Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Návrh a realizace produktu za účelem ověřování a certifikace v oblasti kybernetické bezpečnosti dle platných mezinárodních standardů a legislativy České republiky

Diplomová práce

Autor: Bc. Michal Hager
Studijní obor: K-IM2

Vedoucí práce: Ing. Agáta Milanov, Ph.D.

Hradec Králové duben 2016

Prohlášení

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne

Bc. Michal Hager

Poděkování

Rád bych poděkoval vedoucí mé práce, Ing. Agátě Milanov, Ph.D., za její odborné vedení, ochotu a cenné rady, které mi významným způsobem napomohly při tvorbě této diplomové práce.

Anotace

Diplomová práce se zaměřuje na ověřování a certifikaci v dynamicky rozvíjející se oblasti kybernetické bezpečnosti. Cílem práce je navrhnout produkt se zaměřením právě na ověřování a certifikaci v oblasti kybernetické bezpečnosti a popsat hlavní aspekty jeho realizace. Navržený produkt musí reflektovat požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti, být konkurenceschopný a komplexní. Musí adresovat hlavní výzvy v oblasti kybernetické bezpečnosti – správné nastavení bezpečnostního systému a jeho odolnost, vzdělávání lidí zastávajících bezpečnostní role a provádění bezpečnostních testů. Navržený produkt představuje kombinaci souvisejících a vzájemně se doplňujících služeb. To umožňuje uspokojení potřeb specifických segmentů a zvyšuje přidanou hodnotu jednotlivých služeb. Výsledkem této práce je také shrnutí navrženého produktu, jeho teoretické zhodnocení a popis dalšího možného rozvoje.

Klíčová slova

Kybernetická bezpečnost, ověřování, certifikace, návrh produktu, realizace produktu.

Annotation

Title: Design and realization of a product for the purpose of verification and certification in the field of cyber security in accordance with applicable international standards and legislation of the Czech Republic.

The diploma thesis focuses on the verification and certification in the dynamically developing field of cyber security. The aim is to design a product focusing on the verification and certification in the field of cyber security and to describe the main aspects of its implementation. The designed product must reflect the requirements of the Act no. 181/2014 Coll., On cybersecurity, must be competitive and complex. It must address major challenges in cyber security - proper setting of the security system and its resistance, education of people holding security roles and conducting sucurity tests. The designed product is a combination of related and complementary services. This allows to meet the needs of specific segments and increases the added value of the individual services. The result of this work is also a summary of the designed product, its theoretical evaluation and description of possible further development.

Key words

Cyber security, verification, certification, product design, product realization.

Obsah

Úvod

Dnešní informační společnost čelí v kyberprostoru stále více sofistikovaným hrozbám a útokům. Narůstá počet úspěšných útoků, které po sobě nezanechávají žádné stopy v systému, zvyšuje se počet útočníků v souvislosti s vyšší návratností investic do útoků, rozšiřuje se trh s různými malwary, botnety a zcizenými údaji. Velký boom zažívají hrozby cílící na konkrétní uživatele – sofistikované formy phishingu, ransomwaru apod. Zdaleka již nejsou ohroženi pouze uživatelé stolních počítačů a notebooků. Útočníci se ve stále větší míře zaměřují na mobilní zařízení a jejich operační systémy (zejména Android a iOS). Oblibu u útočníků získávají útoky, které v případě odhalení zaútočí na systém a vyřadí ho z provozu, a útoky, které zcela skryjí veškeré důkazy o své aktivitě v rámci systému a znemožní tak identifikaci rozsahu útoku a ztráty dat. Ani vzrůstající popularita a počáteční vysoká účinnost sandboxů útočníky nezastavila - vyvíjejí malware, který je schopen rozeznat prostředí sandboxu od reálného prostředí.

Ohrožena jsou všechna zařízení, která vstupují do kyberprostoru – tedy i chytré hodinky, chytré televizory, ledničky atd. Tato zařízení tvoří tzv. internet věcí, který již nyní proniká do našich každodenních životů. Senzory bude v budoucnu vybavena i veřejná infrastruktura, zdravotnické přístroje a celé výrobní linky. Přičemž tato špatně zabezpečená zařízení jsou často součástí domácích či korporátních sítí. Komunikují i mezi sebou (M2M komunikace) a stávají se tak terčem pro útoky typu „land and expand“, tedy napadení jednoho zařízení, ze kterého se škodlivý kód rozšíří i na další části systému nebo sítě.

To všechno vytváří velké možnosti a prostor pro útočníky, a zároveň starosti a problémy pro uživatele a bezpečnostní společnosti, které musí na všechny nové a sofistikované hrozby hledat odpovědi a řešení. Kybernetická bezpečnost se musí stát nedílnou součástí dlouhodobých firemních strategií tak, aby rozhodování s ní spojené bylo prováděno na úrovni nejvyššího vedení společností. Naprostou nutností je řešit kybernetickou bezpečnost před útokem, v průběhu i po útoku. Prevence je velmi

důležitá, nikdy však nemůže zajistit stoprocentní úspěšnost blokace a odražení útoků. To, že je potřeba soustředit se na všechny tři fáze, reflektují svým obsahem a požadavky mezinárodní normativní předpisy zaměřující se na problematiku kybernetické bezpečnosti.

První kapitola se zaměřuje na uvedení do problematiky kybernetické bezpečnosti, vysvětlení základních pojmů a specifikuje současný stav kybernetické bezpečnosti. Druhá a třetí kapitola popisuje převážně právní a normativní předpisy související s kybernetickou bezpečností. Praktická část práce je tvořena zejména návrhem jednotlivých částí a úrovní produktu, jeho realizací a shrnutím.

1 Literární rešerše

V souvislosti s tím, o jak dynamicky vyvíjející se oblast se jedná, je dostupných jen málo literárních zdrojů v klasické knižní podobě. Většinu informačních zdrojů, ze kterých je možné čerpat a ze kterých vychází také tato diplomová práce, tak tvoří především platné mezinárodní standardy a právní předpisy České republiky pro oblast kybernetické bezpečnosti. Dále lze za kvalitní a velmi přínosné zdroje označit výroční zprávy významných bezpečnostních společností – Cisco, Kaspersky Lab, Check Point atd. Dalším zdrojem pro tuto diplomovou práci jsou dvě bakalářské práce, odborné články různých autorů a v neposlední řadě také webové portály institucí působících v oblasti kybernetické bezpečnosti a/nebo její certifikace (např. NBÚ – Národní bezpečnostní úřad).

Hager se ve své bakalářské práci [5] zabývá návrhem obchodního modelu poskytujícího služby v oblasti kybernetické bezpečnosti. Soustředí se na průzkum trhu a krátký popis návrhu obchodního modelu – meřitelné cíle, nabízenou hodnotu, zákaznické vztahy, komunikační kanály a klíčové zdroje. Halama se v bakalářské práci [6] věnuje analýze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a jeho porovnání s ISO/IEC 27001. Dále předkládá návrh služeb, které by mohly najít uplatnění v oblasti kybernetické bezpečnosti, a v krátkosti popisuje zákaznická odvětví, lidské zdroje a úrovně služeb. Tyto bakalářské práce tak nastínily základní představu o tom, co je možné v oblasti ověřování a certifikace kybernetické bezpečnosti nabízet a jaké zdroje jsou k tomu zapotřebí. Z tohoto základního rámce tato diplomová práce vychází, navazuje na něj a dále ho rozpracovává. Detailně se věnuje výhradně nabízenému produktu a jeho realizaci.

Většina z použitých literárních zdrojů je dostupná online. Zejména v oblasti kybernetické bezpečnosti je totiž nutné klást důraz na aktuálnost zdrojů, proto je literatura starší 2 a více let využita pouze ve výjimečných případech. Co se týče aktuálnosti normativních a legislativních předpisů - mezinárodní normy jsou aktualizovány nejméně jednou za pět let, legislativní předpisy pak nejčastěji do dvou

let. Dostupnost legislativních předpisů je bezproblémová, jejich aktuální znění je možné dohledat online. Situace u mezinárodních standardů je mnohem složitější. Veškeré normy jsou dostupné až po zakoupení či zaplacení poplatku za možnost jejich studia na pobočce ÚNMZ (Úřad pro technickou normalizaci, metrologii a státní zkušebnictví).

Celkově lze konstatovat, že existuje velké množství online zdrojů věnujících se kybernetické bezpečnosti a zákonu č. 181/2014 Sb., o kybernetické bezpečnosti. Naopak počet knižních zdrojů zaobírajících se touto problematikou lze považovat za nedostatečný. Specifické oblasti kybernetické bezpečnosti, např. kybernetická bezpečnost inteligentních budov, internetu věcí či inteligentních automobilů trpí nedostatkem jakýchkoli literárních zdrojů.

2 Kybernetická bezpečnost

„Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.“

Takto je definována kybernetická bezpečnost ve Výkladovém slovníku kybernetické bezpečnosti [2], za kterým stojí Policejní akademie ČR a společnost AFCEA. Slovník byl vydán pod záštitou NCKB a aktualizován pro rok 2015.

Kybernetickou bezpečnost lze definovat jako odvětví výpočetní techniky, známé také jako informační bezpečnost, uplatňované jak u počítačů, tak sítí. [3] Oba pojmy – informační a kybernetická bezpečnost – mají stejný význam. To, že je možné tyto pojmy zaměňovat, je velmi důležité, protože se lze často setkat s tvrzením opaku a jejich odlišným výkladem. Sobě rovným je staví i samotný zákon č. 181/2014 Sb., o kybernetické bezpečnosti [39], který stejně jako norma ISO/IEC 27001 [83] vyžaduje ustanovení, implementaci, kontrolu a neustálé zlepšování systému řízení bezpečnosti informací (dále jen ISMS). Navíc § 29 vyhlášky č. 316/2014 Sb. [40] hovoří o tom, že pokud má odpovědná osoba nebo orgán spadající pod účinnost zákona (dle § 3) certifikovaný ISMS podle normy ISO/IEC 27001 a prokáže potřebnou dokumentaci, bude to zároveň znamenat, že je v souladu se zákonem.

Problematika kybernetické bezpečnosti je disciplína, která se velice dynamicky rozvíjí. Vznikají stále nové programy jak v oblasti ochrany dat a informací, tak na druhé straně také programy, které vytváří různí útočníci jako např. hackeři, kriminální živly, teroristé apod. Jedná se o nekonečný souboj, ve kterém prozatím aktivnější a častěji vítězící stranou bývají útočníci. [1]

Nejvíce rizikovými oblastmi jsou užívané informační a komunikační technologie a lidské zdroje, tedy zaměstnanci organizace. Snad ve všech výzkumech jsou právě lidé označováni za nejrizikovější faktor vyzrazení, kompromitace, modifikace, úniku a/nebo zničení citlivých dat a informací. [1]

Hlavní důvody pro implementaci kybernetické bezpečnosti v organizaci: [1]

- vzájemné ovlivňování ekonomik a dalších odvětví hospodářství prostřednictvím informačních a komunikačních technologií;
- digitalizace světa, kdy je stále více dat předáváno v digitální formě a nejvýznamnější a nejdůležitější data z pohledu celé organizace jsou uložena v informačních systémech, v poslední době v tzv. cloud computingu;
- způsoby a techniky přenosu dat v sítích jsou všeobecně známé ve formách přenosových a komunikačních standardů, a proto tato data mohou být útočníky ohrožena.

2.1 Úrovně zabezpečení

U kybernetické bezpečnosti lze v rámci organizací rozlišit 5 úrovní vyspělosti zabezpečení následovně (postupně od nejnižší úrovně po nejvyšší). [4]

I. Kybernetická bezpečnost je řešena ad hoc.
- Minimum definovaných bezpečnostních procedur. Žádné formální řízení kybernetické bezpečnosti. Ta je brána jako fixní režijní náklad.
- Důsledky: organizace v podstatě akceptuje neznámé riziko, nechává ji extrémně zranitelnou vůči útokům jak zevnitř, tak z vnějšku. Důsledkem je neustálá zranitelnost organizace.

II. Kybernetická bezpečnost je řešena příležitostně.
- Probíhají základní přípravy na známé druhy útoků. Je stanoven rozpočet pro bezpečnostní opatření poskytovaná vendorem. Kybernetická bezpečnost získává občasnou pozornost vedení organizace.
- Důsledky: možnosti útoků jsou zmírněny, nicméně organizace je stále zranitelná. Zajištěna je pouze základní úroveň ochrany.

III. Kybernetická bezpečnost je řešena opakovaně.
- Dochází k pochopení možných ztrát v případě narušení bezpečnosti. Pro kritické oblasti jsou připraveny plány obnovy v případě kybernetického incidentu. Existuje funkční bezpečnostní výbor, který je pod dohledem vedení organizace. Kybernetická bezpečnost má trvalou pozornost vedení organizace.

- Důsledky: vícevrstvé zabezpečení a zapojení vedení organizace včetně sledování ztrát dělá organizaci méně zranitelnou vůči běžným kybernetickým útokům.

IV. Kybernetická bezpečnost je řízena.

- Je ustanoven systematický proces monitorování a kontrolování v rámci celé sítě. Jsou provedeny počáteční přípravy na kybernetický incident. Manažer kybernetické bezpečnosti (CISO – Chief Information Security Officer) reportuje výsledky vrcholovému managementu organizace.
- Důsledky: zajištění potřebné úrovně integrity, dostupnosti a důvěrnosti. Organizace je připravena na většinu útoků. Problém představují pouze nové nebo nečekané typy útoků.

V. Kybernetická bezpečnost je optimalizována.

- Kybernetická bezpečnost má vysokou prioritu. Spolupráce interních zaměstnanců a vendorů je úzce koordinována. Plán na zajištění bezpečnosti je tvořen na úrovni vrcholového managementu. Představenstvo si uvědomuje důležitost zajištění kybernetické bezpečnosti a své role.
- Důsledky: nepřetržitá připravenost na známé i neznámé hrozby a katastrofy vytváří největší pravděpodobnost, že nedojde k narušení služeb či kontaminaci dat. Organizace je připravena i na situace, kdy k narušení nebo kontaminaci dojde.

2.2 Kyberprostor

Výraz kyberprostor je uměle vytvořené slovo, jež poprvé použil W. Gibson v roce 1984 ve své knize Neuromancer, přičemž vycházel ze základů kybernetiky jako vědního oboru. S narůstajícím rozvojem technologií se tento termín začal běžně užívat i mezi odbornou veřejností. Kybernetickým prostorem chápeme virtuální svět tvořený moderními informačními a komunikačními prostředky (existujícími počítačovými, informačními a komunikačními sítěmi). Tento svět lze označit za paralelní ke světu reálnému. Nicméně se nejedná o svět nijak oddělený, právě naopak – všechno, co se v tomto světě odehraje, má dopad na realitu. [5]

Do tohoto paralelního světa se člověk podle Johna Barlowa (zakladatele Electronic Frontier Foundation) dostane ve chvíli, kdy nějakým způsobem vstoupí do sítě. Pokud tedy například telefonujeme nebo surfujeme po internetu, nacházíme se již v kybernetickém prostoru. [6]

2.3 Hrozby v kyberprostoru a jejich klasifikace

Definice bezpečnostní hrozby: [2]
„Potenciální příčina nežádoucí události, která může mít za následek poškození systému a jeho aktiv, např. zničení, nežádoucí zpřístupnění (kompromitaci), modifikaci dat nebo nedostupnost služeb.“

Obecně si lze pod hrozbou v kyberprostoru představit cokoliv, co může nějakým způsobem vést k nežádoucí změně informace, chování systému nebo jeho parametrů. Hrozby využívají zranitelnosti, které umožňují útočníkům získat neoprávněný přístup. Zranitelnosti jsou využívány úmyslně, nicméně může dojít i k náhodné realizaci určité hrozby (nehody, poruchy, živelné události apod.). Úroveň hrozby se posuzuje podle následujících rysů: [1]

- nebezpečnost hrozby - schopnost způsobit škodu,
- přístup hrozby - pravděpodobnost, že se hrozba dostane k aktivu,
- frekvence výskytu hrozby a
- motivace hrozby - zájem vyvolat hrozbu vůči aktivu.

Hrozby lze kategorizovat na: [7]

- objektivní
    - přírodní, fyzické (požár, povodeň, výpadek napětí, poruchy apod.),
    - fyzikální (např. elektromagnetické vyzařování),
    - technické nebo logické (např. porucha paměti, chyby softwaru, špatné propojení jinak bezpečných komponent, krádež nebo zničení paměťového média);

- subjektivní (plynoucí z lidského faktoru)
    - neúmyslné (např. působení neškoleného uživatele nebo správce informačního systému),
    - úmyslné (činnost špionů, teroristů, konkurentů, hackerů, nejčastěji však vlastních zaměstnanců).

Infrastruktury a systémy organizací bývají obvykle vystaveny působení stejných hrozeb (tzv. obecných neboli generických hrozeb). Níže jsou uvedeny příklady typických hrozeb pro organizace a typických hrozeb pro společnost. [1]

Příklady typických hrozeb pro organizace: [1]

- neautorizovaná modifikace informací, informačních zdrojů a služeb (porušení integrity odchytáváním a modifikací zpráv, vkládáním a replikacemi zpráv),
- neautorizované zpřístupnění informace (např. odposlechem na přenosovém médiu, analýzou toku vyměňovaných zpráv nebo jejich délek),
- neoprávněné kopírování z dočasných paměťových míst (vyrovnávací paměti),
- agregace citlivých informací z méně citlivých dílčích informací,
- dedukce z neoprávněně získaných informací z veřejných zdrojů,
- neautorizované použití zdrojů (krádeže hardwarových a softwarových komponent včetně používání jejich neoprávněných kopií),
- neoprávněné používání informačních systémů a služeb jimi poskytovaných,
- znepřístupnění služeb (zabránění autorizovaným subjektům ve využívání informačního systému).

Příklady typických hrozeb pro společnost: [8]

- internetové podvody a krádeže (ohrožení internetového bankovnictví, krádeže dat z kreditních karet, falešné e-shopy, zneužívání osobních údajů),
- šíření dětské pornografie,
- praní špinavých peněz pomocí virtuálních měn,
- projevy extremismu, teroristická propaganda (i návodů ke konstrukci bomb),
- stalking, internetová šikana, spam a další.

