TECHNICKÁ UNIVERZITA V LIBERCI
Ekonomická fakulta

NÁVRH VYBRANÝCH SLUŽEB KYBERNETICKÉ BEZPEČNOSTI

Bakalářská práce

Studijní program: B6209 – Systémové inženýrství a informatika
Studijní obor: 6209R021 – Manažerská informatika

Autor práce: **Lukáš Halama**
Vedoucí práce: Ing. Zbyněk Hubínka

Liberec 2015

TECHNICAL UNIVERSITY OF LIBEREC
Faculty of Economics

DESIGN OF SELECTED CYBER SECURITY SERVICES

Bachelor thesis

Study programme: B6209 – System Engineering and Informatics
Study branch: 6209R021 – Managerial Informatics

Author: **Lukáš Halama**
Supervisor: Ing. Zbyněk Hubínka

Liberec 2015

TECHNICKÁ UNIVERZITA V LIBERCI
Ekonomická fakulta
Akademický rok: **2014/2015**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Lukáš Halama**
Osobní číslo:	**E12000505**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Manažerská informatika**
Název tématu:	**Návrh vybraných služeb kybernetické bezpečnosti**
Zadávající katedra:	**Katedra informatiky**

Zásady pro vypracování:

1. Analýza aktuálních možností a prostředků v oblasti kybernetické bezpečnosti
2. Rozbor zákonů a norem vztahujících se ke kybernetické bezpečnosti
3. Návrh a tvorba produktů a služeb týkajících se bezpečnosti informací
4. Vytvoření rozpočtu a analýza trhu
5. Zhodnocení vytvořeného portfolia služeb a produktů

Rozsah grafických prací:

Rozsah pracovní zprávy: **30 normostran**

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

Seznam odborné literatury:

Návrh zákona o kybernetické bezpečnosti [online]. 2014. Dostupné z WWW: http://www.govcert.cz/download/nodeid-629/.
DOUCEK, P., L. NOVÁK, L. NEDOMOVÁ a V. SVATÁ. Řízení bezpečnosti informací: 2. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.
POŽÁR, J. Informační bezpečnost. 1. vyd. Plzeň: Aleš Čeněk, 2005. ISBN 80-868-9838-5.
KALAMÁR, Š. a J. POŽÁR. Vybrané aspekty informační bezpečnosti. 1. vyd. Praha: Policejní akademie České republiky v Praze, 2010. ISBN 978-80-7251-339-0.
MARTELLINI, M. Cyber security: deterrence and IT protection for critical infrastructures. 1st ed. Cham: Springer, 2013. ISBN 33-190-2278-4.
Elektronická databáze článků ProQuest (knihovna.tul.cz).

Vedoucí bakalářské práce: **Ing. Zbyněk Hubínka**
Katedra informatiky

Konzultant bakalářské práce: **Jan Chudan**
Elektronický zkušební ústav Praha

Datum zadání bakalářské práce: **31. října 2014**

Termín odevzdání bakalářské práce: **7. května 2015**

doc. Ing. Miroslav Žižka, Ph.D.
děkan

L.S.

Technická univerzita v Liberci
Ekonomická fakulta

doc. Ing. Jan Skrbek, Dr.
vedoucí katedry

V Liberci dne 31. října 2014

Prohlášení

Byl jsem seznámen s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé bakalářské práce pro vnitřní potřebu TUL.

Užiji-li bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Bakalářskou práci jsem vypracoval samostatně s použitím uvedené literatury a na základě konzultací s vedoucím mé bakalářské práce a konzultantem.

Současně čestně prohlašuji, že tištěná verze práce se shoduje s elektronickou verzí, vloženou do IS STAG.

Datum:

Podpis:

Poděkování

Tímto bych chtěl poděkovat vedoucímu mé bakalářské práce Ing. Zbyňku Hubínkovi za odborné vedení a užitečné a kvalifikované rady a připomínky, jenž mi pomohly při vypracování bakalářské práce. Dále bych chtěl poděkovat všem, kteří mi pomohli při hledání potřebných informací a vždy mi dobře poradili. Velké díky patří také konzultantovi mé bakalářské práce Janu Chudanovi.

Anotace

Bakalářská práce se zabývá tématem kybernetické a informační bezpečnosti. Výsledkem práce je návrh produktu a služeb v této oblasti, jehož hlavním zdrojem je nový zákon o kybernetické bezpečnosti. Práce je rozdělena do dvou částí, a to část teoretickou a část praktickou. Teoretická část se věnuje důležitým pojmům z oblasti kybernetické bezpečnosti a analýze aktuálních možností a prostředků v této oblasti nejen v České republice, ale i v zahraničí. Praktická část čerpá ze znalostí nabytých v části teoretické a zaměřuje se na návrh produktu a služeb od úplného počátku až po přípravu finálního produktu pro uvedení na trh. Nejprve rozebírá jednotlivé zákony a normy, které jsou nezbytné pro tvorbu komplexních produktů a služeb kybernetické bezpečnosti a následně vysvětluje tvorbu potřebné dokumentace a následnou tvorbu služeb.

Klíčová slova

Kybernetická bezpečnost, tvorba produktu a služeb, normy, kyberkriminalita

Annotation

Design of selected cyber security services

This thesis deals with the topic of cyber security. The result of this work is design of products and services in this area and it´s main source is new law about cyber security. The work is divided in two parts, the theoretical part and the practical part. The theoretical part deals with important laws and standards of cyber security and analysis of actual possibilities and resources in Czech Republic and abroad. The practical part draws on the knowledge acquired in the theoretical part and deals with design of product and services from the beginning to the preparation of final product for launch on market. Firstly, it analyzes laws and standards which are necessary for design of complex products and services of cyber security and then it describes creating of proper documentation and final design of cyber security services.

Key Words

Cyber security, design of product and services, standards, cyber criminality

Obsah

Seznam tabulek

Seznam obrázků

Seznam zkratek

BCM	Business Continuity Management
BI	Business Intelligence
ČR	Česká republika
ERP	Enterprise Resource Planning
EZÚ	Elektrotechnický zkušební ústav
ICT	Informační a Komunikační technologie
IS	Informační systém
ISG	Information Security Government
ISMS	Information Security Management System
ISVS	Informační systém veřejné správy
IT	Informační technologie
KB	Kybernetická bezpečnost
KII	Kritická informační infrastruktura
KZ	Kybernetické zabezpečení
MD	Man days
NBÚ	Národní bezpečnostní úřad
VIS	Významný informační systém

Úvod

V poslední době jsme svědky obrovského vzrůstu využívání informačních a komunikačních technologií nejen v pracovním prostředí, ale také v osobním životě. Každý z nás již používá tzv. chytrá zařízení, jako jsou telefony, televize apod., která jsou ve většině případů připojena k internetu. Pomocí těchto zařízení se prakticky pohybujeme v kyberprostoru, kde se odehrává veškerá naše komunikace. V tomto prostředí bohužel působí mnoho nebezepečných činitelů, kterým je nutno se vyvarovat a bránit se proti nim.

Informace jsou tedy velmi důležitým aktivem, bez kterého by většina organizací nebyla schopna fungovat. Proto je nutné klást velký důraz na informační bezpečnost a stejně tak na bezpečnost technologií, které s nimi nakládají.

Cílem této práce je navrhnout produkt a služby zaměřené na oblast kybernetické a informační bezpečnosti. Aby bylo možné tohoto cíle dosáhnout, je nutné se seznámit s problematikou této oblasti. Proto se první část práce zaměřuje na definici základních pojmů informační bezpečnosti a popis jejího řízení. Jelikož součástí produktu a služeb je provádění auditů, věnuje se teoretická část i jim. V druhé části práce je nejdříve vytvořen souhrn zákona a přehledy norem, které jsou pro tuto oblast stěžejní a následně je popsán postup tvorby daného produktu a služeb v oblasti kybernetické a informační bezpečnosti a jeho jednotlivé části. Vzhledem k časové náročnosti je v práci detailně popsána pouze první úroveň produktu ze tří, která obsahuje základní systémové požadavky a zajišťuje plnění zákona o kybernetické bezpečnosti.

1. Literární rešerše v oblasti kybernetické bezpečnosti

Co se týče knižních zdrojů, přínosnou publikací byla kniha *„Řízení bezpečnosti informací 2. rozšířené vydání o BCM“*[1]. Tato kniha vysvětluje veškeré základní pojmy v oblasti informační bezpečnosti, popisuje metodiky řízení a hodnocení bezpečnosti a také pojednává o systému řízení informační bezpečnosti, jenž je pro tuto oblast stěžejní. Dále pak jsou zde uvedeny záladní informace o auditech, úřadech, institucích a organizacích, které se danou oblastí zabývají. Další knihou byla *„Kybernetická kriminalita: nejen o hackinu, crackingu, virech a trojských koních bez tajemství“*[2], která popisuje prostředí kyberkriminality. Tato publikace poskytuje široký pohled na kyberprostor, ve kterém popisuje toto téma jak z pohledu v minulosti, tak i z pohledu dnešního. Pojednává o všech aspektech kybrekriminality ať už se jedné o cracking, hacking, kyberterorismus a další nelegální aktivity v kyberprostoru. Nechybí ani popis různých druhů útoků a také metody jejich vyšetřování.

Mezi příspěvky, které mne uvedly do problematiky kybernetické bezpečnosti v České Republice, patří především *„Kybernetická bezpečnost v ČR.“*[3] Stručně popisuje hlavní data, vztahující se k řešení kybernetické bezpečnosti v ČR a to od 15. března 2010, kdy bylo vládou schváleno usnesení č. 205 o řešení problematiky kybernetické bezpečnosti a Ministerstvo Vnitra bylo ustaveno gestorem této problematiky a zároveň národní autoritou pro tuto oblast. Poslední důležitou událostí pak bylo podepsání zákona o kybernetické bezpečnosti prezidentem, které proběhlo 13. srpna 2014 a od 1. ledna 2015 nabývá zákon platnosti. Dalším článkem o současném dění v oblasti kybernetické bezpečnosti v ČR je

---

[1] DOUCEK, P., L. NOVÁK, L. NEDOMOVÁ a V. SVATÁ. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2.přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.

[2] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.

