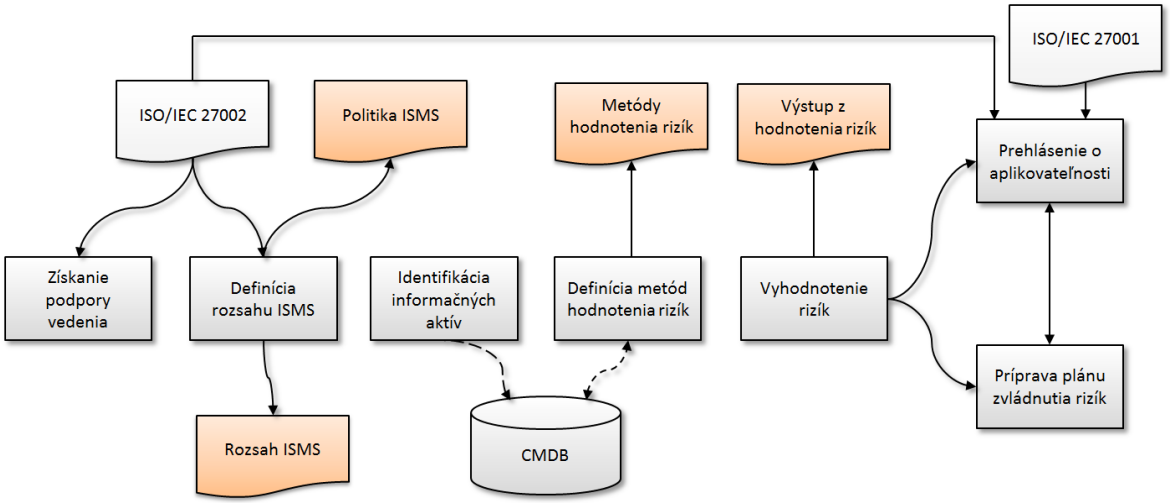
Tento model zavádza kontinuálny systém riadenia bezpečnosti informácií v organizácii. Jednotlivé kroky Plan – Do – Check – Act (Plánuj – Vykonaj – Kontroluj – Pôsob) zaručujú, že zavedenie systému informačnej bezpečnosti nebude len jednorazovou aktivitou, ale neustálym kolobehom. [12]



Obr. 3. PDCA Model pre riadenie bezpečnosti informácii [12]

2.1 Ustanovenie ISMS

Ustanovenie ISMS je prvou fázou PDCA modelu, ktorého úlohou je definícia rozsahu, politiky a systematického prístupu k ohodnoteniu rizík. Obrázok č. 4. zachycuje celý proces fáze ustanovenia systému riadenia informačnej bezpečnosti. [13]



Obr. 4. Ustanovenie ISMS [13]

V tejto fáze plánovania systému riadenia informačnej bezpečnosti je potrebné presvedčiť vedenie o týchto výhodách vysvetlením analýzy rizík a vytvorením obchodného prípadu zavedenia ISMS. Definícia rozsahu ISMS ukazuje, ktoré oddelenia, či systémy budú pokryté systémom riadenia informačnej bezpečnosti. Výstupom tejto definície je politika ISMS a dokument popisujúci konkrétny rozsah a dosah ISMS vo vnútri organizácie a v rámci troch strán. [13]

Identifikácia informačných aktív slúži pre vytvorenie zoznamu sietí, databáz, dátových entít, dokumentov, a pod. Tento zoznam sa spravidla nachádza na konfiguračnej databáze (CMDB) a býva využívaný ako základný zdroj obsahujúci kompletné aktíva organizácie.

S týmto zoznamom následne pracuje krok definície hodnotenia rizík a vyhodnotenia rizík. Vyhodnotenie rizík je vstupom pre vyhodnotenie projektu vedením organizácie a následný súhlas vedenia so zavedením a prevádzkou ISMS. [13]

2.1.1 Ohodnotenie aktív

Ak je potrebné čokoľvek hodnotiť a analyzovať, je potrebné danú entitu najskôr popísať a identifikovať. Identifikácia a ohodnotenie aktív organizácie je základným krokom v celkovom procese analýzy rizík. [12]

Identifikácia aktív

Aktívum je niečo, čo má hodnotu alebo niečo čo je užitočné pre obchodné operácie organizácie alebo pre jej kontinuitu činnosti. To znamená, že aktíva potrebujú ochranu, aby sa zaistili korektné obchodné operácie alebo kontinuita činnosti. [14]

Zjednodušene sú aktíva všetok hmotný a nehmotný majetok spoločnosti, ktorý môžeme rozdeliť do nasledujúcich skupín:

- informačné aktíva (informácie, dáta),
- hardvérové aktíva (technické prostriedky – hardvér),
- softvérové aktíva (technické prostriedky – softvér),
- komunikačné zariadenia (siete, telefóny, modemy),
- dokumenty (zmluvy, zápisy),
- personál (know-how),
- služby poskytované prostredníctvom informačných systémov. [15]

Ohodnotenie aktív

Vo fáze ohodnotenia aktív je základným krokom stanoviť si stupnicu a hodnotiace kritéria, ktoré budú použité v procese ohodnotenia určitého aktíva. Táto stupnica môže byť vyjadrená finančnými alebo kvalitatívnymi hodnotami, pričom je možné obe varianty kombinovať. Dôležité je tiež farebné odlíšenie jednotlivých stupňov. Ak máme rozsiahle tabuľky s hodnotením aktív, k lepšej orientácii nám pomôžu vhodne zvolené farby. [12]

Príklad kvalitatívnej stupnice pre ohodnotenie aktív organizácie je v tabuľke č. 1.

Hodnota aktíva	Označenie	Popis
Nízka	1	Žiadny vplyv na organizáciu
	2	Zanedbateľný vplyv na organizáciu
Stredná	3	Ťažkosti či finančné straty
Vysoká	4	Vážne problémy či podstatné finančné straty
	5	Existenčné problémy organizácie

Tab. 1. Ohodnotenie hrozieb [12]

Hlavným princípom pri ohodnotení aktív sú náklady, ktoré vzniknú v dôsledku porušenia troch základných kritérií informačnej bezpečnosti, ktorými sú:

- ***Dôvernosť*** – ***confidentiality*** – zaistenie, že informácie sú poskytnuté a prístupné len oprávneným osobám.
- ***Dostupnosť*** – ***availability*** – zaistenie, že k informáciám majú neobmedzený prístup len oprávnené osoby.
- ***Integrita*** – ***integrity*** – zaistenie správnosti a úplnosti informácií z hľadiska obsahu a formy. [16]

Výpočet hodnoty aktíva

Pre výpočet ohodnotenia aktíva je možné použiť rôzne postupy. Najjednoduchším a tiež najpoužívanejším je tzv. súčtový algoritmus, ktorého princípom je súčet: [12]

$$\frac{\text{Dô}vernosť+Dostupnosť+Integrita}{3} \tag{1}$$

Tento súčtový algoritmus poskytuje najrýchlejší spôsob ako získať hodnotu aktíva a zároveň odpovedá na otázku, aký dopad pre organizáciu bude mať porušenie dôvernosti, dostupnosti a integrity. Z toho vyplýva, že tieto tri kritéria poskytujú podklad pre ohodnotenie aktív. Napríklad, ak máme aktívum „informácie o zákazníkoch“, typickou otázkou môže byť: „Aký dopad bude mať na spoločnosť nedostupnosť informácií o zákazníkoch?“ Odpovede môžu byť od žiadny dopad pre spoločnosť až po existenčné problémy spoločnosti. [12]

Aktívum	Zdroj	Dostupnosť	Dôvernosť	Integrita	Váha
Informácie o zákazníkoch	systém	5	5	3	4
	sieťové disky	2	5	3	3
	užívateľské stanice	5	5	3	4

Tab. 2. Príklad ohodnotenia aktíva organizácie [15]

2.1.2 Identifikácia hrozieb a zraniteľností

Po identifikácii a ocenení aktív nasleduje ďalší krok, ktorým je identifikácia hrozieb a zraniteľností.

Hrozba

Pod pojmom hrozba rozumieme potenciálnu príčinu incidentu, ktorá môže mať za následok poškodenie aktív. [18]

Pojem hrozba tiež môžeme vysvetliť ako určitý jav, udalosť, proces alebo postup, pomocou ktorého dochádza k útoku na tri základné kritéria informačnej bezpečnosti (dôvernosť, dostupnosť, integrita). [17]

Rozdelenie hrozieb

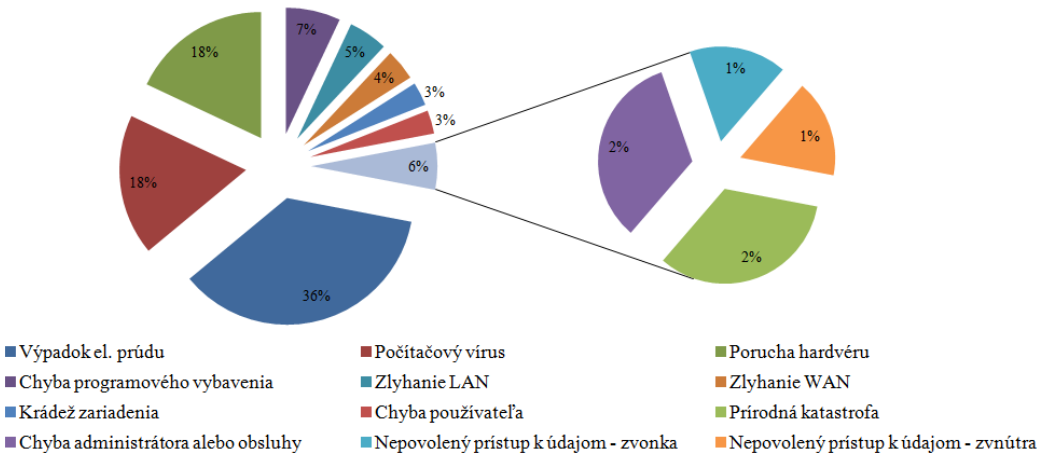
Hrozby môžu mať pôvod:

- prírodný (zemetrasenie, blesk, požiar, povodeň),
- ľudský. [18]

Ľudské hrozby môžeme ďalej deliť na:

- náhodné (vymazanie súboru, chybný príkaz, fyzická nehoda),
- úmyselné (krádež, hacking, odpočúvanie). [18]

Z hľadiska bezpečnosti je žiaduce, aby ako náhodné tak aj úmyselné hrozby boli identifikované a aby mohla byť odhadnutá ich úroveň a pravdepodobnosť. Otázkou je, aké hrozby sú pre danú organizáciu aktuálne. [18]



Obr. 5. Najčastejšie typy hrozieb [18]

Identifikácia hrozieb

Pojmom identifikácia hrozieb rozumieme odhaľovanie možných zdrojov hrozieb, ktoré môžu ohroziť určitú skupinu aktív. V norme ISO 27005 je katalóg častých hrozieb, ktorý je možné použiť v procese posudzovania hrozieb. Podľa svojho pôvodu môžu byť hrozby:

- úmyselné (D) – môžu mať za následok poškodenie alebo stratu základných služieb,
- náhodné (A) – používajú sa pre všetky ľudské činnosti, ktoré môžu náhodne poškodiť informačné aktíva,
- environmentálne (E) – používajú sa pre všetky incidenty, ktoré nie sú založené na ľudskej činnosti. [19]

Typ	Hrozby	Pôvod
Fyzické	**Požiar**	A,D,E
	Poškodenie vodou	A,D,E
	Znečistenie	A,D,E
	Prach, korózia, mrznutie	A,D,E
Prírodné udalosti	**Povodeň**	E
	Klimatický jav	E
	Sopečný jav	E
Strata základných služieb	**Prerušenie dodávky elektriny**	A,D,E
Poruchy spôsobené žiarením	**Elektromagnetické žiarenie**	A,D,E
	Termálne žiarenie	A,D,E
Ohrozenie informácií	**Krádež médií, dokumentov**	D
	Krádež zariadení	D
	Vzdialená špionáž	D
	Odpočúvanie	D
Technické zlyhanie	**Chybné fungovanie zariadenia**	A
	Preťaženie systému	A,D
	Chyba údržby	A,D
Neoprávnené činnosti	**Poškodenie dát**	D
	Nezákonné spracovanie dát	D
Ohrozenie funkčnosti	**Chyba v používaní**	A
	Zneužitie oprávnenia	A,D
	Nedostatok personálu	A,D,E

Tab. 3. Typické príklady hrozieb podľa ISO/IEC 27005 [19]

Zraniteľnosť

Zraniteľnosť spojená s aktívami zahŕňa slabé miesta na úrovni fyzickej, organizačnej, procedurálnej, personálnej, riadiacej, administratívnej, rovnako ako na úrovni hardvéru, softvéru alebo informácií. [20]

Zraniteľné miesta môžu byť využité hrozbami, ktoré môžu spôsobiť poškodenie systému informačnej bezpečnosti alebo obchodných cieľov. Zraniteľnosť sama o sebe nie je príčinou škody. Sama o sebe môže len umožniť hrozbe, aby ovplyvnila aktíva. [21]

Existencia zraniteľných miest je dôsledkom chýb, zlyhania v analýze, v návrhu alebo v zavedení informačného systému v analýze. Tak isto môže byť dôsledkom vysokej hustoty uložených informácií, zložitého softvéru, existencie skrytých kanálov pre prenos informácií inou než zamýšľanou cestou a pod. Podstata zraniteľného miesta môže byť:

- fyzická – napr. umiestnenie informačného systému v mieste, ktoré je ľahko prístupné sabotáži, a pod.
- prírodná – záplava, požiar, blesk,
- v hardvéri alebo v softvéri – nepokrytá bezpečnostná diera v operačnom systéme, poruchové komponenty informačného systému,
- fyzikálna – elektromagnetické vyžarovanie, útoky pri komunikácii na výmenu správy,
- v ľudskom faktore – predstavuje najväčšiu možnú zraniteľnosť všetkých existujúcich variant. [22]

Pravdepodobnosť výskytu hrozieb

Tieto zraniteľné miesta je možné veľmi jednoducho priradiť jednotlivým hrozbám, ktoré boli identifikované podľa oblastí bezpečnosti. Ohodnotenie zraniteľností je vykonávané subjektívnym hodnotiteľom (vlastníkom aktív), ktorý im priradí hodnotu od „1“ do „5“, pričom najpravdepodobnejšia hrozba je na stupnici ohodnotená číslom „5“. Pri určovaní pravdepodobnosti výskytu hrozieb je potrebné tiež skúmať, či sa jedná o javy náhodné a či je možné danú hrozbu vylúčiť z nášho uvažovania. [23]

V tabuľke č. 4. je možné vidieť typické príklady hrozieb a príklady ich súvisiacich zraniteľností.

Identifikovaná hrozba	Pravdepodobnosť hrozby	Príklad súvisiacich zraniteľností
Zlyhanie hardvéru	3	Náchylnosť zariadenia na vlhkosť, prach a ušpinenie
Zlyhanie softvéru	3	Nejasné alebo neúplné špecifikácie pre vývojárov
Krádež	3	Nedostatok fyzickej ochrany budov, dverí a okien
Povodeň	2	Umiestnenia v miestach ktoré sú ohrozované povodňami
Zlomyseľné kódy	5	Nedostatok aktualizácií softvéru na ochranu pred zlomyseľnými kódmi
Neúmyselná modifikácia	5	Nedostatočný výcvik bezpečnosti
Zlyhanie komunikačných služieb	4	Nechránené verejné sieťové pripojenia

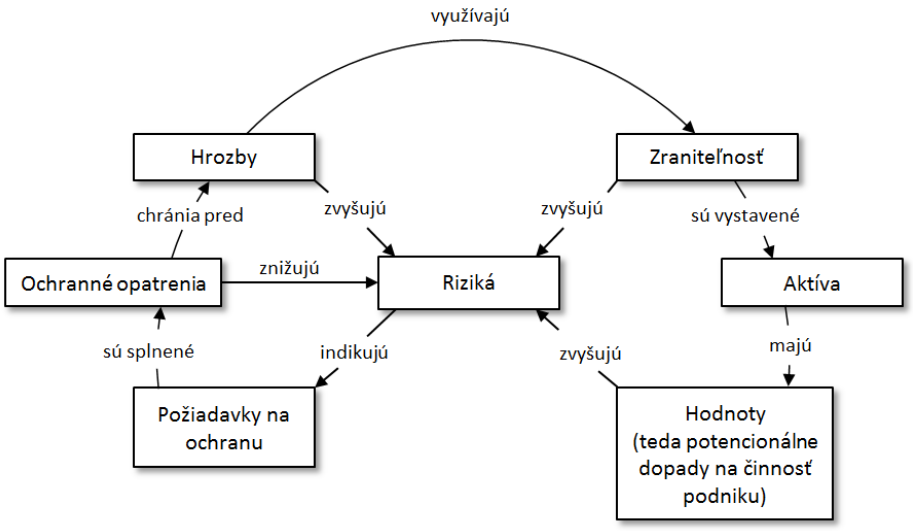
Tab. 4. Pravdepodobnosti jednotlivých hrozieb spolu s príkladmi zraniteľností [23]

2.1.3 Analýza rizík

Analýza rizík je z hľadiska systému riadenia bezpečnosti informácií podstatným krokom, ktorý zahŕňa predovšetkým inventúru aktív a rizík s ich ocenením. Na základe analýzy rizík je možné navrhnúť efektívnu bezpečnostnú politiku a optimalizovať potrebné náklady. [24]

Riziko

Riziko z pohľadu analýzy rizík je definované ako miera ohrozenia aktíva a následný vznik nebezpečenstva. Tým vzniká nežiaduci vplyv a dochádza ku vzniku škody. Je možné povedať, že riziko vzniká vzájomným pôsobením hrozby a aktíva. Aktívum, na ktoré nepôsobí ani jedna hrozba, nie je predmetom analýzy rizík. [25]



Obr. 6. Vzťahy pri manažmente rizík [26]

Rozdelenie analýzy rizík

- analýza rizík – hrubá úroveň,
- analýza rizík – neformálny prístup,
- analýza rizík – kombinovaný prístup,
- analýza rizík – podrobný prístup. [12]

Pri zavádzaní systému informačnej bezpečnosti sa odporúča použiť kombináciu pragmatickej (neformálnej) analýzy rizík a detailnej analýzy rizík. Najskôr je uskutočnená počiatočná analýza rizík na hrubej úrovni pre všetky systémy IT. U systémov, ktoré budú identifikované ako významné pre činnosť organizácie, prípadne, ktoré budú vystavené vysokým rizikám uskutočňujeme podrobnú analýzu rizík. [15]

Analýza rizík na hrubej úrovni

Táto analýza rizík berie v úvahu hodnotu systému informačných technológií pre činnosť organizácie a spracovávaných informácií a rizika z pohľadu činnosti organizácie. Pre rozhodnutie, ktorý prístup je pre ktorý systém IT vhodný, bude mať význam zohľadnenie nasledujúcich skutočností:

- akých cieľov má byť použitím systémov IT dosiahnutých,
- úroveň investícií do tohto systému IT (vývoj, údržba),
- aktíva systému IT, ktorým organizácia priradzuje určitú hodnotu,

- stupeň, v akom činnosť organizácie závisí na systéme IT (či sú funkcie, ktoré organizácia považuje pre svoje prežitie za kritické alebo efektívne, sú závislé na tomto systéme IT). [15]

Po tomto základnom rozdelení vieme, ktoré systémy sú vhodné k nasadeniu základného prístupu (menej kritické, nákladné a pod.) a tie u ktorých je nutné uskutočniť podrobnú analýzu rizík. [12]

Analýza rizík - neformálny prístup

Táto možnosť predstavuje neformálnu, pragmatickú analýzu rizík. Neformálny prístup nie je založený na štruktúrovaných metódach, ale využíva znalosti a skúsenosti jednotlivcov. Výhodou tejto voľby je, že nevyžaduje mnoho zdrojov alebo časov. K uskutočneniu neformálnej analýzy nie je nutné sa naučiť nové dodatočné zručnosti a analýza je uskutočnená rýchlejšie ako podrobná analýza rizík. [12]