2.4 Kybernetický útok

Definice útoku dle ČSN ISO/IEC 27000: [9]
„*Pokus o zničení, vystavení hrozbě, změnu, vyřazení z činnosti, zcizení aktiva nebo získání neoprávněného přístupu k aktivu nebo uskutečnění neoprávněného použití aktiva*.“

Informační technologie nabízejí svým uživatelům možnosti rychlé a efektivní výměny dat, současně ale poskytují značné výhody těm, kteří chtějí kyberprostor zneužít k nekalým záměrům. Zejména anonymita a prostorová neuchopitelnost internetu způsobují, že se stále větší část kriminálních aktivit přesouvá právě do kybernetického prostoru. Ten totiž umožňuje útočníkům rychlé a snadné splnění jejich cílů s minimálním rizikem případného postihu. [8]

Útok je faktickou realizací hrozby. Zahrnuje techniky, které útočníci využívají ke zneužití zranitelností v aplikacích. Spektrum možných útoků lze rozdělit do 4 kategorií následovně: [10]

- aktivní útoky iniciované zvenčí (např. Brute Force Attack, DoS Attack, DDoS Attack, exploit serverů apod.);
- pasivní útoky iniciované zevnitř (virus, malware, spyware, SPAM, phishing a další);
- útoky uvnitř sítě (např. ARP poisoning, DNS poisoning nebo rebinding, MAC a IP spoofing, útok na data – např. Jscript nebo Kryptik);
- útoky proti webovým serverům (např. Cookie Tampering, Cross Site Request Forgery, Cross Site Scripting, SQL Injections).

V poslední době se naplno projevuje problematika moderních kybernetických útoků. Mezi ně lze zařadit zejména cílené útoky, průmyslovou špionáž, zero-day útoky a útoky využívající polymorfní malware. Tyto útoky se vyznačují několika společnými vlastnostmi (např. neznámé signatury, přesná zacílenost, neviditelnost pro tradiční bezpečnostní řešení – antiviry, IDS/IPS, firewally apod.).

2.4.1 Honeypot

Pro pomoc v boji s kybernetickými útočníky byly vytvořeny honeypoty. Ty slouží jako návnada lákající útočníka, přičemž po zachycení potenciálně nebezpečného softwaru dochází k jeho automatizované analýze. V České republice bylo vytvořeno hned několik takových honeypotů CSIRT týmem CZ.NIC, který provozuje webový portál [1], kde je možné sledovat útoky „zlákané“ a zadržené jednotlivými honeypoty v reálném čase. Z portálu je možné stahovat týdenní statistiky, ty jsou ale vzhledem k velkému množství útoků velmi nepřehledné.

2.5 Zranitelnosti

Definice zranitelnosti: [2]
„Slabé místo aktiva nebo opatření, které může být využito jednou nebo více hrozbami.“

2.5.1 Zranitelnosti v softwaru

Zranitelnosti v běžně využívaném softwaru patří k hlavním zdrojům kybernetických bezpečnostních incidentů. Jsou hlavním zdrojem infekcí v počítačích a způsobují úniky kriticky důležitých dat. Zranitelnosti jsou přitom spíše zodpovědností programových vývojářů než uživatelů. Programy jsou zranitelné až do té doby, než jejich tvůrci vydají záplaty v podobě patchů. Jejich pravděpodobnost výskytu roste s růstem komplexnosti softwaru. Vliv mají ale i politiky výrobců, preferujících funkcionalitu a automatické funkce před bezpečností. To vše ve výsledku umožňuje nekontrolovatelné šíření malware, neoprávněný přístup k zařízením, osobním údajům apod.

[1] Webový portál provozovaný CZ.NIC lze nalézt na: https://honeymap.cz/

2.5.2 Zranitelnosti v hardwaru

Hardwarové chyby jsou závažné z toho důvodu, že se těžko opravují. Hlavní úskalí tkví v tom, že bezpečnostní díra může útočníkovi zajistit přístup do nejprivilegovanějších oblastí. V případě jejího zneužití se útočník dostane do oblastí, ke kterým nemá uživatel ani operační systém přístup. Díky tomu se v nich může (např. škodlivý rootkit) ukrýt před detekcí nebo pokusy nakažený systém vyčistit, mezitím může ovlivňovat cokoliv, co uživatel dělá. Kód běžící na úrovni SMM (System Management Mode) je z operačního systému nedosažitelný, pokud se do něj útočník naboural, má nad systémem prakticky plnou kontrolu. Může tak manipulovat celou pamětí nebo probíhajícími operacemi. Na jeho odstranění nestačí ani vymazání pevného disku a reinstalace operačního systému. Malware nacházející se ve firmwaru totiž umožňuje zařízení znovu infikovat.

2.5.3 Lidský faktor

Svět kybernetické bezpečnosti významně ovlivňují lidé. Rizikovost lidského faktoru ještě více umocňuje současný rozmach BYOD (Bring Your Own Device). Patří sem jak úmyslné jednání (krádež, pomsta, zlomyslnost), tak i způsobení újmy neúmyslným jednáním (nezkušenost, neznalost, nedbalost). Problém nastává zejména v případě, kdy dotyčný jedinec zastává důležitou funkci (např. administrátorskou). Počítače se nejčastěji nakazí viry kvůli stahování pirátských souborů, souborů s obsahem pro dospělé nebo neaktualizovanému softwaru. Velmi často za tím stojí také podvodné techniky sociálního inženýrství (např. phishingu) a nezodpovědné chování uživatelů. V těchto případech nepomůže ani používání moderních technologií, využívání procesní politiky, provádění aktualizací, instalování bezpečnostních patchů atd. Jediným možným řešením je důkladné a efektivní vzdělávání uživatelů. Ve firemním prostředí by se nemělo zapomínat na pravidelná školení bezpečnostních politik a k tomu se vážících zásad. Souvisejícím problémem je i zálohování. Většina lidí uchovává na svých zařízeních důvěrné informace, ovšem jen málo z nich zvažuje vytvoření záložní kopie pro případ ztráty dat.

2.6 Kybernetická bezpečnostní událost a kybernetický bezpečnostní incident

Vzhledem k častému zaměňování těchto dvou pojmů budou uvedeny jejich definice a z nich vyplývající rozdíl. Norma ČSN ISO/IEC 27000 definuje událost a incident bezpečnosti informací následovně: [9]

- událost jako *„zjištěný výskyt stavu systému, služby nebo sítě označující možné narušení politiky bezpečnosti informací nebo selhání opatření; nebo předem neznámá situace, která může být pro bezpečnost závažná“,*
- incident jako *„jednotlivá nežádoucí nebo neočekávaná událost bezpečnosti informací nebo série nežádoucích nebo neočekávaných událostí bezpečnosti informací, které mohou s významnou pravděpodobností vyvolat kompromitování operací souvisících s činností organizace a ohrožení bezpečnosti informací.“*

Kybernetická bezpečnostní událost je událost, která může způsobit narušení bezpečnosti informací v informačních systémech, bezpečnosti služeb nebo bezpečnosti a integrity sítí elektronických komunikací. Kybernetický bezpečnostní incident je narušení v důsledku kybernetické bezpečnostní události.

- Ke vzniku incidentu dochází na základě vyhodnocení detekovaných kybernetických bezpečnostních událostí.

O hojném množství incidentů se veřejnost vůbec nedozví. To především díky snaze inkriminovaných organizací a zapojení jejich krizových managementů. Následuje výčet několika v nedávné době zaznamenaných incidentů, detailněji hovoří o současném stavu kybernetické bezpečnosti kapitola 2.9.

- DDoS útoky v ČR (největší v roce 2013) – způsobení nefunkčnosti webových portálů (např. společnosti Seznam, dále různých bank, mobilních operátorů a dalších institucí); [2]

[2] Více informací na: http://technet.idnes.cz/ddos-na-operatory-0m0-/sw_internet.aspx?c=A130307_093529_sw_internet_vse

- krádež údajů 145 miliónů aktivních uživatelů služeb eBay (rok předtím 152 milionů u Adobe); [3]
- ruským hackrům skupiny Dragonfly se podařilo hacknout 1000 energetických firem; [4]
- hackeři napadli lety z Varšavy – letadla nebyla schopná odletět; [5]

2.7 Zodpovědnost za kybernetickou bezpečnost

Zodpovědnost mají zejména koneční uživatelé, výrobci zařízení a jejich dodavatelé. Nicméně všichni, kdo se účastní vývoje, nasazení a používání těchto zařízení, hrají důležitou roli. Definovat lze 6 následujících rolí. [11]

Role výrobců zařízení

Výrobci jsou zodpovědni především za specifikaci bezpečnostních požadavků a jejich implementaci a ověřování. Výrobci zařízení jsou zodpovědni za zvolení správného operačního systému a procesoru (nebo správné zvolení dodavatelů těchto komponent), za používání bezpečných protokolů, bezpečné autentizace a ochranných mechanismů (např. endpoint firewallu).

Role dodavatelů operačních systémů

Výběr správného dodavatele OS (může se jednat také o open source komunitu, která vytváří a udržuje operační systém) je sice zodpovědností výrobců zařízení, nicméně samotný dodavatel operačního systému je také zodpovědný, a to za bezpečnost každé komponenty dodávaného operačního systému. Komunikační protokoly a služby, jež jsou často využívány útočníky jako hlavní vektory pro vedení jejich kybernetických útoků, jsou zpravidla svázány právě s OS.

[3] Více informací lze nalézt na: http://technet.idnes.cz/hackeri-ukradli-udaje-vsech-uzivatelu-ebay-f22-/sw_internet.aspx?c=A140522_090921_sw_internet_skr
[4] Více informací na: http://thehackernews.com/2014/07/dragonfly-russian-hackers-scada-havex.html
[5] Více informací lze nalézt na: http://zpravy.aktualne.cz/zahranici/hackeri-napadli-lety-z-varsavy-zpozdily-se-i-spoje-do-prahy/r~37de1c9e18a311e5b5ba0025900fea04/

Role dodavatelů čipů

To samé platí vzhledem k dalším dodavatelům, například dodavatelům čipů. Tito dodavatelé by měli vyrábět procesory se zabudovanou schopností ověřování kódu, detekce fyzické manipulace spolu se šifrovacími enginy. Takové nástroje umožňují výrobcům vyvinout a nasadit zařízení, která ověřují, zda byl spuštěn autentický kód a zda někdo fyzicky neotevřel zařízení. Jakmile jsou podobné události zjištěny, zařízení by se mělo samo vypnout a událost nahlásit.

Role specializovaných bezpečnostních společností

Výrobci zařízení a koneční uživatelé nemají vždy dostatečnou odbornost a zkušenosti pro řešení všech aspektů bezpečnosti. Specializované bezpečnostní společnosti poskytují potřebnou odbornost, nástroje, specifické bezpečnostní řešení, bezpečnostní audity a verifikační služby. Hrají důležitou roli, a to především díky zajišťování shody s definovanými bezpečnostními požadavky, testování zařízení a poskytování vzdělávání pro výrobce zařízení a konečné uživatele.

Role konečných uživatelů

Konečný uživatel je závislý na schopnosti výrobce vyrobit zařízení, která jsou vybavena adekvátními bezpečnostními vlastnostmi a funkcemi. Úkolem konečného uživatele je, aby bylo zařízení nasazeno a používáno bezpečným způsobem. Jak nám potvrzuje historie, většina narušení bezpečnosti je způsobena lidskou chybou nebo nedbalostí. Lidé jsou náchylní k používání slabých nebo přednastavených hesel. Ponechávají tak útočníkům “otevřené dveře“ a jakákoliv snaha výrobců zařízení může přijít v niveč.

Poskytovatelé síťových služeb

Poskytovatelé služeb mají prostředky k zajištění, že bude bezpečnost zahrnuta do návrhu struktury sítě, a mají dostatečný vliv na výrobce zařízení. Mohou tak usilovat

o to, aby výrobci zařízení vyráběli zařízení bezpečná. Je mnohem pravděpodobnější, že výrobci zařízení budou reagovat na požadavky od poskytovatelů služeb, kteří kupují podstatně větší množství jejich zařízení než koneční uživatelé. Poskytovatelé síťových služeb mohou také zajistit nasazení zařízení s bezpečnými hesly a nastavením. Síť musí být zabezpečena stejně dobře jako specifická zařízení a koncové body do ní připojené.

Shrnutí

Efektivního řešení kybernetické bezpečnosti lze dosáhnout jen skrz koordinovanou snahu všech zodpovědných stran, a to jak ve fázi vývoje, tak i při nasazení a používání zařízení. Bohužel žádná z výše zmíněných rolí nemůže sama svou snahou zajistit dostatečnou úroveň zabezpečení. Celé úsilí musí začít u výrobců zařízení a jejich dodavatelů (OS, čipy). Začneme-li jakousi základní vrstvou, kterou by představovalo zabezpečení podstatných komponent jednotlivých zařízení, mohou poté na této bázi stavět i ostatní zúčastněné subjekty – další výrobci, integrátoři či koncoví uživatelé. Pomocnou ruku v tomto úsilí mohou výrobcům zařízení podat specializované bezpečnostní společnosti. Sdílenou zodpovědnost přehledně zobrazuje Obrázek 1.

Obrázek 1 - Zodpovědnost za kybernetickou bezpečnost
Vlastní tvorba

2.8 Problematické oblasti

Existují oblasti, ve kterých je situace kybernetické bezpečnosti přímo kritická. Jedná se zpravidla o oblasti nově vznikající a/nebo oblasti s dynamickým rozvojem. Za příklad lze uvést oblast internetu věcí a s ním související oblast inteligentních budov. Lze říci, že bezpečnost internetu věcí a inteligentních budov je v současnosti na stejné úrovni jako byla počítačová bezpečnost v devadesátých letech. V té době bylo vše nové a nikdo neměl žádné bezpečnostní standardy nebo možnosti jak monitorovat zařízení pro bezpečnost. Zejména neexistence standardů je opravdu zasádní. [12]

Jedná se přitom o oblasti, kterým je do budoucna předpovídán obrovský rozmach. Světový lídr mezi technologickými výzkumy (společnost Gartner) uvádí, že v roce 2020 bude k internetu připojeno 30 miliard zařízení. Společnost Cisco uvádí téměř dvakrát tolik – 50 miliard zařízení. Komunikace mezi senzory a inteligentními zařízeními má podle společnosti Cisco v roce 2018 představovat pětinu veškerého internetového provozu po celém světě. [12]

Útočníci si to samozřejmě dobře uvědomují a začínají se zaměřovat i na tyto špatně zabezpečené oblasti. Mezi již zaznamenané incidenty (úspěšně využité zranitelnosti) lze uvést například: [12]

- linuxového červa Darlloz, který se zaměřoval speciálně na zařízení internetu věcí (bezpečnostní kamery, set-top boxy, chytré měřiče);
- hacknutí jednoho z nejpopulárnějších zařízení pro inteligentní budovy – termostatu (během 15 sekund). Následně bylo možné ovládnout celý bezpečnostní systém;
- ovládnutí vozu Jeep Cherokee funkčním hackem na palubní systém Uconnect. Útočník mohl ovládat brzdy, stěrače, motor a vůz sledovat skrz GPS; [13]
- zapojení multimediálních centrer, televizorů, domácích směrovačů a ledniček do botnetu.

2.9 Analýza současné situace

Pro analýzu současné situace práce čerpá z výročních zpráv významných bezpečnostních společností. Postupně jsou tak uváděny výstupy a zjištění společností Cisco, Check Point a Ponemon Institute.

2.9.1 Cisco 2015 Annual Security Report

Každým rokem vydává bezpečnostní gigant – společnost Cisco – bezpečnostní report. V roce 2015 se Cisco zaměřilo na analýzu trendů jak z pohledu útočníků, tak i obránců (bezpečnostních společností). Důležitým bodem bylo konstatování, že uživatelé jsou v podstatě chyceni mezi útočící a bránící stranou. Stávají se cílem pro útočníky a často nevědomě pomáhají realizovat kybernetické útoky. Jako největší nebezpečí pro uživatele byly identifikovány neaktualizované prohlížeče, nedůvěryhodné zdroje a adware a s ním související click fraud. [14]

V průzkumu mezi 12 000 zaměstnanci v rámci Evropy, Středního východu, Afriky a Ruska bylo zjištěno, že: [14]

- 69 % zaměstnanců nemá povědomí o nedávných závažných narušení bezpečnosti (například Heartbleed),
- 52% věří, že chování zaměstnanců je druhou největší bezpečnostní hrozbou,
- 58 % si je vědomo, že jejich společnost má stanovenou bezpečnostní politiku,
- 44% dodržuje stanovenou politiku pouze občas a 7% ji dokonce aktivně a vědomě obchází.

Identifikované trendy na straně útočníků: [14]

- změna ve vektorech útoků – Java (-34%); Silverlight (+228%); PDF a Flash (beze změny);
- pokračující trend ve zneužívání uživatelů na úrovni webu a e-mailu – nárůst SPAMu (+250%);

    - snowshoe SPAM – posílání malého množství SPAMu z velkého množství IP adres,
    - metodami phishingu jsou kradeny přihlašovací údaje k e-malům, které jsou následně využívány k rozesílání SPAMu z kompromitovaných, přesto seriózních účtů,
    - posílané zprávy jsou úspěšně upravovány tak, aby nebyly zachyceny filtry a přesto si zachovaly svou základní strukturu. Bylo zaznamenáno až 95 variací stejné zprávy,
- malvertising (malicious advertisement) je na vzestupu a infekce je obtížnější detekovat.

Identifikované trendy na straně obránců: [14]

- efektivní patchování aplikací zůstává pro organizace výzvou (56% OpenSSL verzí je starší než 50 mesíců);
- bezpečnostní technici a CISO se musí vypořádat se sofistikovanými útoky, nevyváženými či nesprávně nastavenými politikami, nesprávným zapojením nebo nezapojením vrcholového managementu organizace a v neposlední řadě také vlivem samotných uživatelů.

2.9.2 Check Point 2015 Security Report

Check Point 2015 Security Report odhaluje nárůst hrozeb v podnikových sítích. Vychází přitom z informací získaných během roku 2014. Základem zprávy je detailní analýza více než 300 000 hodin monitoringu síťového provozu z více než 16 000 bezpečnostních bran a 1 milionu chytrých telefonů. Vyhledáván byl známý i neznámý malware, aplikace s vysokým rizikem a incidenty znamenající ztrátu dat. [15]

Bezpečnostní statistiky dle Check Pointu: [15]

- nárůst nového (neznámého) malwaru o 71%,
- 83% mělo existující infekci botem,
- 42% zažilo incident v oblasti bezpečnosti mobilních zařízení,
- 96% používalo nejméně jednu vysoce rizikovou aplikaci,

- ztráta chráněných dat se za poslední 3 roky zvýšila o 71%,
- každých 24 sekund přistoupí uživatel na škodlivou webovou stránku,
- každých 34 sekund je stažen neznámý malware,
- každých 5 minut je použita vysoce riziková aplikace,
- každých 6 minut je stažen známý malware,
- každých 36 minut jsou citlivá data zasílána mimo prostředí organizace.