[3] *Kybernetická bezpečnost v ČR*. In: CyberSecurity.cz [online]. 2014 [cit. 2015-02-10]. Dostupné z: http://www.cybersecurity.cz/basic.html

„ČR a Izrael budou spolupracovat v oblasti kybernetické bezpečnosti“[4]. Česká Republika a Izrael spolu mají dlouhodobé historické vztahy a s ohledem na aktuální bezpečnostní rizika se rozhodli podepsat Společné prohlášení o spolupráci mezi vládami obou států. Státy tak budou mezi sebou sdílet informace, osvědčené postupy a zkušenosti, které se týkají bezpečnostních hrozeb a událostí. Samozřejmě budou sdíleny také informace o výzkumu a nových projektech.

Při hledání článků v databázích ProQuest jsem nalezl několik článků. Prvním článkem je *„Cyber Attacks: Emerging Threats to the 21st Century Critical Information Infrastructures“*[5], který pojednává o kybernetických útocích. Je rozdělen na tři části. V první části vysvětluje, že kybernetické útoky, kybernetická válka a kybernetická obrana jsou pojmy, které nejsou nijak mezinárodně definovány. V druhé části je analyzována počítačová realita v posledních letech a autor se soustředí na dvě poučení a to, že je složité definovat kybernetickou válku a také se proti ní bránit. V třetí části je pojednáváno o dopadech kybernetických útoků na státy a o roli NATO při zajišťování všeobecné kolektivní kybernetické obrany. Dalším článkem je *„Information security predictions for 2015“*[6], ve kterém autoři předvídají jaké události a rizika budou s největší pravděpodobností hrozit v roce 2015. Bude nutno zvýšit bezpečnostní praktiky např. v kryptografii, která by se měla začít používat více. Dálepak odhadují, že rok 2015 bude rokem tzv. potencionálně nechtěného softwaru, který je většinou do mobilních zařízení instalován spolu s aplikacemi, které jsou zadarmo. Další hrozbou pak bude skutečnost, že

---

[4] PŘECH, Vladimír. *ČR a Izrael budou spolupracovat v oblasti kybernetické bezpečnosti*. In: KYBEZ - Portál Kybernetické bezpečnosti [online]. 2014 [cit. 2015-02-10]. Dostupné z: https://www.kybez.cz/zpravy/-/blogs/cr-a-izrael-podepsaly-prohlaseni-o-spolupraci-v-oblasti-kyberneticke-bezpecnosti

[5] VASILESCU, Cezar. *Cyber Attacks: Emerging Threats to the 21st Century Critical Information Infrastructures*. Univerzita Obrany. Ustav Strategickych Studii. Obrana a Strategie [online]. 2012, č. 1, s. 9 [cit. 2015-02-10]. Dostupné z: http://search.proquest.com/docview/1026970922?accountid=17116

[6] *Information security predictions for 2015*. CIOL [online]. 2015, č. 1 [cit. 2015-02-10]. Dostupné z: http://search.proquest.com/docview/1645898871?accountid=17116

útočníci budou získávat informace např. ze sociálních sítí a tak budou schopní lépe útoky přizpůsobit.

2. Kybernetická a informační bezpečnost

2.1 Kyberprostor[7]

Existuje mnoho definic pro termín kyberprostor. Poprvé tento termín použil ve své knize Neuromancer W. Gibson, avšak v tomto díle se jednalo o fikci popisující napojení mozku k počítači pomocí elektrod. Tímto způsobem se podle Gibsona člověk dostane do tzv. kyberprostoru. S narůstajícím rozvojem technologií se tento termín začal běžně užívat a s tím přišly i přesnější definice, které přiblížily, co tento termín znamená. Kyberprostorem tak chápeme existující počítačové, informační a komunikační sítě.

Podle zakladatele Electronic Frontier Foundation, Johna Barlowa, se člověk v kyberprostoru nachází v tu chvíli, kdy nějakým způsobem vstoupí do sítě. Tím je myšleno, že pokud např. telefonujeme nebo surfujeme po internetu, tak tím „putujeme“ po kyberprostoru.

2.2 Informační bezpečnost[8]

Informační bezpečnost je již dlouhou dobu velmi frekventovaný pojem, který nabývá každým rokem čím dál více na důležitosti obzvláště vzhledem ke stále se rozvíjejícím technologiím. Hodnota informací v organizacích se stále zvyšuje a proto je potřebné je dostatečně a efektivně chránit. Informace nabývají mnoha podob, ať už se jedná o tištěné, elektronické, vypozorované z procesů apod. Rizika úniku informací nehrozí pouze z vnějšího prostředí, ale hlavně i z prostředí vnitřního. Vzhledem k důležitosti a nezanedbatelnosti těchto informací je nutno chránit je takovým způsobem, aby k nim

---

[7] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, s. 17-35. ISBN 978-80-247-1561-2.

[8] Vybrané hrozby informační bezpečnosti organizace [online]. 2011. Dostupné z: http://www.cybersecurity.cz/data/Pozar2.pdf

mohly přistupovat pouze pověřené osoby, byly dostupné v tu chvíli, kdy jsou potřebné a aby bylo možné zjistit, kdo informace vytvořil, změnil nebo odstranil.

Informační bezpečností tedy rozumíme komplexní pohled pomáhající organizacím s poznáním cenných informací a dat a jejich ochranou. Nutností pro účinnou ochranu je pochopení toho, jaké informace a data organizace má a jakou mají pro ni hodnotu. Dále je potřeba stanovit si cíle a jak organizace funguje a na základě těchto informací je teprve možné začít formovat a navrhovat vhodný systém řízení informační bezpečnosti. Díky zavedení řidícího systému informační bezpečnosti organizace snižuje rizika, která jsou spojena s únikem informací. Spolu se snížením těchto rizik klesají také náklady na informační a komunikační technologie.

Tato oblast zaznamenává velice rychlý rozvoj ve vývoji programů pro ochranu dat a informací, nicméně stejným tempem vznikají stále nové programy vytvářené různými útočníky, jako jsou hackeři, teroristé apod. Vzhledem k této skutečnosti je nutné, aby organizace neustále zdokonalovaly svůj systém informační bezpečnosti. Vylepšování systému řízení však neznamená pouze zdokonalování programů a ochrany informačních a komunikačních technologií, ale i dostatečný dohled nad lidskými zdroji. Největším rizikem úniku informací jsou totiž právě lidské zdroje.

Zásadní význam má informační bezpečnost pro firmy, které ji prodávají jako své produkty nebo jako jejich součást. V případě prodeje informační bezpečnosti jako produktu se jedná o softwarové, právnické, zpravodajské a konzultační firmy. V jiných případech pak může bezpečnost informací ovlivnit jakost produktů. Jedná se například o chyby v dokumentaci v jaderném či leteckém průmyslu, kde by tyto chyby mohly způsobit nežádoucí provozní události.

2.3 Úrovně bezpečnosti[9]

Tato podkapitola pojednává o tom, že bezpečnost informací je součástí třech úrovní bezpečnosti. První úrovní je bezpečnost organizace, do které patří právě bezpečnost informací, pod níž spadá i poslední úroveň a to bezpečnost IS/ICT.

2.3.1 Bezpečnost organizace

Bezpečnost organizace je nejvyšší úrovní bezpečnosti. Spadá pod ní zajištění bezpečnosti objektů, majetku organizace, ostraha přístupů do objektů, strážní služba apod. Samozřejmě je propojena i s ostatními úrovněmi. S bezpečností IS/ICT je provázána např. kontrolou oprávnění přístupu do budov.

2.3.2 Bezpečnost informací

Bezpečnost informací má za úkol shrnutí zásad bezpečné práce s informacemi všech možných druhů a typů. Oproti bezpečnosti IS/ICT zahrnuje např. způsob zpracování dat, jejich ukládání a správy archivu nedigitálních dat, zásady skartace materiálů, nakládání s informacemi během jejich transportu, zásady pro poskytování informací novinářům, zásady pro veřejná vystupování pracovníků organizace apod.

2.3.3 Bezpečnost IS/ICT

Hlavním údělem bezpečnosti IS/ICT je ochrana aktiv, která jsou součástí informačního systému organizace podporovaného informačními a komunikačními technologiemi. Je to sice nejužší oblast řízení bezpečnosti, avšak je velmi důležitá a komplikovaná. V dnešní době si stále mnoho lidí neuvědomuje hodnotu dat. Kupříkladu při práci s daty uloženými na CD, vnímá člověk pouze hodnotu média, ale ne obsahu. Důležité je uvědomit si, že

[9] DOUCEK, P. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011, s. 55-57. ISBN 978-80-7431-050-8.

nepracujeme pouze s viditelnými médii, ale především s „neviditelnými“ daty, která jsou na médiích uložena.

2.4 Důležité pojmy informační bezpečnosti[10]

V této kapitole jsou přiblíženy důležité pojmy používané v oblasti informační bezpečnosti.

2.4.1 Aktiva

Z pohledu věcného rozumíme pod výrazem aktiva v oblasti IS/ICT především tyto dva druhy:

- hmotná aktiva
  - mezi tento druh aktiv zařazujeme technické prostředky výpočetní techniky, čímž jsou myšleny počítače, servery, firewally, další aktivní prvky počítačové sítě, kabelové rozvody a technická zařízení (tiskárny, scannery apod.)
- nehmotná aktiva
  - mezi tato aktiva patří zejména pracovní postupy, které organizace využívá v oblasti IS/ICT; data organizací vytvořená nebo převzatá, jež jsou pro její provoz důležitá; základní programové vybavení jako jsou operační systémy, programy nezbytné pro funkcionaliotu počítačových sítí, kryptografické systémy apod. a aplikační programové vybavení zahrnující např. textové editory, tabulkové procesory, programy pro tvorbu grafiky, ERP a BI aplikace; počítačové a komunikační služby a služby, které zajišťují provoz např. světel, topení nebo klimatizací

Dalším významným dělením aktiv je dělení z pohledu řízení bezpečnosti informací:

[10] DOUCEK, P. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011, s. 57-60. ISBN 978-80-7431-050-8.

- primární aktiva
  - jedná se především o informace využívané organizací, funkční procesy a aktivity, know-how a znalosti, které mají určitý význam pro systém řízení bezpečnosti informací
- sekundární aktiva
  - zahrnují hlavně hmotná aktiva jako je technické vybavení, komunikační infrastruktura, ale patří mezi ně i programové vybavení a zaměstnanci podílející se na chodu organizace

2.4.2 Hrozby

Hrozbou rozumíme nějakou potenciální příčinu nechtěného incidentu, jehož důsledkem může dojít k poškození systému či organizace. Hrozba je prakticky zneužitím zranitelnosti. Může na ní však být nahlíženo i z jiného pohledu a to jako na pravděpodobnost útoku, která je odvozena od atraktivnosti systému pro útočníka.