Nevýhodou analýzy je že, bez určitého typu formálneho prístupu alebo detailných zoznamov kontrol vzrastá pravdepodobnosť opomenutia niektorých dôležitých detailov a je obťažné obhájiť implementáciu ochranných opatrení vo vzťahu k rizikám odhadnutým týmto spôsobom. [12]

Analýza rizík – kombinovaná metóda

Pri tejto metóde sa najskôr uskutočňuje analýza rizík na hrubej úrovni pre všetky systémy IT. U každého prípadu sa sústreďuje na hodnotu systému IT pre činnosť organizácie a na vážne riziká, ktorým je systém IT vystavený. [12]

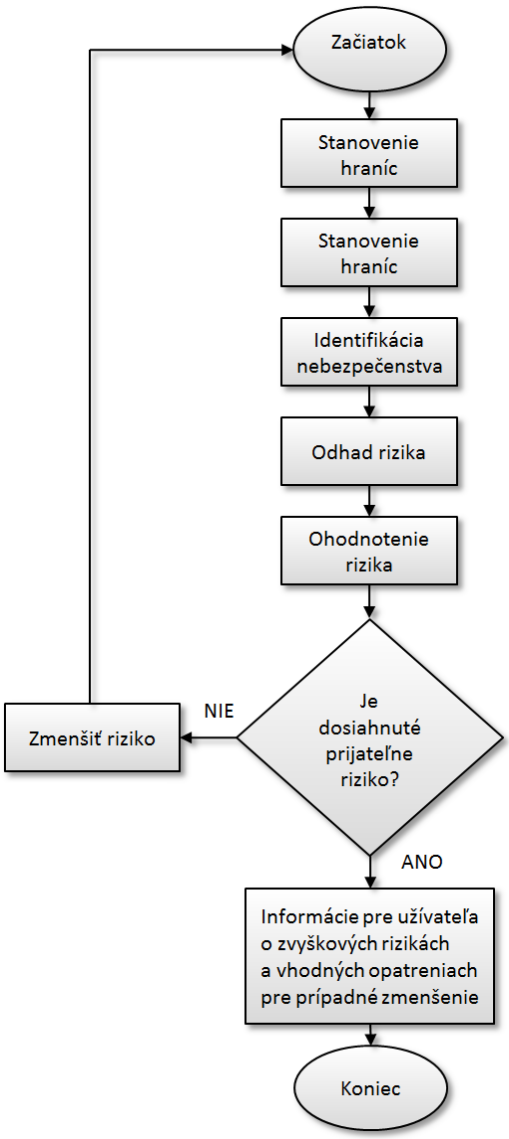
U systémov IT, ktoré sú identifikované ako významné pre činnosť organizácie a/alebo vystavené vysokým rizikám, by mala byť prednostne uskutočnená podrobná analýza rizík. Pre všetky ostatné systémy by mal byť zvolený základný prístup. Táto voľba, ktorá je kombináciou najlepších charakteristík možností umožňuje minimalizáciu času a úsilia venovaného na identifikáciu ochranných opatrení, pričom stále zaisťuje, že vysoké riziká systému sú chránené príslušným spôsobom. [12]

Podrobná analýza rizík

Táto metóda obsahuje identifikáciu súvisiacich rizík a odhad ich veľkosti. Analýza rizík sa uskutočňuje identifikáciou potenciálnych nepriaznivých dopadov nežiaducich udalostí na činnosť organizácie a pravdepodobnosť ich výskytu. Pravdepodobnosť výskytu bude závi-

sieť na tom, ako atraktívne sú aktíva pre potenciálneho útočníka, na pravdepodobnosti výskytu hrozieb a na ľahkosti, s ktorou môžu byť zraniteľnosti využité.

Podrobná analýza rizík zahŕňa hĺbkovú revíziu v každom z krokov uvedených na obrázku č. 7. Týmto dosiahneme vhodného výberu oprávnených ochranných opatrení ako časť procesu manažmentu. Požiadavky na ochranné opatrenia musia byť zakomponované do bezpečnostnej politiky systému IT. [12]



Obr. 7. Vývojový diagram analýzy rizík [12]

Analýza rizík využívajúca maticu aktív, hrozieb a zraniteľnosti

Prvým z dvoch základných prístupov analýzy rizík je analýza rizík využívajúca maticu aktív, hrozieb a zraniteľností. Pri tejto analýze rizík je potrebné v prvok kroku vytvoriť dve tabuľky:

- tabuľka matice zraniteľnosti (tab. 5.),
- tabuľka matice rizík (tab. 6.). [23]

Do tabuľky matice zraniteľnosti najskôr doplníme identifikované aktíva spolu s ich hodnotou. Následne doplníme identifikované hrozby spolu s ich mierou pravdepodobnosti. V ďalšom kroku musíme posúdiť zraniteľnosti jednotlivých aktív (skupín aktív) jednotlivými hrozbami a doplniť tak bunky tabuľky. [23]

	Popis aktíva	**Databáza serveru**	**Databáza skladu**	**Server**	**PC**	**Operačné systémy**	**Databázové systémy**	**Pripojenie serveru**	**Pripojenie PC v sklade**
Popis hrozby	T A	5	5	4	2	3	3	5	4
Zlyhanie hardvéru	3			2	2				
Zlyhanie softvéru	3					2	2		
Záplavy	2			1	1				
Neúmyselná modifikácia	5	2	5						
Zlyhanie komunikačných služieb	4							5	4

Tab. 5. Príklad matice zraniteľnosti [23]

Posledným krokom analýzy rizík je výpočet miery rizika, podľa vzorca: [23]

$$R = T \times A \times V \tag{2}$$

Kde:

- R – miera rizika,
- T – pravdepodobnosť vzniku hrozby,
- A – hodnota aktíva,
- V – zraniteľnosť daného aktíva.

Podľa tohto vzorca vypočítame mieru rizika a doplníme ju do matice rizík, ktorú môžeme vidieť v tabuľke č. 6. Po analýze už zostáva len stanoviť hranice pre nízke (prijateľné), stredné a vysoké (neprijateľné) riziká. [23]

	Popis aktíva	**Databáza serveru**	**Databáza skladu**	**Server**	**PC**	**Operačné systémy**	**Databázové systémy**	**Pripojenie serveru**	**Pripojenie PC v sklade**
Popis hrozby	T A	5	5	4	2	3	3	5	4
Zlyhanie hardvéru	3			24	12				
Zlyhanie softvéru	3					18	18		
Záplavy	2			8	4				
Neúmyselná modifikácia	5	50	125						
Zlyhanie komunikačných služieb	4							100	64

Tab. 6. Príklad matice rizík [23]

Analýza rizík vyhodnocujúca pravdepodobnosť incidentu a jeho dopad

Druhým prístupom analýzy rizík je analýza rizika vyhodnocujúca pravdepodobnosť incidentu a jeho dopad. Táto metóda prezentuje tak trochu odlišný prístup k určeniu miery rizika. Na rozdiel od predchádzajúcej metódy, ktorá využíva tri parametre (aktívum, hrozba a zraniteľnosť), využíva táto metóda len parametre dva (pravdepodobnosť a dopad incidentu).

Rovnako ako u predchádzajúcej metódy sa najskôr doplnia identifikované aktíva a ich hodnoty. Ďalej je nutné k jednotlivým aktívam identifikovať hrozby, zraniteľnosti a existujúce opatrenia. V ďalšom kroku sa odhadne pravdepodobnosť incidentu, že daná hrozba využije zraniteľnosti a ohrozí tým dané aktívum. Pravdepodobnosť incidentu je znižovaná existujúcimi opatreniami. [23]

Miera rizika je následne vypočítaná podľa vzťahu: [23]

$$R = PI \times D \tag{3}$$

Kde:

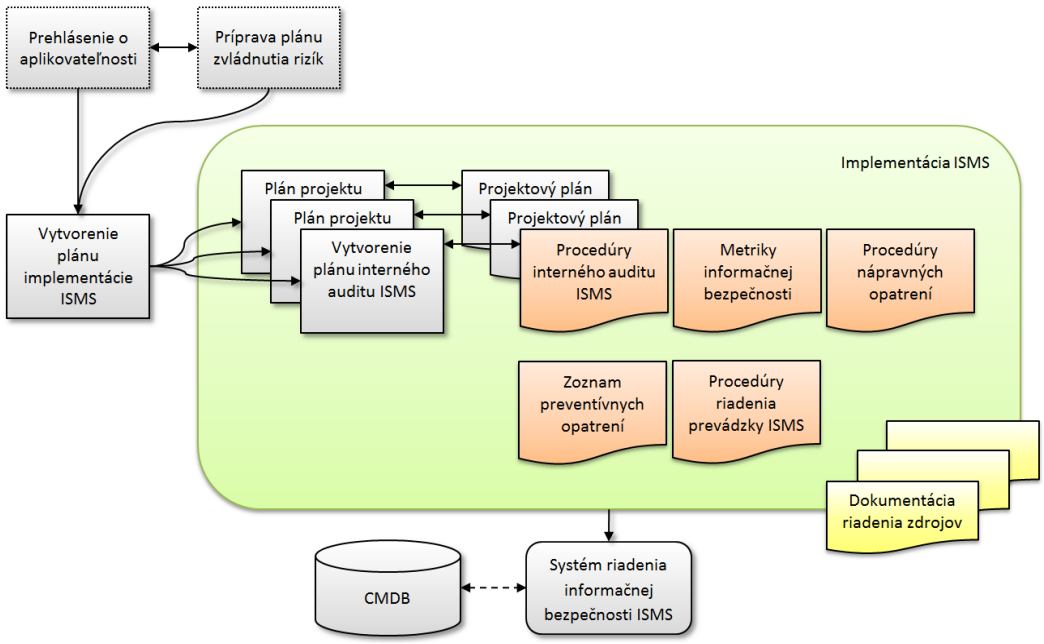
- R – miera rizika,
- PI – pravdepodobnosť incidentu,
- D – dopad.

Aktívum	A	Hrozba	Zraniteľnosti	PI	D	R	Opatrenia
Databáza serveru	5	Neúmyseľná modifikácia	Nedostatočný výcvik bezpečnosti	10	5	50	Pravideľné zálohovanie
Databáza skladu	5	Neúmyseľná modifikácia	Nedostatečný výcvik bezpečnosti	25	5	125	
Server	5	Zlyhanie hardvéru	Náchylnosť zariadenia na vlhkosť, prach a ušpinenie	6			
Server		Spreneverenie aktív	Nedostatok fyzickej ochrany budov, dverí a okien	3			Umiestnenie v zamknutom priestore, prístup iba majiteľ firmy
		Záplavy	Umiestnenie v miestach náchylným k záplavám	2			Umiestnenie serveru v 2. podlaží
...	...	...	...	...	...	...	...

Tab. 7. Analýza rizík [23]

2.2 Zavedenie a prevádzkovanie ISMS

Po fáze ustanovenia ISMS prichádza fáza zavedenia a prevádzkovania systému riadenia informačnej bezpečnosti, ktorej súčasťou je vytvorenie plánu implementácie ISMS a vlastná implementácia skladajúca sa zo zavedenia čiastkových projektov, vytvorenia plánu interného auditu, zavedenia definovaných stratégií do praxe, tvorba, prípadne aktualizácia smernice a procesov a budovanie povedomia o ISMS v rámci organizačnej štruktúry a definovaných úloh vo vnútri organizácie. Obrázok č. 8. zachytáva celý proces zavedenia prevádzkovania systému riadenia informačnej bezpečnosti. [13]



Obr. 8. Zavádzanie a prevádzka ISMS [13]

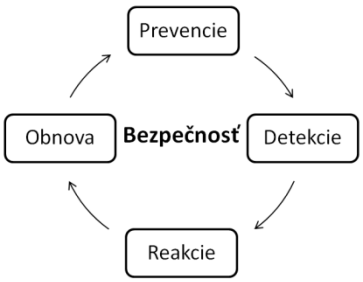
Výstupom tejto fázy je zavedenie systému riadenia informačnej bezpečnosti, vytvorenie procedúr pre vykonávanie interného auditu ISMS, definícia metrík informačnej bezpečnosti, vytvorenie zoznamu preventívnych opatrení, procedúry zabezpečujúce vhodné riadenie prevádzky ISMS a dokumentácia riadenia zdrojov. [13]

2.2.1 Metriky

Pojem metrika znamená presne vymedzený finančný alebo nefinančný ukazovateľ či hodnotiace kritérium, ktoré sú používané k hodnoteniu úrovne efektívnosti konkrétnej oblasti riadenia podnikového výkonu a jeho efektívnej podpory prostriedkami IS/IT. [27]

Pre zaistenie efektivity bezpečnostných opatrení a ich účinnosti je dôležité definovať vhodné metriky, uskutočňovať pravidelné merania a všetko riadne zaznamenávať a dokumentovať. [13]

V prípade informačnej bezpečnosti sa pojem metrika vzťahuje k meraniu efektivity atribútov informačnej bezpečnosti, teda dôvernosti, integrity a dostupnosti. Obrázok č. 9. zobrazuje životný cyklus vývoja metrík v oblasti informačnej bezpečnosti. [13]



Obr. 9. Životný cyklus [13]

Pri hodnotení informačnej bezpečnosti je potrebné brať do úvahy rôzne hodnotiace kritéria, ktoré sa prejavujú pri následnom rozhodovaní. Tieto kritéria sa môžu vzťahovať k podpore strategického rozhodovania hodnotenia kvality alebo taktickému a operatívnemu nadhľadu.

V prípade podpory strategického rozhodovania sa jedná napríklad o plánovanie, alokáciu zdrojov alebo výber vhodných produktov a služieb.

Hodnotenie kvality vyžaduje súlad s bezpečnostnými štandardmi, meraním a identifikáciou zraniteľností a s analýzou známych bezpečnostných hrozieb.

Taktický a operatívny nadhľad je založený na monitorovaní a reportovaní bezpečnosti a jej súlad s príslušnými požiadavkami. Súčasne identifikuje špecifické oblasti, ktoré je potrebné zlepšiť. [13]

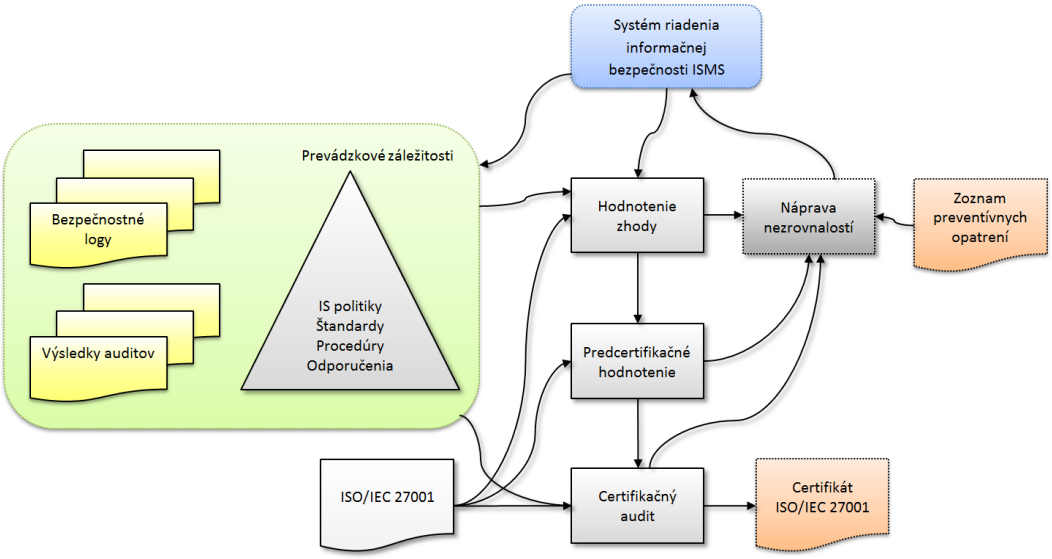
V praxi sa nachádza veľké množstvo už navrhnutých metrík pre hodnotenie úrovne bezpečnosti informácií. Samozrejme je možné navrhnúť si i metriky vlastné, ktoré budú merať presne to, čo merať potrebujeme. Existujú však určité pravidlá, podľa ktorých by dobrá metrika mala byť taká, aby:

- meranie bolo objektívne,
- získanie vstupných dát nebolo nákladné,
- meranie bolo opakovateľné,

- výsledok merania mohol byť vyjadrený ako číslo či percento,
- sa výsledok merania vzťahoval ku konkrétnej veličine. [28]

2.3 Monitorovanie a preskúmanie ISMS

Pre vyhodnotenie zhody s požiadavkami pri zavedení systému riadenia informačnej bezpečnosti je nutné zaistiť monitorovanie systému a prevádzkovanie ďalších súvisiacich kontrol. Tieto kontroly sú uskutočňované internými alebo externými audítormi na presne definovanej časovej báze. Súčasťou hodnotenia zhody implementácie je prehodnotenie zostatkového a akceptovateľného rizika s ohľadom na zmeny týkajúce sa zmien v organizácii, legislatívne zmeny alebo zmeny v požiadavkách regulačných orgánov. Obrázok č. 10. zobrazuje proces monitorovania a preskúmavania systému riadenia informačnej bezpečnosti z pohľadu PDCA modelu. K tejto fázy sa vzťahujú úlohy hodnotenia zhody, predcertifikačné hodnotenie a certifikačný audit. [13]



Obr. 10. Monitorovanie a preskúmavanie ISMS [13]

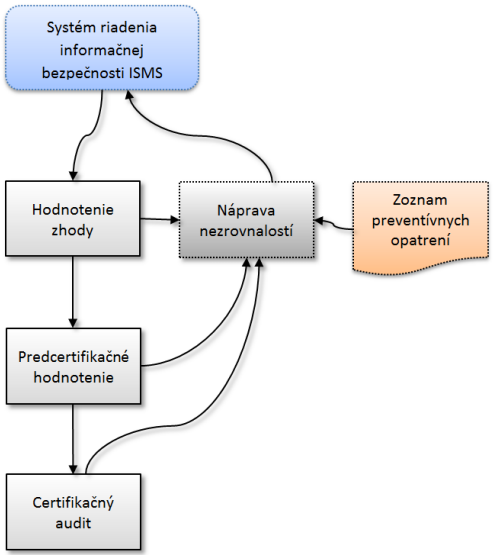
Pre účely vykonávania kontrol a auditov musí byť o ISMS k dispozícii dostatok informácií. Tieto informácie sú získané na základe politík, štandardov, procedúr a doporučení a následne sú spracovávané a vyhodnotené. Prevádzkové informácie môžu tvoriť bezpečnostné logy z prístupových systémov, firewallov, konfiguračných súborov, zo získanej sieťovej infraštruktúry a výstupov z procesu hodnotenia rizík. V stručnosti ide o evidenciu všetkých činností a udalostí, ktoré môžu mať dopad na ISMS.

Predcertifikačné hodnotenie alebo tiež prvá úroveň certifikácie systému riadenia informačnej bezpečnosti sa uskutočňuje pre stabilizáciu systému a poskytuje nezávislý pohľad na fungovanie ISMS a pokrytie rozsahu definovaného v etape plánovania.