2.9.3 Analýza nákladů při úniku dat

Analýza byla zpracována společností Ponemon Institute a sponzorována společností IBM. Byla provedena v roce 2015 ve 350 společnostech z 11 různých zemí. Celková suma nákladů se vyšplhala na 3,8 milionu amerických dolarů (o 23% více než v roce 2013). Průměrná cena za každý ztracený nebo odcizený záznam s citlivými či důvěrnými údaji stoupla o 6% - ze $145 na $154. Za tímto nárůstem vidí Dr. Larry Ponemon, zakladatel společnosti, tři hlavní příčiny. Zaprvé, zvyšující se frekvence kybernetických útoků a nákladnost jejich vypořádání. Zadruhé, finanční následky v podobě ztráty zákazníků. A zatřetí, organizace vynakládají vyšší náklady na forenzní a vyšetřovací činnosti, hodnocení a krizový management. [16]
Analýza uvádí tato klíčová zjištění: [16]

- zapojení vrcholového managementu a sjednání pojištění může snížit náklady na únik dat (v průměru o $5.50 za záznam);
- BCM hraje důležitou roli při snaze o snižování nákladů na únik dat (v průměru o $7.10 za kompromitovaný záznam);
- k nejnákladnějším únikům dat dochází v USA a Německu (v průměru $217 a $211 za kompromitovaný záznam);
- náklady na únik dat se liší podle odvětví (nejvyšší průměrné náklady jsou ve zdravotnictví - $363, nejnižší ve veřejném sektoru - $68);
- nejvíce úniků dat je způsobeno hackery a vlastními zaměstnanci (47%);

2.10 Budoucí vývoj a trendy v kybernetické bezpečnosti pro rok 2016

Předpovědi expertů ze společnosti Sophos pro rok 2016 mají následující podobu: [17]

- Andoid bude stále snadnějším cílem pro útočníky než iOS;
- IoT prozatím zůstane mimo oblast zájmu útočníků;
- útočníci budou více cílit na malé a středně velké podniky;
- změny v legislativě soustředící se na ochranu dat povedou k vyšším pokutám;
- VIP spoofware bude útočníky nadále využíván; [6]
- pokračující a prohlubující se hrozba v podobě ransomwaru; [7]
- metody sociálního inženýrství budou na vzestupu;
- na webu budou opět dominantní exploit kity. [8]

Další předpovědi na rok 2016 a výhled do ještě vzdálenější budoucnosti nabízí například McAfee Labs 2016 Threats Predictions report. [9]

[6] Příkladem VIP spoofingu může být odeslání e-mailu podřízeným, který se jeví jako e-mail od jejich nadřízeného, s pokynem k přesunu značných finančních prostředků.
[7] Např. nedávný úspěšně realizovaný útok na nemocnici v Los Angeles viz: http://www.reuters.com/article/us-california-hospital-cyberattack-idUSKCN0VR085
[8] Nejvyužívanějším exploit kitem současnosti je Angler. Dalším populárním je např. Nuclear.
[9] Zprávu McAfee Labs 2016 Threats Predictions report lze nalézt na: http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf

3 Ověřování a certifikace

3.1 Audit

„Audit je systematický, nezávislý a dokumentovaný proces získání důkazů z auditu a jejich hodnocení s cílem stanovit rozsah splnění kritérií auditu.“ [2]

Audit je slovo převzaté do češtiny a jeho výstižnějším českým synonymem je prověrka. Nicméně ve většině případů je používáno právě slovo audit. Zjednodušeně řečeno, audit je proces posuzování shody se stanovenými požadavky. Nelze ho provádět pouze na základě subjektivního hodnocení auditora, vždy je posuzován reálný stav vůči předem jasně definovaným požadavkům. V praxi jsou proto nejčastěji využívány normy ISO (International OrganizationforStandardization) a další technické normy či metodiky (např. TOGAF - The Open Group Architecture Framework). Kromě normativních požadavků existují také různé zákonné požadavky, které jsou stanovené v zákonech či nařízeních vlády. Součástí auditů jsou i požadavky interních firemních předpisů a pracovních postupů. Zásadní rozdíly mezi právními a normativními předpisy jsou charakterizovány v Tabulce 1.

	Právní předpisy	**Normy**
Účinnost	Na národní úrovni	Na mezinárodní úrovni [10]
Povinnost	Povinný charakter [11]	Dobrovolný charakter [12]

Tabulka 1 – Rozdíly mezi právními a normativními předpisy
Vlastní tvorba

Auditů je celá řada a jsou charakterizovány právě tím, vůči jakému standardu či právnímu předpisu je organizace prověřována. Může se jednat o audity systému řízení jakosti, environmentálního managementu, personální, výrobkové či finanční audity. Vzhledem k rozvoji standardizace a stále narůstajícímu počtu norem a

[10] Týká se zhruba 90% norem.
[11] Pouze pro subjekty a osoby v zákoně určené.
[12] Pokud není soulad s normou vyžadován právním předpisem. V tom případě se jedná o tzv. určené normy. (viz http://www.unmz.cz/urad/harmonizovane-normy)

právních předpisů se v dnešní době provádí zejména audit kombinovaný. Za kombinovaný audit se považuje audit vůči dvěma nebo více předpisům z různých oborů. U systémů řízení mluvíme o integrovaných auditech, protože dochází k integraci do jednoho systému, nicméně principy a procesy auditování zůstávají stejné jako u kombinovaného auditu. [18]

3.2 Principy auditu

Při provádění auditů musí auditoři dbát na dodržování řady zásad a pravidel tak, aby byl audit spolehlivým a efektivním nástrojem. Dodržování zásad jako je etické chování, spravedlivá prezentace, povinnost profesionálního přístupu, nezávislost a průkaznost, je důležitým předpokladem pro zajištění odpovídajících a opakovatelných závěrů. Tyto zásady shrnuje norma ČSN EN ISO 19011 [13] do 6 základních principů auditování (viz níže). Dodržení těchto principů je předpokladem, že závěry z auditu jsou relevantní a dostatečné. [19]

1. Integrita je základem profesionality.
2. Spravedlivé prezentování. Podávávání pouze pravdivých a přesných zpráv.
3. Profesionální přístup. Uplatňování pečlivosti a správného úsudku.
4. Důvěrnost. Bezpečnost informací.
5. Nezávislost. Základ nestrannosti auditu a objektivity závěrů z auditu.
6. Průkaznost. Racionální metoda dosahování spolehlivých a reprodukovatelných závěrů z auditu.

3.3 Základní typy auditů

U auditů lze rozlišit tři základní typy, které jsou společné pro všechny druhy auditů. Rozlišujeme audity interní, dodavatelské a externí. Rozdíl mezi interním a externím auditem je v samotném smyslu auditu. I interní audit může být prováděn externím subjektem. [20]

[13] Informace k ISO 19011 jsou dostupné na: http://seznamcsn.unmz.cz/Detailnormy.aspx?k=90788

Audit první stranou

Audit první stranou je označován jako interní audit. Veškeré cíle, priority a rozsah auditu si stanovuje organizace sama. Audit je využíván k prověření skutečného stavu a slouží jako podklad k rozhodování a provádění změn. Cílem interních auditů je zejména pomáhat organizaci co nejefektivněji plnit její cíle, vyvarovat se rizikům a ztrátám, vnitřní kontrola (např. proti podvodům) a optimalizace procesů, organizace či řízení. [20] Metodickým předpisem k provádění auditů první stranou je ISO 19011.

Audit druhou stranou

Audit druhou stranou je znám také pod názvem zákaznický audit. Jedná se o audit prováděný externím subjektem, jež má vůči dané organizaci určité zájmy (odběratelsko-dodavatelské vztahy). Může se jednat o audity výrobkové, audity procesů, resp. audity celého systému řízení firmy. Audit druhou stranou je často nahrazován doložením certifikátu, kterým dodavatel prokazuje soulad s určitým standardem. [21] Metodickým předpisem k provádění auditů druhou stranou je také ISO 19011.

Audit třetí stranou

Audit třetí stranou je prováděn externí organizací, která je na auditované organizaci zcela nezávislá. Cílem u tohoto typu auditu je nezávisle a objektivně posoudit, zda organizace dodržuje pravidla, ke kterým se hlásí nebo které jí nařizuje legislativa. V rámci externího auditu je vždy vymezen účel auditu a je známo, komu je audit určen. Výsledky mohou být určeny pro vlastníky, investory, veřejnost, státní orgány a/nebo další zájmové skupiny. [20]

Externí audit jsou oprávněny nabízet a vykonávat pouze autorizované organizace (více viz kapitola 3.4). Stejně tak je důležité, aby třetí strana rozuměla oboru auditované organizace, bez toho nebude schopna podat kvalitní výstup. Metodickým

předpisem k provádění auditů třetí stranou je ISO 17021. [14]

3.4 Akreditace a certifikace

„Akreditací se rozumí oficiální uznání, že subjekt akreditace je způsobilý provádět specifické činnosti (zkoušky, kalibrace, certifikace, inspekce atd.).“ [22]

Při nákupu výrobků nebo služeb jsme prostřednictvím prohlášení výrobců nebo různých druhů certifikátů ujišťováni o jejich kvalitě, bezpečnosti a spolehlivosti. Tyto certifikáty vydávají certifikační orgány (dále jen CO). Nástrojem pro zajištění toho, aby CO a další instituce (např. laboratoře) postupovaly v souladu s postupy shodnými s příslušnou specifikací (normou), je akreditace. Akreditace slouží k prokazování odborné způsobilosti a nestrannosti akreditovaných subjektů. Slouží také k rozlišení služeb poskytovaných akreditovanými a neakreditovanými subjekty, kde služby poskytované akreditovanými subjekty jsou považovány za kvalitnější a bezpečnější. Akreditace totiž vytváří tlak na růst dovedností personálu akreditovaných subjektů a na zajištění lepší technické vybavenosti těchto subjektů. [22]

Akreditace je uznání certifikačního orgánu pro provádění certifikací podle jednotlivých norem. V každé zemi existuje zpravidla jeden akreditační orgán (dále jen AO). V České republice je AO Český institut pro akreditaci (více o ČIA viz kapitola 3.5.2). AO jednotlivých zemí jsou sdruženy v Mezinárodním akreditačním fóru – International Accreditation Forum (IAF). Díky tomuto fóru jsou akreditace mezi členskými zeměmi, mezi které patří i Česká republika, vzájemně uznávány. [23]

Certifikace je nezávislé, nestranné a způsobilé posuzování třetí stranou (viz kapitola 3.3). CO musí být pro svou činnost akreditován. Certifikovat, tedy provádět certifikační audity a vydávat akreditované certifikáty, mohou v ČR jen organizace ověřené ČIA. CO získá osvědčení o akreditaci podle příslušné normy a v časově omezené platnosti. Přílohou osvědčení je věcné vymezení rozsahu platnosti

[14] Informace k ISO 17021 jsou dostupné na: http://seznamcsn.unmz.cz/Detailnormy.aspx?k=89654

akreditace (rozsah je identifikován pomocí kódů CZ-NACE a specifikací normativních předpisů). Certifikovat je možné výrobky (stanovené a nestanovené), systémy managementu (např. jakosti nebo bezpečnosti informací) a osoby (např. manažer kvality, specialista vibrační diagnostiky a další).

3.5 Národní normalizační a akreditační organizace

V následujících podkapitolách je krátce charakterizován Úřad pro technickou normalizaci, metrologii a státní zkušebnictví a Český institut pro akreditaci.

3.5.1 Úřad pro technickou normalizaci, metrologii a státní zkušebnictví

Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (dále jen ÚNMZ) byl zřízen zákonem č. 20/1993 Sb., o zabezpečení výkonu státní správy v oblasti technické normalizace, metrologie a státního zkušebnictví [15]. Jeho působnost je dále stanovena také zákonem č. 22/1997 Sb., o technických požadavcích na výrobky [16], zákonem č. 505/1990 Sb., o metrologii [17] a dále vyplývá z příslušných usnesení vlády a mezinárodních smluv, jimiž je Česká republika vázána. [25] ÚNMZ je organizační složkou státu v resortu Ministerstva průmyslu a obchodu ČR a jeho hlavním posláním je zabezpečovat úkoly vyplývající ze zákonů České republiky upravujících technickou normalizaci, metrologii a státní zkušebnictví a úkoly v oblasti technických předpisů a norem uplatňovaných v rámci členství ČR v Evropské unii. Od roku 2009 zajišťuje tvorbu a vydávání českých technických norem, do roku 2009 zajišťoval tuto činnost Český normalizační institut. [24]

[15] Více informací o zákoně č. 20/1993 Sb. lze nalézt na: http://www.zakonyprolidi.cz/cs/1993-20
[16] Více informací o zákoně č. 22/1997 Sb. lze nalézt na: http://www.zakonyprolidi.cz/cs/1997-22
[17] Více informací o zákoně č. 505/1990 Sb. lze nalézt na: http://www.zakonyprolidi.cz/cs/1990-505

3.5.2 Český institut pro akreditaci, o.p.s.

Český institut pro akreditaci (dále jen ČIA) je obecně prospěšná společnost. ČIA je národní akreditační orgán založený vládou České republiky, který poskytuje své služby v souladu s platnými právními předpisy ve všech oblastech akreditace státním i privátním subjektům. Princip jednotného evropského akreditačního systému tvořeného národními akreditačními orgány, které fungují podle jednotných pravidel a akreditují podle mezinárodně uznávaných norem, vychází z postoje ES specifikovaného v Globální koncepci o přístupu ke zkoušení a certifikaci. V souladu s požadavky mezinárodních norem (např. ČSN EN ISO/IEC 17011 [18]) a dokumentů ČIA provádí nestranné, objektivní a nezávislé posouzení způsobilosti (akreditaci). ČIA je členem mezinárodních organizací (např. IAF) a podepsala mezinárodní multilaterální dohody (na evropské i celosvětové úrovni) o vzájemném uznávání výsledků akreditací. [26]

[18] Více informací o ČSN EN ISO/IEC 17011 lze nalézt na: http://seznamcsn.unmz.cz/Detailnormy.aspx?k=72378.

4 Ověřování a certifikace v oblasti kybernetické bezpečnosti

4.1 Standardizace v oblasti kybernetické bezpečnosti

Standardizace hraje klíčovou roli při zajištění toho, aby byly bezpečnostní produkty nasazovány do systémů, které jsou schopné detekce a reakce na skutečné události. Zejména standardní rozhraní a protokoly umožňují, aby integrace systémů byla mnohem jednodušší. Umožňují také spolupráci produktů v heterogenním prostředí. Standardizace zkušebních metod umožňuje porovnávat bezpečnostní produkty smysluplným způsobem a poskytuje prostředky pro koncového uživatele k posouzení nových produktů nebo služeb z hlediska schopnosti těchto produktů a služeb splnit určité bezpečnostní požadavky. Standardizace přístupu k zavádění nových technologií a obchodních modelů pomáhá snížit složitost podnikatelského prostředí, což ve výsledku usnadňuje jeho zabezpečení. [27]

V nepřítomnosti standardizace může být komunikace problematická a procesy neúčinné. To platí především pro organizace s mezinárodní působností, které musí při své činnosti zohledňovat právní předpisy různých zemí. Přijetí standardů usnadňuje zákazníkům pochopit, jak fungují procesy organizace a snižují se náklady na audit a hloubkových kontrol. Navzdory tomu, že řádné využívání standardů je jednoznačně prospěšné při dosahování vysoké úrovně zabezpečení, lze identifikovat také spoustu výzev při snaze o dosažení těchto cílů v praxi. Mezi tyto výzvy lze zahrnout např. výzvy organizačního charakteru, nedostatek agility standardů a jejich konkurenční sady a nedostatečné povědomí o kybernetické bezpečnosti. [27]

4.2 Standardy v oblasti kybernetické bezpečnosti

V současnosti nejpoužívanější bezpečnostní standardy patří do rodiny ISO/IEC 27XXX. Tato rodina vychází z řady norem BS 7799, které byly vytvořeny BSI, a obsahuje i neznámější normu v této oblasti – ISO/IEC 27001 [83]. Ta stanovuje obecné

požadavky vycházející z osvědčených postupů (best practice) v oblasti informační bezpečnosti. Rodina obsahuje také normy věnující se informační bezpečnosti v různých oborech (zdravotnictví, bankovnictví apod.).

Existuje velké množství norem v různých oblastech, které se kybernetické bezpečnosti věnují okrajově. Jedním příkladem za všechny může být norma ISO/IEC 20000-1 [84] věnující se kvalitě poskytovaných IT služeb, která se ve svém bodě 6.6 zaměřuje právě na problematiku informační bezpečnosti.

4.2.1 Rodina norem ISO/IEC 27XXX

Normy této rodiny jsou zaměřeny na ustanovení, provozování, kontrolování a kontinuální zlepšování ISMS (Information Security Management System). Je složena ze vzájemně souvisejících norem, přičemž některé z nich jsou stále ve fázi přípravy či schvalování. Obsahuje technické normy popisující požadavky na ISMS a požadavky na certifikační orgány a organizace certifikující shodu s ISO/IEC 27001. Další technické normy poskytují návod pro různé oblasti implementace ISMS a zabývají se generickým procesem. [9] Kompletní a graficky zpracovaný přehled všech norem patřících do rodiny ISO/IEC 27XXX poskytuje na svém webovém portálu nezávislá poradenská společnost RAC. [19] Schéma nezobrazuje nejaktuálnější stav, nicméně ho lze považovat za relevantní (tvořeno v roce 2015).

U norem patřících do rodiny ISO/IEC 27XXX rozlišujeme celkem pět rolí: [9]

a) normy popisující přehled a terminologii;
b) normy specifikující požadavky;
c) normy popisující obecné směrnice;
d) normy popisující směrnice specifické podle odvětví a
e) normy popisující směrnice specifické podle oblasti řízení.

[19] Schéma znázorňující všechny normy rodiny ISO/IEC 27XXX lze nalézt na: http://www.iso27000.cz/rac/homepage.nsf/CZ/ISO27000/$FILE/Family%2027000%20150421.png

Specifikace dílčích norem a jejich předmětu a účelu je z důvodu zachování přehlednosti práce vložena do tabulky v Příloze A. U norem, pro které nebyl dosud vytvořen jejich český ekvivalent, byl jejich název volně přeložen do češtiny – nejedná se o oficiální název normy. Aktuálnost verze, názvu a popisu normy je zajištěna k datu 25. 1. 2016.

4.2.1.1 ISO/IEC 27001

Mezinárodní norma ISO/IEC 27001 [20] byla naposledy revidována 1. října 2013. První verze byla oficiálně publikována 15. října 2005, kdy nahradila jejího předchůdce - normu BS 7799-2:2002. [28] Pro tento mezinárodní standard byl vypracován český ekvivalent pod označením ČSN ISO/IEC 27001:2014 [83] a propojení se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti zmiňuje v § 29 samotná vyhláška o kybernetické bezpečnosti. [40]

Normu tvoří požadavky na systém řízení bezpečnosti informací (ISMS). Do jejího těla je včleněn dobře známý Demingův cyklus (PDCA), protože ISMS je potřeba nejen zavést a provozovat, ale i monitorovat, průběžně vyhodnocovat jeho účinnost a neustále zlepšovat. [28] Konkrétní kroky prováděné ve smyslu ISO/IEC 27001 v jednotlivých částech PDCA cyklu popisuje Tabulka 6 v Příloze B. Standard evokuje pět následujících činností: [29]

- **identifikaci** (řízení aktiv; posouzení rizik; navázání na cíle, vedení a aktivity organizace; definice procesů, postupů a politik),
- **ochranu** (kontrola přístupu; povědomí a školení; bezpečnost dat; údržba a opravy komponent; dodržování procesů a postupů k ochraně informací; řízení technických bezpečnostních prvků),
- **detekci** (neustálé sledování bezpečnosti; nastavení detekčních procesů),
- **reakci** (plánování reakcí; řízení komunikace; provádění analýzy; případná zmírnění dopadu incidentu a jeho eliminace; zlepšování reakčních činností) a
- **obnovu** (provádění a udržování obnovovacích procesů a postupů).