Hrozby lze rozdělit na:

- přírodní a fyzické
  - tyto hrozby jsou z většiny těžko předvídatelné a jedná se hlavně o živelné pohromy a nehody (povodně, hurikány, přerušení dodávky elektřiny apod.)
- technické a technologické
  - jedná se zejména o poruchy různých zařízení či komponent jako jsou poruchy počítačů, nosičů dat, poruchy sítí, nesprávná funkčnost programového vybavení apod.
- lidské
  - tyto hrozby mohou být buďto neúmyslné, čili zaviněné např. neznalostí nebo zanedbáním některých povinností anebo úmyslné, čímž je myšleno, že je hrozba způsobena zásahem zvenku (hackeři, teroristé, spionáž apod.), nebo zevnitř (návštevníci, hosté, zaměstnanci apod.)

Lidské hrozby jsou přitom nejčetnějšími ze všech a to hlavně ty zaviněné nedbalostí. Při pohledu na informační aktiva, jsou nejčastějšími hrozbami:

- prozrazení vnitřních informací
- upravení dat, které má za následek porušení integrity
- zničení dat systému
- bránění autorizovaným uživatelům při snaze data získat

2.4.3 Zranitelnosti

Zranitelnost můžeme definovat jako slabé místo aktiva či opatření, jenž může být zneužito hrozbou. Tato slabá místa mají často za příčinu neautorizovaný přístup k datům a zdrojům organizace.

Zranitelnost dělíme na:

- fyzickou, která zahrnuje budovy a počítačové místnosti
- technického a programového vybavení projevená chybou či poruchou
- nosičů dat, kde se jedná o selhání s následnou nečitelností dat
- elektromagnetických zařízení, která lze smazat při styku se silným magnetickým polem
- komunikačních systémů a kabelových rozvodů, kde lze rozvody přerušit či napíchnout
- personální, kde se jedná zejména o úmyslné či neúmyslné chování osob

2.4.4 Bezpečnostní událost[11]

Bezpečnostní událost definujeme jako nějaký identifikovaný stav informačního systému, služby nebo počítačové sítě, který může narušit bezpečnost a pravidla její politiky, způsobit selhání některého zavedeného opatření anebo se jedná o dříve neznámou či nepředpokládanou situaci ovlivňující bezpečnost. V případě, že je bezpečnostní událost vyhodnocena, může být kvalifikována jako bezpečnostní incident.

2.4.5 Bezpečnostní incident

Bezpečnostní incident vzniká v případě jedné nebo více nechtěných bezpečnostních událostí, které mohou s vysokou pravděpodobností narušit bezpečnost informačního systému organizace či podporu jejích hlavních nebo podpůrných procesů.

2.4.6 Opatření

Opatřením rozumíme řízení rizika a snahu o snížení síly hrozeb. Zahrnuje i řízení politik, postupů, směrnic, běžných postupů nebo organizačních struktur. Cílem je tedy pomocí vhodných opatření předejít hrozbě či zmírnit její sílu.

Opatření mohou mít charakter:

- administrativní
  - k těmto opatřením patří hlavně směrnice pro práci s IS/ICT, které zajišťují např. pravidelné zálohování dat, správné používání elektronické pošty apod.
- fyzický
  - patří mezi ně zejména opatření týkající se např. dostatečného zabezpečení budov zámky, čipovými kartamy apod.

[11] Bezpečnostní incidenty IS/ICT a jejich řešení [online]. 2005. Dostupné z: www.cssi.cz/cssi/system/files/all/doucek.pdf

- technický a technologický
  - tato opatření zahrnují např. dostatečnou autentizaci při přístupu k aktivům, vstup do systému organizace pomocí hesel apod.

2.4.7 Riziko

Riziko lze definovat jako určitá nejistota zda bude systém napaden či ne. Záleží samozřejmě na tom, zda existuje zranitelnost, a když ano, tak jak vážná. Dále je nutné vzít v potaz, zda byla zavedena nějaká opatření, která danou zranitelnost úplně odstranila nebo alespoň zmírnila sílu hrozby. Dle vážnosti situace pak můžeme vnímat případy, kdy může v systému být mnoho zranitelností a organizace s tím nic nedělá. V tu chvíli podstupuje organizace velké riziko, že bude napadena. V opačném případě může organizace zvolit vhodná opatření k napravení zranitelností a tím riziko snížit.

2.4.8 Dopad

Dopadem rozumíme situaci, kdy došlo k hrozbě, která měla určitý efekt na organizaci jako např. ztrátu finančních prostředků. Tyto dopady mohou mít různorodý charakter. Místo okamžitého efektu může k dopadům docházet postupně. Když je to možné, tak se veškeré dopady vyčíslují ve finančních prostředcích z důvodu lepšího porovnání nákladů na opatření se ztrátami, které hrozba způsobila.

2.5 Information Security Governance[12]

Řízení informační bezpečnosti je odpovědností statutárních orgánů a vrcholového vedení organizací. Musí být propojeno spolu s Enterprise Governance a IT Governance, aby byl zajištěn správný a efektivní chod. Statutární orgány mají za úkol hlídat, aby byla správa

[12] DOUCEK, P. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011, s. 57-60. ISBN 978-80-7431-050-8.

bezpečnosti součástí procesů řízení kritických zdrojů organizací, zatímco vrcholové vedení musí brát v úvahu a reagovat na závislosti, které jsou vyvolané požadavky na bezpečnost informací. Společně se však musí shodnout na očekáváních od programu bezpečnosti informací, jeho implementování, hodnocení současné bezpečnosti a také formulování budocího vývoje.

Aby bylo možné blíže vymezit pojem Information Security Governance, musí se klást důraz a tyto aspekty:

- žádoucí výstupy,
- znalosti a ochrana informačních aktiv,
- přínosy pro organizaci,
- integrace procesů.

2.5.1 Žádoucí výstupy

Aby byla organizační struktura a procesy úspěšné, musí být zajištěna efektivní komunikace mezi všemi zúčastněnými jednotkami podílejícími se na ISG. Tato komunikace musí být založená na společné terminologii, konstruktivních vztazích a podpoře definovaných cílů. Mezi hlavní výstupy ISG patří propojení strategie informační bezpečnosti se strategií organizace, efektivní řízení zdrojů, které by mělo být schopno využívat dosavadních znalostí v oboru informační bezpečnosti a samozřejmě důkladné hodnocení realizace cílů ISG pomocí měření, monitoringu a reportingu.

2.5.2 Znalosti a ochrana informačních aktiv

Základním zdrojem informací jsou data. Tato data jsou sama o sobě nepoužitelná, avšak v případě, že získají nějaký význam, účel a jsou řádně uspořádána, stávají se informacemi, které jsou základem pro znalost. Znalost se tedy tvoří z informací, které jsou určitým způsobem seskupeny za účelem vytvoření něčeho smysluplného.

V souvislosti s informační bezpečností jsou tedy informace a znalosti brány jako informační aktiva, která je nutno zabezpečovat, jelikož by bez nich organizace v dnešní době nemohla existovat.

2.5.3 Přínosy pro organizaci

ISG generuje mnoho významných přínosů, které zvyšují hodnotu organizace. Mezi tyto významné přínosy patří např. zajištění souladu s veřejnými a právními požadavky na správnost informací, zajištění efektivní politiky bezpečnosti a jejího dodržování, zajištění nezávadných informací při kritických rozhodnutích apod.

2.5.4 Integrace procesů

V dnešní době se činnosti související s řízením informační bezpečnosti často realizují samostatně. Tento způsob je vysoce neefektivní a může způsobit i duplicitu či mezery v procesech. ISG se však opírá o doporučený koncepční model, který tyto nedostatky odstraňuje.

2.6 Audit a testování informační bezpečnosti[13]

2.6.1 Úrovně hodnocení bezpečnosti

Pro řízení bezpečnosti je důležité používat vhodné techniky a nástroje, díky kterým mají odpovědní pracovníci dokonalý přehled o skutečném stavu věcí a o míře dosažené bezpečnosti. V praxi se těchto technik využívá hned několik a jednou z nich je i metodika

[13] DOUCEK, P. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011, s. 173-184. ISBN 978-80-7431-050-8.

Information Assurance Methodology připravená americkou NSA. Tato metodika pracuje se třemi úrovněmi:

- 1. úroveň – Assessment
  - v této úrovni se prověřují procesy a postupy, pomocí kterých se realizuje proces řízení informační bezpečnosti
  - cílem této úrovně posuzování je ověřit, jakým způsobem organizace identifikuje rizika, navrhuje potřebná bezpečnostní opatření a zda je schopna bezpečnost účinně prosadit do svého běžného fungování
- 2. úroveň – Evaluation
  - tato úroveň se zabývá ověřováním nastavení bezpečnostních parametrů informačních a komunikačních technologií používaných organizací
  - cílem této úrovně je prohledání informačních a komunikačních technologií pomocí automatizovaných nástrojů a následné vytváření přehledu o dostupných službách a možných slabinách v bezpečnosti
- 3. úroveň – Blue&Red Team
  - v této úrovni dochází k přímému testování, které simuluje skutečné útoky na informační systém a aktiva organizace
  - testování se provádí pomocí tzv. penetračních testů
  - běžně se tyto testy používají jen na kritické části ICT, jelikož jsou velmi časově náročné
  - existují i techniky, které jsou schopné dočasně znepřístupnit celý informační systém nebo některé služby

První úroveň a zároveň základní je nazývána bezpečnostní audit, zatímco druhá a třetí úroveň jsou brány jako bezpečnostní testy.

2.6.2 Principy auditu

„Audit je systematický, nezávislý a dokumentovaný proces získání důkazů z auditu a jejich hodnocení s cílem stanovit rozsah splnění kritérií auditu.“[14]

Při provádění auditů musejí auditoři dbát na dodržování řady zásad a pravidel, díky kterým je audit tak spolehlivým a efektivním nástrojem pro podporu účinného řízení bezpečnosti. Dodržování zásad, jako je etické chování, spravedlivá prezentace, povinnost profesionálního přístupu, nezávislost a průkaznost, je pro auditora předpokladem pro zajištění odpovídajících, dostatečných a opakovatelných závěrů.