Certifikačný audit je najdôkladnejšie overenie ISMS v súlade s ISO/IEC 27001. Výsledkom je tvrdenie, ktoré potvrdí, že systém riadenia informačnej bezpečnosti je implementovaný v zhode s ISO/IEC 27001. Pokiaľ príde pri kontrole zhody k zisteniu nedostatkov, sú tieto nezhody následne odstránené vo fázy udržovania a zlepšovania ISMS. [13]

2.4 Udržovanie a zlepšovanie ISMS

Poslednou fázou v PDCA modely je udržovanie a zlepšovanie ISMS. Úlohou tejto fázy je vyhodnotiť výsledky auditu a kontrol funkčnosti implementovaných bezpečnostných opatrení a tiež vyhodnotenie i samotného ISMS a dať podnet k naštartovaniu ďalšieho PDCA modelu, v ktorom budú naplánované, implementované, skontrolované a znovu vyhodnotené všetky nápravné a preventívne opatrenia. Obrázok č. 11. zobrazuje poslednú fázu, ktorá je naviazaná na všetky hodnotenia systému riadenia informačnej bezpečnosti. [13]



Obr. 11. Udržovanie a zlepšovanie ISMS [13]

Proces udržovania a zlepšovania ISMS pokračuje v zladení s obchodnými požiadavkami, rizikami a možnosťami informačnej bezpečnosti. Spoločne so systémami riadenia kvality poskytuje vedeniu organizácie možnosť systematicky riadiť procesy informačnej bezpečnosti. [13]

2.5 Požiadavky na dokumentáciu

Systém ISMS rozlišuje dva druhy dokumentácie:

- povinnú – dokumentácia, ktorú norma taxatívne požaduje,
- nepovinnú – pomocná dokumentácia, ktorú norma nespomína a ktorá popisuje niektoré konkrétne činnosti. [12]

Riadenie dokumentov

Dokumenty požadované ISMS musia byť chránené a riadené. Musí byť vytvorený dokumentovaný postup tak, aby vymedzil riadiace činnosti potrebné k:

- schvaľovaniu obsahu dokumentov pred ich vydaním,
- preskúmaniu dokumentov, prípadne k ich aktualizácii a opakovanému schvaľovaniu,
- zaisteniu identifikácie zmien dokumentov a aktuálneho stavu revízie dokumentov,
- zaisteniu dostupnosti príslušných verzií aplikovateľných dokumentov v mieste ich používania,
- zaisteniu čitateľnosti a ľahkosti identifikovateľnosti dokumentov,
- zaisteniu dostupnosti dokumentov pre všetkých, ktorý ich potrebujú, zaistenie prenášania, ukladania a likvidácie dokumentov v súlade s postupmi odpovedajúcimi ich klasifikácii,
- zaisteniu identifikácie dokumentov externého pôvodu,
- zaisteniu riadenej distribúcie dokumentov,
- zabráneniu neúmyselného použitia zastaraných dokumentov,
- aplikovaniu ich vhodnej identifikácie pre prípad ďalšieho použitia. [29]

3 CERTIFIKÁCIA ISMS PODĽA ISO 27001

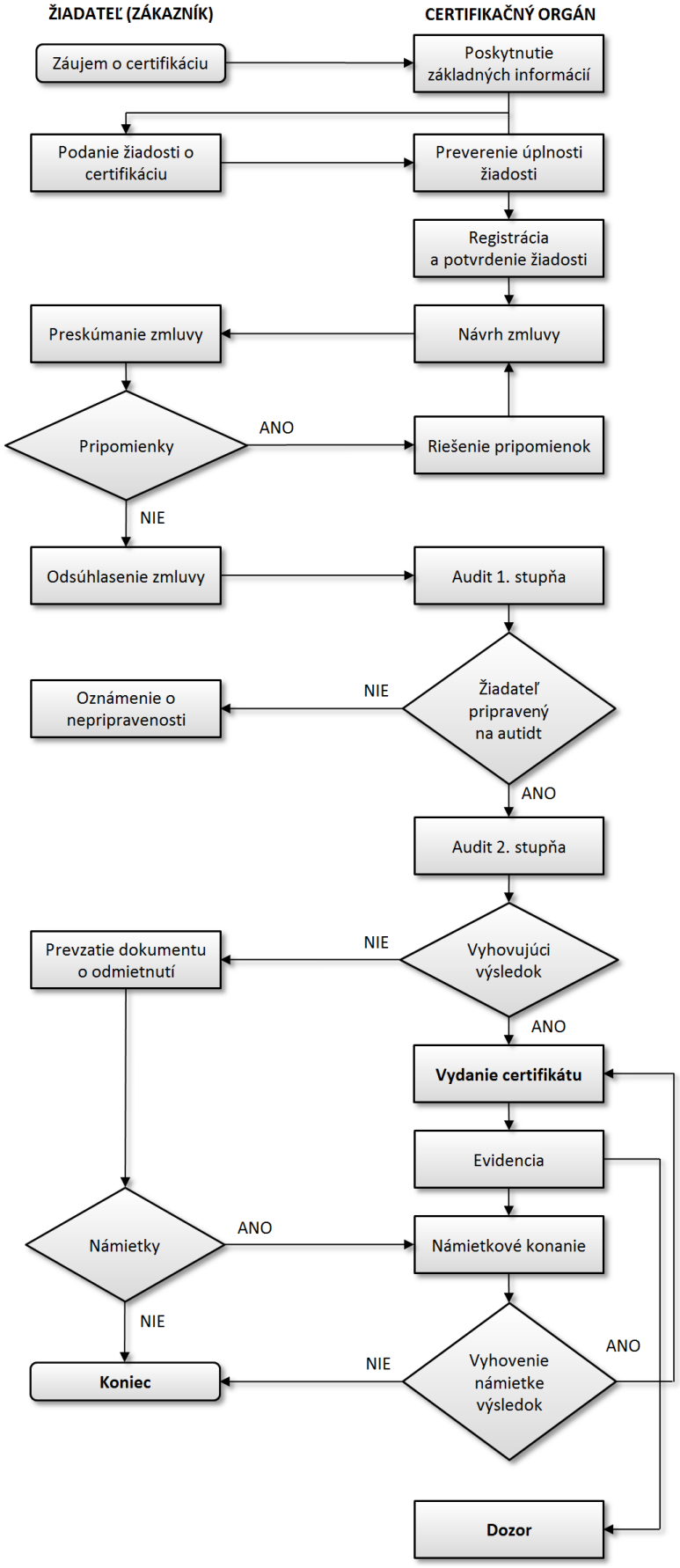
Certifikácia, inak nazývaná aj posudzovanie zhody, je definovaná ako akcia, ktorá je vykonávaná nezávislou treťou stranou, ktorá osvedčuje, že existuje dostatok dôvery, že príslušne označený výrobok, postup alebo služba je v zhode s určitou normou. [30]

Proces posúdenia, či realizovaná implementácia ISMS odpovedá požiadavkám štandardu ISO 27001 je označovaný pojmom ***certifikačný audit ISMS***. Pozitívny výsledok certifikačného auditu je predovšetkým známkou úrovne manažmentu bezpečnosti informácií v smere úplnosti, efektivity implementácie, celistvosti vo vzťahu k riadeniu bezpečnosti informácií. [31]

Certifikácia ISMS je objektívnym dôkazom, prostredníctvom ktorého vlastníci a manažment certifikovanej organizácie potvrdzujú, že vnímajú nielen zodpovednosť k bezpečnosti informácií, ale tiež deklarujú naplňovanie svojho záväzku, že uplatňované zásady v správaní a prístupu k bezpečnosti informácií sú súčasťou podnikania. [32]

Certifikácia ISMS podľa ISO 27001 prináša mnohé výhody, pričom niektoré z nich môžu byť:

- zabezpečenie informácií je integrálnou časťou celého systému riadenia organizácie,
- hlavné faktory ovplyvňujúce podnikateľskú súťaž, informácie a ich zabezpečenie je v riadenom režime,
- preukázanie prístupu k manažmentu bezpečnosti informácie a to aj v komunikácii so zákazníkmi, investormi, občianskou verejnosťou, štátnymi i súkromnými inštitúciami a ďalšími stranami,
- sprehľadnenie dôsledkov incidentov a ich zníženie, odhaľovanie rizík, nezhôd a incidentov s nežiaducimi dopadmi na dôvernosť, integritu a dostupnosť informácií a tým aj na chod organizácie,
- zvýšenie podnikateľskej dôveryhodnosti pre investorov, banky a poisťovne,
- úspora na pokutách a iných sankciách, ktoré sú spojené s únikom informácií. [32]



Obr. 12. Vývojový diagram certifikácie ISMS [33]

3.1 Prípravná časť certifikačného auditu

Ak sa organizácia rozhodne získať certifikát podľa normy ISO 27001 je potrebné, aby v prvom kroku kontaktovala certifikačný orgán a podala nezáväznú ***Žiadosť o zostavenie ponuky na certifikáciu ISMS***. Oslovený certifikačný orgán žiadosť prešetrí a následne organizácia dostane ***Cenovú ponuku na certifikáciu ISMS***. Pokiaľ je cenová ponuka prijateľná, podá organizácia záväznú Žiadosť o certifikáciu ISMS. Na základe tejto žiadosť je organizácii pridelené registračné číslo – ***Oznámenie o zaregistrovaní žiadosti*** a je uzatvorená ***Zmluva o certifikácii ISMS***. [30]

Pre vykonanie certifikácie je nutné, aby organizácia poskytla nasledovné doklady:

- základné smernice ISMS,
- právne normy a predpisy týkajúce sa predmetu certifikovanej činnosti,
- politiku ISMS/prehlásenie o aplikovateľnosti,
- register dôležitých rizík,
- program/y ISMS. [30]

Doručením týchto dokladov organizácia splní požiadavky pre ďalší postup certifikácie. V prípade, že doklady pre certifikáciu nie sú kompletné, certifikačný orgán oznámi organizácii a prehodnotí s ňou ďalší možný postup. [30]

3.2 Samotný proces certifikácie ISMS

Proces certifikácie ISMS pozostáva z nasledujúcich etáp:

I. etapa auditu

Po odovzdaní a prehodnotení všetkých potrebných dokumentov vypracuje a odsúhlasí certifikačný orgán spolu s organizáciou ***Plán I. etapy auditu*** a ***Termín I. etapy auditu***. Cieľom prvej etapy auditu je posúdiť pripravenosť organizácie na certifikačný audit a objaviť nezhody, ktoré by mohli zamedziť alebo inak obmedziť ďalší výkon certifikácie. V prípade, ak sa počas tejto fázy auditu zistia nezhody, musia byť odstránené v stanovenej lehote. Zistenia z auditu sú spracovávané certifikačným orgánom a zasielané organizácii v ***Protokole z I. etapy auditu***. [30]

II. etapa auditu (certifikačný audit)

V rámci tejto fáze auditu sa vypracuje a schváli ***Plán. II. etapy auditu*** a ***Termín II. etapy auditu***. Cieľom tejto etapy je potvrdenie, že:

- organizácia dodržiava stanovené postupy a napĺňa svoju politiku ISMS,
- organizácia dosahuje stanovené ciele a hodnotí riziká,
- systém zodpovedá všetkým požiadavkám ISO 27001.

Výsledkom II. etapy auditu je ***Protokol z II. etapy auditu ISMS***. [30]

Vydanie certifikátu

Ak certifikačný orgán potvrdí súlad ISMS so štandardom je spoločnosti odovzdaný certifikát s platnosťou 3 roky. V prípade, ak boli počas auditu zistené nezrovnalosti, ktoré je možné odstrániť do 3 mesiacov, je certifikát odovzdaný po ich odstránení. V prípade, že nie je možné odovzdať certifikát do 3 mesiacov po vykonaní certifikačného auditu, musí byť vykonaný nový certifikačný audit po odstránení nezrovnalostí. [30]

3.3 Dozorná činnosť

V priebehu platnosti certifikátu sú certifikačným orgánom v plánovaných termínoch uskutočňované pravidelné dozorné audity, ktorých cieľom je zistiť, či certifikovaná organizácia plní a má i naďalej predpoklady plniť požiadavky normy ISO 27001. Dozorné audity sú vykonávané aspoň raz za rok. Dátum prvého dozorného auditu nasledujúceho po prvotnej certifikácii nesmie byť stanovený neskôr ako 12 mesiacov od posledného dňa II. etapy auditu. [34]

Program dozoru bežne zahŕňa nasledujúce oblasti:

- interné audity a preskúmanie manažmentu,
- preskúmanie opatrení prijatých pre odstránenie nezhôd identifikovaných v priebehu predchádzajúceho auditu,
- vyšetrenie sťažností,
- súčinnosť ISMS s ohľadom na dosahovanie cieľov certifikovaného zákazníka,
- postup plánovaných činností, ktorých cieľom je trvalé zlepšovanie,
- trvalé prevádzkové riadenie,

- preskúmanie všetkých zmien,
- používanie značiek a/alebo iných odkazov na certifikáciu. [34]

3.4 Recertifikácia

Ak má certifikovaná organizácia záujem o pokračovanie certifikácie a dodržiava podmienky dozoru, musí sa pol roku pred ukončením platnosti certifikátu prihlásiť u certifikačného orgánu k opakovanej certifikácii – recertifikácii. [33]

Postup recertifikácie je zhodný s postupom certifikácie s tým rozdielom, že audit zahŕňa len jeden stupeň, za predpokladu, že je opakované posúdenie uskutočnené ešte v dobe platnosti súčasného certifikátu (t.j. pred vypršaním platnosti). [34]

II. PRAKTICKÁ ČASŤ

4 SPOLOČNOSŤ PROTHERM PRODUCTION S. R. O.

Nami zvolená spoločnosť je Protherm Production s.r.o. Skalica, ktorá je popredným výrobcom vykurovacej techniky pre 24 trhov Európy, Ázie a Afriky. Firma Protherm Production bola založená v roku 1991 pod názvom Transkom, pričom pôvodne bola len predajnou spoločnosťou. V roku 1999 sa výroba vykurovacích zariadení vyrábaná v spoločnosti Didaktik, vrátane zamestnancov, presťahovala do výrobného závodu Protherm. V súčasnosti má firma 483 zamestnancov a je členom medzinárodnej spoločnosti Vaillant Group, ktorá zahŕňa 10 výrobných závodov v Európe a Ázii. Na úspech firmy má kľúčový vplyv kvalita používaných technológií, vysoká úroveň výrobného a vývojového procesu, logistiky či prístupu k zamestnancom. [35]

Výrobná paleta spoločnosti zahŕňa:

- plynové kotly,
- plynové prietokové ohrievače,
- elektrické kotly a konvektory,
- kotly na tuhé palivo,
- solárne systémy,
- zásobníky teplej vody,
- regulačná technika,
- príslušenstvo. [35]

V súčasnosti sa vo firme ročne vyrobí okolo 360 000 kotlov, pričom medzi top produkty patria plynové nekondenzačné a kondenzačné kotly, ktoré putujú do rôznych krajín Európy, Ázie či Afriky, najviac však do Nemecka, Ruska a Talianska. [35]

Okrem montáže hotových produktov je spoločnosť zameraná aj na:

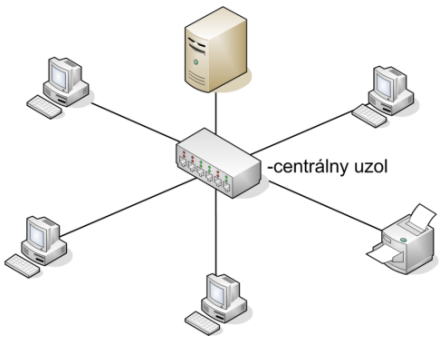
- výrobu plechov lisovaním,
- práškovanie komponentov,
- výrobu plynových ventilov,
- predmontáž komponentov použitím technológie klinčovania. [35]

Za úspechom spoločnosti stojí aj fakt, že sa pýši jedným z najmodernejších vývojových centier v Európe s výkonnými pracovnými stanicami, moderným laboratóriom a kvalitnou technikou. Členovia vývojového tímu sa primárne podieľajú na inováciách súčasných kotlov a zavádzaní nových výkonnejších modulov. [35]

4.1 Analýza informačného systému spoločnosti

Vo firme sa nachádza 110 pracovných staníc a 8 serverov. Na všetkých pracovných staniciach a notebookoch beží operačný systém Windows 7 Enterprise, pričom aktualizácie softvéru a operačného systému uvoľňuje a koordinuje externá firma Hewlett Packard (HP). Pracovné stanice siete sú pripojené k centrálnemu uzlu samostatnými linkami, čo znamená, že topológia lokálnej siete je hviezdicová. Schému hviezdicovej topológie môžeme vidieť na obrázku č. 13.

Ďalej spoločnosť vlastní päť sieťových tlačiarní značky Konica minolta C360SeriesPCL a jeden Ploter-HP DesignJet 120NR.



Obr. 13. Hviezdicová topológia [36]

Pre prácu využíva spoločnosť predovšetkým MS SharePoint, MS Outlook a MS Office 2007 v základnom balíku. Pre individuálne požiadavky je možné tento balík rozšíriť o MS Lync a MS Project. Na pracovných staniciach oddelenia vývoja je nainštalovaný program PTC Creo, ktorý je využívaný k vyhotovovaniu a dopĺňaniu výkresovej dokumentácie.

Pre skladové hospodárstvo, plánovanie výroby, zásobovanie, účtovníctvo, evidenciu dodávateľov sú v súčasnosti nasadené moduly SAP, ktoré sú ďalej využívané na správu dodávaných komponentov a kusovníkov.

V najbližších rokoch je plánovaná implementácia PLM Windchill, ktorý zachytáva proces riadenia životného cyklu jednotlivých výrobkov. Pre manažment a evidenciu pracovných staníc, notebookov a licencií sa využíva aplikácia AuditPro, ktorá umožňuje ľahkú a rýchlu kontrolu.

IT infraštruktúra spoločnosti sa musí používať výlučne na oficiálne firemné účely s výnimkou ďalšieho výslovne dovoleného osobného požívania.

4.2 Všeobecné pravidlá bezpečnosti definované v spoločnosti Protherm production s. r. o.

Infraštruktúra IT spoločnosti Protherm Production je spravovaná centrálne spoločnosťou VAICON a od 1. Mája 2006 ju prevádzkuje spoločnosť Hewlett Packard. Údaje uložené na osobných počítačoch, ktoré patria do infraštruktúry IT skupiny Vaillant sú vlastníctvom skupiny Vaillant. Zamestnancom sa udeľuje právo používať infraštruktúru IT, ktorá je potrebná na realizáciu ich pracovnej činnosti. Uvedené užívacie právo je časovo obmedzené. Pravidlá bezpečnosti definované v spoločnosti Protherm Production sú technicky zabezpečené divíziou Vaillant Group IT. V prípadoch, kedy nie je technické zabezpečenie možné, je zamestnanec povinný sa postarať o realizáciu uvedených pravidiel. [37]

4.2.1 Fyzická bezpečnosť

Každý zamestnanec je povinný pýtať sa hocijakej neznámej alebo podozrivej osoby v priestoroch spoločnosti, ktorú považujú za bezpečnostné riziko, na dôvoď ich prítomnosti. Po skončení práce, resp. počas dlhšej neprítomnosti sa musia dvere kancelárií podľa možnosti zamykať.

4.2.2 Pracovný počítač

Pri opustení pracoviska (aj na krátky čas) sa PC musí uzamknúť (kombináciu kláves Ctrl+Alt+Del, alebo Windows+L). Táto povinnosť platí aj vtedy, ak používateľ opustí kanceláriu.

Rozlišujeme tri štandardné modely:

- stolný počítač pre kancelárske prostredie,
- notebook pre mobilné prostredie,
- pracovná stanica CAD, ktorá vyhovuje náročným požiadavkám.

Zamestnanec je po ukončení práce povinný vypnúť, resp. odstaviť tie zariadenia, ktoré už nepoužíva. Tým sa znižuje požiarne zaťaženie spôsobené zapnutým zariadením a celková spotreba elektrickej energie.

Aby bol k dispozícii vopred definovaný postup a vopred zaručená časová doba reakcie na zlyhanie, automaticky sa pracovná stanica objednáva s 3 až 4 ročnou zárukou.

Programové vybavenie a licencie

Všetky programové prostriedky používané na PC musia byť zakúpené a legálne poskytnuté a musia mať platnú licenciu, t.j. uvedené programové prostriedky sa budú inštalovať iba na tie počítače, na ktoré sa vzťahuje príslušná licencia.

Všetky počítače v spoločnosti majú antivírusové programové vybavenie od spoločnosti Symantec, ktorý sa automaticky aktualizuje. Uvedený program sa nesmie deaktivovať ani odstraňovať z počítača, nakoľko predstavuje prvotnú ochranu proti škodlivým programovým prostriedkom.