[20] Struturu standardu je možné vidět na: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

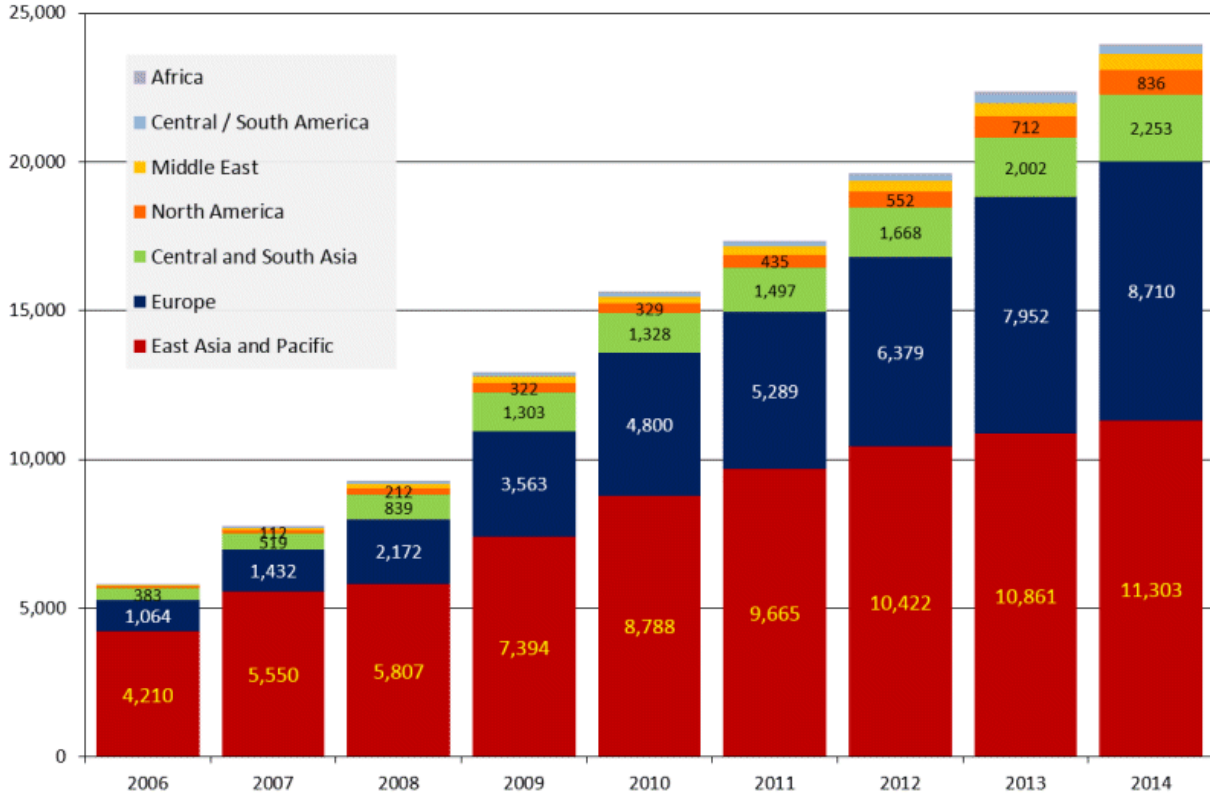
4.2.1.2 Certifikace ISMS dle ISO/IEC 27001

Certifikace ISMS dle ISO/IEC 27001 je aplikovatelná v jakékoliv organizaci. Je objektivním důkazem, prostřednictvím kterého vlastníci a management certifikované organizace potvrzují svým vlastníkům, zaměstnancům, zákazníkům a dalším zainteresovaným stranám, že vnímají odpovědnost k bezpečnosti informací. Certifikace dle ISO/IEC 27001 je v současné době nezbytností v mnoha oblastech podnikání, je vyžadována v obchodních vztazích a zvyšuje důvěryhodnost organizace. Organizace, která chce provozovat činnost certifikace a vydávat certifikáty ISO/IEC 27001, musí splnit akreditační požadavky definované v ISO/IEC 17021 a získat osvědčení o akreditaci. [30]

Podle studie ISO [21] bylo v roce 2014 v celkem 109 zemích světa 23 972 platných certifikátů ISO/IEC 27001. Vývoj v oblasti certifikace ISMS dle ISO/IEC 27001 od roku 2006 do roku 2014 znázorňuje Obrázek 2. [31]

- 83 % těchto certifkátů bylo na území Evropy, Východní Asie a v Pacifické oblasti (zejména USA) – zemí s největším počtem certifikátů bylo Japonsko (7181);
- celkový počet narostl oproti roku 2013 o 1623 certifikátů (z toho 758 v Evropě) – nárůst o 7 %;
- v České republice se jednalo o 276 platných certifikátů;
- nejvíce certifikátů bylo vydáno organizacím působícím v oblasti informačních technologií.

[21] Kompletní výsledky studie je možné stahnout zde: http://www.iso.org/iso/iso-survey_2014.zip



Obrázek 2 – Vývoj v oblasti certifikace ISMS dle ISO/IEC 27001 [31]

4.2.2 ISO/IEC 15408

ISO/IEC 15408 je série mezinárodních standardů pro certifikaci počítačové bezpečnosti, pro kterou byl vytvořen český ekvivalent v podobě ČSN ISO/IEC 15408. Převádí tzv. společná kriteria (celým názvem Common Criteria for Information Technology Security Evaluation nebo ve zkratce CC) pro vyhodnocení bezpečnosti informačních technologií do normalizované podoby. CC vznikla na základě již dříve používaných kritérií hodnocení, zejména amerických TCSEC (Trusted Computer System Evaluation Criteria) a Federal Criteria, evropských ITSEC (Information Technology Security Evaluation Criteria) a kanadských CTCPEC (Canadian Trusted Computer Product Evaluation Criteria). [32]

Hodnocení podle CC se soustřeďuje na hodnocení produktů IT (např. operační systémy, databázové systémy, síťové produkty, specializované bezpečnostní

produkty). Hodnotí sady bezpečnostních požadavků a specifikací pro daný produkt nazývané v CC bezpečnostní cíl (Security Target, ST). Hodnotí také implementačně nezávislé sady bezpečnostních požadavků nazývané profil ochrany (Protection Profile, PP). ST a PP se hodnotí převážně z hlediska úplnosti, konzistence a technické správnosti, a tedy vhodnosti pro proklamované použití. [32]

Při certifikaci se vychází z metodologie stanovené v ISO/IEC 18045. Jako formální základ pro vzájemné uznávání hodnocení byla uzavřena v roce 1998 dohoda CCRA (celým názvem „Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security"). Ta byla následně rozšířena o další země a pozměněna tak, že rozlišovala země provozující národní schéma pro hodnocení a certifikaci informačních technologií podle CC a země, které nemají vyvinuto vlastní schéma pro hodnocení a certifikaci dle CC - rozhodly se deklarovat, že uznávají hodnocení a certifikáty vydávané v rámci CCRA. Aktuální situace vypadá následovně: [33]

- členské země vydávající certifikáty:
    - Austrálie, Kanada, Francie, Německo, Indie, Itálie, Japonsko, Malajsie, Nizozemsko, Nový Zéland, Norsko, Korejská republika, Španělsko, Švédsko, Turecko, Spojené království, Spojené státy americké;
- členské země uznávající certifikáty:
    - Rakousko, Česká republika, Dánsko, Finsko, Řecko, Maďarsko, Izrael, Pákistán.

Země provozující vlastní schéma hodnocení a certifikace IT vydávají seznamy již certifikovaných produktů [22] (EPL – Evaluated Products List) a seznamy produktů, které jsou právě v procesu hodnocení. PP, které úspěšně prošly hodnocením, jsou zaznamenány do registrů PP [23] a mluví se o nich jako o certifikovaných, někdy také registrovaných profilech. Tyto profily jsou dostupné pro obecné použití.

[22] Dostupné zde: http://www.commoncriteriaportal.org/products/
[23] Dostupné zde: http://www.commoncriteriaportal.org/pps/

V České republice zatím není možné vydávat akreditované certifikáty pro ČSN ISO/IEC 15408, protože ČIA tuto akreditaci nenabízí. Souvísí to s pozicí České republiky v CCRA a zejména s obrovskou náročností (finanční, časovou i odbornou) kladenou těmito obsáhlými a komplexními standardy na laboratoře a certifikační orgány. Z těchto důvodů není prozatím v České republice žádná laboratoř hodnotící IT produkty podle tohoto standardu, a tudíž ani žádný certifikační orgán.

Série má celkem tři části [24]:

- ČSN ISO/IEC 15408-1 Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 1: Úvod a obecný model [85]
- ČSN ISO/IEC 15408-2 Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 2: Bezpečnostní funkční komponenty [86]
- ČSN ISO/IEC 15408-3 Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 3: Komponenty bezpečnostních záruk [87]

4.2.3 Kryptografické standardy

Kryptografické standardy nalézají využití jak v procesu vývoje, tak hlavně při provádění bezpečnostních testů. Základem pro níže uvedené standardy byly FIPS (postupně FIPS 140-1, poté FIPS 140-2). FIPS 140-2 byl publikován již v roce 2001. Následující snaha o aktualizaci na verzi 140-3 ztroskotala ve fázi hlasování o návrhu standardu a FIPS 140-3 byl nahrazen níže specifikovanými mezinárodními standardy.

- ISO/IEC 19790 – Informační technologie – Bezpečnostní techniky - Bezpečnostní požadavky pro kryptografické moduly
    - standard specifikuje bezpečnostní požadavky pro kryptografické moduly používané v rámci bezpečnostního systému ochrany citlivých dat v počítačových a telekomunikačních systémech. [34]

[24] Více informací o jednotlivých částech lze nalézt např. zde: https://www.enisa.europa.eu/activities/risk-management/current-risk/laws-regulation/rm-ra-standards/iso-iec-standard-15408

- ISO/IEC 24759 - Informační technologie – Bezpečnostní techniky – Testové požadavky pro kryptografické moduly
    - standard specifikuje metody, které mají být použity zkušebními laboratořemi k testování, zda je kryptografický modul v souladu s požadavky specifikovanými v ISO/IEC 19790. [35]
- ISO/IEC 17825 Information technology - Security techniques - Testing methods for the mitigation of non-invasive attack classes against cryptographic modules
    - standard specifikuje testovací metriky pro testy zmírnění neinvazivních útoků při dodržení shody s požadavky uvedenými v ISO/IEC 19790. Testovací metriky jsou spojeny s bezpečnostními funkcemi specifikovanými v ISO/IEC 19790. [36]

4.3 Legislativa

Právo chápe kybernetickou bezpečnost v užším významu, než jak ji vnímá podniková praxe. Bezpečnostní manažer musí pracovat vedle legislativy týkající se přímo kybernetické bezpečnosti též s rozsáhlou trestní, správní a civilní legislativou upravující právní povinnosti související s nejrůznějšími formami získávání, zpracovávání, ukládání a předávání informací. [37]

Kybernetickou bezpečnost právo vnímá především jako ochranu národního kyberprostoru před bezpečnostními hrozbami. Jednotlivé bezpečnostní incidenty mohou dosáhnout takové intenzity, že se negativně projeví v národním měřítku (např. výpadek páteřní sítě). Většina běžně se vyskytujících incidentů nedosahuje takové závažnosti. S těmito jevy se právo vypořádá za užití standardních ochranných institutů trestního, správního a civilního práva. [37]

V České republice se podobně jako v ostatních euroatlantických zemích intenzivně pracovalo na specifické právní úpravě národní kybernetické bezpečnosti. Tato snaha vyústila v roce 2014 v dokončení a přijetí zákona č. 181/2014 Sb., o kybernetické

bezpečnosti a s ním souvisejících prováděcích předpisů. Současně došlo v gesci Národního bezpečnostního úřadu (NBÚ) k vytvoření vládního dohledového pracoviště – Národního centra kybernetické bezpečnosti [25], které funguje jako středisko ochrany významné (tedy státní) a kritické informační infrastruktury. [37]

4.3.1 Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti vychází z Věcného záměru zákona o kybernetické bezpečnosti. [26] Při tvorbě záměru byly zohledněny jak vnější a vnitřní vlivy přispívající k nutnosti vytvoření zákona, tak i stav realizace kybernetické bezpečnosti v zahraničí (převážně státech EU). Záměr předložil návrh věcného řešení a zhodnotil také předpokládaný hospodářský a finanční dopad zákona. [38]

Zákon nabyl platnosti vyhlášením ve Sbírce zákonů dne 29. 8. 2014. Účinný je od 1. 1. 2015 a žádná novelizace zatím neproběhla. Důležitou skutečností je, že se zákon nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi. Zákon si klade za cíl zavést do praxe soubor oprávnění a povinností s cílem zvýšit bezpečnost kybernetického prostoru a nastavit mechanismus aktivní spolupráce mezi soukromým sektorem a veřejnou správou, a to za účelem vyšší efektivity řešení kybernetických bezpečnostních incidentů. Nesměřuje k eliminaci veškerých rizik, která se mohou dotknout všech uživatelů kybernetického prostoru, ale snaží se ochránit tu část infrastruktury, která je pro fungování státu významná a jejíž narušení by vedlo k poškození nebo ohrožení zájmů České republiky. Pro určené subjekty (v § 3 zákona) jsou stanoveny povinnosti, prostřednictvím kterých dojde ke zvýšení ochrany jejich informačních systémů, resp. sítí, které provozují. Tyto povinnosti lze přitom vnímat jako minimalistické, avšak dostatečně zajišťující dosažení stanoveného cíle. [39]

[25] Hlavní činnosti NCKB viz http://www.govcert.cz/cs/
[26] Kompletní znění Věcného záměru zákona o kybernetické bezpečnosti je dostupné na: https://www.nbu.cz/download/nodeid-1216/

Konkrétní povinnosti „namapované“ k jednotlivým subjektům a souborům aktiv přehledným způsobem zobrazuje schéma zveřejněné na webovém portálu NBÚ [27]. Jedná se především o povinnost zavést a provádět bezpečnostní opatření a vést o nich bezpečnostní dokumentaci, povinnost detekovat kybernetické bezpečnostní události a hlásit kybernetické bezpečností incidenty a povinnost oznamovat kontaktní údaje NBÚ nebo provozovateli národního CERT (provozovatelem je od konce roku 2015 na dobu neurčitou sdružení CZ.NIC [28]).

Pro správné pochopení funkce zákona v legislativním prostředí ČR a správné a včasné splnění povinností zákona zveřejnil NBÚ následující materiály:

- blokové schéma k zákonu a jeho prováděcím předpisům; [29]
- lhůty pro plnění povinností podle zákona o kybernetické bezpečnosti; [30]
- schéma procesu určování prvku kritické informační infrastruktury; [31]
- schéma procesu určování významného informačního systému. [32]

4.3.2 Související právní předpisy - zákony

Se zákonem o kybernetické bezpečnosti okrajově souvisí řada dalších právních předpisů. Následuje výčet platných souvisejících zákonů.

- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti [33]
- Zákon č. 240/2000 Sb., krizový zákon [34]
- Zákon č. 480/2004 Sb., o některých službách informační společnosti [35]

[27] Schéma povinností orgánů a osob podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti lze stahovat z: http://www.govcert.cz/download/nodeid-686/
[28] Více informací viz: http://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/nbu-a-cznic-uzavrely-smlouvu-o-provozovani-narodniho-cert/
[29] Blokové schéma k zákonu lze nalézt na: http://www.govcert.cz/download/nodeid-839/
[30] Lhůty pro plnění povinností podle zákona o kybernetické bezpečnosti lze nalézt na: http://www.govcert.cz/download/nodeid-584/
[31] Schéma procesu určování prvku kritické informační infrastruktury je dostupné na: http://www.govcert.cz/download/nodeid-673/
[32] Schéma procesu určování významného informačního systému lze nalézt na: http://www.govcert.cz/download/nodeid-714/
[33] Více informací o zákoně č. 412/2005 Sb. lze nalézt na: http://www.zakonyprolidi.cz/cs/2005-412
[34] Více informací o zákoně č. 240/2000 Sb. lze nalézt na: http://www.zakonyprolidi.cz/cs/2000-240

- Zákon č. 101/2000 Sb., o ochraně osobních údajů [36]
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy [37]
- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím [38]
- Zákon č. 127/2005 Sb., o elektronických komunikací [39]
- Zákon č. 227/2000 Sb. o elektronickém podpisu [40]

4.3.3 Prováděcí předpisy k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti

Prováděcí právní předpisy k zákonu o kybernetické bezpečnosti jsou celkem čtyři. Všechny byly rozeslány 19. 12. 2014 v rámci částky 127. [40]

- Nařízení vlády č. 314/2014 Sb., o úpravě náhrady za ztrátu na služebním příjmu po skončení neschopnosti ke službě vzniklé služebním úrazem nebo nemocí z povolání a o úpravě náhrady nákladů na výživu pozůstalých a na zřízení pomníku nebo desky.
- Nařízení vlády č. 315/2014 Sb., kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.
- Vyhláška 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).
- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.