2.6.3 Postup auditu

První částí je zahájení auditu, při kterém je nutno jmenovat vedoucí auditorský tým, stanovit cíle, rozsah, předmět a kritéria auditu, zhodnotit proveditelnost auditu, vytvořit auditní tým a navázat první kontakt s auditovanou organizací.

Dále je nutné přezkoumat dokumentaci a připravit činnosti spojené s auditem. Díky prostudování dokumentace si auditorský tým vytvoří lepší představu o prostředí auditované organizace a je tak schopen lépe navrhnout plán auditu. V této části auditu také probíhá příprava pracovních dokumentů auditního týmu.

Další fází je již přímé provedení auditu na místě. Dochází ke sběru informací o skutečném fungování systému, ověřování zjištěných skutečností a shromažďování potřebných důkazů. Prvně dojde k setkání s auditovanou organizací, kde jsou prezentovány cíle a rozsah auditu, členi týmu, stanovují se způsoby komunikace a zajišťují se potřebná zařízení a prostory. Během auditu pak průběžně komunikuje tým s auditovanou organizací a

[14] DOUCEK, P. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011, s. 174. ISBN 978-80-7431-050-8.

informuje je o průběhu. V průběhu auditu se shromažduje a ověřuje dokumentace, formulují se nálezy a připravuje se závěr auditu.

Na závěr se veškeré zjištěné skutečnosti vyhodnocují a dochází i k zvážení možných negativních dopadů auditu na organizaci. Výstupem je závěrečná zpráva z auditu. Je také nutné, aby po provedení auditu auditoři vyhodnotili jeho úspěšné a neúspěšné stránky.

2.6.4 Základní typy auditů

Audity je možné z hlediska použití jejich výsledků rozdělit na:

- Audity první stranou
  - jsou také označovány jako interní audity
  - jsou zpravidla prováděny organizací samou nebo externím subjektem, který má v dané oblasti bohatší zkušenosti
  - veškeré cíle, priority a rozsah si stanovuje organizace sama a výsledek auditu slouží k zjištění správného směru zlepšování
- Audity druhou stranou
  - jsou označovány jako odběratelské
  - jedná se o audity prováděné externími subjekty, které mají vůči dané organizaci určité zájmy (odběratelsko-dodavatelské vztahy)
  - audity převážně vyplívají ze vzájemných smluvních vztahů mezi organizací a externím subjektem
- Audity třetí stranou
  - tyto audity jsou prováděny externí organizací, která je na auditované organizaci zcela nezávislá
  - cílem těchto auditů je poskytnout objektivní informace o stavu určité oblasti v auditované organizaci třetí osobě, která např. rozhoduje o vydání certifikátu apod.

3. Praktická část

3.1 Souhrn zákona č. 181/2014 Sb., o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti byl 13.8.2014 podepsán prezidentem republiky a od 1.1.2015 nabývá platnosti.

3.1.1 § 1 Předmět úpravy

V § 1 je stanoveno, že tento zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické a informační bezpečnosti. Informačních a komunikačních systémů, které nakládají s utajovanými informacemi, se tento zákon netýká.

3.1.2 § 2 Vymezení pojmů

Pro dostatečné pochopení zákona je nutné, aby na začátku byly vymezeny pojmy v zákoně používané. V tomto paragrafu jsou tedy vysvětleny pojmy jako kybernetický prostor, kritická informační infrastruktura, významný informační systém, správce informačního či komunikačního systému apod.

3.1.3 § 3 Orgány a osoby, kterým jsou ukládány povinnosti v oblasti KB

Tento paragraf určuje, které orgány a osoby mají povinnost plnit požadavky určené zákonem a jeho vyhláškami. Tyto orgány a osoby jsou fyzické nebo právnické osoby.

Za orgány a osoby, které jsou povinny plnit dané požadavky v oblasti kybernetické bezpečnosti, se podle tohoto zákona považují:

a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací, pokud není orgánem nebo osobou podle písmene b)

b) orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem komunikačního systému podle písmene d)
c) správce informačního systému kritické informační infrastruktury
d) správce komunikačního systému kritické informační infrastruktury
e) správce významného informačního systému

3.1.4 § 4 Bezpečnostní opatření

K zajišťování bezpečnosti informací a dostupnosti služeb a sítí v oblasti KB, je nutné zavádět a provádět bezpečnostní opatření. Orgány a osoby uvedené v § 3 písm. c) až e) jsou povinny bezpečnostní opatření zavádět a provádět v rozsahu nezbytném pro zajištění KB. Tato opatření jsou prováděna zejména pro informační systémy kritické informační infrastruktury, komunikační systémy kritické informační infrastruktury nebo významné informační systémy. Opatření však olivňují také výběr dodavatelů, jelikož jsou orgány a osoby uvedené v § 3 písm. c) až e) povinny při výběru zohledňovat požadavky, jež vyplývají z bezpečnostních opatření.

Bezpečnostní opatření jsou v zákoně rozdělena na dva druhy a to organizační a technická. V § 5 jsou pak jednotlivá opatření obou druhů vypsána a v § 6 je popsáno, co vše stanoví prováděcí předpis (obsah bezpečnostních opatření, obsah a strukturu bezpečnostní dokumentace apod.).

3.1.5 § 7 Kybernetická bezpečnostní událost a kybernetický bezpečnostní incident

Tento paragraf poskytuje definice těchto pojmů, které jsou již zmíněny v této práci v podkapitolách 2.4.4 a 2.4.5. Orgány a osoby uvedené v § 3 písm. c) až e) jsou povinny detekovat veškeré kybernetické bezpečnostní události.

3.1.6 § 8 Hlášení kybernetického bezpečnostního incidentu

Komu mají být incidenty hlášeny, se liší dle druhu orgánu či osoby, která incident nahlašuje. Orgány a osoby uvedené v § 3 písm. b) jsou povinny hlásit detekované incidenty provozovateli národního CERT a orgány a osoby uvedené v § 3 písm. c) až e) hlásí detekované incidenty Národnímu bezpečnostnímu úřadu.

3.1.7 § 9 Evidence

Národní bezpečnostní úřad vede evidenci kybernetických bezpečnostních incidentů, ve které nalezneme hlášení incidentu, identifikační údaje systému, ve kterém byl incident nalezen, údaje o zdroji tohoto incidentu a nakonec postup, který byl využit při řešení incidentu a jeho výsledek. Údaje z evidence incidentů poskytuje NBÚ orgánům veřejné moci pro výkon jejich působnosti. Dále může informace od NBÚ získat provozovatel národního CERT, orgány vykonávající působnost v oblasti KB v zahraničí a jiné osoby působící v oblasti KB. Vždy lze získat informace pouze v rozsahu nezbytném pro zajištění ochrany kybernetického prostoru.

3.1.8 § 11 Opatření

Jedná se o úkony, kterých je třeba k ochraně ochraně informačních systémů nebo služeb a sítí elektronických komunikací před hrozbou v oblasti kybernetické bezpečnosti nebo před kybernetickým bezpečnostním incidentem anebo k řešení již nastalého kybernetického bezpečnostního incidentu. Tato opatření se rozdělují na:

- Varování
  - zveřejňuje je NBÚ v případě, že se zejména z vlastní činnosti nebo z podnětu provozovatele národního CERT dozví o hrozbě v oblasti KB
  - uvedeno v § 12
- Ochranné opatření
  - NBÚ ho ukládá za účelem zvýšení ochrany informačních systémů nebo služeb a sítí elektronických komunikací

- ukládáno na základě analýzy již vyřešeného incidentu
- uvedeno v § 14

- Reaktivní opatření
  - NBÚ vydá rozhodnutí, ve kterém ukládá osobě či orgánu provedení reaktivního opatření k řešení incidentu
  - Popsáno v § 13

3.1.9 § 16 Kontaktní údaje

Popisuje, co vše je považováno za kontaktní údaje u právnických osob, fyzických osob a orgánu veřejné moci. Tyto údaje jsou poté orgány a osoby uvedené v § 3 písm. a) a b) povinny oznamovat provozovateli národního CERT a orgány a osoby uvedené v § 3 písm. c) až e) je oznamují NBÚ. NBÚ vede patřičnou evidenci těchto údajů a v případě kybernetického nebezpečí má právo vyžádat si kontaktní údaje shromážděné provozovatelem národního CERT.

3.1.10 § 21 Stav kybernetického nebezpečí

Stav kybernetického nebezpečí nastává ve chvíli, kdy je ohrožena bezpečnost informací v informačních systémech nebo bezpečnost a integrita služeb nebo sítí elektronických komunikací. V takovém případě by mohlo dojít k porušení nebo by došlo k ohrožení zájmu České republiky ve smyslu zákona, který upravuje ochranu utajovaných informací. Stav kybernetického nebezpečí vyhlašuje ředitel NBÚ jeho vyvěšením na úřední desce a následném celoplošném ohlášení v rozlhasovém a televizním vysílání. Tento stav se vyhlašuje na dobu nezbytně nutnou, avšak nejdéle na 7 dnů. Tuto lhůtu může ředitel NBÚ prodloužit, ale souhrnná doba trvání nesmí překročit 30 dní. V případě, že nelze odvrátit ohrožení bezpečnosti informací v rámci stavu kybernetického nebezpečí, ředitel NBÚ neprodleně žádá vládu o vyhlášení nouzového stavu. Tento stav končí uplynutím doby, na kterou byl vyhlášen nebo ředitel NBÚ rozhodne o jeho zrušení před uplynutím této doby, nebo je vyhlášen nouzový stav.

3.1.11 § 23 Kontrola

NBÚ kontroluje jak orgány uvedené v § 3 plní povinnosti, jenž byly stanoveny tímto zákonem a rozhodnutími a opatřeními obecné povahy vydanými NBÚ. Dále kontroluje, zda orgány a osoby uvedené v § 3 dodržují prováděcí právní předpisy v oblasti KB.

Orgány a osoby uvedené § 3 písm. a) a b) musí plnit povinnosti uložené NBÚ za stavu kybernetického nebezpečí.

Orgány a osoby uvedené § 3 písm. c) až e) musí plnit veškeré povinnosti za jakéhokoliv stavu.