Dáta

Dáta, ktoré vyžadujú vyšší stupeň ochrany sú označované ako „dôverné alebo osobné“. Tieto sa musia uchovávať v zašifrovanej podobe. Rovnako toto pravidlo platí aj pre interne zálohované dáta.

Zálohovanie dát

Každý používateľ zodpovedá za ukladanie lokálnych dát na svojom počítači. Zálohy sa musia vykonávať na externé zariadenia (externý disk, externý server, DVD-ROM atď.), ktoré sú vo vlastníctve spoločnosti Protherm Production. Výslovne je zakázané používanie tzv. cloudových služieb ako napr. Dropbox a iných.

4.2.3 Nosiče dát

Externé nosiče dát, ako USB flash disky, ktoré sú vo vlastníctve Protherm Production je možné pripájať iba v prípade, ak nie je vírusová databáza staršia ako tri dni. Používanie akýchkoľvek prenosných nosičov dát je dovolené len na počítačoch pripojených do siete, ak je nosič dát majetkom spoločnosti alebo ak bol poskytnutý obchodnými partnermi na použitie súvisiace s činnosťou spoločnosti. Nosiče dát vo vlastníctve spoločnosti sa nesmú používať na súkromné účely.

4.2.4 Elektronická pošta a internet

Spoločnosť Protherm Production poskytuje svojím zamestnancom program elektronickej pošty (e-mailový klient) MS Outlook ako aj interný a externý prístup k elektronickej pošte a k používaniu internetu.

Používanie elektronickej pošty si musia byť zamestnanci vedomí skutočnosti, že správy elektronickej pošty sú obchodnými dokumentmi rovnako ako každý list, fax, obežník alebo

správa. Správy elektronickej pošty, ktoré odchádzajú zo spoločnosti, budú zvonka implicitne rozpoznávané ako odoslané zo spoločnosti aj vtedy, keď sa v správe nenachádza nič, čo by na túto skutočnosť poukazovalo – teda majú rovnakú dôležitosť ako iné obchodné listy. Z toho vyplýva, že uvedené správy elektronickej pošty musia byť vybavené aktuálnym e-mailovým podpisom.

Používanie elektronickej pošty

V podniku je pre e-mailovú komunikáciu používaný program MS Outlook, pričom pre synchronizáciu pošty a udalostí z kalendára je využívaný softvér MS Exchange. Za žiadnych okolností nie je dovolené odosielať správy elektronickej pošty, ktorých obsah sa môže považovať za urážlivý, hanlivý, rasistický atď.

Preposielanie správ elektronickej pošty z firemného účtu elektronickej pošty na adresy elektronickej pošty bez súvisu s oficiálnou činnosťou je zakázané. Každá správa elektronickej pošty, ktorá odchádza zo spoločnosti Protherm Production musí obsahovať e-mailový podpis s údajmi o spoločnosti.

Internet

Spoločnosť Protherm Production poskytuje svojím zamestnancom ako pracovný nástroj sieťový prístup do internetu prostredníctvom programu Internet Explorer. Prístup do internetu sa spravidla poskytuje na firemné účely (vyhľadávanie a komunikácia súvisiaca s oficiálnou činnosťou spoločnosti). Na zabezpečenie podnikovej siete používa spoločnosť Protherm Production bezpečnostné mechanizmy, ako sú firewally, webové filtre a antivírusové programy. Používanie internetu zamestnancami na súkromné účely je prísne zakázané.

4.2.5 Servery

Serverová infraštruktúra je zabezpečená externou firmou. V spoločnosti sa nachádza osem serverov ProLiant DL380 G5 od spoločnosti HP. Niektoré servery sú fyzické, iné sú len virtuálne, čo znamená, že majú svoj hlavný operačný systém MS Windows Server a za pomoci virtualizácie je skrz neho spustený MS Hyper-V.

Rozlišujeme dva typy serverov:

- servery infraštruktúry,
- aplikačné servery.

Servery infraštruktúry poskytujú technickú funkčnosť, napr. prihlasovanie, prístup do siete, tlač, ukladanie súborov, atď., nebežia však na nich obchodné aplikácie Protherm Production, keďže tieto spravujú príslušné aplikačné servery.

Záložný zdroj UPS

Servery infraštruktúry sú zabezpečené proti výpadku prúdu UPS záložným zdrojom od firmy APC. UPS je zariadenie, ktoré zaisťuje dodávku elektrickej energie pre zariadenia, ktoré nesmú byť vypnuté. Zdroj funguje ako akumulátor – pokiaľ nie je dodávka elektriny z primárneho zdroja prerušená, je batéria udržovaná v nabitom stave. V okamihu prerušenia dodávky elektriny zaisťuje napájanie zariadenia až do obnovenia napätia alebo do svojho vybitia.

Umiestnenie serverov

Serverovňa sa nachádza v administratívnej budove na druhom nadzemnom podlaží. Pre správu hardvéru a softvéru sú určení dvaja pracovníci HP a jeden zamestnanec spoločnosti. Prístup do serverovne je obmedzený pomocou kľúča. Serverovňa je vybavená vlastnou klimatizáciou. Každý server spolu s rozvádzačom HP Procurve 4202VL je umiestnený v rackovej skrini. Racková skriňa je oceľová konštrukcia s presne danými rozmermi, jedná sa o špeciálny systém pre montáž a prepojovanie jednotlivých serverových komponentov do jednej štruktúry, ktorú možno jednoducho pripojiť do siete. Skriňa je uzamknutá, kľúč vlastní správca siete a prístup do skrine je obmedzený.

Zálohovanie serverov

Vďaka nízkej cene médií a dlhodobej životnosti sa zálohy vykonávajú na magnetické pásky. Na takéto zálohovanie sa využíva v spoločnosti zálohovacia mechanika HP DAT72. Na zálohovanie sa využívajú technológie LTO-2, LTO-3 a LTO-4.

4.2.6 Budova firmy

V spoločnosti Protherm Production, a v jej okolí je nainštalovaný kamerový monitorovací systém na sledovanie pohybu v objekte spoločnosti a v jej bezprostrednom okolí. Na evidenciu zamestnancov je použitý vstup prostredníctvom karty zamestnanca.

5 ANALÝZA RIZÍK V SPOLOČNOSTI

Pre lepšie spoznanie vonkajších ale aj vnútorných faktorov, ktoré majú v organizácii vplyv na informačnú bezpečnosť sme vytvorili SWOT analýzu. Podstatou tejto analýzy je identifikovať kľúčové ***silné a slabé stránky*** vo vnútri, teda v čom je organizácia (alebo jej časť) dobrá a v čom naopak zlá. Rovnako je dôležité identifikovať kľúčové ***príležitosti a hrozby***, ktoré sa nachádzajú v okolí, teda vo vonkajšom prostredí.

SWOT analýza zameraná na zhodnotenie súčasného stavu informačnej bezpečnosti v spoločnosti bola vykonaná pred analýzou rizík, s cieľom aby bola pozornosť upriamená na zvýšenie silných stránok a príležitostí a na redukciu hrozieb a slabých stránok.

Údaje pre SWOT analýzu boli poskytnuté formou diskusie s pracovníkom IT oddelenia spoločnosti. Vo všeobecnosti platí, že SWOT analýza sa skladá z dvoch častí, pričom každá má dve podčasti:

- ***interná časť*** – silné a slabé stránky,
- ***externá časť*** – príležitosti a hrozby.

Pri definovaní interných faktorov sme sa zamerali priamo na našu spoločnosť, pričom sme popísali v čom sme na jednej strane dobrý a na druhej strane sme popísali to čo sa nám nedarí a vyžaduje si našu pozornosť. Zjednodušene povedané sme vytvorili zoznam „pro a proti“.

Externá časť analýzy bola zameraná na naše okolie, ktoré sami môžeme len ťažko ovplyvniť, ale ktoré výrazne môže ovplyvniť nás. Preto sú na jednej strane popísané príležitosti, ktoré nám naše okolie poskytuje a na druhej strane hrozby, ktoré nás z okolia ohrozujú.

Po zadefinovaní všetkých štyroch faktorov sa tieto usporiadajú do tzv. SWOT matice, ktorá predstavuje koncepčný rámec pre systematickú analýzu dát a uľahčuje ich porozumenie a porovnanie.

Z uvedených faktorov vyplýva, že silné stránky spoločnosti prevažujú nad slabými a tak isto aj príležitosti nad hrozbami. Na základe čoho môžeme pre spoločnosť zvoliť stratégiu, v rámci ktorej pomocou silných stránok využije príležitosti poskytovaných externým prostredím. Nemôžeme však zabúdať aj na slabšie stránky a vyhýbanie sa potenciálnym hrozbám, resp. rizikám.

Silné stránky	Slabé stránky
STRENGTS	WEAKNESSES
Podpora materskej firmy v Nemecku	Neodbornosť nových zamestnancov
Kvalifikovaný a skúsený tým ľudí	Obmedzená vôľa pri rozhodovaní
Jasné, prehľadné a popísané procesy	Skryté náklady
Kvalitná technologická základňa	Nedostatok zdrojov
Príležitosti	Ohrozenia
OPPORTUNITIES	THREATS
Využitie noriem a štandardov	Snaha o poškodenie aktív
Prístup manažmentu k fondom EÚ	Bezpečnostné riziká vo vzťahu k ITC
Pákový efekt IT pre skupinu (SharePoint)	Neautorizované použitie systému
Zabezpečovacia technológia šifrovania	Krádež identity

Tab. 8. SWOT matica

5.1 Ohodnotenie aktív spoločnosti Protherm Production

Prvým krokom v rámci analýzy rizík je ohodnotenie aktív spoločnosti v rámci ISMS. Zoznam aktív sme získali na základe diskusie so zamestnancom IT oddelenia spoločnosti a vedením.

V rámci organizácie bolo identifikovaných 27 aktív súvisiacich s informačnou bezpečnosťou, ktoré sme hodnotili z hľadiska dostupnosti, dôvernosti a integrity. Pre každý hodnotený aspekt sme použili stupne miery ohrozenia v rozmedzí od 1 do 5, pričom 5 predstavuje najväčšiu mieru ohrozenia. Výslednú váhu aktíva sme získali pomocou vzorca (1) popísaného v kapitole 2.1.1.

Skupina aktíva	Aktívum	Zdroj	Do	Dô	Int	Váha
Know - how	Výkresy v el. forme	PC zamestnancov	3	3	3	3
	Pracovné postupy	PC zamestnancov	4	5	4	4
	Rozpracované projekty	Intranet	3	4	3	3
	Ukončené projekty	Intranet	3	4	3	3
	Zálohy serverov	Serverovňa	5	5	5	5

Tab. 9. Ohodnotenie aktív v organizácii

Komunikácia	Podniková sieť (kabeláž)	Celý areál podniku	5	5	5	5
	Switche HP	Budova firmy	4	3	5	4
	Routery HP	Budova firmy	4	3	5	4
Softvér	Windows 7	PC zamestnancov	5	5	5	5
	Creo	PC zamestnancov	2	3	2	2
	Internet Explorer	PC zamestnancov	5	4	3	4
	SAP	PC zamestnancov	5	5	5	5
	Microsoft Office	PC zamestnancov	5	5	5	5
Hardvér	Pracovné stanice	Kancelárie	5	5	5	5
	Tlačiarne	Chodby	1	1	1	1
	Plotter	Kancelária vývoja	1	1	1	1
	Servery	1.NP , 2.NP	5	5	5	5
	Notebooky	Kancelárie	1	3	2	2
	Tablety	Kancelárie	1	3	2	2
	Smartfóny	Zamestnanci	3	3	3	3
Zamestnanci	Zmluvy so zamestnancami	Personálne oddelenie	5	5	5	5
Zákazníci	Objednávky zákazníkov	Oddelenie nákupu	5	5	5	5
	Databáza zákazníkov	Oddelenie nákupu	3	2	3	3
Dodávatelia	Objednávky dodávateľov	Oddelenie nákupu	4	4	4	4
	Databáza dodávateľov	Oddelenie nákupu	3	2	3	3
Image firmy	Web stránka	Externý poskytovateľ webhostingu	2	2	2	2
	Budova firmy	Skalica	5	5	5	5

Pokračovanie Tab. 9. Ohodnotenie aktív v organizácii

5.2 Identifikácia hrozieb

Počas konzultácie s IT oddelením a nahliadnutím do príkladných hrozieb, ktoré sú uvedené v norme ISO/IEC 27005 sme identifikovali možné hrozby a popis súvisiacich zraniteľností. Každej hrozbe bola pridelená miera pravdepodobnosti podobne ako pri hodnotení aktíva, pričom sme použili rovnakú stupnicu.

Typ	Hrozba	Popis	Váha
Technické zlyhanie	Poškodenie sieťových prvkov	Nevhodné umiestnenie	2
	Preťaženie prevádzky	Nestabilná dodávka energie	2
	Výpadok LAN	Vysoké požiadavky sieťových aplikácií	2
	Výpadok serveru	Poškodenie/aktualizácia sieťových prvkov	3
	Zlyhanie HW	Nedostatočná údržba	5
Strata základných služieb	Výpadok elektriny	Zlyhanie prenosovej sústavy	2
	Zlyhanie komunikačných služieb	Zlyhanie telekomunikačného zariadenia	2
Prírodné udalosti	Povodeň	Umiestnenie v oblasti kde hrozí záplava	1
Ohrozenie informácií	Krádež	Nedostatočná ochrana budovy, dokumentov	4
Ohrozenie funkčnosti	Malware	Neaktualizovaný AV	3
	Zlyhanie SW	Nesprávne použitie	2
	Zneužitie oprávnenia	Nesprávne pridelenie prístupov	4
Neoprávnené činnosti	Poškodenie dát	Neúmyselná modifikácia	1

Tab. 10. Zoznam hrozieb spolu s popisom a váhou pravdepodobnosti

5.3 Matica zraniteľností

Na základe definovania aktív a ich hodnoty (A) a definovania pravdepodobnosti hrozieb (T) sme vytvorili maticu zraniteľností. Každému aktívu bola pridelená miera pravdepodobnosti zraniteľnosti danou hrozbou, pričom tieto boli hodnotené stupnicou od 1 do 5. Zraniteľnosť danou hrozbou nemusí ovplyvňovať všetky aktíva spoločnosti.

	Popis aktíva		Výkresy v el. forme	Pracovné postupy	Rozpracované projekty	Ukončené projekty	Zálohy serverov	Podniková sieť (kabeláž)	Switche HP	Routery HP	Windows 7
Popis hrozby	**T**	**A**	3	4	3	3	5	5	4	4	5
Poškodenie sieťových prvkov	2							4	2	2	
Preťaženie prevádzky	2							1	2	2	
Výpadok LAN	2							2	2	2	
Výpadok serveru	3		2	2	2	3	4				
Zlyhanie HW	5							2	2	2	
Výpadok elektriny	2								2	2	
Zlyhanie komunikačných služieb	2										
Povodeň	1								1	1	
Krádež	4			2			3		2	2	
Malware	3										2
Zlyhanie SW	2										4
Zneužitie oprávnenia	4										3
Poškodenie dát	1		2	2	3	2	4				2

Tab. 11. Matica zraniteľností časť 1.

	Popis aktíva		Creo	Internet Explorer	SAP	Microsoft Office	Pracovné stanice	Tlačiarne	Plotter	Servery	Notebooky
Popis hrozby	**T**	**A**	2	4	5	5	5	1	1	5	2
Poškodenie sieťových prvkov	2									4	
Preťaženie prevádzky	2						3	1	1	5	1
Výpadok LAN	2		3	1	2	2	3	1	1	3	
Výpadok serveru	3							1	1	5	
Zlyhanie HW	5						5	2	2	2	1
Výpadok elektriny	2						3	1		5	1
Zlyhanie komunikačných služieb	2										
Povodeň	1						1	1	1		1
Krádež	4						1	1	1		2
Malware	3		1	5	1	1					
Zlyhanie SW	2		4	3	4	3					
Zneužitie oprávnenia	4		3	1	4	4					
Poškodenie dát	1		1	1	2						

Tab. 12. Matica zraniteľností časť 2.

	Popis aktíva		Tablety	Smartfóny	Zmluvy so zamestnan-cami	Objednávky zákazníkov	Databáza zákazníkov	Objednávky dodávate-ľov	Databáza dodávateľov	Web stránka	Budova firmy
Popis hrozby	**T**	**A**	2	3	5	5	3	4	3	2	5
Poškodenie sieťo-vých prvkov	2										
Preťaženie pre-vádzky	2										
Výpadok LAN	2										
Výpadok serveru	3										
Zlyhanie HW	5		1	1							
Výpadok elektriny	2										3
Zlyhanie komuni-kačných služieb	2										
Povodeň	1		1	1							2
Krádež	4		1	1	2						
Malware	3										
Zlyhanie SW	2										
Zneužitie oprávnenia	4										
Poškodenie dát	1				3	3	3	3	3	1	

Tab. 13. Matica zraniteľností časť 3.

Identifikáciou zraniteľností sme zistili slabiny určitého aktíva vo vzťahu k:

- fyzickému prostrediu,
- zamestnancom,
- programovému a technickému vybaveniu počítača.

5.4 Matica rizík

Z matíc zraniteľností sme následne zostavili matice rizík. Tieto riziká boli vypočítané ako súčin hodnoty aktíva, pravdepodobnosti hrozby a pravdepodobnosti rizika.

	Popis aktíva		Výkresy v el. forme	Pracovné postupy	Rozpracované projekty	Ukončené projekty	Zálohy serverov	Podniková sieť (kabeláž)	Switche HP	Routery HP	Windows 7
Popis hrozby	**T**	**A**	3	4	3	3	5	5	4	4	5
Poškodenie sieťových prvkov	2							40	16	16	
Preťaženie prevádzky	2							10	16	16	
Výpadok LAN	2							20	16	16	
Výpadok serveru	3		18	24	18	27	60				
Zlyhanie HW	5							50	40	40	
Výpadok elektriny	2								16	16	
Zlyhanie komunikačných služieb	2										
Povodeň	1								4	4	
Krádež	4			32			60		32	32	
Malware	3										30
Zlyhanie SW	2										40
Zneužitie oprávnenia	4										60
Poškodenie dát	1		6	8	9	6	20				10

Tab. 14. Matica rizík časť 1.

	Popis aktíva		Creo	Internet Explorer	SAP	Microsoft Office	Pracovné stanice	Tlačiarne	Plotter	Servery	Notebooky
Popis hrozby	**T**	**A**	2	4	5	5	5	1	1	5	2
Poškodenie sieťových prvkov	2									40	
Preťaženie prevádzky	2						30	2	2	50	4
Výpadok LAN	2		12	8	20	20	30	2	2	30	
Výpadok serveru	3							3	3	75	
Zlyhanie HW	5						125	10	10	50	10
Výpadok elektriny	2						30	2		50	4
Zlyhanie komunikačných služieb	2										
Povodeň	1						5	1	1		2
Krádež	4						20	4	4		16
Malware	3		6	60	15	15					
Zlyhanie SW	2		16	24	40	30					
Zneužitie oprávnenia	4		24	16	80	80					
Poškodenie dát	1		2	4	10						

Tab. 15. Matica rizík časť 2.

	Popis aktíva		Tablety	Smartfóny	Zmluvy so zamestnan-cami	Objednávky zákazníkov	Databáza zákazníkov	Objednávky dodávate-ľov	Databáza dodávateľov	Web stránka	Budova firmy
Popis hrozby	**T**	**A**	2	3	5	5	3	4	3	2	5
Poškodenie sieťo-vých prvkov	2										
Preťaženie pre-vádzky	2										
Výpadok LAN	2										
Výpadok serveru	3										
Zlyhanie HW	5		10	15							
Výpadok elektriny	2										30
Zlyhanie komuni-kačných služieb	2										
Povodeň	1		2	3							10
Krádež	4		8	12	40						
Malware	3										
Zlyhanie SW	2										
Zneužitie oprá-vnenia	4										
Poškodenie dát	1				15	15	9	12	9	2	

Tab. 16. Matica rizík časť 3.