[35] Více informací o zákoně č. 480/2004 Sb. lze nalézt na: http://www.zakonyprolidi.cz/cs/2004-480
[36] Více informací o zákoně č. 101/2000 Sb. lze nalézt na: http://www.zakonyprolidi.cz/cs/2000-101
[37] Více informací o zákoně č. 365/2000 Sb. lze nalézt na: http://www.zakonyprolidi.cz/cs/2000-365
[38] Více informací o zákoně č. 106/1999 Sb. lze nalézt na: http://www.zakonyprolidi.cz/cs/1999-106
[39] Více informací o zákoně č. 127/2005 Sb. lze nalézt na: http://www.zakonyprolidi.cz/cs/2005-127
[40] Více informací o zákoně č. 227/2000 Sb. lze nalézt na: http://www.zakonyprolidi.cz/cs/2000-227

Blíže popsána bude pouze nejdůležitější z nich – vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti, jejíž aktuální verze je platná od 1. 1. 2015. Podrobně upravuje především obsah bezpečnostních opatření a rozsah, v jakém jsou jednotlivé skupiny subjektů, na něž dopadá regulace zákona o kybernetické bezpečnosti, povinny zavést a provádět bezpečnostní opatření. Definuje rozsah a doporučenou strukturu bezpečnostní dokumentace, stanovuje konkrétní kategorie, typy kybernetických bezpečnostních incidentů a způsob jejich hlášení. V neposlední řadě stanovuje základní náležitosti oznámení o provedení reaktivního opatření a jeho výsledku s cílem zajištění zpětné vazby. [40]

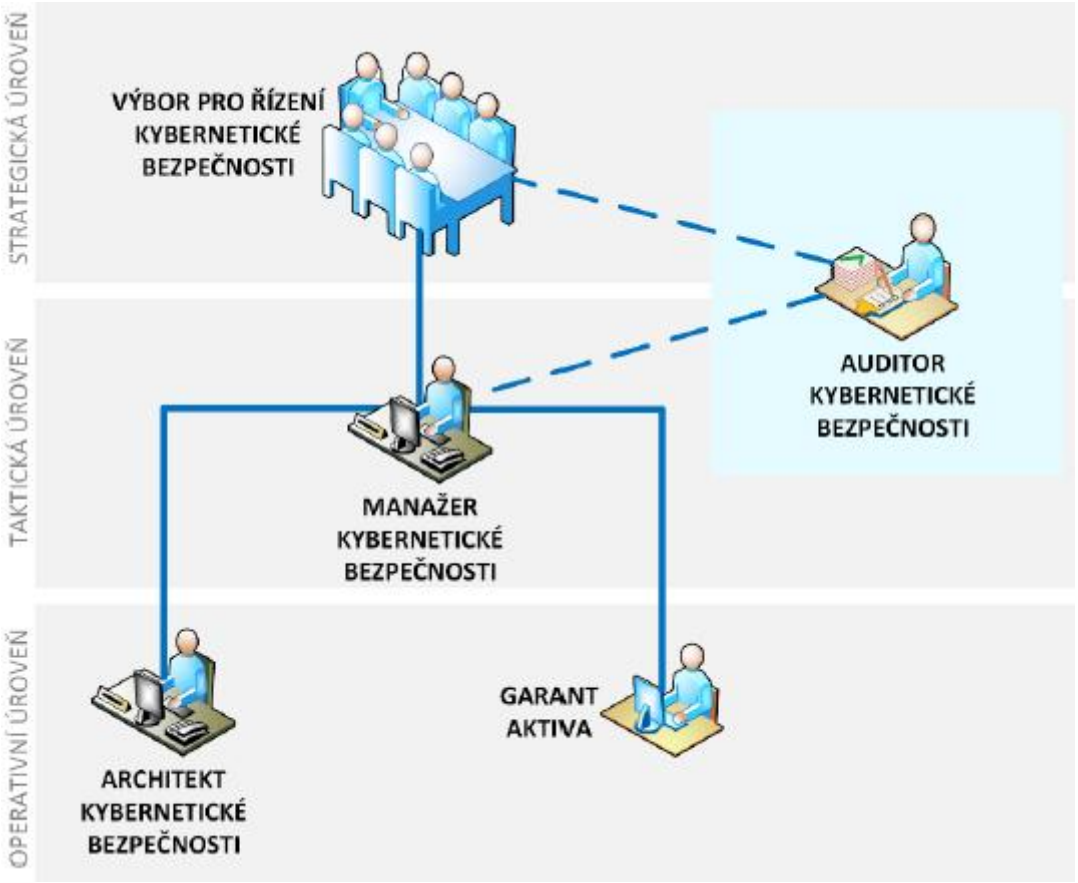
Jednotlivá bezpečnostní opatření vycházejí především z pravidel stanovených ISO/IEC 27001 [83], které jsou upraveny tak, aby jejich zavedení a následné dodržování bylo proveditelné jak osobami soukromého práva, tak orgány veřejné moci. Platí přitom zásada, že úroveň zabezpečení informačních a komunikačních systémů KII (kritické informační infrastruktury) je vyšší než úroveň zabezpečení VIS (významných informačních systémů). Vedle jmenného výčtu dokumentů, které musí dotčené subjekty vést, je v příloze vyhlášky nastíněna i jejich doporučená struktura. Zásadním paragrafem vyhlášky je § 29, podle kterého dotčené subjekty certifikované dle příslušné technické normy (ISO/IEC 27001:2013, resp. ČSN ISO/IEC 27001:2014) akreditovaným certifikačním orgánem splňují požadavky vyhlášky č. 316/2014 Sb. v případě, že doloží požadované dokumenty.

Požadavky vyhlášky o kybernetické bezpečnosti lze rozdělit do tří kategorií: [40]

- požadavky na technická opatření (např. kamerový systém, nástroj pro řízení přístupových oprávnění, nástroj pro ochranu před škodlivým kódem, kryptografické prostředky);
- požadavky na organizační opatření (řízení rizik, řízení aktiv, bezpečnostní politika apod.);
- požadavky na dokumentaci (metodika identifikace a hodnocení rizik, strategie řízení kontinuity, plán zvládání rizik, prohlášení o aplikovatelnosti).

Důležitou součástí vyhlášky o kybernetické bezpečnosti jsou požadavky na bezpečnostní role. Definováno je celkem pět bezpečnostních rolí, přičemž splnění kvalifikačních požadavků je důsledně požadováno především po subjektech uvedených v § 3 písm. c) a d) zákona o kybernetické bezpečnosti. Jejich názvy a vzájemný vztah ukazuje Obrázek 3. Příklad matice procesů (aktivit) a rolí, které mají k dané aktivitě předem definovaný vztah, znázorňuje RACI matice v Tabulce 2. Tento vztah může nabývat 4 různých podob: [41]

- Zodpovědný (Accountable) –odpovědnost za aktivitu jako celek
- Odpovědný (Responsible) –práce na aktivitě
- Konzultovaný (Consulted) – podpoření aktivity konzultací
- Informovaný (Informed) – informovanost o výsledku nebo postupu aktivity



Obrázek 3 – Hierarchie bezpečnostních rolí
[41]

Role / Procesy	Výbor KB	Manažer KB	Architekt KB	Auditor KB	Garant aktiva
Celkové řízení a rozvoj KB	A, R	C, I	C, I	C, I	C, I
Zajištění rozvoje, použití a bezpečnosti aktiva	I, C	A, C, I	C, I	C	R
Systém řízení bezpečnosti informací	A, I, C	R	C, I	C	C, I
Návrh bezpečnostních opatření	I, C	A, C, I	R	C	C, I
Implementace bezpečnostních opatření	I, C	A, C, I	R	C	C, I
Audit KB	A, I, C	C, I	C, I	R	C, I

Tabulka 2 – RACI matice

[41]

4.3.4 Související právní předpisy – vyhlášky

Další okrajově související vyhlášky a identifikace jejich aktuálního znění [41]: [42]

- Vyhláška č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti ve znění vyhlášky č. 415/2013 Sb. (aktuální znění od 1. 1. 2014)
- Vyhláška č. 432/2011 Sb. o zajištění kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 417/2013 Sb. (aktuální znění od 1. 1. 2014)
- Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění nařízení vlády č. 240/2008 Sb. (aktuální znění od 1. 8. 2008)
- Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění vyhlášky č. 453/2011 Sb. (aktuální znění od 1. 1. 2012)

[41] Pro zjištění aktuálního stavu byl použit webový portál www.zakonyprolidi.cz

- Vyhláška č. 525/2005 Sb. o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 434/2011 Sb. (aktuální znění od 1. 1. 2012)
- Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb. a vyhlášky č. 454/2011 Sb. (aktuální znění od 1. 1. 2012)
- Vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů. (aktuální znění od 1. 1. 2016)

4.3.5 Usnesení vlády

- Usnesení vlády České republiky č. 105/2015 [43]
    - Usnesení vlády ze dne 16. 2. 2015 se vztahuje k Národní strategii kybernetické bezpečnosti České republiky. Tímto usnesením se schvaluje Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020 a ukládají se jím úkoly řediteli NBÚ, členům vlády a vedoucím ostatních ústředních správních úřadů. [42]
- Usnesení vlády České republiky č. 382/2015 [44]
    - Usnesení vlády ze dne 25. 5. 2015 se vztahuje k Akčnímu plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020. Usnesením je schválen Akční plán a ukládají se jím úkoly členům vlády a vedoucím ostatních ústředních správních úřadů a řediteli NBÚ. [43]
- Usnesení vlády České republiky č. 781/2011 [45]
    - Tímto usnesením byl Národní bezpečnostní úřad ustaven gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. Byla jím mimo jiné zřízena Rada pro kybernetickou

[42] Informace o Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020 lze nalézt na: http://www.govcert.cz/download/nodeid-1004/
[43] Informace o Akčním plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020 lze nalézt na: http://www.govcert.cz/download/nodeid-973/

bezpečnost a schválen vznik Národního centra kybernetické bezpečnosti.

- Usnesení vlády České republiky č. 624/2001 [46]
    - Toto usnesení z roku 2001 definuje ve své příloze pravidla, zásady a způsob zabezpečování kontroly užívání počítačových programů. Jedná se o závazný dokument pouze pro orgány státní správy a jimi řízené organizace.

4.4 Certifikace osob v oblasti kybernetické bezpečnosti

Dosud byla řeč pouze o standardech a právních předpisech zaměřujících se na kybernetickou bezpečnost organizací. V rámci certifikace osob existuje jediný platný mezinárodní standard – ISO/IEC 17024 [88]. Ten obsahuje principy a požadavky na orgány certifikující osoby a na vývoj a údržbu certifikačního schéma. Konkrétní požadavky na certifikované osoby si však musí orgány stanovit samy. [47]

Vydávány jsou osobní certifikáty vztahující se jednotlivým normám, určité činnosti či pracovní pozici. V současné době jsou nejpopulárnější certifikáty pro role definované v zákoně o kybernetické bezpečnosti (manažera, architekta a auditora kybernetické bezpečnosti). V oblasti kybernetické bezpečnosti patří k nejznámějším osobní certifikáty společnosti ISACA (Information Systems Audit and Control Association). [44] Jsou akreditované a mají celosvětový význam. V České republice působí pouze kolem 150 takto certifikovaných profesionálů, což souvisí zejména s náročností závěrečného testu. ISACA nabízí následující osobní certifikáty: [48]

- CISA – Certified Information Systems Auditor,
- CISM - Certified Information Security Manager,
- CGEIT – Certified in the Governance of Enterprise IT,
- CRISC – Certified in Risk and Information Systems Control.

[44] Více o certifikátech společnosti ISACA lze nalézt na: http://www.isaca.org/CERTIFICATION/Pages/default.aspx

5 Návrh produktu

Pátá kapitola této diplomové práce se zaměřuje na návrh produktu, jeho jednotlivých částí a úrovní, specifikaci cílových oblastí a přínosů produktu. Produkt je navrhován pro státní podnik s názvem Elektrotechnický zkušební ústav (dále jen EZÚ), jehož záměrem je proniknout na trh v oblasti kybernetické bezpečnosti. Navržený produkt představuje kombinaci souvisejících a vzájemně se doplňujících služeb. Tvoří klasický balíček služeb, který eliminuje působení faktoru času, zvyšuje efektivnost jednotlivých služeb a jejich rentabilitu a umožňuje uspokojení potřeb specifických segmentů. Tím je dosaženo zajištění trvalé kvality, možnosti plánovat prostředky předem, většího pohodlí a uspokojení specializovaných zájmů na straně zákazníků. A zároveň snažšího předvídání vývoje podnikání, zlepšení efektivnosti, zvýšení tržeb na jednoho zákazníka a prodloužení délky trvání služby na straně EZÚ.

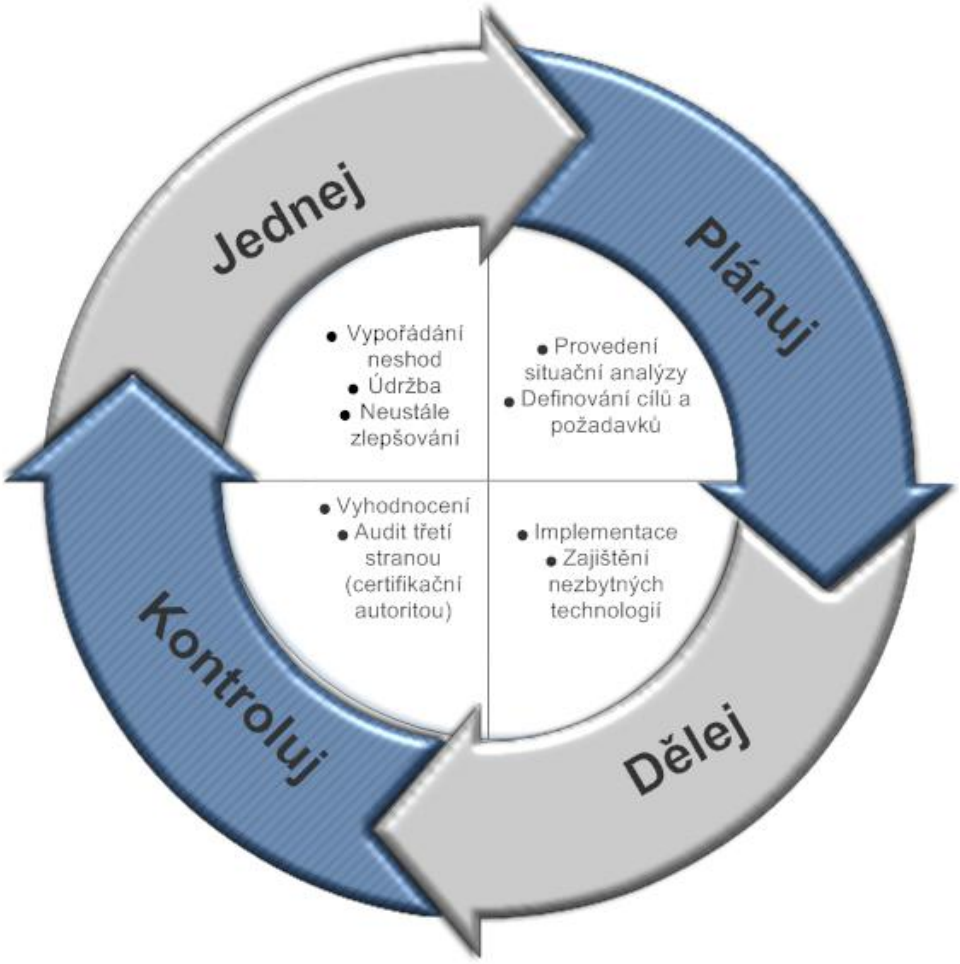
EZÚ [45] je společností s dlouholetou tradicí a zkušenostmi - na našem trhu působí již od roku 1926. Je autorizovanou osobou č. 201 a notifikovanou osobou č. 1014. Je členem významných evropských a světových certifikačních systémů, u mnoha z nich patří mezi zakládající členy. EZÚ je také členem mnoha národních a mezinárodních organizací (např. AAAO - Asociace akreditovaných a autorizovaných organizací). Nabízí činnosti akreditované zkušební laboratoře, certifikačního orgánu pro výrobky a systémy řízení a akreditované metrologické laboratoře. Za nejdůležitější skutečnost vzhledem k zaměření této diplomové práce lze označit, že EZÚ je akreditovaným certifikačním orgánem pro ISO/IEC 27001 a ISO/IEC 20000.

Životní cyklus produktu, tedy všech jeho částí, lze „namapovat“ na dobře známý Demingův cyklus (PDCA) – viz Obrázek 4. Z důvodu nutnosti zachování dvou prioritních hodnot EZÚ – nezávislosti a nestrannosti – není možné nabízet a realizovat tento produkt bez navázání partnerských vztahů s dalšími organizacemi. Musí být dodržena obecná zasáda platná při auditní činnosti – tatáž organizace nemůže předmět auditu (např. ISMS) navrhovat a implementovat, a zároveň

[45] Více informací o EZÚ a nabízených službách lze nalézt na: http://ezu.cz/#homepage

i auditovat. Proto je nutné navázat partnerské vztahy s organizacemi nabízejícími služby zaměřené na návrh a implementaci. Stejně tak není možné realizovat ochranu v oblasti kybernetické bezpečnosti bez příslušných technologií a nástrojů. Za tímto účelem je nutné navázat vztahy s technologickými partnery – dodavateli hardwaru a softwaru. Tito partneři vstupují do životního cyklu produktu ve fázích „Dělej“ (Do) a „Jednej“ (Act). V těchto fázích dochází k zajištění potřebných technologií a implementaci (zakoupených technologií, ISMS atd.), respektive k údržbě a vypořádání identifikovaných neshod z fáze „Kontroluj“ (Control). Na obrázku jsou tyto oblasti vyznačeny šedou barvou.

Klient může implementovat technologie a systémy i svépomocí po určení a vyškolení odpovědných zaměstnanců. Stejně tak může realizovat činnosti ve fázi „Jednej“ (Act). Může si vybrat, s kým bude v těchto fázích spolupracovat. Přínosem navázání těchto partnerských vztahů je rozšíření obchodní působnosti EZÚ, a zároveň nabídnutí klientům možnost zakoupení produktů a služeb od osvědčených společností. EZÚ vstupuje do životního cyklu produktu v úvodní fázi „Plánuj“ (Plan) a následně ve fázi „Kontroluj“ (Control). Cílem a smyslem takto definovaného životního cyklu produktu je správné zavedení a neustálé zlepšování kybernetické bezpečnosti v organizaci klienta (na obrázku zbarveno do modra).



Obrázek 4 – Životní cyklus produktu
Vlastní tvorba

5.1 Hlavní předpoklady pro vznik produktu

Narůstající užití informačních a komunikačních technologií v činnostech organizací, firem i jednotlivců vyžaduje, aby při zpracování, přenosu, ukládání a opětovném využití objemu dat nedocházelo ke ztrátě životně důležitých údajů, ke vzniku chyb a jejich kompromitaci nebo neoprávněné modifikaci. To a mnohem více řeší právě kybernetická bezpečnost.

Jak závažná je situace a jaké jsou výhledy do budoucna, nastínily již kapitoly č. 2.9 a 2.10. Svět kybernetické bezpečnosti se vyvíjí dynamicky, stále je to ale svět, který ve velké míře ovlivňují lidé. Rizika úniku a zneužití informací hrozí zejména zevnitř organizace. Rizikovost ještě umocňuje například rozmach BYOD či cloud computingu.

Problém představují i bezpečnostní chyby (zranitelnosti) v samotných zařízeních a jejich softwaru - viz kapitola č. 2.5. Většina nezabezpečených míst není zřejmá, o to užitečnější jsou rady profesionálů s bohatými zkušenostmi.

Pro úspěšné zvládání dnešních bezpečnostních výzev musí organizace posoudit model zabezpečení holisticky a získat viditelnost a kontrolu v rámci celého kontinua útoku.