3.1.12 § 25 Správní delikty

Orgány a osoby uvedené v § 3 se mohou při nesplnění určitých povinností dopustit správního deliktu. Podle vážnosti správního deliktu se odvíjí také pokuta, která se vyměřuje od 10 000 Kč do 100 000 Kč. Veškeré správní delikty projednává NBÚ.

3.2 Popis vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti

Vyhláška o kybernetické bezpečnosti více specifikuje jednotlivé části zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Nalezneme v ní především požadavky na jednotlivé aspekty, kterými se zákon zabývá, ale také podklady a vzory pro jejich plnění.

Pomocí této vyhlášky jsou stanoveny:

- Obsah a struktura bezpečnostní dokumentace
- Obsah bezpečnostních opatření a rozsah jejich zavedení
- Typy a kategorie kybernetických bezpečnostních incidentů a jejich způsob hlášení

- Náležitosti oznámení o provedení reaktivního opatření a jeho výsledku
- Vzor oznamování kontaktních údajů

Požadavky obsažené ve vyhlášce jsou zaměřeny na orgány a osoby uvedené v § 3 písm. c) až e) zákona, přitom u každého požadavku je stanoveno, který z těchto orgánů či osob má za povinnost jej plnit.

Obsah této vyhlášky doplněný o určité požadavky ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti je základem pro tvorbu dostatečného zabezpečení na alespoň základní úrovni.

3.3 Popis normy ČSN ISO/IEC 27001

Tato mezinárodní norma poskytuje požadavky na ustavení, implementování, udržování a neustálé zlepšování systému řízení bezpečnosti informací (ISMS). Ustavení a implementace ISMS je velmi ovlivněna potřebami a cíli organizace, požadavky na bezpečnost, používanými procesy a velikostí a strukturou organizace. Tento systém je integrován do celkové struktury řízení organizace a je součástí procesů.

Mimo požadavků na ustavení, implementování, udržování a neustálé zlepšování ISMS se tato norma zabývá také posuzováním a ošetřením rizik bezpečnosti informací, jenž je přizpůsobené potřebám organizace.

Požadavky této normy lze obecně použít a aplikovat na jakoukoliv organizaci bez ohledu na její typ, velikost a povahu činností.

3.4 Porovnání zákona č. 181/2014 Sb., o kybernetické bezpečnosti a souvisejících vyhlášek s normou ČSN ISO/IEC 27001

Informační bezpečnost byla řešena již dávno před tím, než byl vytvořen zákon týkající se kybernetické bezpečnosti. K tomu sloužila a nadále slouží norma ČSN ISO/IEC 27001, která obsahuje jak požadavky týkající se procesů informační bezpečnosti, tak i požadavky

pojednávající o systému řízení informační bezpečnosti (ISMS). S jistotou lze konstatovat, že sama norma byla jedním ze vzorů při tvorbě zákona a tak je samozřejmostí tyto dva dokumenty porovnat a nalézt možné podobnosti, které by mohly při tvorbě služeb kybernetické bezpečnosti pomoci k dosáhnutí komplexnosti jednotlivých služeb. Navíc existuje mnoho organizací, které již mají zavedený ISMS podle normy ČSN ISO/IEC 27001. V tomto případě pak lze předpokládat, že by organizace mohla již úplně či částečně splňovat požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti a souvisejících vyhlášek.

Nejdříve je nutné u všech dokumentů zpracovat požadavky a následně zjistit jejich počet. U normy ČSN ISO/IEC 27001 je to snadnější, jelikož je celá norma požadavková, avšak nesmí být opomenuta příloha, která má taktéž požadavkový charakter. Výsledný počet požadavků u normy ČSN ISO/IEC 27001 tak činí 137 požadavků.

U zákona č. 181/2014 Sb., o kybernetické bezpečnosti a především u vyhlášky o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti je získání počtu požadavků složitější obzvláště kvůli faktu, že tyto dokumenty mají požadavky rozděleny mezi jednotlivé orgány a osoby uvedené v § 3. Samotný zákon hovoří o všech orgánech a osobách uvedených v § 3 a vyhláška je zaměřena pouze na osoby a orgány uvedené v § 3 písm. c) až e). Pro co nejefektivnější zpracování je tedy ideální rozdělit obsah zákona a jeho vyhlášky na požadavky pro orgány a osoby uvedené v § 3 písm. c) a d) (dále jen KII) a požadavky pro osoby a orgány uvedení v § 3 písm. e) (dále jen VIS). Po tomto rozdělení je jednoznačné, že pro KII je v zákoně a vyhlášce 97 požadavků a pro VIS jich je 55. Některé z těchto požadavků jsou však pro KII a VIS stejné.

3.5 Určení cílových oblastí služeb

Pro výběr správných prostředků k zajištění kybernetické bezpečnosti je důležité stanovit cílové oblasti, pro které služby budou vytvářeny. Základy bezpečnosti jsou pro většinu oblastí stejné, avšak při hlubším proniknutí do problematiky kybernetické bezpečnosti zjistíme, že každá oblast (státní správa, zdravotnictví, IT apod.) má svoje specifické

požadavky. Důvodem jsou rozdílné nároky na HW a SW vybavení, důležitost informací, s nimiž organizace v dané oblasti nakládá a mnoho dalších aspektů. V případě, že služby budou vytvářeny pro větší počet oblastí, tak je vhodné rozdělit oblasti do několika úrovní podle priority.

3.6 Vytvoření přehledů norem a legislativních dokumentů

Základem pro vytvoření služeb kybernetické bezpečnosti je vyhledání potřebných norem a legislativních dokumentů a vytvoření stručných přehledů, ve kterých budou obsaženy nejdůležitější informace o jednotlivých normách a legislativních dokumentech. Přehledy se tedy sestávají z těchto částí:

- Celý název normy či dokumentu
- Stručný obsah
- Určení druhu organizace, pro kterou je norma či dokument určen
- Struktura

Tyto přehledy pak slouží pro zákazníky, kteří se mohou rychle seznámit se strukturou a obsahem normy a hlavně pro marketingové a obchodní oddělení, které na jejich základě vytvoří nabídku a podklady k propagaci služeb.

3.7 Tvorba scopů pro cílové oblasti

Pro dostatečnou přehlednost je nutné sepsat jednotlivé normy a legislativní dokumenty dohromady a rozdělit je do několika skupin podle jejich zaměření. Díky tomuto rozdělení je pak možné získat větší přehled o tom, co vše bude pomocí těchto norem a dokumentů pokryto. Normy a dokumenty se rozdělí do těchto skupin:

1. Lidé
2. Software
3. Hardware
4. Úložiště dat

5. Přenos dat
6. Systémy řízení
    a. Akreditované
    b. Neakreditované
    c. Proprietární

Při tvorbě scopů je důležité vyhledat potenciální návaznosti mezi normami či dokumenty a tyto návaznosti ve scopech zdůraznit. Existuje totiž mnoho norem, které např. vysvětlují procesy popsané v jiné normě nebo obsahují metodologii pro zavedení systému popsaného v další normě.

Scopy se vytvářejí pro každou cílovou oblast zvlášť.

3.8 Tvorba check-listů norem a legislativních dokumentů

Jelikož by bylo nevhodné při provádění auditů nahlížet do jednotlivých norem a podle jejich požadavků kontrolovat zda subjekt plní či ne tyto požadavky, vytvaří se tzv. check-listy. Samotné požadavky jsou totiž v normách či legislativních dokumentech popisovány rozsáhle a právě check-listy obsahují zestručněné znění požadavku, avšak formulované tak, aby bylo možné zkontolovat celé plnění daného požadavku.

Samotný check-list se skládá z následujících částí:

- Číselné označení požadavku (např. 5.1.1)
- Název požadavku
- Znění požadavku
- Prostor pro zapsání plnění či důvodů, proč subjekt požadavek neplní

Díky tomuto složení má auditor k dispozici dokument, který mu při provádění auditu napomáhá ke kontrole plnění požadavků normy či legislativního dokumentu.

Dalším využití nalezneme při tvorbě služeb kybernetické bezpečnosti a to při provádění porovnání norem či legislativních dokumentů, které jsou obsahově podobné. Pokud je

úmyslem tvorby služeb zahrnutí dokumentů s podobným obsahem, můžeme díky srovnání check-listů nalézt požadavky, které jsou totožné a vytvořit tak např. check-list, jenž by zahrnul oba dokumenty a neobsahoval by duplicitní požadavky. Této techniky tato práce využívá např. při porovnání normy ČSN ISO/IEC 27001 se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti.

3.9 Návrh služeb

3.9.1 Myšlenka EZÚ, s.p. v oblasti kybernetické bezpečnosti

Nabízet kvalitní a komplexní služby v oblasti kybernetické bezpečnosti, v jejichž rámci zajistit plnění zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Poskytnout ucelený, ale zároveň i flexibilní produkt, zahrnující tyto služby, který bude přizpůsobitelný dle požadavků zákazníka.

3.9.2 Měřitelné cíle pro první rok

První rok (od 1. září 2014 do 1. září 2015) je spojen se založením laboratoře kybernetické bezpečnosti. Je tedy nutné vytvořit dostatečné zázemí pro laboratoř a zajistit personální zdroje. Dále je nezbytně nutné vytvoření potřebné dokumentace pro auditory, marketing, zákazníky a partnery. Tyto dokumentace zahrnují:

- Výpisy norem a legislativních dokumentů
- Přehledy norem a legislativních dokumentů
- Scopy pro jednotlivé cílové oblasti
- Check-listy norem a legislativních dokumentů
- Schémata produktu a služeb
- Dokumenty pro lektory (náplň školení, prezentace apod.)
- Dokumenty pro zákazníky (testy, certifikáty apod.)

Hlavním cílem je vytvoření první úrovně produktu pro všechny cílové oblasti, jenž zahrnuje zajištění kybernetické bezpečnosti na systémové úrovni. To zahrnuje vytvoření veškeré dokumentace, zajištění dostatečných personálních zdrojů (auditoři, lektoři, administrativa) a dostatečné proškolení interních zaměstnanců.

Jakmile dojde k dokončení první úrovně produktu, začít tuto úroveň nabízet zákazníkům a postupně rozpracovávat další úrovně produktu.