5.5 Výber vhodných opatrení pre zvládanie rizík

Matice rizík znázorňujú mieru náchylnosti aktíva na možnú hrozbu. Vypočítaním aritmetického priemeru hrozieb pri jednotlivých aktívach zistíme, ktoré sú najviac náchylné na poškodenie. Desatinné čísla sme zaokrúhlili podľa pravidiel matematiky.

Zjednotenie hodnôt časť 1.	**Aktívum**								
	Výkresy v el. forme	Pracovné postupy	Rozpracované projekty	Ukončené projekty	Zálohy serverov	Podniková sieť (kabeláž)	Switche HP	Routery HP	Windows 7
Aritmetický priemer	12	21	14	17	47	30	20	20	35

Tab. 17. Zjednotenie hodnôt časť 1.

Zjednotenie hodnôt časť 2.	**Aktívum**								
	Creo	Internet Explorer	SAP	Microsoft Office	Pracovné stanice	Tlačiarne	Plotter	Servery	Notebooky
Aritmetický priemer	12	22	33	36	40	3	4	49	7

Tab. 18. Zjednotenie hodnôt časť 2.

Zjednotenie hodnôt časť 3.	**Aktívum**								
	Tablety	Smartfony	Zmluvy so zamestnancami	Objednávky zákazníkov	Databáza zákazníkov	Objednávky dodávateľov	Databáza dodávateľov	Web stránka	Budova firmy
Aritmetický priemer	7	10	28	15	9	12	9	2	20

Tab.19. Zjednotenie hodnôt časť 3.

Pre definovanie nápravných opatrení proti zabráneniu možných hrozieb je potrebné stanoviť si stupnicu, v rámci ktorej definujeme hranice pre nízke (prijateľné), stredné a vysoké (neprijateľné) riziká, pričom:

- ***Vysoké riziko – netolerovateľné riziko***. Je potrebné urýchlene podniknúť nápravné opatrenia na zníženie rizika a vytvoriť plán zvládania rizika.
- ***Stredné riziko – významné riziko***. Opatrenia by mali byť implementované v rámci určitého časového úseku, tak aby sa riziká preniesli do nízkej kategórie.
- ***Nízke riziko – tolerovateľné riziko***. Riziko je akceptovateľné z dôvodu, že náklady na jeho riadenie nie sú úmerné škodám, ktoré by mohli vzniknúť využitím zraniteľnosti hrozbou.

Z toho vyplýva, že nápravné opatrenia by mali redukovať riziká na akceptovateľnú úroveň.

Rozsah	Stupeň rizika
0 - 20	Nízke riziko
21 - 30	Stredné riziko
31 - viac	Vysoké riziko

Tab. 20. Stupnica pre ohodnotenie rizík

Podľa doporučení normy ISO/IEC 27001 boli vybrané vhodné opatrenia pre jednotlivé skupiny aktív.

5.5.1 Opatrenia pre aktíva, ktoré môžu spôsobiť existenčné problémy organizácie

Do tejto kategórie patria tri typy aktív, a to:

- servery,
- zálohy serverov,
- pracovné stanice.

Návrh opatrení pre servery

Vo firme sa nachádzajú dva typy serverov. Servery infraštruktúry sú zabezpečené proti výpadku prúdu UPS záložným zdrojom firmy APC, pričom aplikačné servery toto zabezpečenie nemajú. Z tohto dôvodu navrhujeme dokúpenie ešte jedného záložného zdroja Smart UPS 1000 pre aplikačné servery spoločnosti.

Návrh opatrení pre zálohy serverov

Zálohy serverov sa vykonávajú na magnetické pásky. Súčasná situácia v spoločnosti je taká, že v prípade zničenia zariadenia sa dáta nedajú obnoviť. Po mesiaci sa dáta prepisujú novou zálohou. Záloha sa vykonáva každý pracovný deň a taktiež je vykonávané testovanie v pravidelných intervaloch. Manipulácia so zálohou serverov je vykonávaná externou firmou, z čoho vyplývajú nasledujúce riziká:

- poskytnutie záloh konkurencii,
- nepravidelná výmena pások,
- chýbajúca výmena pások,
- prístup k citlivým dátam.

Z tohto dôvodu navrhujeme ako dlhodobé nápravné opatrenie inštaláciu programu HP PC Connected Backup, ktorý automaticky vykonáva takého zálohy a pomáha eliminovať rizi-

ko straty dát. HP Connected Backup je súčasťou balíčka Autonomy Protect, ktorý zaisťuje archiváciu dát a ich vysokú dostupnosť, správu elektronických dát a informácií (eDiscovery), spracovanie všetkých neštruktúrovaných informácií (Enterprise Content Management), či komplexný proces integrácie a správy dát (Information governance).

Ako krátkodobé opatrenie proti poskytnutiu záloh konkurencii navrhujeme vykonávať dozornú činnosť pracovníka z lokálneho IT oddelenia.

Návrh opatrení pre pracovné stanice

Pre zaistenie dostupnosti a integrity pracovných staníc je potrebné aby boli správne udržované. V rámci spoločnosti je jednou z hlavných zložiek údržby hardvérová podpora. Pre zvýšenie bezpečnosti pracovných staníc a obmedzenie zneužitia prístupu navrhujeme častejšiu zmenu hesla, s tým, že toto heslo bude musieť spĺňať nasledujúce kritériá:

- musí mať najmenej 8 znakov,
- musí obsahovať minimálne jedno písmeno a jeden zvláštny znak (@, ?, !) alebo číslo (0,1,2, ... 9),
- musí sa líšiť od predchádzajúcich 5 hesiel,
- musí sa meniť minimálne raz za 180 dní.

5.5.2 Opatrenia pre aktíva, ktoré môžu spôsobiť ťažkosti či finančné straty organizácie

V rámci tejto kategórie sme navrhli nápravné opatrenia pre aktíva, ktoré majú v rámci skupiny najvyššiu pravdepodobnosť ohrozenia. Medzi tieto aktíva patria:

- softvér,
- podniková sieť,
- zmluvy so zamestnancami.

Návrh opatrení pre softvér

V rámci celej spoločnosti sa využíva program SAP, v rámci ktorého sú zamestnancom prideľované prístupy podľa jednotlivých oddelení. Problém vzniká pri prestupe zamestnanca na inú pracovnú pozíciu, pretože mu zostávajú oprávnenia na používanie transakcií spojených s predchádzajúcou pozíciou v spoločnosti. Z tohto dôvodu navrhujeme inštaláciu modulu SAP GRC Access Control, ktorý je primárne zameraný na užívateľov a na nastavenie ich oprávnení a riadenie celkového prístupu do vnútropodnikových systémov. Proaktívne

chráni citlivé informácie a predchádza podvodom či omylom vďaka automatizovanej kontrole rizík.

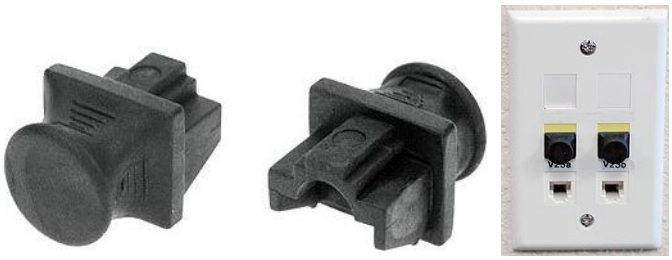
Pre internú ale aj externú komunikáciu je v spoločnosti využívaný program MS Outlook. V rámci tohto programu sa sleduje len príjemca elektronickej pošty, odosielateľ, preto ako nápravné opatrenie navrhujeme zaviesť monitorovanie predmetu a veľkosti správ.

Zamestnancom spoločnosti je ako pracovný nástroj poskytnutý prístup do internetu pomocou softvéru Internet Explorer. Používanie internetu na súkromné účely je prísne zakázané avšak toto nie je žiadnym spôsobom monitorované. Preto odporúčame monitorovať URL adresy, názov stránky, čas prístupu a čas strávený na webových stránkach.

Návrh opatrení pre podnikovú sieť

V kanceláriách zamestnancov sú umiestnené sieťové zásuvky, ktoré nie sú plne využívané. Pre ich ochranu navrhujeme zakúpenie ochranných krytov pre prázdne porty RJ45, aby sa zabránilo ich znečisťovaniu prachom.

Podobné ochranné kryty je možné využiť aj pre samotné káble s konektorom RJ45, nachádzajúce sa v konferenčných miestnostiach spoločnosti. Tieto sú využívané viacerými zamestnancami, čím sa zvyšuje riziko ich poškodenia.



Obr. 14. Krytky RJ45[38]

Návrh opatrení pre zmluvy so zamestnancami

Zmluvy so zamestnancami sa nachádzajú v elektronickej podobe v počítači zamestnancov personálneho oddelenia. Je dôležité aby tieto záznamy boli chránené proti strate, poškodeniu, falšovaniu a neoprávnenému prístupu. Ako nápravné opatrenie zálohovanie pracovných zmlúv podpísaných na dobu neurčitú na dátové média a ich uloženie do archívu spoločnosti, ktorý je prístupný len oprávneným osobám. U každého typu pamäťového média je nutné stanoviť dobu uchovania. Je dôležité, vziať do úvahy životnosť dátového média a predísť tak strate dát. Samostatné skladovanie médií musí byť v súlade s odporučením výrobcu.

5.5.3 Opatrenia pre aktíva, ktoré majú zanedbateľný vplyv na organizáciu

Do tejto kategórie patria malé zariadenia, ako sú napríklad smartfóny, tablety a notebooky. Pri týchto aktívach je najväčším rizikom možnosť ukradnutia. Pre zvýšenie bezpečnosti smartfónov a tabletov odporúčame zaviesť nariadenie, v rámci ktorého budú ich majitelia povinný používať uzamknutie zariadenia pomocou čísla PIN alebo vzoru.

Pre zníženie nákladov podniku navrhujeme ako nápravné opatrenie zaviesť monitorovanie volaných čísiel aby sa zamedzilo zneužívaniu služobných telefónov na osobné účely. V rámci tohto opatrenia by bolo monitorované volané číslo, trvanie a čas hovoru.

Pre zvýšenie bezpečnosti notebookov odporúčane zaviesť opatrenie, v rámci ktorého sa notebook automaticky uzamkne pri prechode do režimu spánku alebo pri spustení šetriča obrazovky.

5.5.4 Nápravné opatrenia vyplývajúce z interného auditu ISMS

Pred riešením diplomovej práce bol v podniku vykonaný interný audit prostredníctvom checklistu, ktorý je v súlade s normou ISO 27001. Výsledok tohto auditu je možné vidieť v prílohe P I. Audit bol však vykonávaný internými pracovníkmi a preto sme ho nepovažovali za dostatočne objektívny a vytvorili sme vlastnú analýzu rizík.

Po vypracovaní analýzy rizík a následnom návrhu nápravných opatrení sme si výsledky porovnali s výsledkami z interného auditu. Na základe porovnania sme zistili, že analýza rizík sa sústredila len na informačné aktíva a nezahŕňala oblasti týkajúce sa ľudských zdrojov.

Z interného auditu vyplynuli dve nezhody, ktoré neboli zohľadnené v analýze rizík. Pre tieto nezhody sme sa rozhodli definovať nápravné opatrenia, pretože po dôslednom zvážení sme zistili, že môžu viesť k bezpečnostným incidentom, ktoré by mohli mať za následok poškodenie dobrého mena spoločnosti a poškodenie aktív. Týmito nezhodami boli:

- A.7.1.1 Preverovanie,
- A.11.2.9 Politika čistého stola a čistej obrazovky.

Ďalšími nezhodami zistenými pri internom audite boli:

- A.9.2.5 Preskúmavanie prístupových práv,
- A.9.4.3 Systém riadenia hesiel,
- A.11.2.2 Podporné služby,

- A.11.2.3 Bezpečnosť kabeláže,
- A.12.3.1 Zálohovanie informácií,
- A.12.4.1 Zaznamenávanie udalostí,
- A.18.1.3 Ochrana záznamov.

Tieto oblasti bezpečnosti boli zohľadnené v analýze rizík a preto už boli navrhnuté nápravné opatrenia.

A.7.1.1 Preverovanie

Pod pojmom preverovanie sa v internom audite myslí to, že pracovníci sú pred nástupom do zamestnania dostatočne preverení. V spoločnosti sa však nevykonáva verifikačná previerka uchádzačov o zamestnanie v súlade s príslušnými zákonmi, právnymi nariadeniami a etikou.

Preto pre zaistenie primárnej úrovne bezpečnosti navrhujeme preverovanie zamestnancov a to nasledujúcimi spôsobmi:

- overená kopia dosiahnutého vzdelania (diplom, maturitné vysvedčenie),
- overenie bezúhonnosti podľa výpisu z registra trestov,
- overenie totožnosti podľa dokladov.

A.11.2.9 Politika čistého stola a čistej obrazovky

Politika čistého stola a čistej obrazovky znamená, že zamestnanci po opustení kancelárie nezanechávajú na stole dôležité alebo dôverné dokumenty a prenosné média, na ktorých sú uložené citlivé informácie. Rovnako na ploche pracovnej stanice, by nemali byť uložené informácie tohto druhu.

Preto pre zníženie rizika zneužitia dôverných dokumentov navrhujeme aby tieto spolu s prenosnými médiami boli ukladané do uzamykateľných šuplíkov, ktoré má každý zamestnanec k dispozícii.

6 IMPLEMENTÁCIA NÁPRAVNÝCH OPATRENÍ V SPOLOČNOSTI

V súčasnej dobe počítačov a výpočtovej techniky je veľmi dôležité aby informačná bezpečnosť bola riadená nezávisle na tom, či ide o malú spoločnosť s 10 zamestnancami alebo o veľkú s 4500. Pre všetky firmy norma definuje rovnaký postup implementácie ISMS, pričom rozdielny môže byť len výklad jednotlivých doporučení a postupov ako dosiahnuť stanovený cieľ bezpečnosti.

Ako bolo spomínané v teoretickej časti celý systém riadenia bezpečnosti je neustálym kolobehom, ktorý sa riadi Demingovým cyklom zvaným PDCA model. Pri rozhodnutí o implementácii nápravných opatrení sa nachádzame vo fáze D – Do (urob).

Implementácia ISMS nemôže byť uznesením len jedného zamestnanca ale musí byť strategickým rozhodnutím vedenia organizácie. Preto je pri zavádzaní systému riadenia bezpečnosti požadovaný súhlas vedenia spoločnosti s nasadením ISMS. Získanie tohto súhlasu teda považujeme za prvý krok.

Pred riešením diplomovej práce sme získali súhlas vedenia spoločnosti len ústne v rámci riešenia práce, ktorý bol pridelený najmä z hľadiska možného prínosu pre spoločnosť. Pri oficiálnej implementácii ISMS v spoločnostiach musí mať tento súhlas papierovú formu tak ako ju definuje norma ISO/IEC 27001.

Druhým krokom počas implementácie ISMS je vytvorenie zoznamu aktív spoločnosti spolu s ich ohodnotením a vypracovanie analýzy rizík, ktorá tvorí celý základ bezpečnosti informácií.

Analýza rizík nám ukázala, ktoré z aktív nie sú dostatočne zabezpečené voči možným hrozbám. Preto nasledoval návrh nápravných opatrení, čo môžeme považovať za tretí krok v rámci implementácie celého ISMS. Keďže systém riadenia bezpečnosti je silno integrovaný do najrôznejších procesov organizácie, boli nápravné opatrenia konzultované s pracovníkom IT oddelenia a následne predložené vedeniu spoločnosti.

Na základe vykonanej analýzy rizík sa vedenie spoločnosti rozhodlo pre implementáciu niekoľkých nápravných opatrení. Tieto opatrenia boli implementované na základe nízkej finančnej náročnosti a možnosti vykonania ich internými zamestnancami. Nápravné opatrenia, ako napríklad kúpa nových softvérových nástrojov, budú prejednávané pri rozdeľovaní rozpočtov na ďalší rok.

6.1 Realizované nápravné opatrenia

Z analýzy rizík vyplynulo, že najviac ohrozenými aktívami sú servery a zálohy serverov a ich poškodenie by mohlo spôsobiť existenčné problémy spoločnosti. Hoci ide o finančný náklad pre spoločnosť, kúpa nového záložného zdroja pre aplikačné servery bola v uvažovaní už minulý rok a zarátaná do rozpočtu pre IT oddelenie. Spoločnosť sa tak rozhodla na základe vykonaného interného auditu, ktorý sa uskutočnil v septembri 2015. Z neho jasne vyplynulo, že aplikačné servery nie sú chránené proti výpadku elektrickej energie a pri vzniku takejto udalosti by prišlo k nefunkčnosti vybraného softvéru.

Popis realizácie:

- typ záložného zdroja – APC Smart – UPS C 1000VA LCD,
- realizácia – marec 2016,
- doba trvania – 1 týždeň,
- cena – 400 €,
- vykonal – pracovník IT oddelenia.

Ďalším možným rizikom, ktoré sa týka záloh serverov je to, že tieto zálohy sú uskutočňované externou firmou. Ako dočasné nápravné opatrenie bola zavedená dozorná činnosť pracovníkom IT oddelenia, ktorý dohliada na pravidelnú výmenu pások a na zaobchádzanie s páskami počas manipulácie externou firmou.

Pre elimináciu straty dát bolo vedeniu spoločnosti predložené dlhodobé nápravné opatrenie v podobe programu HP PC Connected Backup. Vedenie spoločnosti táto možnosť zaujala a o kúpe programu bude rozhodovať v priebehu nasledujúcich dvoch rokov.

Posledným kritickým aktívom pre spoločnosť sú pracovné stanice, kde môže prísť k zneužitiu prístupu kľúčového užívateľa. V tomto prípade bolo ako nápravné opatrenie navrhnutá častejšia zmena hesla. Toto opatrenie bolo realizované zmenou nastavení zásad hesiel v operačnom systéme Windows 7 Enterprise pod položkou ***secpol.msc*** – miestne nastavenia zabezpečenia.

Popis realizácie:

- realizácia – apríl – máj 2016,
- doba trvania – 2 mesiace,
- vykonal – pracovník IT oddelenia.

Ďalšími aktívami boli softvér, podniková sieť a zmluvy so zamestnancami. Poškodenie týchto aktív by mohlo spôsobiť ťažkosti alebo finančné straty spoločnosti.

Najviac ohrozeným softvérom používaným v celej spoločnosti, je SAP. V rámci tohto programu sú zamestnancom prideľované prístupy na určité operácie potrebné k výkonu ich práce. Pri prestupe na inú pracovnú pozíciu sa prístup zamestnancovi neodoberá. Navrhnutým nápravných opatrením je inštalácia modulu SAP GRC Access Control, ktorý by bol schopný tieto prístupy kontrolovať. Ide však o veľmi nákladné riešenie z hľadiska zakúpenia licencie a potrebných školení a preto bude spoločnosť uvažovať o inom riešení rizikovej situácie.

V prípade softvérových nástrojov slúžiacich na komunikáciu vo vnútri ale aj mimo firmy sme ako nápravné opatrenie navrhli zvýšenie monitorovacej činnosti. Toto opatrenie by platilo v prípade e-mailovej komunikácie, kedy by sa monitoroval predmet a veľkosť odosielaných správ a v prípade internetových stránok by sa sledoval čas strávený na URL adrese a jej názov. Vedenie podniku však toto nápravné opatrenie neprijalo z hľadiska zachovania priateľského pracovného prostredia a dôvery k svojím zamestnancom

Z našich zistení je najväčším rizikom pre podnikovú sieť jej fyzické poškodenie. Z tohto dôvodu sme navrhli zakúpenie špeciálnych krytov pre ochranu sieťových zásuviek a konektorov RJ45. Vedenie spoločnosti toto opatrenie prijalo, pretože protiprachová ochrana predstavuje nízkorozpočtovú položku.

Popis realizácie:

- typ protiprachovej ochrany – FL RJ45 PROTECT CAP,
- realizácia – apríl 2016,
- doba trvania – 2 týždne,
- cena – 200 ks – 40 €,
- vykonal – pracovníčka recepcie.