- Před útokem. Organizace si musí být vědoma toho, co je do její sítě připojeno, čím je tvořena (zařízení, operační systémy, služby, aplikace, uživatelé). Kromě toho musí implementovat kontrolu přístupu, vynucovat bezpečnostní zásady a politiky, blokovat aplikace a celkový přístup ke kritickým aktivům. Tato opatření mají za cíl snížit plochu útoku, nicméně vždy je potřeba počítat s tím, že určité procento útočníků úspěšně dosáhne svých cílů. Velmi důležitou aktivitou, která by měla být v této fázi prováděna, je testování (např. penetrační testy).
- Během útoku. Organizace musí řešit širokou škálu možných vektorů útoku a aplikovat řešení, která fungují všude, kde se hrozba může projevit - na síti, na koncových bodech, na mobilních zařízeních i ve virtuálním prostředí. Díky vhodně nastaveným řešením budou odborníci na bezpečnost v lepší pozici při blokování hrozeb a ochraně infrastruktury.
- Po útoku: Některé útoky budou přes všechnu snahu ve fázi prevence úspěšné. To znamená, že organizace musí mít formální plán, který jí umožní stanovit rozsah škod, zvládnout bezpečnostní incidenty a přivést všechny incidentem dotčené procesy zpět do normálu co nejrychleji.

Když si, v tom lepším případě, vedení organizací uvědomí všechna hrozící rizika, často je jejich reakcí nákup různých zařízení a nástrojů renomovaných firem, které jsou jim prezentovány jako „všelék“ pro kybernetickou bezpečnost. Jedná se zpravidla o technologie zaměřené na:

- bezpečnost na perimetru (firewall, IDS/IPS, UTM, aplikační firewall, web filtr);
- bezpečnost koncových stanic (antivir, personální firewall, antimalware, antirootkit, endpoint DLP);

- bezpečnost vnitřní sítě (flow monitoring, NBA – behaviorální analýza, automatická detekce anomálií).

Existují také komplexní řešení kombinující dvě a více výše uvedených technologií. Nelze říci, že tato řešení nepomáhají zlepšovat kybernetickou bezpečnost, naopak – jedná se o nezbytnou součást celkového řešení. V první řadě je ale nutné provést audit vlastních digitálních aktiv, jehož výsledkem by měla být důkladná analýza rizik, která mohou nastat a soubor opatření, jak na ně reagovat. K pořízení kvalitních technologií a nástojů řešících kybernetickou bezpečnost a jejich správnému nasazení a provozování je v celkovém řešení nezbytné vytvoření a především dodržování systematické bezpečnostní strategie, a také kvalifikace a připravenost bezpečnostního týmu. Jakékoliv jednorázové investice nevedou k systematické bezpečnostní strategii, pouze vyčerpávají rozpočet a způsobují provozní komplikace.

Stěžejní část celkového řešení představuje implementace požadavků a doporučení stanovených v mezinárodních standardech zaměřených na oblast kybernetické bezpečnosti a následné ověření a certifikace. Implementace a certifikace těchto standardů má dopad do všech oblastí – software, hardware i lidský faktor. Standardy do svých požadavků zapracovaly osvědčené postupy (best practice) v oblasti kybernetické bezpečnosti a jsou průběžně aktualizovány.

Je nutné dívat se na kybernetickou bezpečnost z mnoha různých úhlů pohledu a řešit ji komplexně. K tomu samotné pořízení a instalování technologií nestačí. Pro účinnou ochranu je důležité pochopit, jaké informace organizace má a jakou hodnotu pro ni znamenají. Je také zásadní uvědomit si cíle a reálné fungování organizace. Jen tak lze navrhnout opravdu účinné a efektivní řešení kybernetické bezpečnosti. Cílem není pouze jeho zavedení, ale také zaručená dlouhodobá funkčnost a rozvoj – kontinuální zlepšování. Právě proto musí být v pravidelných intervalech ověřováno a certifikováno. Mělo by být schopné reagovat na změny v organizaci i jejím okolí. Jediným způsobem, kterým lze cílového stavu dosáhnout, je zapojení vrcholového managementu organizace a pravidelné školení zaměstnanců o kybernetické bezpečnosti.

Právě výše zmíněné předpoklady představují hlavní důvody pro vznik tohoto produktu. Důležitým faktorem je také účinnost nového zákona o kybernetické bezpečnosti od 1. 1. 2015.

5.2 Přínosy produktu

V této kapitole jsou definovány přínosy produktu, které reagují na výše popsané problémy, se kterými se v oblasti kybernetické bezpečnosti a dnešní informační společnosti setkáváme. Následuje výčet těch nejvýznamnějších přínosů.

- Zmapování současného stavu kybernetické bezpečnosti a identifikování návrhů na zlepšení.
- Zajištění kybernetické bezpečnosti a jejího neustálého zlepšování (tvorba provozního prostředí zaručujícího kybernetickou bezpečnost a ochranu soukromí všech subjektů, jejichž data jsou zpracována).
- Ochranu před velkými finančními ztrátami a poškozením nebo zničením aktiv.
- Zkvalitnění a zrychlení procesů (zvláště u IT služeb).
- Efektivní vynaložení nákladů na zajištění kybernetické bezpečnosti vzhledem k hodnotě chráněných aktiv organizace.
- Zabezpečení jednotlivých částí IT infrastuktury (až na úrovni firmwaru a mikroprocesorů).
- Zabezpečení dodavatelského řetězce.
- Zvýšení povědomí o bezpečnosti a odpovědnosti zaměstnanců, zvýšení povědomí o bezpečnosti u pracovníků a případně u pracovníků třetích stran.
- Zaměstnanci jsou odpovědni za zabezpečení informací svých pracovišť i svých zákazníků.
- Proškolení zaměstnanců v oblasti kybernetické bezpečnosti (především pracovníků vykonávajících bezpečnostní role).
- Splnění legislativních požadavků (např. zákona č. 181/2014 Sb.), včetně požadavků na pravidelné audity.

- Ověření správného nastavení bezpečnostní politiky a její uplatňování napříč organizací.
- Zvýšení konkurenční výhody.
- Snížení rizik (např. nedostupnosti, úniku či ztráty dat).
- Snížení nákladů souvisejících s odstraňováním následků bezpečnostních incidentů, výpadkem informačního systému organizace a se zajištěním nouzového zpracování dat, včetně optimalizace nákladů při obnově chodu informačního systému organizace po jeho výpadku.
- Prokázání úsilí o ochraně dat klientů, partnerů, nadřízených orgánů, orgánů státní správy a veřejnosti, znamenající zvýšení podnikatelské důvěryhodnosti pro investory, banky a pojišťovny.

5.3 Rozlišení úrovní produktu

V rámci produktu lze rozlišit celkem tři úrovně. Ty značí řešení kybernetické bezpečnosti stupňovaně. Při snaze o zajištění kybernetické bezpečnosti je nutné začít od úplných základů a postupně se dopracovat k požadovanému stupni zabezpečení. Návaznost na níže obecně popsané úrovně produktu neplatí pro všechny jeho části. Platí pro následující části produktu:

- certifikaci kybernetické bezpečnosti;
- osobní certifikaci;
- bezpečnostní testy a
- situační analýzu.

U ostatních částí nelze definovat stupňovitost, díky čemuž neexistuje návaznost na obecné úrovně produktu.

Úroveň 1

První úroveň je zaměřena na zajištění základní úrovně kybernetické bezpečnosti. To je uskutečněno především úspěšným a vhodně ustanoveným ISMS dle příslušných

mezinárodních standardů z rodiny ISO/IEC 27XXX a zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Pro to, aby se jednalo o dlouhodobý stav, musí být ISMS vhodně udržován, kontrolován a vylepšován. Ve výsledku to pro organizaci přináší především ochranu před bezpečnostními incidenty, popř. jejich vhodné zvládnutí a minimalizaci dopadu (škod). Díky provádění analýzy rizik dochází také k identifikaci rizikových oblastí a definici nejzávažnějších hrozeb pro organizaci, což umožňuje efektivnější vynaložení nákladů na zajištění kybernetické bezpečnosti.

První úroveň se vyznačuje čistě systémovým pohledem a představuje základní stavební kámen k důkladnému kybernetickému zabezpečení dosahovaného v druhé a třetí úrovni.

Úroveň 2

Druhá úroveň produktu navazuje na úroveň první a představuje rozšíření systémového pohledu na kybernetickou bezpečnost. Toto rozšíření spočívá v zahrnutí platných mezinárodních standardů soustředících se na bezpečnost softwaru, úložišť, sítí a dodavatelských řetězců. Do druhé úrovně jsou také zahrnuty bezpečnostní testy jako důležitá součást při snaze o zajištění kybernetické bezpečnosti. V rámci této úrovně je řešena kybernetická bezpečnost vztažená k jednotlivých částem IT infrastruktury dotyčné organizace a jejího dodavatelského řetězce. Zejména díky zahrnutí dalšího standardu z rodiny ISO/IEC 27XXX dochází k ještě větší efektivitě při uvolňování nákladů na kybernetickou bezpečnost.

Úroveň 3

Třetí úroveň opět navazuje na předešlé úrovně, především na úroveň 2. Představuje nejhlubší pohled na kybernetickou bezpečnost, který zahrnuje konkrétní bezpečnostní komponenty. Zaměřuje se především na hardware a jeho firmware. Podrobněji se zabývá také bezpečností softwaru a důkladnějšími a náročnějšími bezpečnostními testy. Nejdůležitějším mezinárodním standardem této úrovně je ISO/IEC 15408. Tento standard představuje normalizovanou podobu CC (více viz

kapitola 4.2.2) a váží se k němu další mezinárodní standardy, které ho dále rozšiřují a doplňují.

5.4 Charakteristika jednotlivých částí produktu

Předně je produkt potřeba rozdělit do dvou hlavních kategorií. Důvodem pro toto rozdělení je výše zmíněná nutnost zachování nestrannosti a nezávislosti.

- Kategorie realizovaná EZÚ.
- Kategorie realizovaná klientem, který může, ale nemusí využít služeb nabízených osvědčenými partnery EZÚ.

Tato práce se blíže zabývá pouze první kategorií. Druhé kategorii se nevěnuje, protože je pouze na klientovi (popř. partnerské organizaci), jak přistoupí k implementaci, provedení analýzy rizik či řešení neshod. EZÚ nabízí seznam osvědčených partnerských organizací, které poskytují profesionální služby. Za účelem podpory klientů (popř. i partnerů) je součástí produktu také školení a osobní

certifikace v oblasti kybernetické bezpečnosti. Tyto části produktu mají hromadný charakter a neodporují tak prioritním hodnotám EZÚ.

V následujících podkapitolách budou popsány jednotlivé části produktu realizovaného EZÚ.

- ❖ Úvodní informační školení
- ❖ Situační analýza kybernetické bezpečnosti
- ❖ Školení v oblasti kybernetické bezpečnosti
- ❖ Osobní certifikace v oblasti kybernetické bezpečnosti
- ❖ Certifikace kybernetické bezpečnosti
- ❖ Bezpečnostní testy
- ❖ Zajištění bezpečnostní role auditora kybernetické bezpečnosti

5.4.1 Úvodní informační školení

Úvodní informační školení (ÚIŠ) je poskytováno za účelem informování o produktu, který EZÚ v oblasti kybernetické bezpečnosti nabízí a realizuje. Je zaměřeno na dvě různé skupiny. První skupinu představují potenciální zákazníci, kterým je prezentován produkt s cílem představení, vysvětlení, zaujmutí a následného prodeje. Druhou skupinu tvoří potenciální partneři, kterým je produkt představen, vysvětlen, nikoliv však za účelem prodeje, nýbrž za účelem navázání oboustranně výhodné spolupráce.

V závislosti na cílové skupině se liší také náplň ÚIŠ. Pro potenciální partnery se neuvažuje vliv rozdílných oblastí působnosti. Při tvorbě náplně ÚIŠ je vycházeno z předpokladu, že tyto organizace působí ve více než jedné cílové oblasti (viz kapitola č. 5.5). Pro skupinu představovanou potenciálními zákazníky se využije upravené ÚIŠ, přizpůsobené oblasti působnosti posluchačů. Při malém počtu zájemců lze uvažovat o provedení ÚIŠ i pro potenciální zákazníky z různých oblastí. V takovém případě se použije verze ÚIŠ určená pro potenciální partnery jakožto společný základ a následné odlišnosti lze po projevení zájmu zákazníka řešit individuálně.

Z uvedených charakteristik plyne skutečnost, že ÚIŠ nemá návaznost na obecné úrovně produktu. Konkrétní verze je vybrána na základě charakteritiky skupiny posluchačů, popř. oblasti působnosti. Do ÚIŠ jsou zapracovány především přínosy produktu a jeho jednotlivých úrovní a je zdůrazněna komplexnost představovaného řešení. Zmíněna je povinnost plnění zákonných požadavků (např. zákona o kybernetické bezpečnosti a zákona o informačních systémech veřejné správy). Hlavní důraz je kladen na vnímání kybernetické bezpečnosti jako důležitého faktoru ovlivňujícího samotný chod společnosti.

5.4.2 Situační analýza kybernetické bezpečnosti

Situační analýza kybernetické bezpečnosti je prováděna na základě zadaných kritérií auditu se zaměřením na vhodnost a přiměřenost uplatňovaných pravidel. Příkladem takového kritéria je rozsah ISMS. Cílem situační analýzy je vyhodnocení aktuálního stavu kybernetické bezpečnosti s důrazem na systémový přístup a procesní řízení ve vazbě na související platné mezinárodní standardy a legislativní úpravu České republiky.

Situační analýza má návaznost na obecné úrovně produktu. Situační analýza v rámci první úrovně je velmi podobná klasickému auditu. Namísto konstatování neshod či nedostatků jsou definovány spíše oblasti, kterým je nutné věnovat pozornost. K těmto problematickým oblastem jsou definována konkrétní doporučení. Výstupem ze situační analýzy je zpráva, která obsahuje zmapování aktuálního stavu a identifikaci návrhů na zlepšení, které poslouží i při optimalizaci analýzy rizik, definování potřebných technologií a implementaci těchto technologií a systémů. Slouží také k určení potřebných dokumentů, záznamů a informací. V druhé a třetí úrovni nabývá situační analýza podoby prostého pre-auditu.

5.4.3 Školení kybernetické bezpečnosti

Školicí kurzy jsou zaměřeny na platné mezinárodní standardy a legislativní předpisy České republiky související s kybernetickou bezpečností. Hlavním výstupem a zároveň přínosem této části produktu je dokonalá znalost standardu či předpisu. Dokonalá znalost je zajištěna především vhodným a srozumitelným výkladem standardu a jeho požadavků či doporučení a poskytnutím osvědčených postupů (best practice) od zkušených auditorů.

Školení jsou součástí všech tří úrovní produktu. V rámci první úrovně je školení nabízeno pro následující právní a normativní předpisy:

- ČSN ISO/IEC 27001:2014 Informační technologie -- Bezpečnostní techniky -- Systémy řízení bezpečnosti informací -- Požadavky;
- ČSN ISO/IEC 20000-1:2012 Informační technologie -- Management služeb -- Část 1: Požadavky na systém managementu služeb;
- zákon č. 181/2014 Sb., o kybernetické bezpečnosti;
- zákon č. 365/2000 Sb. o informačních systémech veřejné správy;
- usnesení vlády České republiky č. 624/2001;

Výše zmíněné standardy a předpisy jsou pouze základními stavebními kameny. Váží se k nim další standardy z příslušných rodin a vyhlášky, které jsou do školení zapracovány pro lepší porozumění a využitelnost v praxi.

Vyšší úrovně produktu zahrnují další normativní a legislativní předpisy, podle kterých je prováděno ověřování a certifikace. Stejně tak je pro tyto předpisy vytvořeno školení, které pomůže posluchačům poznat a porozumět těmto často složitým předpisům se specifickými termíny a formulacemi.

5.4.4 Osobní certifikace

Vzhledem k nově definovaným bezpečnostním rolím ve vyhlášce o kybernetické bezpečnosti a především reálné potřebě těchto rolí v organizacích je jednou z částí produktu osobní certifikace. Osobní certifikace je rozdělelna do dvou částí - proškolení a následné ověření znalostí v podobě certifikační zkoušky.

Školení je zaměřeno na platné mezinárodní standardy a legislativu související s kybernetickou bezpečností. Konkrétní náplň se mění v závislosti na zvolené bezpečnostní roli a na úrovni odbornosti. Pro každou bezpečnostní roli jsou definovány tři úrovně odbornosti, které mají návaznost na obecné úrovně produktu. Základní úroveň v rámci osobní certifikace je pojmenována „specialist“, vyšší úroveň „expert“ a nejvyšší úroveň „master“. Kurz je zakončen certifikační zkouškou. Po jejím úspěšném dokončení je absolventovi udělen osobní certifikát pro zvolenou bezpečnostní roli. Absolvování certifikační zkoušky je možné i bez předešlé účasti na

školení, nicméně vzhledem k náročnosti dané problematiky je absolvování školení doporučeno. Získaný certifikát nemá časově omezenou platnost.

V souvislosti s bezpečnostními rolemi definovanými ve vyhlášce č. 316/2014 Sb. jsou nabízeny tři osobní certifikace. Jejich popis je obsažen v následujících podkapitolách.

5.4.4.1 Manažer kybernetické bezpečnosti

Manažer kybernetické bezpečnosti zodpovídá za kybernetickou bezpečnost jako celek. Roli manažera kybernetické bezpečnosti, tedy osoby odpovědné za systém řízení bezpečnosti informací, by měla dle požadavků vyhlášky zastávat osoba, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s řízením bezpečnosti informací po dobu nejméně tří let. V praxi je mezistupněm mezi nejvyšším vedením organizace a operativní úrovní. Manažer kybernetické bezpečnosti komunikuje se všemi ostatními bezpečnostními rolemi – architektem i auditorem kybernetické bezpečnosti, výborem pro řízení kybernetické bezpečnosti a garanty aktiv. Tuto bezpečnostní roli by měl zastávat interní zaměstnanec organizace, protože jinak si lze velmi těžko představit správné nastavení a řízení ISMS, navázání na vrcholové vedení organizace, na její cíle a strategii. Bez toho je systém nefunkční a spíše než přínos znamená přítěž.

Manažer kybernetické bezpečnosti – specialist

Manažer kybernetické bezpečnosti zodpovídá za kybernetickou bezpečnost v rámci celé organizace. Řídí například aktivity spojené s managementem rizik, hrozeb, realizací bezpečnostních opatření a zajišťuje proaktivní činnost. Další významnou činností je provádění interních auditů. Cílem činnosti manažera kybernetické bezpečnosti je zajištění kybernetického zabezpečení organizace a jeho neustálé zlepšování.

Konkrétní náplň tohoto základního kurzu se nepatrně mění spolu s různými oblastmi působnosti organizací, ve kterých jsou účastníci kurzu zaměstnáni. Školení se v této úrovni zaměřuje především na relevantní požadavky zákona o kybernetické bezpečnosti a ISO/IEC 27001 na ISMS. V oblasti státní správy je třeba věnovat se také problematice atestace ISVS – tedy požadavkům zákona č. 365/2000 Sb.