3.9.3 Měřitelné cíle v horizontu 3 let

Při pohledu na cíle v delším časovém období, přesněji v horizotnu 3 let, bude stěžejní vytvoření kompletního produktu, což zahrnuje tvorbu dokumentace, zajištění personálních zdrojů (auditoři, lektoři, IT odborníci apod.) a dostatečné školení interních zaměstnanců. Důležité bude také průběžné hodnocení výsledků, ve kterém se zhodnotí dosavadní stav návrhu a jeho přínosy. Díky 2. a 3. úrovni je možné proniknout hlouběji do problematiky KB a tak je nezbytné navázání kontaktů s možnými partnery, se kterými by bylo možné spolupracovat nejen na vývoji a vylepšování produktu, ale také díky nim doplnit produkt o další služby. Díky partnerům by bylo možné doplnit portfolium služeb i o ty služby, které EZÚ sám nesmí nabízet (např. poradenství).

3.9.4 Zákaznická odvětví

Při návrhu služeb kybernetické bezpečnosti je jedním ze stěžejních aspektů výběr odvětví, na které se bude služba orientovat. První úroveň produktu přímo nevyžaduje, aby bylo určeno, na jaké odvětví se bude zaměřovat, jelikož se jedná o systémový pohled a náplň této úrovně tak lze zobecnit pro jakoukoliv oblast působení zákazníka. Neznamená to však, že první úroveň není možno přizpůsobit pro určitou oblast (např. ISVS pouze pro státní správu). Produkt však poskytuje i další dvě úrovně, které se zaměřují na problematiku kybernetické bezpečnosti více do hloubky a proto jsou v nich použity normy a legislativní dokumenty zaměřující se přímo na specifická odvětví. Z tohoto důvodu je vhodné navrhnout produkt pro jednotlivá odvětví, kterým bude výsledný produkt nabízen. V případě, že jsou určitá odvětví upřednostňována, rozdělí se dále do skupin podle priority.

Vybraná odvětví pro účel této bakalářské práce jsou následující:

1. Nejvyšší priorita
    a. Státní správa
    b. Zdravotnictví
    c. IT sektor
2. Střední priorita
    a. Smart Grids
    b. Smart Homes
    c. Energetika
    d. Datová úložiště
    e. Komunikace
3. Nejmenší priorita
    a. Řídící automatizační systémy
    b. Hazardní automaty
    c. Finance

3.9.5 Lidské zdroje

Pro poskytování služeb kybernetické bezpečnosti jsou důležitým faktorem lidské zdroje. Pro vytvoření oddělení, které by zajistilo organizaci kompletních služeb kybernetické bezpečnosti, jsou nutné zařídit tyto lidské zdroje:

- Auditoři KB
- Referent KB
- Vedoucí laboratoře KB
- Manažer produktu KB
- IT technik
- Lektoři

Náplní práce auditorů KB je provádění auditů, což znamená jejich příprava a následná kontrola plnění požadavků norem v organizaci. Mimoto může být auditor také garantem

určité normy a poté je jeho povinností, pokud je to třeba, vytvořit podklady pro školení normy, jejíž je garantem.

Referent KB má na starosti veškerou administrativní práci ať už se jedná o přípravu materiálů pro auditory či zákazníky nebo jiné interní dokumenty či jde o vytváření podkladů pro školení. Dále vytváří a řídí program auditů a stará se o zakázky.

Vedoucí laboratoře KB má na starost celý její chod. Do své laboratoře vybírá zaměstnance a sám se i aktivně podílí na činnosti laboratoře. Dále zodpovídá za formální správnost výsledků auditů a technickou správnost poskytovaných informací.

Manažer produktu má za úkol orientovat se na trhu, monitorovat aktuální trendy a identifikovat je. Na základě výsledků jeho monitoringu a analýzy trhu pak vytváří strategický plán, včetně návrhu, tvorby a uvedení nových produktů. Stará se o zpracování poptávek a vytvoření nabídek pro zákazníky.

IT technik je důležitou součástí laboratoře KB. Plnění požadavků a záležitosti týkající se norem a legislativních dokumentů zvládají auditoři, avšak IT technik doplňuje tyto znalosti o zkušenosti s funkční stránkou problematiky KB. Navíc je IT technik využíván v druhé a třetí úrovni na provádění bezpečnostních testů.

Pro zajištění kvalitního vzdělávacího a školícího systému, je nutné zajistit kvalifikované lektory, kteří mají znalost v oboru a komunikační schopnosti na vysoké úrovni.

3.9.6 Partneři

Jelikož je v této bakalářské práci předpokládáno zaměření na více odvětví, je nutné vzít v potaz možné navázání spolupráce s potenciálními partnery. Je mnoho organizací, které se zabývají různými oblastmi kybernetické bezpečnosti a právě díky navázání partnerských vztahů, je možné využít spolupráce více odborníků, kteří mohou např. společně řešit určitou problematiku. Navíc v případě, že jedna organizace působí jako certifikační orgán a druhá jako dodavatel hardwaru či softwaru, budou se tyto organizace vhodně doplňovat. Další výhodou partnerství, je doplnění certifikační činnosti o činnost poradenskou, kde

jedna organizace pomůže zákazníkovi s implementací např. ISMS a druhá organizace zákazníkovi implementovaný systém zkontroluje a při splnění veškerých požadavků vydá certifikát. Velkou příležitostí je také navázání partnerského vztahu pro vytváření společných školení, ať už se jedná o spojení know how obou organizací, či poskytnutí lektorů apod.

3.9.7 Úrovně služeb

Cílem a zároveň přínosem první úrovně produktu je zajištění základní úrovně kybernetické bezpečnosti (dále jen KB), a to napříč celou organizací. Ve výsledku to pro organizaci znamená zajištění ochrany před velkými finančními ztrátami či poškozením aktiv organizace při realizaci určité hrozby (bezpečnostním incidentu), popř. zmenšení dopadu takové realizace. Přináší ale také zkvalitnění a zrychlení procesů v organizaci (zvláště týkajících se IT služeb) a efektivní vynaložení nákladů na zajištění KB.

První úroveň se vyznačuje čistě systémovým pohledem a představuje jakýsi odrazový můstek k opravdu důkladnému zajištění KB dosahované v úrovních 2 a 3. Tato úroveň se soustředí na zavedení a kontrolu základních procesů nutných k vytvoření kybernetického zabezpečení (dále jen KZ), např.:

- Řízení rizik
- Řízení hrozeb a zranitelností
- Příprava a realizace bezpečnostních opatření
- Neustálé zlepšování
- Provádění interních auditů

Druhá úroveň produktu se vyznačuje přechodem z čistě systémového pohledu na KB na pohled zahrnující také bezpečnost software, sítí a úložišť a bezpečnostní testy. I samotný systémový pohled je pro další navýšení KZ organizace rozšířen. Druhá úroveň navazuje na úroveň první, proto dochází k uvolnění prvního kroku, rozšíření požadavků a činností v krocích následujících a přidání jednoho kroku nového. V návaznosti k přínosům první úrovně produktu se v této úrovni přidává KZ dodavatelského řetězce organizace a

jednotlivých částí IT infrastuktury organizace. Přináší také ještě větší efektivitu při uvolňování nákladů na KZ. Realizovat tuto úroveň je možné pouze po úspěšné certifikaci první úrovně produktu v dané organizaci. Ověřování a následná certifikace této úrovně, může nastat po uplynutí minimálně 1 roku od vydání certifikátu.

Třetí úroveň produktu navazuje na úroveň předešlou a představuje nejhlubší pohled na KB. Tento pohled zahrnuje konkrétní bezpečnostní komponenty a podrobněji pohlíží také na bezpečnost software, úložišť, dodavatelských řetězců a bezpečnostní testy. Nově se objevuje zaměření také na bezpečnost hardware a firmware. Díky tomu dochází k zajištění nejvyšší možné úrovně KZ. Realizovat tuto úroveň je možné pouze po úspěšné certifikaci druhé úrovně produktu v dané organizaci. Ověřování a následná certifikace této úrovně, může nastat po uplynutí minimálně 1 roku od vydání certifikátu.

3.9.8 Postup při implementaci produktu

Prvním krokem při implementaci produktu je provedení pre-auditu což znamená zjištění aktuální situace a nedostatků v KZ. Pokud má organizace již z minulosti certifikát pro některou část produktu a projde pre-auditem v této oblasti bez zjištěného nedostatku, bude tato část považována za zabezpečenou a při následném kroku 4. se již nebude ověřovat.

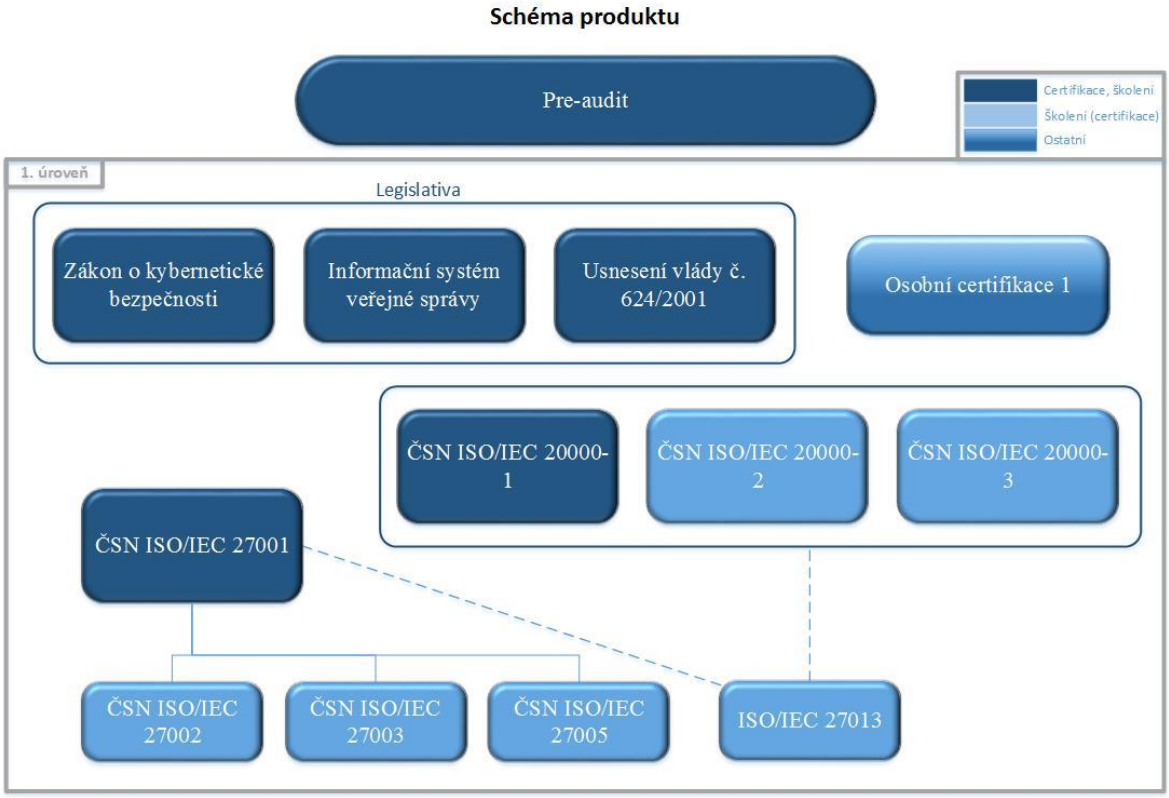
Dále následují osobní certifikace, které zahrnují školení a následnou certifikaci interního pracovníka/ů organizace, zodpovědného/ých za implementaci, údržbu a neustálé zlepšování KB v rámci organizace.