Zmluvy so zamestnancami sú uchovávané v elektronickej podobe len v počítači zamestnancov personálneho oddelenia. Tu hrozí riziko straty údajov a preto pre väčšie zabezpečenie bolo navrhnuté archivovanie zmlúv na prenosné média a ich uskladnenie v archíve. Opäť ide o finančne nenáročnú operáciu a preto bolo toto nápravné opatrenie v spoločnosti zavedené. Pracovníci personálneho oddelenia boli preškolení pracovníkom IT oddelenia o bezpečnosti a archivácii údajov.

Popis realizácie:

- typ archivačného média – DATA TRESOR DISC (archivačné DVD),
- realizácia – marec 2016,
- doba trvania – školenie 1 hodina + individuálne trvanie zálohy,
- cena –50 ks – 70 €,
- vykonal – pracovník IT oddelenia + zamestnanci personálneho oddelenia.

Poslednou ohrozenou skupinou informačných aktív sú malé zariadenia, ako napríklad smartfóny, tablety a notebooky. Pri týchto aktívach je najväčším ohrozením riziko krádeže a teda následné zneužitie údajov v nich uložených. Preto sme pre zvýšenie bezpečnosti navrhli zavedenie nariadenia, podľa ktorého budú zamestnanci povinní používať uzamykacie nástroje dostupné v zariadeniach. Spoločnosť opatrenie prijala a vlastníci notebookov, smartfónov a tabletov boli preškolení o ich používaní a novom bezpečnostnom nariadení. Po preškolení sa svojím podpisom zaviazali o dodržiavaní nariadenia.

Popis realizácie:

- realizácia – marec 2016,
- doba trvania – školenie 1 hodina, celkovo 5 školení v rámci troch týždňov,
- vykonal – pracovník IT oddelenia + zamestnanci manažmentu spoločnosti.

Z interného auditu vyplynuli ešte ďalšie dve nezhody – preverovanie a politika čistého stola a čistej obrazovky. Pre obe sme navrhli nápravné opatrenia avšak spoločnosť sa rozhodla, že tieto budú implementované len pre preverovanie. Pracovníci personálneho oddelenia boli upozornení na riziko, ktoré môže vzniknúť nedostatočným preverením zamestnancov pred nástupom do pracovného pomeru. Pre zaistenie primárnej bezpečnosti sú zamestnanci personálneho oddelenia povinný vyžadovať od uchádzačov o zamestnanie výpis z registra trestov a overenú kópiu dosiahnutého vzdelania. Politika čistého stola a čistej obrazovky nebude v spoločnosti implementovaná v takom rozsahu ako ju definuje norma.

Prijatím a zavedením nápravných opatrení sa ukončila fáza Demingovho cyklu – Do (urob). Ako sme už spomínali ISMS je nekončiaci proces, ktorý si vyžaduje neustále udržovanie a zlepšovanie. Preto po vykonaní nápravných opatrení nasleduje etapa s názvom Check – kontroluj. Počas tejto fázy sa vykonáva kontrola zavedených nápravných opatrení a interné audity, ktoré vedú k zisťovaniu efektívnosti prijatých opatrení a takisto k odhaľo-

vaniu nových hrozieb a nezhôd. Cieľom je príprava na certifikáciu, o ktorej spoločnosť Protherm Production v súčasnosti zatiaľ neuvažuje. Vedenie spoločnosti si však uvedomilo význam a dôležitosť informačnej bezpečnosti a preto sa rozhodla vykonávať údržbu zariadení a činnosti, ktoré sústavne prispievajú k zvýšeniu bezpečnosti a teda aj k neustálemu zlepšovaniu, čo je poslednou etapou PDCA cyklu – Act – pôsob.

ZÁVER

Každá organizácia bez ohľadu na jej veľkosť potrebuje pre svoje efektívne fungovanie využívať prostriedky, medzi ktoré patria informácie, informačné systémy alebo ľudské zdroje. Súhrne je možné tieto prostriedky nazvať aktívami spoločnosti, ktoré sú využívané každý deň a obsahujú slabé miesta, ktoré môžu byť potenciálne zneužité. Riziko ovplyvňujúce spoločnosť vzniká kombináciou pravdepodobnosti výskytu negatívnej udalosti a jej dopadu na aktívum.

Najpriaznivejšou cestou ako limitovať tieto neefektívne a pre organizáciu potenciálne nebezpečné rizikové prvky je implementácia ISMS – Systému riadenia informačnej bezpečnosti podľa normy ISO/IEC 27001.

Diplomová práca sa zaoberá témou informačnej bezpečnosti. Naším cieľom bolo v rámci práce vytvoriť analýzu rizík pre konkrétnu spoločnosť spolu s návrhom nápravných opatrení a ich následnou realizáciou.

Prvá časť práce predstavuje literárny prehľad a priblíženie informačnej bezpečnosti, ktorá je definovaná medzinárodným štandardom ISO/IEC 27001. Pre lepšie pochopenie problematiky sme popísali postup implementácie ISMS a dôležité kroky, ktoré musia byť v rámci podniku uskutočnené pre odhalenie možného rizika. Záver teoretickej časti je venovaný popisu certifikačného auditu vykonávaného na základe spomínanej normy.

Aby bolo možné vytvoriť efektívne informačné zabezpečenie je potrené zhodnotiť stávajúci stav spoločnosti a uviesť riziká, ktoré môžu poškodiť jej aktíva. Z tohto dôvodu bolo prvým krokom v praktickej časti práce vytvorenie zoznamu informačných aktív a ich ohodnotenie na základe dostupnosti, dôvernosti a integrity. Po identifikovaní aktív spoločnosti nasledovalo určenie hrozieb a pravdepodobnosť ich výskytu. Kombináciou týchto faktorov boli vytvorené matice zraniteľnosti a matice rizík, z ktorých sme zistili aké aktíva sú v spoločnosti najviac ohrozené.

Výsledky rizikovej analýzy sme si porovnali s interným auditom, ktorý bol v spoločnosti vykonaný pred riešením diplomovej práce. Výsledkom bolo zistenie, že riziková analýza je zameraná len na informačné aktíva spoločnosti a nezahŕňa ľudský faktor. Následne sme na základe výsledkov rizikovej analýzy a interného auditu navrhli nápravné opatrenia a to tak, aby sa znížilo alebo úplne odstránilo riziko poškodenia konkrétnych aktív.

Záver práce je venovaný implementácii nápravných opatrení v spoločnosti Protherm Production Skalica, ktorá je z hľadiska zabezpečenia dát na veľmi dobrej úrovni. Výsledky rizikovej analýzy boli prediskutované s pracovníkom IT oddelenia a následne aj s vedením spoločnosti. Keďže spoločnosť mala schválený rozpočet na tento rok nebolo možné implementovať všetky navrhnuté opatrenia. Tie, ktoré boli realizované priniesli výrazný pokles doterajších rizík.

ZÁVER V ANGLIČTINE

Every single corporation despite of its dimension needs appropriate resources in order to work effectively. The resources mean; a lot of information, information systems and human resources. In general, these resources are called the company assets. They are used every single day and they have weak parts which can be potentially misused. The potential risk in the company derives from the possible combination of probable negative incidents and its effects to the company assets.

The most appropriate way how to limit these ineffective and potentially risky elements in the company is to implement the ISMS norm – Information Security Management System, a norm ISO/IEC 27001.

The diploma thesis is dealing with the topic of the information security. The aim of this work is to model the analysis of insecure elements in the company, and to suggest corrective measurements and resultantly to implement them.

The first part of the diploma theses presents the literal overview about the topic and description of the information security that is defined by the international standard ISO/IECC 27001. On behalf of being explicit, we define the process of the ISMS implementation and important methods that must be held in the company in order to reveal possible risks. The conclusion of the theoretical part defines the certificate audit that is performed according to this norm.

An effective information security is substantial and there must be an evaluation of the present state of the company and a presentation of possible risks that possibly harm the company assets. This is the reason why the practical part of the diploma thesis focuses on forming the list of the information assets and consequently to evaluate the assets on the basis of accessibility, confidentiality and integrity. The assets definition in the company was followed by setting the threats and setting the probability of their occurrence. There were created the matrix of vulnerability and the matrix of risks. These defined which assets in the company are threatened the most.

The results of the substandard analysis were compared to the internal audit of the company that was completed before the diploma thesis. The result was that the substandard analysis focused just on the information assets and it did not include the human factor. Consequently, on the basis of the substandard analysis and the internal audit, the corrective measurements were proposed. The corrective measurements are used to eliminate or resolve the risk of assets damage.

The conclusion of the diploma thesis dedicates to the implementation of the corrective measurements in the company Protherm Production Skalica. In general, the company's corrective measurements are good quality. The results of the substandard analysis were discussed with an IT worker and the management of the company. Considering the company did approved the annual budget, all the proposed corrective measurements were not possible to implement. However, those corrective measurements that were implemented resulted in a significant decrease in present risks.

ZOZNAM POUŽITEJ LITERATÚRY

[1] Linuxservices. *Kybernetická bezpečnost* [online]. 2016 [cit. 2016-02-09]. Dostupné z: https://www.linuxservices.cz/kyberneticka-bezpecnost.

[2] Cybersecurity. *Cyber Security* (Kybernetická bezpečnost) [online]. 2010 [cit. 2016-02-09]. Dostupné z: http://www.cybersecurity.cz/basic.html

[3] Národní centrum kybernetické bezpečnosti. *Strategie pro oblast kybernetické bezpečnosti ČŘ na období 2012 - 2015* [online]. 2011 [cit. 2016-02-09]. Dostupné z: https://www.govcert.cz/download/nodeid-727/

[4] T-soft. *Zákon o kybernetické bezpečnosti* [online]. 2014 [cit. 2016-02-09]. Dostupné z: http://www.tsoft.cz/zakon-o-kyberneticke-bezpecnosti/

[5] Epravo. *Zákon o kybernetickej bezpečnosti* [online]. 2016 [cit. 2016-02-09]. Dostupné z: http://www.epravo.sk/top/clanky/zakon-o-kybernetickej-bezpecnosti-758.html

[6] Kybernetická bezpečnosť na Slovensku a v Európe. *EurActiv* [online]. 2003 [cit. 2016-02-09]. Dostupné z: http://euractiv.sk/veda-a-inovacie/kyberneticka-bezpecnost-na-slovensku-a-v-europe-000338/

[7] Rokovania. *Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020* [online]. 2010 [cit. 2016-02-09]. Dostupné z: http://www.rokovania.sk/File.aspx/ViewDocumentHtml/Mater-Dokum-187874?prefixFile=m_

[8] RiskAnalysisConsultants. *ISO/IEC 27002:2013* [online]. 2016 [cit. 2016-02-09]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/27002

[9] Iso27001security. *ISO/IEC 27001:2013* Information technology [online]. 2016 [cit. 2016-02-09]. Dostupné z: http://www.iso27001security.com/html/27001.html

[10] Kiwiki. *Systém manažérstva informačnej bezpečnosti* [online]. 2011 [cit. 2016-02-09]. Dostupné z: http://www.kiwiki.info/index.php/Syst%C3%A9m_mana%C5%BE%C3%A9rstva_informa%C4%8Dnej_bezpe%C4%8Dnosti

[11] ISO Auditor. *Systém manažérstva informačnej bezpečnosti* [online]. 2016 [cit. 2016-02-09]. Dostupné z: http://www.isoauditor.sk/iso-iec-27001

[12] Zavedení systému řízení bezpečnosti. *ISMS* [online]. [cit. 2016-02-09]. Dostupné z: http://www.chrantesidata.cz/cs/art/1148-dil-2/

[13] Blog Brichacek. *Audit informační bezpečnosti – systém řízení informační bezpečnosti (ISMS)* [online]. 2015 [cit. 2016-02-09]. Dostupné z: http://blog.brichacek.net/audit-informacni-bezpecnosti-system-rizeni-informacni-bezpecnosti-isms/

[14] HUDEC, Ladislav. *Ohodnotenie rizík aktív IS – základný predpoklad dobrého manažmentu bezpečnosti IS* [online]. FIIT STUBA [cit. 2016-02-28]. Dostupné z: http://www.informatizacia.sk/ext_dok-seminar_bs_2009_07_21_hudec/6210c. Seminár

[15] Vysoké učení technické v Brně. *Aktiva v ISMS* [online]. 2013 [cit. 2016-02-09]. Dostupné z: http://www.vutbr.cz/www_base/priloha.php?dpid=74651

[16] EMI journal. *Informačná bezpečnosť v spoločnosti* [online]. 2013 [cit. 2016-02-09]. Dostupné z: http://emi.mvso.cz/EMI/2011-01/04%20Solc/Solc.pdf

[17] HANÁČEK, Petr a Jan STAUDEK. *Bezpečnost informačních systémů: metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií*. 1. vyd. Praha: Úřad pro státní informační systém, 2000, 127 s. ISBN 80-238-5400-3.

[18] ČERMÁK, Igor. *Řízení rizik* [online]. ČVUT [cit. 2016-02-28]. Dostupné z: https://edux.fit.cvut.cz/oppa/MI-IBE/prednasky/MI-IBE_6.pdf. Prednáška

[19] HUDEC, Ladislav. *Analýza bezpečnostných rizík informačného systému* [online]. FIIT STUBA [cit. 2016-02-28]. Dostupné z: http://www2.fiit.stuba.sk/~lhudec/PIS/3_prednaska.ppt. Prednáška

[20] Security revue. *Manažment informačnej bezpečnosti v malých a stredných podnikoch* [online]. 2012 [cit. 2016-02-10]. Dostupné z: http://www.securityrevue.com/article/2012/06/manazment-informacnej-bezpecnosti-v-malych-a-strednych-podnikoch/]

[21] REMEŠOVÁ, Miroslava. *Bezpečnosť digitálneho prostredia v SR*. Nitra, 2011. Diplomová práca. Vedoucí práce Doc. Ing. Klára Hennyeyová, CSc. [cit. 2016-02-10] Dostupné z: http://crzp.uniag.sk/Prace/2011/R/F7A9586D1D0D4701AE9BC89B5E044794.pdf

[22] ŠEMELÁK, Michal. *Bezpečnosť digitálneho prostredia v SR*. *Nitra*, 2008. Diplomová práca. Vedoucí práce Ing. Eva Olahová. [cit. 2016-02-10] Dostupné z: http://www.slpk.sk/eldo/zp/2008/fem/fem2008-michalsemelak-ing596707.pdf

[23] Bpm-tema. *Případová studie analýzy rizik informační bezpečnosti* [online]. 2007 [cit. 2016-02-10]. Dostupné z: http://bpm-tema.blogspot.sk/2007/11/ppadov-studie-analzy-rizik-informan.html

[24] ISMS. *Analýza rizik* [online]. 2016 [cit. 2016-02-10]. Dostupné z: http://www.isms.cz/index.php?option=com_content&view=article&id=55&Itemid=71&lang=cs

[25] BUČINSKÝ, Miloš. *Analýza rizik bezpečnosti IS STAG*. České Budějovice, 2009. Bakalárska práca. Vedoucí práce Ing. Ladislav Beránek, CSc., MBA. [cit. 2016-02-10] Dostupné z: http://theses.cz/id/lx5xki/downloadPraceContent_adipIdno_12530

[26] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 2., aktualiz. a rozš. vyd. Praha: Grada, 2006, 296 s. Expert (Grada). ISBN 80-247-1667-4.

[27] UČEŇ, Pavel. *Metriky v informatice: jak objektivně zjistit přínosy informačního systému.* 1. vyd. Praha: Grada, 2001, 139 s. Management v informační společnosti. ISBN 80-247-0080-8.

[28] JAQUITH, Andrew. *Security metrics: replacing fear, uncertainty, and doubt*. Upper Saddle River, NJ: Addison-Wesley, 2007, xxvii, 306 p. ISBN 9780321349989.

[29] ČSN ISO/IEC 27001. *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky*. [s.l.] : Český normalizační institut, 2014. 28 s. ISSN 8590963958057

[30] Certicom. *Certifikácia systémov manažérstva bezpečnosti informácií (ISMS) podľa ISO 27001* [online]. 2016 [cit. 2016-02-10]. Dostupné z: http://www.certicom.sk/certifikacia/iso-27001/

[31] ISMS. *Certifikace ISMS* [online]. 2016 [cit. 2016-02-10]. Dostupné z: http://www.isms.cz/index.php?option=com_content&view=article&id=58&Itemid=74&lang=cs

[32] CQS - Sdružení pro certifikaci systému jakosti. *ISMS, ITSM, BCMS – kdy se zabývat certifikací organizace a jaký to má přínos?* [online]. 2016 [cit. 2016-02-10]. Dostupné z: http://www.cqs.cz/Novinky/ISMS-ITSM-BCMS-kdy-se-zabyvat-certifikaci-organizace-a-jaky-to-ma-prinos.html

[33] Stavcert. *Informace pro žadatele a držitele certifikátu ISMS* [online]. 2016 [cit. 2016-02-10]. Dostupné z: http://www.stavcert.cz/cs/certifikace-isms

[34] Euco cert group. *Základní informace* [online]. 2016 [cit. 2016-02-10]. Dostupné z: http://www.eurocert.cz/ke-stazeni/zakladni_informace_cz.pdf?x=1454834780

[35] Protherm. *O spoločnosti* [online]. 2015 [cit. 2016-03-27]. Dostupné z: http://www.protherm.sk/pre-nasich-zakaznikov/vyrobny-zavod/o-spolocnosti/index.sk_sk.html

[36] Počítačové siete. *Hviezdicová topológia (STAR)* [online]. 2015 [cit. 2016-03-27]. Dostupné z: http://upol.jecool.net/sk/hviezdicova-topologia-star/

[37] Bezpečnosť IT a informačná bezpečnosť: *Smernica skupiny Vaillant Group*. Germany, 2012.