Manažer kybernetické bezpečnosti – expert

Při rozhodnutí organizace jít při své snaze o kybernetické zabezpečení více do hloubky, jsou na manažera kybernetické bezpečnosti kladeny další nároky. Ty jsou spojeny s přechodem od čistě systémového pohledu na pohled zahrnující bezpečnost softwaru, sítí, úložišť, dodavatelských řetězců a bezpečnostní testy. I samotný systémový pohled je rozšířen.

Rozšíření pohledu na kybernetickou bezpečnost je dosaženo školením dalších platných a souvisejících mezinárodních standardů soustředících se právě na bezpečnost softwaru, sítí a úložišť. Druhá úroveň osobní certifikace je zaměřena na kybernetickou bezpečnost dodavatelského řetězce organizace a jednotlivých částí IT infrastuktury organizace. Součástí druhé úrovně produktu jsou také bezpečnostní testy. Neznamená to, že manažer kybernetické bezpečnosti musí tyto testy provádět, nicméně by měl této problematice rozumnět, znát jednotlivé druhy bezpečnostních testů a jejich přínosy. Právě manažer kybernetické bezpečnosti určuje ve spolupráci s vedením dané organizace, zda a popřípadě jaké bezpečnostní testy se mají v organizaci provádět. Konkrétní náplň školení a certifikační zkoušky se opět nepatrně mění spolu s oblastmi působnosti organizací účastníků kurzu.

Manažer kybernetické bezpečnosti – master

Nejdetailnějšího pohledu manažera kybernetické bezpečnosti je dosaženo školením zaměřeným na bezpečnost samotných bezpečnostních komponent a podrobněji pohlížejícím také na software, úložiště a bezpečnostní testy. Nově se školení zaměřuje na bezpečnost hardwaru a jeho firmwaru. Školen je především mezinárodní standard

ISO/IEC 15408 a k němu se vážící standardy. Dále je školení zaměřeno na standardy přímo navazující a rozšiřující ty, které jsou obsaženy v druhé úrovni, a také na pokročilejší techniky při provádění bezpečnostních testů.

5.4.4.2 Auditor kybernetické bezpečnosti

Auditor kybernetické bezpečnosti zodpovídá za ověření (audit) kybernetické bezpečnosti. Roli auditora by měla vykonávat osoba odborně způsobilá (s praxí s prováděním auditů kybernetické bezpečnosti po dobu nejméně tří let). Výkon této role by měl být nestranný a striktně oddělený od výkonu všech ostatních bezpečnostních rolí. I přes to může být tato role vykonávána interním zaměstnancem organizace. Auditor nesmí současně zastávat funkci manažera ani architekta kybernetické bezpečnosti a nesmí auditovat vlastní práci. Výsledky své práce prezentuje auditor výboru pro řízení kybernetické bezpečnosti.

Získaná kvalifikace, znalosti a schopnosti pomohou účastníkům kurzu při ověřování správného nastavení systému, řízení rizik a dalších činností podle platných mezinárodních standardů a legislativy České republiky vztahující se ke kybernetické bezpečnosti. Důraz je kladen především na pochopení struktury a obsahu aktuálních verzí těchto předpisů a rozvoj auditorských dovedností (vytváření auditních zpráv, správná formulace a kategorizace neshod, nedostatků a doporučení). Na kurzu se účastník naučí orientaci v souvisejících právních a normativních předpisech, jak plánovat a provádět interní audity kybernetické bezpečnosti, jak shromažďovat objektivní důkazy v průběhu auditu, jak vyhodnocovat a přesně reportovat výsledky auditu, jak vypracovat závěrečnou zprávu z auditu a jak posoudit efektivnost nápravných opatření (včetně definovaných termínů a zodpovědností).

Stejně jako u manažera kybernetické bezpečnosti, jsou i u auditora kybernetické bezpečnosti rozlišovány tři úrovně odbornosti (specialist, expert a master). Charakteristika a odlišnost jednotlivých úrovní odbornosti opět souvisí s úrovněmi produktu. Je tak velmi podobná jako v případě osobní certifikace manažera

kybernetické bezpečnosti (systémový pohled → rozšířený pohled – software, sítě, úložiště → nejdetailnější pohled – hardware a firmware). Přechod na vyšší úroveň je vždy spojen s aplikováním dalších mezinárodních standardů, které musí auditor, stejně jako architekt i manažer, také znát a ovládat.

5.4.4.3 Architekt kybernetické bezpečnosti

Architekt kybernetické bezpečnosti musí být pro tuto činnost vyškolen a schopen prokázat tříletou praxi s navrhováním bezpečnostní architektury. Architekt je zodpovědný za návrh bezpečné architektury (od infrastruktury až po bezpečnost na aplikační úrovni) a její následnou implementaci. Role architekta může být zajištěna i externě, nicméně pouze při úzce navázané spolupráci s manažerem kybernetické bezpečnosti a garanty aktiv.

V rámci první úrovně odbornosti – specialist - účastník kurzu získá či dále prohloubí své znalosti potřebné pro budování bezpečné a stabilní architektury ISMS v organizaci dle ISO/IEC 27001, s využitím zejména ISO/IEC 27002 a ISO/IEC 27011, a splňující požadavky zákona o kybernetické bezpečnosti. Tato osobní certifikace umožní účastníkům splnění kvalifikačního požadavku zákona o kybernetické bezpečnosti a nastíní možnosti využití ISO/IEC 27001 a dalších standardů z rodiny ISO/IEC 27XXX pro tvorbu vhodné a správné architektury ISMS. V organizacích, které budou mít takto vyškoleného architekta, by již nemělo docházet k tradičním chybám a problémům – nákup a správa navzájem nepropojených bezpečnostních produktů a/nebo jejich nefunkčnost. Kurz je zaměřen především na požadavky vyhlášky č. 316/2014 Sb., směřující na nástroje potřebné k zajištění kybernetické bezpečnosti (např. nástroje pro detekci kybernetických bezpečnostních událostí či nástroje pro řízení přístupových oprávnění).

V rámci dalších úrovní odbornosti – expert a master – je účastníkům představen způsob, jakým mohou do svých stávajících řešení (architektury) zahrnout požadavky dalších mezinárodních standardů objevujících se v druhé a třetí úrovni produktu.

5.4.5 Certifikace kybernetické bezpečnosti

V této části produktu je návaznost na jeho obecné úrovně nejzřetelnější, i proto se jedná o stěžejní část. Certifikace kybernetické bezpečnosti je definována ve třech na sebe navazujících úrovních.

5.4.5.1 První úroveň

První úroveň tvoří základní stavební kámen pro jakoukoliv společnost, která klade důraz na kybernetickou bezpečnost a uvědomuje si možná rizika a hrozby přicházející z kyberprostoru. Před sestavením první úrovně z jednotlivých komponent byla provedena srovnávací (GAP) analýza vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti, která definuje konkrétní požadavky na orgány a osoby spadající pod působnost zákona o kybernetické bezpečnosti, a mezinárodního standardu ISO/IEC 27001. Na první pohled se zdá, že se oba předpisy shodují a lze je považovat za rovnocenné. Při jejich detailnějším zkoumání je ale zřejmé, že tomu tak není. Procentuální výsledky provedené GAP analýzy jsou obsaženy v Tabulce 3. Z výsledků plyne, že je vhodné do produktu zařadit oba předpisy, protože se navzájem doplňují a rozšiřují. A proto není produkt nabízen jen subjektům spadajícím pod gesci zákona - mít nastavené postupy a politiky kybernetické bezpečnosti by měla mít každá organizace.

	Pro VIS	Pro KII
Procento požadavků ISO/IEC 27001 obsažených ve vyhlášce o kybernetické bezpečnosti (%)	24,83	40,35
Procento požadavků vyhlášky o kybernetické bezpečnosti tvořené požadavky ISO/IEC 27001 (%)	54,56	55,22

Tabulka 3 - Procentuální výsledky GAP analýzy
Vlastní tvorba

Tato úroveň se soustředí na ověření procesů nutných k vytvoření základního kybernetického zabezpečení (řízení rizik, řízení hrozeb a zranitelností, příprava a realizace bezpečnostních opatření, neustálé zlepšování a provádění interních auditů).

Tyto procesy musí být nastaveny a být v souladu zejména s následujícími standardy a legislativními předpisy. V souvislosti s různými oblastmi působnosti auditovaných organizací jsou do této úrovně zakomponovány další specifické předpisy (pro oblast státní správy např. zákon č. 365/2000 Sb., o informačních systémech veřejné správy).

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a vyhláška č. 316/2014, o kybernetické bezpečnosti.
- ČSN ISO/IEC 27001 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky.
- ČSN ISO/IEC 20000-1 Informační technologie – Management služeb – Část 1: Požadavky na systém managementu služeb.

Po úspěšném ověření naplnění požadavků určených předpisů jsou organizaci uděleny dva certifikáty. První certifikát představuje českou verzi a nese název „Základní certifikát kybernetické bezpečnosti“. Anglická mutace má název „Essential Certificate of Cybersecurity“.

5.4.5.2 Druhá úroveň

Druhá úroveň certifikace kybernetické bezpečnosti zahrnuje ověřování dle dalších mezinárodních standardů. Ty jdou více do detailu a zaměřují se i na bezpečnost softwaru, sítí, úložišť dat a dodavatelských řetězců. Při kladném výsledku ověření, tedy konstatování shody s příslušnými předpisy, jsou organizaci opět uděleny dva certifikáty. Česká verze certifikátu nese název „Rozšířený certifikát kybernetické bezpečnosti“. Anglická verze má název „Enhanced Certificate of Cybersecurity“.

Ověřování (audit) v druhé úrovni této části je vztaženo zejména k níže uvedeným standardům, které tvoří bázi společnou pro všechny cílové oblasti. K ní jsou následně přidány oborově specifické standardy (např. ISO 80001). Názvy mezinárodních standardů jsou volně přeloženy do češtiny – nejedná se o oficiální názvy norem.

- ČSN EN ISO 22301 - Ochrana společnosti - Systémy managementu kontinuity podnikání - Požadavky

- ISO/IEC 27036 – Informační technologie – Bezpečnostní techniky - Bezpečnost informací pro dodavatelské řetězce
- ISO/IEC TR 15443 - Informační technologie – Bezpečnostní techniky - Rámec pro zajištění bezpečnosti
- ISO/IEC 12207 - Systémy a softwarové inženýrství - Procesy v životním cyklu softwaru
- ISO/IEC 27033 - Informační technologie - Bezpečnostní techniky - Bezpečnost sítě
- ISO/IEC 27040 - Informační technologie - Bezpečnostní techniky – Bezpečnost úložišť

5.4.5.3 Třetí úroveň

Třetí úroveň představuje ověřování kybernetické bezpečnosti vztažené přímo na jednotlivé komponenty zařízení a nástrojů. Pohlíženo je především na bezpečnost hardwaru a jeho firmwaru. Zahrnuty jsou také audity podle mezinárodních standardů, které se hlouběji zabývají bezpečností softwaru a úložišť dat. Udělovány jsou stejně jako v obou předchozích případech dva certifikáty – „Certifikát nejvyšší úrovně kybernetické bezpečnosti“ a „Top-level Certificate of Cybersecurity“.

Ověřování ve třetí úrovni certifikace kybernetické bezpečnosti je vztaženo zejména k následujícím standardům. Vzhledem k širokému zaměření hlavní komponenty – ČSN ISO/IEC 15408, ke které se váží i další komponenty (např. ISO/IEC TR 19791), nejsou v této úrovni žádné oblastně specifické standardy. Názvy mezinárodních standardů jsou volně přeloženy do češtiny – nejedná se o oficiální názvy norem.

- ČSN ISO/IEC 15408 - Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT
- ISO/IEC TR 19791 - Informační technologie - Bezpečnostní techniky - Zhodnocení bezpečnosti operačních systémů
- ISO 14764 - Softwarové inženýrství - Procesy v životním cyklu softwaru - Údržba

5.4.6 Bezpečnostní testy

Aby byla síť a aktiva účinně chráněna, je potřeba testovat celý integrovaný systém a jeho jednotlivé prvky. Většinu bezpečnostních testů není nutné provádět v ročních intervalech. Provádět by se měly v případě významných změn v rámci ICT infrastruktury. Testem, který by měl být prováděn i v menších než ročních intervalech, je sociální inženýrství. To zahrnuje spoustu různých technik. Z těch nejznámějších lze jmenovat např. baiting, phishing, pretexting a quid pro quo (něco za něco). Zdaleka nejčastěji realizovanými bezpečnostními testy jsou testy penetrační (testování odolnosti systému).

Výstupem z bezpečnostních testů je vyhodnocení testované oblasti a problematiky, včetně návrhů na zlepšení (např. správnou konfuguraci testovaných bezpečnostních prvků). Pro testování systému a jeho jednotlivých prvků lze použít různé bezpečnostní testy. Kromě již zmíněného sociálního inženýrství a penetračního testování to jsou např.:

- operační testy - funkčnost všech zařízení,
- zátěžové testy – provoz systému při zvýšené zátěži,
- vzdálené testy - možnosti při vzdáleném ovládání všech komponent,
- testování dodatečných služeb - dodržení všech SLA (Service Level Agreement).

V rámci této části produktu jsou nabízeny níže uvedené bezpečnostní testy. Tuto nabídku je možné rozšířit a doplnit o další bezpečnostní testy poskytované organizacemi, se kterými naváže EZÚ partnerský vztah. Bezpečnostní testy na trhu úspěšně nabízí např. ESET software spol., Trustica, e-Business Services či CompuNet.

- Penetrační test webové aplikace a webového serveru.
  - Cílem testu je odhalit co největší množství kritických zranitelností ve webové aplikaci nebo webovém serveru, odhalit způsob jejich využití a případnou možnost získání privilegovaného přístupu. Test je možné provádět jak pomocí komerčních, tak i open-source nástrojů.

- Penetrační test interní sítě.
  - Test je realizován jak z pohledu potenciálního anonymního útočníka, který má fyzický přístup do interní sítě, tak z pohledu běžného zaměstnance společnosti. Cílem je demonstrovat kompromitování interní sítě zákazníka (např. získání doménového administrátora). Součástí je také analýza bezpečnosti bezdrátových sítí zákazníka. Testování probíhá v několika fázích realizovaných v souladu s OSSTMM (Open Source Security Testing Methodology Manual).
- Sociální inženýrství.
  - Sociální inženýrství představuje netechnickou formu prolomení bezpečnostních postupů a opatření. Jedná se o útok založený na schopnosti ovlivňování a manipulace lidí. Sociální inženýrství těží z potenciálního selhání lidského faktoru, který je nedílnou součástí informační bezpečnosti. Hlavním cílem útočníka je narušit vnitřní prostředí organizace nebo získat citlivé a důvěrné informace s využitím různých psychologických her, manipulace či dokonce výhružek. Bezpečnostní test je prováděn simulací takového chování a sledování reakce zaměstnanců.

5.4.7 Zajištění bezpečnostní role auditora kybernetické bezpečnosti

V rámci následného fungování již implementovaného systému je nutné minimálně jednou ročně provést interní audit celého systému. Realizaci tohoto auditu je vhodné svěřit externí, zkušené firmě, která disponuje profesionálními auditory. EZÚ disponuje kvalifikovanými auditory (IRCA, EOQ, CISA atd.), kteří jsou schopni realizovat interní audity dle příslušných standardů.

Role auditora kybernetické bezpečnosti je jednou z rolí definovaných v § 6 vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti. Auditor kybernetické bezpečnosti odpovídá za provádění auditů a velmi důležitá je jeho nestrannost a odborná způsobilost (délka praxe s prováděním auditů kybernetické bezpečnosti). Tím se

auditoři EZÚ vyznačují, a právě proto je součástí produktu také služba zajištění role auditora kybernetické bezpečnosti. Tento auditor provádí interní audity kybernetické bezpečnosti (audity první stranou). V případě, že má zákazník zájem také o externí certifikaci (viz kapitola 5.3.5), je opět nutné dodržení nestrannosti a nezávislosti – v tomto případě to znamená, že oba audity nesmí provádět tentýž auditor.

Interní auditor v rámci auditu kybernetické bezpečnosti posuzuje soulad bezpečnostních opatření s právními předpisy, vnitřními předpisy, jinými předpisy a souvisejícími smluvními závazky. Dále určí opatření k prosazování auditu a provádí a dokumentuje pravidelné kontroly dodržování bezpečnostní politiky. Výsledky těchto kontrol jsou následně zohledňovány v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik.

5.5 Segmentace cílových oblastí a jejich specifika

Za cílové pro navrhovaný produkt lze označit celkem 8 oblastí:

1) státní správa;
2) IT/ICT sektor;
3) zdravotnictví;
4) řídící a automatizační systémy;
5) energetika (smart grids);
6) smart homes a smart buildings;
7) datová úložiště;
8) finační sektor;

Takto definovaným oblastem byly přiřazeny 3 úrovně priorit. Ty určují, kterými oblastmi se má EZÚ zabývat nejdříve a kterými později. Rozdělení do tří úrovní podle priorit přehledně zobrazuje Tabulka 4.

Priorita	Oblast
1 - Nejvyšší	Státní správa IT/ICT sektor Zdravotnictví
2 - Střední	Řídící a automatizační systémy Energetika (Smart Grids) Smart Homes a Smart Buildings
3 - Nižší	Datová úložiště Finanční sektor

Tabulka 4 – Oblasti dle priorit
Vlastní tvorba

Oblastem státní správy, IT/ICT sektoru a zdravotnictví je přiřazena nejvyšší priorita, protože se jedná o oblasti, pro které je kybernetická bezpečnost zásadní. V těchto oblastech byla navíc identifikována řada informačních a komunikačních systémů spadajících do kritické informační infrastruktury a významných informačních systémů. Zejména v oblastech státní správy a zdravotnictví je situace ohledně kybernetické bezpečnosti velmi špatná a otázka zabezpečení dlouho neřešená. Zároveň se jedná o oblasti, ve kterých již EZÚ, jež je sám státním podnikem, působí a nabízí své služby. Jedná se tedy o oblasti hůře zabezpečené a s velkým potenciálem.

Střední priorita je přiřazena oblastem, ve kterých je předpokládán velký boom. V oblasti průmyslových řídících systémů to souvisí zejména se čtvrtou průmyslovou revolucí (nejčastěji označovanou jako Industry 4.0). V oblasti energetiky se jedná o tzv. chytré sítě (smart grids). Stávající technologie a systémy implementované v oblasti energetiky jsou považovány za velmi dobře zabezpečené. Oblastí s velkým potenciálem je smart homes a smart buildings. V případě řídících a automatizačních systémů a oblasti energetiky lze potenciál pro EZÚ označit za středně velký. V připadě smart homes a smart buildings se jedná o oblast s velmi špatným řešením kybernetické bezpečnosti a zároveň vysokým potenciálem pro EZÚ. Vzhledem ke skutečnosti, že se jedná o oblasti, kde stále nebyly vytvořeny odpovídající standardy, se nelze v současnosti zaměřit na využití tohoto potenciálu.