Třetím krokem je implementace požadavků platných mezinárodních standardů a legislativy zaměřujících se na KB pro zajištění základní úrovně KZ (ISVS, zákon č. 181/2014 Sb., o kybernetické bezpečnosti, ČSN ISO/IEC 27001 a ČSN ISO/IEC 20000); včetně zajištění potřebného hardware a software.

Poslední částí je ověřování a následná certifikace základního KZ podle platných mezinárodních standardů a legislativy související s KB a provedení auditu nezávislou třetí stranou (certifikační autoritou).

3.9.9 Podrobný popis 1. úrovně produktu

Jak již bylo zmíněno, první úroveň se vyznačuje čistě systémovým pohledem. Pro organizace to znamená zajištění základních požadavků pro kybernetickou a informační bezpečnost a tím i odrazový můstek k více komplexnímu zabezpečení.



Obrázek 1: Schéma 1. úrovně produktu kybernetické bezpečnosti pro státní správu
Zdroj: vlastní

Základem pro tuto úroveň je zákon č. 181/2014 Sb., o kybernetické bezpečnosti a s ním spojené vyhlášky, kterými jsou konrétně:

- Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti
- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích
- Novela nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury

Vzhledem k podobnosti většiny požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti s požadavky normy ČSN ISO/IEC 27001 není prováděn audit pro obojí zvlášť, ale požadavky normy jsou obohaceny o požadavky zákona, jež jsou v zákoně navíc. Díky tomu budou požadavky obou dokumentů splněny zároveň.

Jelikož i sama norma ČSN ISO/IEC 27001 vyžaduje plnění veškeré nutné legislativy, první úroveň je také doplněna o usnesení vlády ČR č. 624/2001, které obsahuje pravidla, zásady a způsob zabezpečování kontroly užívání počítačových programů v souladu s právními předpisy a licenčními ujednáními.

Další normou, která je předmětem auditu a certifikace je ČSN ISO/IEC 20000-1. Pro audit a certifikaci je použita pouze první část, jelikož je jediná požadavková. Plněním požadavků této normy získá organizace systém managementu služeb, který naplánuje, ustanoví, zavede, provozuje, sleduje, přezkoumává, udržuje a neustále zlepšuje. Tato norma využívá známé metodiky postupného zlepšování PDCA (plánuj, dělej, kontroluj, jednej), která pokrývá celý cyklus, kterým organizace projde od zavádění až po konečné udržování a zlepšování SMS.

Další normy či jiné dokumenty k certifikaci jsou již rozdílné podle odvětví, ve kterém působí zákazník. Mezi tyto normy a dokumenty patří např.:

- Atestace ISVS,
- ČSN EN ISO 9001,
- ČSN ISO/IEC 12207,
- ISO 27799,
- ISO/IEC 27040.

Do první úrovně patří také osobní certifikace, která se skládá z výše uvedených norem a navíc z několika dalších norem, které nejsou požadavkové, ale obsahují metodologie a pokyny např. pro implementací systémů apod. Patří mezi ně tyto normy:

- ČSN ISO/IEC 20000-2
    - Obsahuje pokyny pro použití SMS

- ČSN ISO/IEC 20000-3
  - Obsahuje pokyny pro vymezení rozsahu a použitelnosti ČSN ISO/IEC 20000-1
- ISO/IEC 27013
  - Poskytuje návod k integrované implementaci norem ČSN ISO/IEC 27001 A ČSN ISO/IEC 20000-1
- ČSN ISO/IEC 27002
  - Určena k použití jako doporučení pro výběr opatření v rámci procesu zavádění ISMS
- ČSN ISO/IEC 27003
  - Nabízí praktická doporučení při vývoji plánu implementace ISMS
- ČSN ISO/IEC 27005
  - Poskytuje doporučení pro řízení rizik bezpečnosti informací v organizaci s ohledem na požadavky ISMS
- ISO/IEC TR 24748
  - Obsahuje pokyny k obecnému řízení životního cyklu a také k aplikaci normy ISO/IEC 12207

3.9.10 Nacenění první úrovně produktu

Cenový rozpočet se bude lišit nejen pro jednotlivá odvětví, ale také se bude odvíjet od velikosti organizace, pro kterou bude vytvářen. Proto je nutné pro účel této práce vytvořit rozpočet pro jednu fiktivní organizaci. Tento příklad bude vypočítáván pro středně velkou organizaci působící v oblasti státní správy. Tato organizace zaměstnává 40 lidí v rámci informační bezpečnosti a 20 lidí v rámci služeb.

Prvním krokem při tvorbě cenového rozpočtu první úrovně produktu je stanovení tzv. man days, určující počet dní průběhu auditu, na základě informací získaných o zákazníkovi. Tyto MD se vypočítají pomocí kalkulačky pro auditory, kde se zadává počet zaměstnanců, normy, které budou auditovány a počet auditorů společně s jejich kvalifikací. Po zadání všech potřebných informací vyšel počet MD pro normu ČSN ISO/IEC 27001 na 7,74 dní a počet MD pro normu ČSN ISO/IEC 20000 na 3 dny. Pomocí vzorce v tabulce č.1 byl dále

do MD započítán koeficient náročnosti posouzení zákona o kybernetické bezpečnosti a koeficient vyjadřující jaká část normy ČSN ISO/IEC 27001 není pokryta požadavky zákona o kybernetické bezpečnosti. Výsledkem tohoto výpočtu je celkový počet MD pro audit celé první úrovně produktu, které je roven 14,27 dní. Dále je nutné započítat samostatně atestaci ISVS, která trvá v rozmezí dvou dnů podle náročnosti.

Tabulka 1: Vzorec pro výpočet MD produktu

$MD_{produkt} = (k_{ZKB} \times MD_{27001}) + (k_{27001} \times MD_{27001}) + MD_{20000} + MD_{ISVS}$

$MD_{produkt}$ - celkový počet man days produktu MD_{27001} - počet man days pro normu ČSN ISO/IEC 27001 MD_{20000} - počet man days pro normu ČSN ISO/IEC 20000 MD_{ISVS} - počet man days pro atestaci ISVS k_{ZKB} - koeficient náročnosti posouzení podle ZKB k_{27001} - koeficient vyjadřující pokrytí požadavků ZKB požadavky normy ČSN ISO/IEC 27001

Zdroj: Vlastní

Druhým krokem při tvorbě cenového rozpočtu první úrovně produktu je výpočet cen jednotlivých prvků produktu. Pro nacenění bude sloužit stanovený ceník EZÚ, který oceňuje 1 MD na 15 000 Kč. Pro tuto zakázku je využito dvou auditorů, mezi které budou rozděleny MD. Jeden MD je považován jako klasický pracovní den, jenž má trvání 8h. Podrobné rozpočítání cen je znázorněno níže v tabulce č.2.

Tabulka 2: Nacenění první úrovně produktu

Položky	Stanovení ceny	Cena
Audit	15 000*14	210 000 Kč
Atestace ISVS	20 000	20 000 Kč
Školení	15000*3	45 000 Kč
Příprava a vyhodnocení	10000*4	40 000 Kč
Celkem		315 000 Kč

Zdroj: vlastní

První položka zahrnuje nacenění samotného provedení auditu bez zpracovávání dokumentace. Cena atestace ISVS se odvíjí obzvláště od velikosti organizace pro kterou je vypracovávána a zahrnuje veškeré úkony, které jsou potřeba k atestaci dlouhodobého řízení ISVS. Školení probíhá v prostorách zákazníka a je vedeno zkušenými lektory, kteří

mají praxi v oboru či jsou dokonce auditoři. Cena je stanovena na den a délka školení jsou tři dny. Příprava trvá dva dny a zahrnuje přezkoumání dokumentace zákazníka a přípravu podkladů pro audit a školení. Konečné vyhodnocení auditu je rozloženo do dvou dní, během kterých jsou zpracována veškerá data získaná během auditu, a při splnění veškerých požadavků je zákazníkovi vystaven certifikát. Všechny ceny jsou uvedeny bez DPH, jejíž sazba v tomto případě činí 21%. Celková kalkulace obsahuje obvyklou marži a její struktura dává prostor pro případná cenová vyjednávání ze strany klienta.

3.10 Zhodnocení návrhu služeb

Vzhledem k tomu, že se jedná o vytvoření nových služeb, které nebyly dříve nabízeny, je počítáno s tím, že minimálně první dva roky bude produkt spíše proděličný. První úroveň je sice nabízena již v prvním roce, avšak obsahuje většinu částí, které již podnik poskytuje a zisk ze zakázek první úrovně nepokryje náklady na přípravu dalších úrovní. Se ziskovostí produktu se počítá od třetího roku zavedení provozu laboratoře kybernetické bezpečnosti.

V rámci tvorby služeb byla vytvořena první úroveň produktu, která zajišťuje plnění požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti doplněného o další normy obsahující požadavky jak pro informační bezpečnost, tak i management služeb. Tato úroveň tak zajistí základní zabezpečení, které by měli společnosti mít. V rámci návrhu je zahrnuto i zajištění potřebných lidských zdrojů s popisem pozic. Vzhledem k tomu, že kybernetická bezpečnost se neustále rozvíjí a přibývají stále nové normy a legislativa, očekává se, že v průběhu času bude nutné jednotlivé úrovně produktu přizpůsobovat a upravovat.