[38] PHOENIX CONTACT. *Protiprachová ochrana* [online]. [cit. 2016-04-24]. Dostupné z: https://www.phoenixcontact.com/online/portal/cz?uri=pxc-oc-itemdetail:pid=2832991&library=czcs&tab=1

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

APC American Power Conversion Corporation

AV Anti-vírusový program

BSI British Standards Institution (Britský štandardizačný inštitút)

CMDB Configuration management database (konfiguračná databáza)

CSIRT Computer Security Incident Response Team (Jednotka pre riešenie počítačových incidentov)

č. Číslo

GmbH Gesellschaft mit beschränkter Haftung

HP Hewlett Packard

HW Hardvér

IEC International Electrotechnical Commission (Medzinárodná elektrotechnická komisia)

IS Informačný systém

ISMS Information Security Management System (Systém manažérstva informačnej bezpečnosti)

ISO International Organization for Standardization (Medzinárodná organizácia pre štandardizáciu)

IT Informačné technológie

ITC Information and communication Technologies (Informačné a komunikačné technológie)

LTO Linear Tape-Open

MS Microsoft

PDCA Plan-Do-Check-Act (Plánuj-Vykonaj-Kontroluj-Pôsob)

PIN Personal identification number (Osobné identifikačné číslo)

SR Slovenská Republika

STN Slovenská technická norma

SW	Softvér
SWOT	Strengths-Weaknesses-Opportunities-Threats (Silné stránky-Slabé stránky-Príležitosti-Ohrozenia)
UPS	Uninterruptible Power Supply
URL	Uniform resource locator (Jednotný vyhľadávač zdrojov)

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ZOZNAM PRÍLOH

PRÍLOHA P I: ISO 27001 CHECKLIST

Referencia			Výsledok	
Štandard		Otázka	Zistenie	
A.5	**Politiky informačnej bezpečnosti**			
A.5.1	**Usmernenie pre informačnú bezpečnosť**			
A.5.1.1	Politiky informačnej bezpečnosti	Je politika informačnej bezpečnosti definovaná a schválená manažmentom, pre vydanie a oznámenie všetkým zamestnancom a tretím stranám?	Dokument bezpečnostnej politiky je definovaný a schválený manažmentom v Nemecku a je dostupný všetkým zamestnancom a tretím stranám.	100%
A.5.1.2	Preskúmanie politiky informačnej bezpečnosti	Preskúmava sa politika informačnej bezpečnosti v plánovaných intervaloch, ako aj okamžite pri výskyte významných zmien, čím sa zabezpečí jej kontinuálna vhodnosť, primeranosť a efektivita?	Politika informačnej bezpečnosti sa preskúmava v plánovaných intervaloch ako aj okamžite pri výskyte významných zmien.	100%
A.6	**Organizácia informačnej bezpečnosti**			
A.6.1	**Vnútorná organizácia**			
A.6.1.1	Roly a zodpovednosť v informačnej bezpečnosti	Je každá bezpečnostná zodpovednosť jednoznačne zadefinovaná a pridelená?	V spoločnosti je informačná bezpečnosť riadená centrálou v Nemecku. V spoločnosti je pridelený pracovník IT oddelenia ktorý riadi bezpečnosť lokálne.	90%
A.6.1.2	Oddelenie právomocí	Sú oddelené konfliktné povinnosti a oblasti zodpovednosti, aby sa znížila možnosť na neoprávnenú úpravu alebo zneužitie aktív organizácie?	V spoločnosti sú oddelené konfliktné povinnosti a oblasti zodpovednosti.	95%
A.6.1.3	Kontakty s orgánmi moci	Udržiavajú sa príslušné kontakty s relevantnými orgánmi štátnej moci?	V spoločnosti sa udržiavajú príslušné vzťahy s orgánmi štátnej moci.	90%
A.6.1.4	Kontakt so špeciálnymi záujmovými skupinami	Udržiavajú sa príslušné kontakty so špecifickými záujmovými skupinami alebo inými fórami bezpečnostných špecialistov a s profesijnými komorami?	V spoločnosti sa udržiavajú príslušné kontakty.	90%
A.6.1.5	Informačná bezpečnosť v projektovom riadení	Je ošetrená informačná bezpečnosť aj v riadení projektov bez ohľadu na typ projektu?	Informačná bezpečnosť je ošetrená aj v riadení projektov bez ohľadu na jeho typ.	100%
A.6.2	**Mobilné zariadenia a práca na diaľku**			
A.6.2.1	Politika pre mobilné zariadenia	Je v organizácii prijatá politika a podporné bezpečnostné opatrenia pre používanie mobilných zariadení?	V spoločnosti je prijatá politika a podporné bezpečnostné opatrenia pre mobilné zariadenia.	100%
A.6.2.2	Práca na diaľku	Sú vyvinuté a implementované postupy, prevádzkové plány a politiky chrániace informácie prístupné a spracovávané pri práci na diaľku, alebo uložené na mieste odkiaľ sa vykonáva práca na diaľku?	V spoločnosti sú vyvinuté a implementované postupy, plány, politiky chrániace informácie prístupné a spracované pri práci na diaľku.	100%

A.7	**Personálna bezpečnosť**			
A.7.1	**Pred nástupom do zamestnania**			
A.7.1.1	Preverovanie	Vykonáva sa verifikačná previerka personálneho pozadia všetkých uchádzačov o zamestnanie v súlade s príslušnými zákonmi, právnymi nariadeniami a etikou, ako aj vzhľadom na obchodné požiadavky, klasifikačný stupeň informácií, ku ktorým sa bude pristupovať, ako aj na vnímané riziká ?	Uchádzači o zamestnanie, nie sú preverovaní. V spoločnosti sa verifikácia od zamestnancov nevyžaduje.	0%
A.7.1.2	Pracovná náplň a podmienky zamestnania	Definuje zmluvná dohoda so zamestnancom a zmluvným partnerom ich zodpovednosť a zodpovednosť organizácie za informačnú bezpečnosť?	V spoločnosti je presne definovaná zmluvná dohoda so zamestnancom za informačnú bezpečnosť.	90%
A.7.2	**Počas zamestnania**			
A.7.2.1	Manažérska zodpovednosť	Vyžaduje manažment od zamestnancov a zmluvných partnerov uplatňovanie bezpečnosti v súlade so zavedenými politikami a postupmi organizácie?	Manažment od zamestnancov vyžaduje dodržiavanie bezpečnosti v súlade so zavedenými politikami a postupmi.	100%
A.7.2.2	Povedomie o informačnej bezpečnosti, vzdelávanie a školiaca činnosť	Absolvujú všetci zamestnanci organizácie a zmluvní partneri vhodné školenie v oblasti bezpečnostného povedomia a poskytujú sa im pravidelne aktualizované verzie politík a postupov organizácie, tak ako si to vyžaduje ich pracovné zaradenie?	Všetci zamestnanci spoločnosti, zmluvný partneri a tretie strany absolvujú školenia pri vstupe do pracovného pomeru a pravidelné školenia na základe smerníc.	100%
A.7.2.3	Disciplinárny proces	Existuje formálny a od komunikovaný disciplinárny proces pre zamestnancov, ktorí spôsobili bezpečnostný incident?	V spoločnosti existuje formalizované disciplinárne riadenie.	100%
A.7.3	**Ukončenie a zmena zamestnania**			
A.7.3.1	Zodpovednosť pri ukončení alebo zmene zamestnania	Sú definované zodpovednosti a povinnosti v oblasti informačnej bezpečnosti, ktoré budú platiť po ukončení alebo zmene zamestnania?	V spoločnosti sú presne definované zodpovednosti a povinnosti pre prípad ukončenia alebo zmeny zamestnania v pracovnej smernici.	100%
A.8	**Riadenie aktív**			
A.8.1	**Zodpovednosť za aktíva**			
A.8.1.1	Inventárny zoznam aktív	Sú aktíva prepojené s informáciami a zariadeniami, ktoré informácie spracúvajú? Sú aktíva označené, a je vytvorený ich zoznam, ktorý sa udržiava?	V spoločnosti sú aktíva označené je vytvorený zoznam aktív ktorý je pravidelne udržiavaný. Aktíva sú prepojene s informáciami a zariadeniami.	95%
A.8.1.2	Vlastníctvo aktív	Majú udržiavané aktíva v inventári svojho vlastníka?	Všetky informácie a aktíva v inventári majú určeného svojho vlastníka.	95%
A.8.1.3	Prijateľné používanie aktív	Sú identifikované, zdokumentované a implementované pravidlá na prijateľné používanie informácií a aktív spojených s prostriedkami na spracúvanie informácií?	V spoločnosti sú identifikované, zdokumentované a do praxe zavedené pravidlá pre prípustné použitie informácií a aktív.	100%

A.8.1.4	Vrátenie aktív	Vracajú zamestnanci a zmluvný partneri po ukončení ich pracovného pomeru akékoľvek aktíva patriace organizácii?	Zamestnanci v spoločnosti a zmluvný partneri sú povinný po ukončení pracovného pomeru odovzdať všetky aktíva patriace spoločnosti prostredníctvom výstupného listu.	100%
A.8.2	**Klasifikácia informácií**			
A.8.2.1	Klasifikácia informácií	Sú klasifikované informácie na základe ich právnych požiadaviek, hodnoty, kritickosti a citlivosti na neautorizované prezradenie alebo úpravu?	V spoločnosti je vytvorená klasifikačná schéma na klasifikáciu informácií a informačné aktíva sú zaradené do tried dôverností.	100%
A.8.2.2	Označovanie informácií	Je zostavený a implementovaný príslušný súbor postupov na označovanie informácií a zaobchádzanie s nimi, a to v súlade s klasifikačnou schémou, ktorú organizácia prijala?	V spoločnosti sú stanovené a implementované pravidlá označovania a zaobchádzania s informačnými aktívami. Každá informácia musí byť označená triedou dôvernosti.	100%
A.8.2.3	Zaobchádzanie s aktívami	Sú vytvorené postupy na prácu s aktívami v súlade so schémou klasifikácie informácií, ktorá sa prijala v organizácii?	V spoločnosti sú stanovené pravidlá označovania a zaobchádzania s informačnými aktívami.	100%
A.8.3	**Zaobchádzanie s médiami**			
A.8.3.1	Riadenie prenosných médií	Sú zavedené postupy na riadenie prenosných médií v súlade s klasifikačnou schémou, ktorú prijala organizácia?	V spoločnosti sú zavedené postupy na riadenie prenosných médií, avšak nie sú v súlade s klasifikačnou schémou.	80%
A.8.3.2	Likvidácia médií	Sú médiá, ak nie sú viac potrebné, likvidované bezpečným spôsobom použitím formálnych postupov?	V spoločnosti sú média likvidované v súlade so schválenými postupmi.	100%
A.8.3.3	Fyzický prenos médií	Sú médiá obsahujúce informácie chránené pred neautorizovanými prístupmi, pred zneužitím alebo poškodením pri prenose?	V spoločnosti sú média fyzicky chránené pred neautorizovanými prístupmi.	95%
A.9	**Riadenie prístupov**			
A.9.1	**Požiadavky na riadenie prístupu**			
A.9.1.1	Politika riadenia prístupov	Je zavedená politika riadenia prístupu, dokumentovaná a preskúmavaná na základe pracovných a bezpečnostných požiadaviek?	V spoločnosti je zavedená, zdokumentovaná a v závislosti na aktuálnych bezpečnostných požiadaviek preskúmavaná politika riadenia prístupov.	100%
A.9.1.2	Prístup do sietí a sieťových služieb	Je používateľom udelený prístup len do siete a k cieľovým službám, na ktorých použitie boli konkrétne autorizovaní?	V spoločnosti je udelený prístup používateľom len k tým sieťovým službám boli konkrétne autorizovaní.	100%
A.9.2	**Riadenie používateľských prístupov**			
A.9.2.1	Deregistrácia a registrácia používateľov	Je zriadený formálny proces registrovania a deregistrovania používateľov?	V spoločnosti existuje formálny proces pri registrácii a deregistrácii ktorý zaistí autorizovaný prístup ku všetkým informačným systémov a služieb.	100%
A.9.2.2	Realizácia používateľských prístupov	Je zavedený formálny proces na stanovenie prístupov a na priradenie alebo zrušenie prístupových práv pre všetky typy používateľov, systémov a služieb?	V spoločnosti je zavedený formálny proces na stanovenie prístupov a na priradenie a zrušenie práv.	95%
A.9.2.3	Riadenie privilégií	Je riadené a obmedzené prideľovanie a využívanie privilégií?	V spoločnosti je prideľovanie privilégií obmedzené a riadené.	100%

A.9.2.4	Riadenie utajených autentizačných údajov	Je prideľovanie utajených autentizačných údajov riadené prostredníctvom formálneho riadiaceho procesu?	V spoločnosti je prideľovanie utajených autentizačných údajov prideľované prostredníctvom formálneho procesu.	100%
A.9.2.5	Preskúmavanie prístupových práv	Preskúmava vlastník aktív prístupové práva používateľov v pravidelných intervaloch?	Vlastník aktív v spoločnosti preskúmava prístupové práva len pri začatí a skončení pracovného pomeru.	50%
A.9.2.6	Odstránenie alebo prispôsobenie prístupových práv	Odstraňujú sa prístupové práva všetkých zamestnancov a tretích strán, ktorí používajú informácie a zariadenia, ktoré spracúvajú informácie, pri ukončení ich zamestnania, zmluvy alebo dohody?	V spoločnosti sa odstraňujú prístupové práva všetkých zamestnancov a tretích strán pri ukončení zamestnania, zmluvy a dohody.	100%
A.9.3	**Zodpovednosť používateľov**			
A.9.3.1	Používanie utajených autentizačných údajov	Požaduje sa od používateľov, aby pri používaní autentizačných informácií dodržiavali postupy prijate v organizácii?	V spoločnosti sa vyžadujú od užívateľov dodržiavali postupy prijaté v organizácii.	100%
A.9.4	**Riadenie systémových a aplikačných prístupov**			
A.9.4.1	Obmedzenie prístupu k informáciám	Riadi sa prístup k informáciám a funkciám aplikačných systémov definovanou politikou riadenia prístupu?	Prístup k informáciám a funkciám sa v spoločnosti riadi definovanou politikou prístupu.	100%
A.9.4.2	Bezpečnostné postupy prihlasovania	Je riadený prístup do operačných systémov prostredníctvom bezpečného postupu prihlasovania ? (log-on)	V spoločnosti je riadený prístup do operačných systémov prostredníctvom log-on	100%
A.9.4.3	Systém riadenie hesiel	Sú systémy na riadenie hesiel interaktívne a je potrebné zvoliť komplexné heslá ?	Systémy na riadenie hesiel sú v spoločnosti interaktívne ale nie je potrebné zvoliť komplexné heslá a v pravidelných intervaloch ich meniť.	70%
A.9.4.4	Používanie privilegovaných programov	Je prísne riadené a obmedzené používanie programov (utilít), ktoré môžu mať schopnosť obísť systémové a aplikačné opatrenia?	V spoločnosti je prísne riadené a obmedzené používanie utilít, ktoré môžu mať schopnosť obísť systémové a aplikačné opatrenia.	80%
A.9.4.5	Riadenie prístupu k zdrojovým kódom programu	Je obmedzený prístup ku zdrojovému kódu?	V spoločnosti je prístup ku zdrojovému kódu obmedzený.	100%
A.10	**Kryptografia**			
A.10.1	**Kryptografické opatrenia**			
A.10.1.1	Politika používania kryptografických opatrení	Sú zavedené a vytvorené politiky na používanie kryptografických opatrení na ochranu informácií?	V spoločnosti je zavedená politika pre používanie kryptografických opatrení na ochranu informácií.	100%
A.10.1.2	Správa kľúčov	Je vytvorená a zavedená politika na používanie, ochranu a riadenie životného cyklu kryptografických kľúčov na celý ich životný cyklus?	Na podporu používania kryptografických kľúčov v spoločnosti existuje v spoločnosti politika pre správu kľúčov.	100%
A.11	**Fyzická bezpečnosť a bezpečnosť prostredia**			
A.11.1	**Zabezpečené oblasti**			
A.11.1.1	Perimeter fyzickej bezpečnosti	Sú použité bezpečnostné perimetre by mali na ochranu citlivých alebo kritických informácií a zariadení spracúvajúcich tieto informácie?	V spoločnosti sú použité bezpečnostné perimetre (vstup na karty, recepcie, bariéry).	100%

A.11.1.2	Riadenie fyzických prístupov	Sú zabezpečené oblasti chránené primeranými opatreniami na vstupe, aby sa zabezpečilo, že vstúpiť môžu len autorizované osoby?	V spoločnosti sú zabezpečené oblasti chránené vhodným systémom vstupných kontrol.	100%
A.11.1.3	Zabezpečenie kancelárií, miestností a prostriedkov	Je navrhnutá a aplikovaná fyzická bezpečnosť pre kancelárie, miestnosti a zariadenia?	V spoločnosti je navrhnutá a aplikovaná fyzická bezpečnosť pre kancelárie, miestnosti a zariadenia.	100%
A.11.1.4	Ochrana pred externými hrozbami a hrozbami prostredia	Počíta sa s vytvorením a aplikovaním fyzickej ochrany pred prírodnými katastrofami, útokmi alebo nehodami?	V spoločnosti sú navrhnuté a aplikované príslušné opatrenia pred prírodnými katastrofami, útokmi a nehodami.	100%
A.11.1.5	Práca v bezpečnostných priestoroch	Sú aplikované príslušné postupy pre prácu v zabezpečených oblastiach?	Pre prácu v zabezpečených oblastiach sú navrhnuté a aplikované prvky fyzickej ochrany.	100%
A.11.1.6	Priestory na nakladanie a vykladanie	Sú kontrolované prístupové body, napr. priestory na nakladanie a vykladanie, ako aj iné body, kde môže neautorizovaná osoba získať prístup do priestorov organizácie?	V spoločnosti sú kontrolované miesta pre nakladanie, vykladanie a ďalšie miesta kde sa môžu neoprávnené osoby dostať do priestorov spoločnosti.	100%
A.11.2	**Bezpečnosť zariadení**			
A.11.2.1	Umiestnenie zariadení a ich ochrana	Sú umiestené a chránené zariadenia s cieľom obmedziť riziká vyplývajúce z hrozieb prostredia a riziká a príležitosti neautorizovaného prístupu?	Zariadenia sú umiestnené a chránené aby sa obmedzil neoprávnený prístup.	100%
A.11.2.2	Podporné služby	Sú zariadenia chránené pred výpadkami elektrickej energie a inými anomáliami spôsobenými zlyhaním dodávky podporných služieb?	V spoločnosti sú z časti chránené zariadenia proti zlyhaniu napájania, podpornými službami.	40%
A.11.2.3	Bezpečnosť kabeláže	Je chránená elektrická alebo telekomunikačná kabeláž prenášajúca dáta alebo podporujúce informačné služby pred odpočúvaním, manipuláciou alebo poškodením?	Telekomunikačné kabeláže sú chránené pred odpočúvaním, manipuláciou a len dôležitá kabeláž je chránená proti poškodeniu.	75%
A.11.2.4	Údržba zariadení	Sú zariadenia správne udržiavané, aby sa zaistila ich nepretržitá dostupnosť a integrita?	Každé zariadenie je správne udržiavané.	100%
A.11.2.5	Odstránenie aktív	Odnášajú sa prístroje, informácie alebo softvér bez autorizácie mimo pracoviska?	Odnášanie prístrojov, informácií a softvéru je podmienené autorizáciou.	90%
A.11.2.6	Bezpečnosť zariadení mimo organizácie	Aplikuje sa bezpečnosť aj na zariadenia mimo priestorov organizácie?	Používanie zariadení mimo priestory spoločnosti je zabezpečené voči rizikám, ktoré vyplávajú z jeho použitia.	100%
A.11.2.7	Bezpečnostné vyradenie alebo opätovné používanie zariadení	Kontrolujú sa všetky prvky zariadení obsahujúce úložné médiá, čím sa zabezpečí, že všetky citlivé dáta a licencovaný softvér sú bezpečne zmazané alebo prepísané ešte pred vyradením alebo opätovným použitím zariadenia?	V spoločnosti všetky zariadenia ktoré obsahujú pamäťové média sú kontrolované aby bolo možné zaistiť že pred likvidáciou alebo opakovaným použitím boli dáta odstránené alebo bezpečne prepísané.	100%
A.11.2.8	Neobsluhované zariadenia	Je zabezpečené aby aj neobsluhované zariadenia mali vhodnú ochranu?	V spoločnosti každé neobsluhované zariadenia majú príslušne aplikovanú ochranu (napr. rack)	100%