Závěr

Cílem této bakalářské práce pod názvem „Návrh vybraných služeb kybernetické bezpečnosti“ bylo navrhnout první úroveň produktu kybernetické bezpečnosti, která obsahuje jednotlivé služby, jako jsou certifikace, audity, školení apod. Tento návrh je přímo aplikovatelný na společnost EZÚ, jenž má v záměru proniknout na trh v oblasti kybernetické bezpečnosti.

Začátek práce se věnuje základním pojmům informační bezpečnosti, které jsou důležité pro pochopení norem a legislativy. Dále jsou v teoretické části popsány jednotlivé úrovně bezpečnosti a základy řízení informační bezpečnosti. Jelikož je důležitou součástí produktu audit, jsou i v teoretické části popsány základy auditu, z čeho se skládá a jak se provádí.

V praktické části jsou nejdříve popsány normy a legislativní dokumenty, které jsou základním stavebním kamenem pro první úroveň produktu kybernetické bezpečnosti a následně jsou popsány popstupy pro přípravu veškeré potřebné dokumentace. Závěr této části se pak přímo věnuje návrhu první úrovně produktu, včetně jednotlivých služeb, které obsahuje. Nechybí ani přiblížení obsahu dalších úrovní a závěrečné nacenění první úrovně.

Seznam použité literatury

DOUCEK, P., L. NOVÁK, L. NEDOMOVÁ a V. SVATÁ. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2.přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.

DOUCEK, P. *Bezpečnostní incidenty IS/ICT a jejich řešení* [online]. 2005. Dostupné z: www.cssi.cz/cssi/system/files/all/doucek.pdf

JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.

KALAMÁR, Š. a J. POŽÁR. *Vybrané aspekty informační bezpečnosti*. Vyd. 1. Praha: Policejní akademie České republiky v Praze, 2010, 190 s. ISBN 978-80-7251-339-0.

Kybernetická bezpečnost v ČR. In: CyberSecurity.cz [online]. 2014 [cit. 2015-02-10]. Dostupné z: http://www.cybersecurity.cz/basic.html

PŘECH, V. *ČR a Izrael budou spolupracovat v oblasti kybernetické bezpečnosti*. In: KYBEZ - Portál Kybernetické bezpečnosti [online]. 2014 [cit. 2015-02-10]. Dostupné z: https://www.kybez.cz/zpravy/-/blogs/cr-a-izrael-podepsaly-prohlaseni-o-spolupraci-v-oblasti-kyberneticke-bezpecnosti

POŽÁR, J. *Vybrané hrozby informační bezpečnosti organizace* [online]. 2011. Dostupné z: http://www.cybersecurity.cz/data/Pozar2.pdf

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

MARTELLINI, M. *Cyber security: deterrence and IT protection for critical infrastructures*. Cham: Springer, 2013. ISBN 33-190-2278-4.

SystemOnLine [online]. 2014. Dostupné z: http://www.systemonline.cz/it-security/pravni-aspekty-prijeti-zakona-o-kyberneticke-bezpecnosti.htm.

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti. In: *181/2014*. 2014. Dostupné z: http://www.sagit.cz/_texty/sb14181.htm/.

Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). In: *316/2014*. 2014. Dostupné z: http://www.sagit.cz/_texty/sb14316.htm/.

ČSN ISO/IEC 27001. *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky*. 2. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, září 2014. 28 s. Třídící znak 39 9797.

ČSN ISO/IEC 20000. *Informační technologie - Management služeb - Část 1: Požadavky na systém managementu služeb*. 2. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, červenec 2012. 40 s. Třídící znak 36 9074.

Elektronická databáze ProQuest:

VASILESCU, Cezar. *Cyber Attacks: Emerging Threats to the 21st Century Critical Information Infrastructures*. Univerzita Obrany. Ustav Strategickych Studii. Obrana a Strategie [online]. 2012, č. 1, s. 9 [cit. 2015-02-10]. Dostupné z: http://search.proquest.com/docview/1026970922?accountid=17116

Information security predictions for 2015. CIOL [online]. 2015, č. 1 [cit. 2015-02-10]. Dostupné z: http://search.proquest.com/docview/1645898871?accountid=17116

Seznam příloh

Přílohy

Příloha A Přehled normy ČSN ISO/IEC 27003

Příloha A obsahuje ukázku přehledu normy. Příkladem je norma ČSN ISO/IEC 27003, která je použita pro první úroveň produktu.

ČSN ISO/IEC 27003

Obsah normy

Účelem této mezinárodní směrnicové normy je poskytnout praktická doporučení při vývoji plánu implementace pro systém řízení bezpečnosti informací (ISMS) v organizaci v souladu s ISO/IEC 27001:2005. Skutečná implementace ISMS se obvykle provádí jako projekt. Proces popsaný v této mezinárodní normě byl navržen tak, aby poskytoval podporu pro zavedení ISO/IEC 27001:2005 (příslušné části z kapitol 4, 5, a 7 včetně) a zdokumentoval přípravu zahájení plánu implementace ISMS v organizaci, definování organizační struktury pro projekt a získání souhlasu vedení organizace, kritické činnosti pro projekt ISMS a příklady naplnění požadavků normy ISO/IEC 27001:2005.

Pro koho je norma určena

Tato mezinárodní norma je určena pro organizace, které zavádějí ISMS. Je aplikovatelná pro všechny typy organizací (například: obchodní podniky, vládní organizace, neziskové organizace) všech velikostí. Složitost a rizika každé organizace jsou jedinečná a její specifické požadavky budou hnací silou pro implementaci ISMS. Menší organizace shledají, že činnosti zmíněné v této mezinárodní normě jsou pro ně použitelné a lze je ještě zjednodušit. Velké společnosti mohou shledat, že pro účinné řízení činností popsaných v této mezinárodní normě bude zapotřebí víceúrovňová organizační struktura nebo systém řízení. V obou případech však lze plánovat příslušné činnosti za použití této mezinárodní normy.

Struktura normy

5. Získání souhlasu vedení organizace se zahájením projektu ISMS

5.1. Přehled

5.2. Upřesnění priorit organizace k vytvoření ISMS

5.3. Definování předběžného rozsahu ISMS

5.4. Vytvoření důvodové studie a projektového plánu pro souhlas vedení organizace

6. Definování rozsahu, hranic a politiky ISMS

6.1. Přehled

6.2. Definování rozsahu a hranic organizace

6.3. Definování rozsahu a hranic informačních a komunikačních technologií (ICT)

6.4. Definování fyzického rozsahu a hranic

6.5. Integrování rozsahů a hranic ISMS

6.6. Vytvoření politiky ISMS a získání souhlasu vedení organizace

7. Provedení analýzy požadavků bezpečnosti informací

7.1. Přehled

7.2. Definování požadavků bezpečnosti informací pro proces ISMS

7.3. Identifikace aktiv v rámci rozsahu ISMS

7.4. Provedení hodnocení bezpečnosti informací

8. Provedení hodnocení rizik a plánování zvládání rizik

8.1. Přehled

8.2. Provedení hodnocení rizik

8.3. Výběr cílů opatření a jednotlivých bezpečnostních opatření

8.4. Získání povolení ze strany vedení organizace k implementaci a provozu ISMS

9. Návrh ISMS

9.1. Přehled

9.2. Návrh organizace bezpečnosti informací

9.3. Návrh bezpečnosti informací ICT a fyzické bezpečnosti

9.4. Návrh specifické bezpečnosti informací ISMS

9.5. Vytvoření finálního plánu projektu SMS

Příloha B Scope pro normy zaměřené na lidi a software státní správy

Příloha B obsahuje ukázku náplně scopu pro státní správu. V této ukázce je předvedena část scopu pro normy zaměřené na lidi a software.

Státní správa

1. **Lidi**

- Osobní certifikace (osvědčení)
    - ZKB a s oblasti související normy, standardy
    - Výsledek certifikačního školení

2. **Software**

- Certifikace ČSN ISO/IEC 15408 [+ možné rozšíření o ISO/IEC 18045 (CEM), ISO/IEC TR/19791]
- Certifikace ČSN ISO/IEC 12207 [+ možné rozšíření o ISO/IEC 14764, ISO/IEC TR 24748, možné napojení na ČSN ISO/IEC 15288]
- Školení
    - ČSN ISO/IEC 15408 [+ rozšíření o ISO/IEC 18045 (CEM), ISO/IEC TR/19791, ISO/TR 20004]
    - ČSN ISO/IEC 12207 [+ rozšíření o ISO/IEC 14764, ISO/IEC TR 24748, možné napojení na ČSN ISO/IEC 15288]
- Bezpečnostní testy
    - Penetrační testy

- Pre-audit pro výše zmíněné normy

Příloha C Část souhrnného check-listu pro ISMS a ZKB

Příloha C obsahuje ukázku souhrnného check-listu ISMS a ZKB ve formě tabulky, která obsahuje část check-listu popisující požadavky čtvrté kapitoly normy ČSN ISO/IEC 27001 doplněné o některé související požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti.

Tabulka 3:Část souhrnného check-listu ISMS a ZKB

	Požadavky normy		Doporučený výklad
4		Kontext organizace *Context of the organization*	
4.1		Porozumění organizaci a jejímu kontextu	Určit externí a interní souvislosti, které mají či mohou mít vliv na bezpečnost informací
4.2		Porozumění potřebám a očekáváním zainteresovaných stran	Stanovit a) zainteresované strany b) potřeby (požadavky) těchto stran, včetně legislativních
4.3		Určení rozsahu ISMS	Určit celkový rozsah (hranice a využitelnost) ISMS; potřeba zvážit výstupy bodů 4.1 a 4.2, závislosti mezi činnostmi vykonávanými firmou a jejím okolím. Rozsah ISMS musí být dostupný ve formě dokumentované informace.
4.4		Systém managementu bezpečnosti informací	Organizace musí vytvořit, zavést, udržovat a zlepšovat ISMS.
4.5		Aktualizace ISMS a příslušné dokumentace	Aktualizovat ISMS a příslušnou dokumentaci v souvislosti s prováděnými nebo plánovanými změnami.
4.6		Řízení provozu a zdrojů ISMS, zaznamenávání činností spojených s ISMS a řízením rizik	Řídit provoz a zaznamenávat činnosti spojené s ISMS a řízením rizik.

Zdroj: vlastní