A.11.2.9	Politika čistého stola a čistej obrazovky	Je zavedená politika čistého stola, pokiaľ ide o dokumenty a prenosné médiá, a politika čistej obrazovky, pokiaľ ide o prostriedky spracúvania informácií?	V spoločnosti je z časti zavedená politika čistého stola. Politika čistej obrazovky nie je zavedená.	45%
A.12	**Bezpečnosť prevádzky**			
A.12.1	**Prevádzkové postupy a zodpovednosť**			
A.12.1.1	Dokumentované prevádzkové postupy	Sú dokumentované a udržiavané prevádzkové postupy, dostupné pre všetkých používateľov, ktorí ich potrebujú?	Prevádzkové postupy sú dokumentované, udržiavané a dostupné všetkým užívateľom podľa potreby.	100%
A.12.1.2	Riadenie zmien	Sú riadené zmeny v organizácii, obchodných procesoch, prostriedkoch spracúvajúcich informácie a systémoch?	V spoločnosti sú riadené zmeny systému a prostriedky pre spracúvanie informácií.	100%
A.12.1.3	Riadenie kapacít	Sú monitorované a dolaďované použitie prostriedkov za účelom odhadu budúcich požiadaviek na kapacity, čím sa zabezpečí dosiahnutie požadovaného výkonu systému?	V spoločnosti boli zavedené prostriedky pre monitorovanie a dolaďovanie použitie prostriedkov.	100%
A.12.1.4	Oddelenie prevádzkových, vývojových a testovacích prostredí	Sú tieto prostredia oddelené?	Pre zníženie rizika neoprávneného prístupu k prevádzkovanému systému a jeho zmien sú tieto prostredia oddelené.	100%
A.12.2	**Ochrana pred škodlivým softvérom**			
A.12.2.1	Opatrenia proti škodlivému softvéru	Sú implementované opatrenia detekcie, predchádzania a obnovy na ochranu pred škodlivým softvérom, kombinované s budovaním povedomia používateľov?	V spoločnosti sú implementované opatrenia na detekciu škodlivých programov.	100%
A.12.3	**Zálohovanie**			
A.12.3.1	Zálohovanie informácií	Testujú a robia sa pravidelne záložné kópie dôležitých informácií a softvéru v súlade so schválenou politikou zálohovania?	Záložné kópie informácií a programového vybavenia spoločnosti sú zálohované a testované v pravidelných intervaloch externou firmou kde vznikajú riziká.	30%
A.12.4	**Zaznamenávanie dát a monitorovanie**			
A.12.4.1	Zaznamenávanie udalostí	Vytvárajú a preskúmavajú sa záznamy udalostí zaznamenávajúce aktivity používateľov, výnimky a udalosti informačnej bezpečnosti?	V spoločnosti je len z časti zavedené zaznamenávanie aktivity používateľov.	50%
A.12.4.2	Ochrana záznamov informácií	Sú chránené informácie obsiahnuté v záznamoch, ako aj prostriedky na ich tvorbu pred neoprávnenými zásahmi a neautorizovaným prístupom?	Prostriedky pre zaznamenávanie informácií ako aj prostriedky na ich tvorbu sú chránené proti sfalšovaniu a neoprávnenému prístupu.	100%
A.12.4.3	Záznamy činnosti správcov a operátorov	Zaznamenávajú sa aktivity systémového správcu a záznamy sa chránia a pravidelne preskúmavajú?	V spoločnosti sú aktivity systémového správcu zaznamenávané, chránené a pravidelne preskúmavané.	100%
A.12.4.4	Synchronizácia času	Sú hodiny na všetkých relevantných systémoch synchronizované podľa jediného časového zdroja?	Hodiny na všetkých systémoch sú v spoločnosti synchronizované podľa časového zdroja.	100%
A.12.5	**Riadenie prevádzkového softvéru**			
A.12.5.1	Inštalácia softvéru na prevádzkové systémy	Sú zavedené postupy na riadenie inštalácie softvéru na prevádzkové systémy?	V spoločnosti sú zavedené postupy na riadenie inštalácie softvéru na prevádzkové systémy.	100%

A.12.6	**Riadenie technickej zraniteľnosti**			
A.12.6.1	Riadenie technickej zraniteľnosti	Zhromažďujú sa včasné informácie o technickej zraniteľnosti využívaných informačných systémov a zhodnocuje sa miera vystavenia sa zraniteľnosti?	V spoločnosti sa zhromažďujú včasné informácie o technickej zraniteľnosti využívaných informačných systémoch a zhodnocuje sa miera vystavenia sa zraniteľnosti.	90%
A.12.6.2	Obmedzenia pri inštalácii softvéru	Sú zavedené pravidlá na strategické riadenie inštalácie softvéru používateľmi?	V spoločnosti sú zavedené pravidlá na inštaláciu softvéru používateľmi. Používateľom je dovolené inštalovať len odsúhlasené programy.	100%
A.12.7	**Audit informačných systémov**			
A.12.7.1	Opatrenia auditu informačných systémov	Plánujú a odsúhlasujú sa požiadavky na audit a aktivity zahŕňajúce kontroly prevádzkových systémov, aby sa minimalizovalo riziko prerušení podnikových procesov ?	V spoločnosti sa pravidelne vykonávajú interné audity za účelom kontroly prevádzkových systémov, za účelom zníženie rizika porušenia podnikových procesov.	100%
A.13	**Komunikačná bezpečnosť**			
A.13.1	**Riadenie bezpečnosti v sieťach**			
A.13.1.1	Sieťové opatrenia	Sú siete primerane riadené a spravované, čím sa zabezpečí ochrana informácií v systémoch a aplikáciách?	V spoločnosti sú siete vhodným spôsobom spravované a kontrolované pre zaistení ochrany pred možnými hrozbami.	95%
A.13.1.2	Bezpečnosť sieťových služieb	Sú identifikované a zahrnuté do ustanovení o sieťových službách bezpečnostné funkcie?	Bezpečnostné funkcie sú v spoločnosti identifikované a zahrnuté do ustanovení ako aj v prípadoch kedy sú zaistené interne, tak aj v prípadoch outsourcingu.	100%
A.13.1.3	Oddeľovanie sietí	Sú oddeľované skupiny informačných služieb, používateľov a informačných systémov?	V spoločnosti sú oddeľované skupiny informačných služieb, používateľov a informačných systémov.	100%
A.13.2	**Prenos informácií**			
A.13.2.1	Politiky a postupy pri prenose informácií	Sú formálne politiky, postupy a opatrenia týkajúce sa výmeny zavedené s cieľom chrániť výmenu informácií vykonávanú prostredníctvom všetkých druhov komunikačných zariadení?	V spoločnosti sú ustanovené a do praxe zavedené formálne politiky na ochranu informácií pri ich výmene.	100%
A.13.2.2	Zmluvy o výmene informácií	Sú uzavreté zmluvy o výmene softvéru a informácií medzi organizáciou a tretími stranami?	Výmena informácií a softvéru je založená na dohodách uzatvorených medzi spoločnosťou a externým subjektom.	100%
A.13.2.3	Výmena elektronických správ	Sú chránené informácie, ktoré spadajú do kategórie vymieňaných elektronických správ?	V spoločnosti sú elektronické správy ktoré prenášajú informácie dostatočne chránené.	100%
A.13.2.4	Zmluvy o dôvernosti alebo utajení	Sú definované, pravidelne preskúmavané a dokumentované požiadavky na zmluvy o dôvernosti alebo utajení, ktoré zohľadňujú potreby organizácie na ochranu informácií?	V spoločnosti sú definované, pravidelne preskúmavané a dokumentované požiadavky na zmluvy o dôvernosti alebo utajení.	95%

A.14	Akvizícia, vývoj a údržba informačných systémov			
A.14.1	**Bezpečnostné požiadavky na informačné systémy**			
A.14.1.1	Analýza a špecifikácia bezpečnostných požiadaviek	Sú začlenené požiadavky spojené s informačnou bezpečnosťou do požiadaviek pre nové informačné systémy alebo do požiadaviek rozšírenia existujúcich informačných systémov?	V spoločnosti sú začlenené požiadavky do požiadaviek rozšírenia existujúcich informačných systémov.	95%
A.14.1.2	Zabezpečenie aplikačných služieb vo verejných sieťach	Sú informácie, ktoré sa používajú v aplikačných službách, používajúc verejné dátové siete, chránené pred podvodnými aktivitami, aktivitami spochybňujúcimi zmluvné podmienky a neautorizovaným vyzradením alebo úpravou?	Informácie ktoré sú v spoločnosti publikované na verejno prístupných systémoch sú chránené proti neoprávnenou modifikáciou.	100%
A.14.1.3	Ochrana pri transakciách aplikačných služieb	Sú informácie obsiahnuté v transakciách aplikačných služieb chránené, aby sa zabránilo nekompletným prenosom, nesprávnemu smerovaniu, neautorizovaným úpravám správ, neautorizovanému prezradeniu, neautorizovanému duplikovaniu správ alebo neautorizovaným odpovediam?	V spoločnosti je vhodne zaistená ochrana informácií ktoré sú prenášané pri on-line transakciách,	100%
A.14.2	**Bezpečnosť pri vývoji a pri podporných procesoch**			
A.14.2.1	Politika bezpečného vývoja	Sú pravidlá na vývoj softvéru a systémov vytvorené a zavedené do procesu vývoja v rámci organizácie?	V spoločnosti sú zavedené pravidlá na vývoj softvéru a systémov a sú zavedené do procesov v rámci organizácie.	100%
A.14.2.2	Postupy riadenia systémových zmien	Je implementácia zmien do systémov v rámci životného cyklu riadená prostredníctvom formálnych procedúr riadenia zmien?	V spoločnosti sú zavedené formálne postupy pri implementácii zmien.	100%
A.14.2.3	Technické preskúmanie aplikácií po zmene operačného systému	Vykonáva sa pri zmene operačného systému revízia kritických aplikácií, ako aj testovanie s cieľom zabezpečiť, že to nebude mať za následok negatívny vplyv na prevádzku organizácie alebo na bezpečnosť?	V prípade zmeny operačného systému sú v spoločnosti otestované kritické aplikácie, aby bolo zaistené, že zmeny nemajú dopad na prevádzku alebo bezpečnosť organizácie.	100%
A.14.2.4	Obmedzenia zmien v softvérových balíkoch	Predchádza sa neopodstatneným modifikáciám softvérových balíkov a vykonávajú sa nevyhnutné zmeny?	Modifikácia programových balíkov je v spoločnosti obmedzená. Všetky vykonávané zmeny musia byť riadené.	100%
A.14.2.5	Princípy bezpečného vývoja systémov	Vytvárajú, dokumentujú a udržiavajú sa princípy bezpečného vývoja systémov pre všetky činnosti spojené so zavedením informačných systémov?	V spoločnosti sa vytvárajú, dokumentujú a udržiavajú princípy bezpečného vývoja pre všetky činnosti spojené so zavedením informačných systémov.	100%
A.14.2.6	Prostredie na bezpečný vývoj	Vytvára organizácia a primerane chráni vývojové prostredie na vývoj systémov a ich integráciu s úsilím, ktoré pokryje celý životný cyklus vývoja?	Spoločnosť vytvára a priemerne chráni vývojové prostredie na vývoj systémov.	100%
A.14.2.7	Vývoj prostredníctvom outsourcingu	Je vývoj softvéru prostredníctvom outsourcingu (externých zdrojov) pod dohľadom organizácie a monitoruje aktivity vývoja systému, ktorý sa vykonáva formou outsourcingu?	V spoločnosti je vývoj pod dohľadom a monitorujú sa aktivity vývoja.	100%

A.14.2.8	Testovanie bezpečnosti systémov	Testujú sa počas vývoja bezpečnostné funkcie?	V spoločnosti sa počas vývoja testujú bezpečnostné funkcie.	100%
A.14.2.9	Akceptačné testy systémov	Vytvárajú sa pre nový informačný systém, aktualizáciu a novú verziu, programy akceptačného testovania s príslušnými kritériami?	V spoločnosti sa vytvárajú akceptačné testy s príslušnými kritériami.	100%
A.14.3	**Testovacie údaje**			
A.14.3.1	Ochrana testovacích údajov	Vyberajú, chránia a riadia sa testovacie údaje?	V spoločnosti sa testovacie údaje chránia a riadia.	100%
A.15	Riadenie vzťahov s dodávateľmi			
A.15.1	**Informačná bezpečnosť vo vzťahoch s dodávateľmi**			
A.15.1.1	Politika informačnej bezpečnosti na vzťahy s dodávateľmi	Sú odsúhlasené s dodávateľom a formálne zdokumentované požiadavky informačnej bezpečnosti na zníženie rizík spojených s dodávateľskými prístupmi do aktív organizácie?	V spoločnosti sú odsúhlasené požiadavky informačnej bezpečnosti rizík spojených s dodávateľskými prístupmi do aktív.	100%
A.15.1.2	Ošetrenie bezpečnosti v zmluvách s dodávateľmi	Sú definované všetky relevantné požiadavky informačnej bezpečnosti a odsúhlasené s každým dodávateľom, ktorý môže mať prístup k informáciám organizácie, spracúvať ich, ukladať, komunikovať alebo poskytovať infraštruktúrne komponenty?	V spoločnosti sú definované všetky požiadavky informačnej bezpečnosti a odsúhlasené s dodávateľmi.	100%
A.15.1.3	Dodávateľské reťazce informačných a komunikačných technológií	Sú v zmluvách s dodávateľmi obsiahnuté požiadavky týkajúce sa rizík informačnej bezpečnosti spojených s informačnými a komunikačnými službami a produktmi siete dodávateľov?	V zmluvách s dodávateľmi sú obsiahnuté požiadavky týkajúce sa rizík informačnej bezpečnosti.	95%
A.15.2	**Riadenie dodávateľských služieb**			
A.15.2.1	Monitorovanie a preskúmanie dodávateľských služieb	Vykonávajú sa pravidelne audity a monitorovania služieb dodávateľov?	U dodávateľov sa pravidelne vykonávajú audity a monitorujú sa dodávateľské služby.	80%
A.15.2.2	Riadenie zmien v službách dodávateľa	Sú zmeny v ustanoveniach služieb vrátane udržiavania a zlepšovania aktuálnych politík informačnej bezpečnosti, postupov a opatrení riadené?	V spoločnosti sú riadené uvedené zmeny.	90%
A.16	**Riadenie incidentov informačnej bezpečnosti**			
A.16.1	**Riadenie incidentov informačnej bezpečnosti a zlepšovania**			
A.16.1.1	Zodpovednosť a postupy	Sú zavedené zodpovednosti a postupy riadenia incidentov s cieľom zaistiť rýchly a efektívny ohlas na bezpečnostné incidenty?	Pre zaistenie rýchlej, účinnej systematickej reakcie na bezpečnostné incidenty sú v spoločnosti zavedené postupy pre zvládanie bezpečnostných incidentov.	100%
A.16.1.2	Informovanie o udalostiach informačnej bezpečnosti	Informuje sa o udalostiach vhodnými riadiacimi kanálmi, tak rýchlo ako je to možné?	V spoločnosti sa informuje o udalostiach tak rýchlo ako je to možné.	80%
A.16.1.3	Informovanie o slabinách informačnej bezpečnosti	Požaduje sa od zamestnancov a zmluvných partnerov, ktorí používajú informačný systém a služby organizácie, aby zaznačovali každý pozorovaný alebo podozrivý nedostatok v systémoch alebo službách a informovali o ňom?	V spoločnosti je požadované informovanie o nedostatkoch v systémoch alebo službách.	90%

A.16.1.4	Posúdenie udalostí informačnej bezpečnosti a rozhodnutia o nich	Posudzujú a rozhodujú sa udalosti informačnej bezpečnosti, či budú klasifikované ako incidenty informačnej bezpečnosti?	V spoločnosti sa posudzujú a rozhodujú udalosti informačnej bezpečnosti, či budú klasifikované ako incidenty.	100%
A.16.1.5	Reakcia na incidenty informačnej bezpečnosti	Reaguje sa na incidenty informačnej bezpečnosti v súlade s dokumentovanými postupmi?	V spoločnosti sú definované procedúry upravujúce spôsob reakcie na identifikované bezpečnostné udalosti.	95%
A.16.1.6	Poučenie z incidentov informačnej bezpečnosti	Používajú sa poznatky získané z analýzy a riešenia incidentov informačnej bezpečnosti na zníženie pravdepodobnosti alebo následkov budúcich incidentov?	V spoločnosti existujú mechanizmy, ktoré umožňujú kvantifikovať a monitorovať typy, rozsah a náklady bezpečnostných incidentov.	95%
A.16.1.7	Zber dôkazov	Definovala a prijala organizácia postupy na identifikáciu, zber, získanie a ochranu informácií, ktoré môžu slúžiť ako dôkaz?	V spoločnosti sú stanovené procedúry na vyšetrovanie bezpečnostných incidentov.	95%
A.17	**Aspekty informačnej bezpečnosti v riadení kontinuity**			
A.17.1	**Kontinuita informačnej bezpečnosti**			
A.17.1.1	Plánovanie kontinuity informačnej bezpečnosti	Určuje organizácia svoje požiadavky na informačnú bezpečnosť a kontinuitu riadenia informačnej bezpečnosti v nepriaznivých situáciách, napr. počas krízy alebo katastrofy?	Spoločnosť určuje požiadavky na informačnú bezpečnosť počas krízy alebo katastrofy.	100%
A.17.1.2	Implementovanie kontinuity informačnej bezpečnosti	Vytvorila, zdokumentovala a zaviedla organizácia procesy, postupy a opatrenia na zabezpečenie požadovanej úrovne kontinuity pre informačnú bezpečnosť počas nepriaznivých situácií?	V spoločnosti sú vytvorené, zdokumentované a zavedené procesy a opatrenia na zabezpečenie požadovanej úrovne počas nepriaznivých situácií.	100%
A.17.1.3	Overenie, preskúmanie a vyhodnotenie kontinuity informačnej bezpečnosti	Overuje organizácia vytvorené a zavedené opatrenia na kontinuitu informačnej bezpečnosti v pravidelných intervaloch, aby sa zabezpečila ich platnosť a efektívna funkčnosť počas nepriaznivých situácií?	Spoločnosť overuje vytvorené a zavedené opatrenia na kontinuitu informačnej bezpečnosti aby zabezpečila efektívnu funkčnosť počas nepriaznivých situácií.	100%
A.17.2	**Refundácia**			
A.17.2.1	Dostupnosť zariadení na spracovanie informácií	Sú zariadenia na spracúvanie informácií zriadené s dostatočnou redundanciou, aby sa dosiahli požiadavky na dostupnosť?	V spoločnosti sú zariadenia na spracúvanie informácií zriadené s dostatočnou redundanciou.	100%
A.18	**Súlad**			
A.18.1	**Súlad s právnymi a zmluvnými požiadavkami**			
A.18.1.1	Identifikácia platnej legislatívy a zmluvných požiadaviek	Sú všetky relevantné štatutárne, regulačné a zmluvné požiadavky explicitne definované, dokumentované a udržiavané v aktuálnej podobe pre každý informačný systém a organizáciu ako celok?	V spoločnosti je pre každý informačný systém jednoznačne definovaný, dokumentovaný a udržiavaný v aktuálnej podobe pre každý celok.	100%
A.18.1.2	Práva duševného vlastníctva	Sú implementované vhodné postupy, ktoré by zabezpečili súlad so zákonnými, regulačnými a zmluvnými požiadavkami, pokiaľ ide o používanie materiálu v zmysle práv duševného vlastníctva a používania patentovaných softvérových produktov?	V spoločnosti sú pre zaistenie súladu so zákonnými, regulačnými a zmluvnými požiadavkami zavedené vhodné postupy.	100%

A.18.1.3	Ochrana záznamov	Sú záznamy chránené pred stratou, zničením a falzifikáciou v súlade so štatutárnymi, regulačnými, zmluvnými alebo podnikovými požiadavkami?	Dôležité záznamy spoločnosti sú chránené pred stratou, zničením a falzifikáciu ale nie všetky sú pravidelne zálohované.	70%
A.18.1.4	Súkromie a ochrana osobných údajov	Je súkromie a ochrana osobných údajov zabezpečená na základe požiadaviek príslušnej legislatívy a príslušných nariadení?	V spoločnosti je súkromie a ochrana osobných údajov dostatočne zabezpečené.	100%
A.18.1.5	Nariadenie o kryptografických opatreniach	Sú kryptografické opatrenia zavedené s cieľom dosiahnuť súlad so všetkými platnými dohodami, zákonmi a právnymi nariadeniami?	V spoločnosti sú kryptografické opatrenia v súlade s príslušnými dohodami, zákonmi a predpismi.	100%
A.18.2	**Preskúmanie informačnej bezpečnosti**			
A.18.2.1	Nezávislé preskúmanie informačnej bezpečnosti	Preskúmava prístup organizácie k riadeniu informačnej bezpečnosti (napr. ciele riadenia, opatrenia, politiky, procesy a postupy informačnej bezpečnosti) nezávislá entita v plánovaných intervaloch, alebo keď sa uskutočnia závažné zmeny?	Prístup k riadeniu sa v spoločnosti preskúmava nezávislou entitou v pravidelných intervaloch.	100%
A.18.2.2	Súlad s bezpečnostnými politikami a normami	Preverujú pravidelne manažéri súlad spracúvania informácií v rámci ich rozsahu zodpovednosti so znením príslušných bezpečnostných politík, noriem a iných bezpečnostných požiadaviek?	V spoločnosti pravidelne manažéri preverujú súlad spracúvania informácií.	100%
A.18.2.3	Preskúmanie technického súladu	Preskúmavajú sa informačné systémy z hľadiska súladu s politikami a normami informačnej bezpečnosti organizácie?	V spoločnosti sa pravidelne preskúmavajú informačné systémy.	100%