Důvodem pro přiřazení nižších priorit u významných sektorů jako je finanční sektor a datová úložiště je skutečnost, že instituce v těchto oblastech mají kybernetickou bezpečnost zpravidla zajištěnou na vysoké úrovni. Bez toho by prakticky ani nemohly existovat. Jedná se tedy o sektory, kde hraje kybernetická bezpečnost důležitou roli, avšak s malým potenciálem pro EZÚ.

Práce se dále zabývá pouze oblastmi s nejvyšší prioritou. Důvodem pro toto rozhodnutí je potřeba nastartování nového produktu, nabrání potřebných zkušeností a referencí, a také potřeba rozšíření personálních zdrojů kontinuálním způsobem.

5.5.1 Cílové oblasti s nejvyšší prioritou

Státní správa

Stále více agend v rámci státní správy a samosprávy je a bude převáděno do digitální podoby, což umožňuje jejich efektivnější a rychlejší využívání (v souladu se základními koncepčními a strategickými dokumenty: „Strategický rámec rozvoje veřejné správy a eGovernmentu 2014+“ a „Digitální Česko 2.0“). Zároveň se tak ale veřejná správa a samospráva stává zranitelnější vůči útokům a hrozbám, přicházejícím z kybernetického prostoru, což pro ni představuje novou bezpečnostní výzvu. Zapotřebí bylo vytvoření jednotného a pevně stanoveného zákonného rámce. Tím se v nedávné době stal zákon o kybernetické bezpečnosti a s ním související prováděcí předpisy. Zákon je potřeba vnímat především jako určitý stimul a návod, jakým směrem se vydat. Tím by se měly vydat všechny státní organizace bez ohledu na to, zda spadají pod působnost zákona, nebo ne.

Pro oblast státní správy byly identifikovány veškeré mezinárodní standardy a legislativní předpisy České republiky související s kybernetickou bezpečností. Jejich identifikaci, celý název a zaměření obsahuje Obrázek 7 v Příloze C. Tyto definované právní a normativní předpisy jsou základem pro jednotlivé komponenty, ze kterých jsou následně formovány jednotlivé části a úrovně produktu. Z toho plyne, že

konkrétní podoba částí a úrovní produktu se liší podle toho, pro jakou oblast je produkt nabízen. Jak bude patrné z dalších odstavců, rozdíly mezi jednotlivými oblastmi nejsou významného charakteru.

IT/ICT sektor

Tento sektor je důležitý, protože zahrnuje organizace dodávající produkty a služby, jež často významným způsobem ovlivňují kybernetickou bezpečnost jejich zákazníků. Lze tedy říci, že tato oblast ovlivňuje všechy ostatní oblasti, a to včetně těch nejkritičtějších. Zajištění kybernetické bezpečnosti v oblasti IT/ICT je tak základním stavebním kamenem pro dosažení jakékoliv úrovně kybernetické bezpečnosti i v ostatních oblastech. Poskytované produkty a služby, stejně jako organizace samotná, musí být v souladu s veškerými souvisejícími legislativními předpisy, a také s příslušnými mezinárodními standardy.

IT/ICT sektor je široký pojem zahrnující organizace nabízející produkty a služby s různým zaměřením. Z tohoto důvodu je sektor dále rozčleněn na následující oblasti:

- dodavatelé softwaru;
- poskytovatelé cloudových služeb;
- provozovatelé digitálních úložišť;
- telekomunikace.

Stejně jako pro oblast státní správy, byl i pro oblast IT/ICT vytvořen soupis veškerých souvisejících normativních a legislativních předpisů. Větší část tvoří normy obsažené již v soupisu pro státní správu, z toho důvodu budou níže uvedeny pouze rozdílové předpisy.

- Standardy
  + ČSN ISO 16363
  + ISO/IEC 27017
  + ISO/IEC 27018

    + ČSN ISO/IEC 27034
    – ISO/IEC 27010
- Legislativa
    – zákon č. 365/2000 Sb.
    – usnesení vlády České republiky č. 624/2001

Zdravotnictví

Zdravotnictví je kritickou oblastí s velmi citlivými daty. Přitom jde o oblast, která kybernetické bezpečnosti nevěnuje žádnou nebo malou pozornost. To se mělo změnit příchodem zákona o kybernetické bezpečnosti, který se ale v současné době nevztahuje například na většinu nemocnic. Je potřeba aby si tyto organizace uvědomily závažnost situace a důležitost kybernetické bezpečnosti.

Stejně jako v předchozím případě jsou níže uvedeny pouze předpisy vztahující se k této oblasti, které nebyly zahrnuty v soupisu týkajícího se oblasti státní správy.

- Standardy
    + ISO/TR 16056
    + ČSN EN 62304
    + ČSN EN 13606
    + ČSN EN ISO 14971
    + ČSN EN ISO 27789
    + ČSN EN ISO 27799
    + ČSN EN 80001-1
- Legislativa
    – zákon č. 365/2000 Sb.
    – usnesení vlády České republiky č. 624/2001

6 Realizace produktu

6.1 Postup při realizaci produktu

Popis realizace produktu je vztažen k činnosti EZÚ. Zaměřuje se na jednotlivé části produktu s výjimkou implementace a dodávky potřebných technologií. Tato část je zajišťována přes partnerské organizace. Pro realizaci kompletního produktu tak, aby přinášel zákazníkovi největší přidanou hodnotu, je nutné navázat partnerské vztahy s dodavateli technologií (zjednodušeně hardwaru a softwaru) a organizacemi, které se zaměřují na implementaci normativních a legislativních požadavků (např. implementaci ISMS). Detailněji o problematice partnerských vztahů pojednává kapitola 6.3.2.

Při realizaci produktu musí být dodržovány požadavky normativních předpisů zaměřujících se zejména na auditní činnost v oblasti kybernetické bezpečnosti (např. ČSN ISO/IEC 27006). Dále musí být striktně dodržovány interní směrnice (metodiky) vztahující se k realizovaným činnostem. Postupovat v souladu s těmito interními dokumenty musí i externí zaměstnanci účastnící se realizace produktu.

Modelovou podobu realizace produktu zobrazuje diagram datových toků na Obrázcích 8 a 9 v Příloze D. V rámci tohoto diagramu je zahrnuta většina částí produktu.

6.1.1 Školení a úvodní informační školení

Školení jednotlivých právních a normativních předpisů je stejně tak jako úvodní informační školení realizováno prostřednictvím přednášky s prezentací v MS PowerPoint. Může probíhat v prostorách EZÚ – v případě školení zástupců několika různých firem; v případě školení většího počtu (5-12) zájemců ze stejné společnosti lze nabídnout školení v místě působnosti zákazníka. Školitelé jsou odborníci s dlouholetou praxí v oboru, nejčastěji se jedná o auditory, kteří provádí audity dle

příslušných mezinárodních standardů a jsou garanty za tuto normu v EZÚ. Rozdíl mezi jednotlivými školeními je především v jejich časové náročnosti.

6.1.2 Situační analýza

Provedení situační analýzy je jedním z prvních kroků při realizaci produktu. Při jejím provedení jsou zjišťovány nedostatky a problémy současného stavu kybernetické bezpečnosti v organizaci. Provedení situační analýzy není krokem povinným, nicméně velmi důležitým, tudíž doporučovaným. To platí zejména pro organizace, které nemají z minulosti implementován žádný systém řízení bezpečnosti informací, certifikaci či se kybernetickou bezpečností doposud nezabývaly. Řádné provedení situační analýzy totiž zajistí nejen lepší přípravu a podklady pro implementaci, ale následně také hladší a bezproblémový průběh auditu a certifikace.

Svou náplní připomíná provedení situační analýzy klasický audit, při kterém jsou zjišťovány silné stránky a nedostatky vzhledem k požadavkům právních a normativních předpisů. Při situační analýze je však kladen větší důraz na specifické části (např. analýzu rizik), na důkladné definování zjištěných nálezů a především na zevrubné popsání návrhů na vypořádání nálezů a zlepšení daného procesu či stavu. Právě tyto návrhy na zlepšení jsou následně využity ve fázi implementace technologií a bezpečnostních systémů.

6.1.3 Osobní certifikace

Osobní certifikace zahrnují školení a certifikační zkoušku. Nabízena je osobní certifikace pro manažera, architekta a auditora kybernetické bezpečnosti. Vzhledem k realizaci není důležité, o jakou bezpečnostní roli se jedná. Školení jsou realizována prostřednictvím přednášky s prezentací v MS PowerPoint a individuálních úkolů zpracovávaných v rámci klasického workshopu. Certifikační zkouška je tvořena testem, který se skládá z otevřených otázek. V souvislosti s úrovněmi osobních

certifikací jsou vytvořeny tři prezentace a tři testy pro každou bezpečností roli. Test je nutné splnit z:

a) 50% pro zisk osobního certifikátu úrovně specialist;
b) 60% pro zisk osobního certifikátu úrovně expert;
c) 70% pro zisk osobního certifikátu úrovně master.

Stejně jako u certifikace kybernetické bezpečnosti existuje návaznost mezi úrovněmi Z tohoto důvodu je nutné pro zisk osobního certifikátu úrovně expert nejprve získat osobní certifikát úrovně specialist apod.

6.1.4 Certifikace kybernetické bezpečnosti

Nejdůležitější část produktu je realizována prostřednictvím auditu EZÚ jako nezávislou třetí stranou (certifikační autoritou). Při auditu je ověřována shoda hned s několika různými právními a normativními předpisy a jeho provedení je tak složitým úkolem, kterého se mohou zhostit jen ti nejzkušenější auditoři. Audity jsou prováděny s roční periodicitou stejně jako veškeré další audity systémů řízení. Rozlišují se tři druhy auditů – certifikační, dozorový a recertifikační. Toto rozlišení souvisí s dobou platnosti certifikátů – 3 roky. Certifikační audit je realizován v případě, že organizace dosud nevlastnila příslušný certifikát, nebo v případě, že platnost certifikátu již vypršela. Následuje provedení dvou dozorových auditů a poté audit recertifikační. Při úspěšném recertifikačním auditu je organizaci vydán nový certifikát, opět s platností tří let. Následně je dodržován tříletý cyklus složený ze dvou dozorových a jednoho recertifikačního auditu. Tato časová souslednost a rozdíly mezi jednotlivými druhy auditu jsou také znázorněny na Obrázcích 8 a 9 v Příloze D.

V případě, že organizace již měla k některému ze souvisejících standardů platný certifikát, je tento certifikát uznán i přes to, že nebyl vydán EZÚ. V případě, že má organizace stále platný certifikát, ale přeje si přejít v rámci zajištění kompletnosti produktu k EZÚ, bude k příslušnému předpisu proveden mimořádný audit. Ten je menšího rozsahu než certifikační audit a zaměřuje se na nejdůležitější požadavky

příslušných předpisů. Pokud není při tomto auditu nalezena žádná závažná neshoda, zůstane platnost původního certifikátu nezměněna. Změní se pouze orgán vydávající tento certifikát. V obou případech se jedná o certifikáty související s jednotlivými právními nebo normativními předpisy. Z tohoto důvodu je audit prováděn vždy, odlišný je pouze jeho rozsah. Až na základě úspěného ověření shody se všemi definovanými předpisy může zákazník získat příslušný certifikát.

Realizovat druhou úroveň certifikace kybernetické bezpečnosti je v dané organizaci možné pouze po úspěšné certifikaci první úrovně. Stejně tak tomu je v případě úrovně třetí, kterou je možné realizovat až v případě úspěšné certifikace druhé úrovně. Ověřování a následná certifikace vyšší úrovně může nastat po uplynutí nejméně jednoho roku od vydání certifikatu předešlé úrovně.

6.1.4.1 Realizace auditu

Plán auditu

Plán auditu musí být vytvořen a zaslán zákazníkovi nejméně 14 dní před termínem konání auditu. Je komunikován se zákazníkem ještě před jeho finálním zasláním, protože je potřeba pro jednotlivé části a body plánu zajistit příslušnou součinnost ze strany zákazníka a zajistit přítomnost příslušných zaměstnanců organizace zákazníka, kteří jsou zodpovědni za jednotlivé oblasti. Pro tvorbu plánu musí být vypočtena časová náročnost auditu, určen druh auditu a identifikovány veškeré předpisy, podle kterých má být audit proveden. Před tvorbou plánu musí být známé složení auditního týmu. Pro zakázku se určuje potřebný počet auditorů v rámci výpočtu MD zakázky. Pro každou komponentu produktu musí být určen vedoucí auditor, jež řídí svůj auditní tým. Složení auditního týmu musí být odsouhlaseno zákazníkem a musí respektovat potřeby EZÚ v rámci plánování personálních zdrojů celého oddělení.

Plán auditu může být upravován i v průběhu auditu. Mohou nastat nenadálé události (neposkytnutí součinnosti, nepřítomnost potřebných zaměstnanců zákazníka, změna rozsahu auditu apod.). Finální verze plánu je součástí závěrečného výstupu odesílaného zákazníkovi.

Příprava na audit

Na audit se připravují všechny zúčastněné strany. Příprava spočívá ve studiu nastavených procesů v auditované organizaci a toho, jak jsou tyto procesy zdokumentovány, popsány. Je potřeba, aby měl auditovaný rozumný přehled o procesech, za které je osobně odpovědný, a věděl jaké požadavky jakých norem, interních směrnic a případně legislativních předpisů jsou vzhledem k těmto procesům relevantní. Musí obhájit, že jsou tyto požadavky naplňovány. Nejlepším nástrojem k pochopení fungování organizace a jednotlivých procesů je vytvoření tzv. mapy procesů, ve které jsou k jednotlivým procesům přiřazeny jednotlivé dokumenty – směrnice. Dalším vhodným nástrojem jsou vývojové diagramy, díky kterým si mohou i auditoři ujasnit a dobře představit materiálové a informační toky. Pro méně zkušené auditory nebo auditory provádějící audit podle komponenty produktu, která není jejich primární činností, je doporučeno připravit si sadu otázek k jednotlivým požadavkům normativních a legislativních předpisů. Tyto otázky by měly být vztaženy přímo na konkrétního zákazníka, konkrétní organizaci.

Veškeré dokumenty potřebné k realizaci auditu by měly být předem připraveny ve formě šablon (checklistů). Tyto šablony je nutné dále rozpracovat a upravit na míru zákazníkovi. Právě do těchto dokumentů může auditor vkládat připravené otázky.

Audit v místě působnosti zákazníka

Po příjezdu auditního týmu proběhne úvodní jednání auditorů s vedením auditované organizace. V rámci tohoto jednání dojde k přivítání a seznámení v případě, že se jedná o první audit v této organizaci. Během jednání je probrán časový harmonogram auditu a případné změny plánu auditu, které je nutné vzhledem k současné situaci

provést tak, aby byl zajištěn plynulý průběh auditu nenarušující významně chod firmy. Definován je také způsob komunikace (audit je možné provádět i vzdáleně) a ověřuje se zajištění potřebných zařízení a prostor pro konání auditu.

Vlastní auditování spočívá v několika činnostech. Tou zdaleka nejdůležitější z nich je kladení otázek auditovaným pracovníkům formou interview. Pracovníci jsou nejčastěji zpovídáni z toho, jakou činnost provádějí, jak a podle kterých směrnic či předpisů ji provádějí, jak vědí, že ji provádějí správně a kde jsou o tom případné záznamy. Výsledkem auditu je posouzení a vyjádření shody (popř. neshody) s požadavky norem či legislativních předpisů. Auditoři využívají při auditu předem připravené check-listy k jednotlivým předpisům nebo jeden check-list, který zahrnuje veškeré požadavky všech předpisů. Check-list je pro auditory pomůckou, ze které je zřejmé, zda se věnovali všem požadavkům příslušných norem.

Při auditu na místě dochází ke sběru potřebných informací o skutečném fungování systému, ověřování plnění požadavků normativních a legislativních předpisů a jsou shromažďovány důkazy o plnění nebo neplnění těchto požadavků. Na základě takto zjištěných podkladů jsou v závěrečné zprávě z auditu identifikovány silné a slabé stránky systému. Jsou identifikovány neshody, nedostatky a doporučení. Tím je vyznačena různá úroveň závažnosti nálezu. Neshody jsou nejzávažnějším nálezem, který musí být odstraněn nejlépe ihned. O neshodách musí být sepsány zvláštní záznamy do k tomu určených formulářů. O těchto neshodách je zákazník informován při závěrečném jednání, kde je k nim poskytnut potřebný komentář auditorů a jejich opodstatnění je projednáno i s vedením auditované organizace. Bez řádně vypořádaných identifikovaných neshod nelze vydat certifikát.

Veškeré finální výstupy, zejména závěrečná zpráva z auditu, musí být přezkoumány certifikačním orgánem EZÚ, který vydává konečné stanovisko – konstatuje shodu nebo neshodu. Rozhoduje, zda bude certifikát udělen hned, po vypořádání neshod, po realizaci dalšího (mimořádného) auditu nebo že certifikát z důvodu nálezu velkého množství závažných neshod udělen nebude (či bude odejmut v případě dozorového auditu).

Po auditu

Zpráva z auditu je vhodné zaslat spolu s ostatními výstupy zákazníkovi do 14 dnů po dokončení auditu na místě. Pokud zákazník s výsledky nebo postupem auditorů nesouhlasí, může zaslat nesouhlas a případné připomínky ke zprávě z auditu. Identifikované neshody musí být vyřešeny hned, bez nich není možné vydat certifikát. Nedostatky je potřeba řešit formou tvorby náprávných opatření do příštího dozorového nebo recertifikačního auditu. V případě jejich nevyřešení je pravděpodobné, že budou v příštím auditu klasifikovány jako neshody. Doporučení mají mírnější charakter. Je pouze na zákazníkovi, jak naloží s identifikovanými doporučeními – zda k nim vytvoří nápravná opatření, nebo ne. Ověření realizace a správnosti těchto nápravných opatření je rovněž ověřováno při následujícím auditu.

6.1.5 Bezpečnostní testy

Bezpečnostní testy definované v kapitole 5.4.6 jsou realizovány v rámci druhé a třetí úrovně produktu. Jejich provedení je uskutečněno buď v místě působnosti zákazníka, v EZÚ nebo při spolupráci s partnerem EZÚ - v partnerské organizaci. Záleží na tom, o jaký bezpečnostní test se jedná a především na konkrétních požadavcích zákazníka.

6.1.6 Zajištění bezpečnostní role auditora kybernetické bezpečnosti

V rámci realizace této části produktu je dotyčné organizaci poskytnut interní nebo externí zaměstnanec EZÚ, který je zkušeným auditorem kybernetické bezpečnosti. Ten působí v inkriminované organizaci jako interní auditor. Při realizaci je potřeba dávat pozor především na kapacitní možnosti jednotlivých auditorů, tedy na jejich dokonalé plánování a řízení, protože se jedná o činnost časově náročnou.

6.2 Časová náročnost a nacenění jednotlivých částí produktu

Jelikož se jedná o službu, je výpočet ceny spjat s výpočtem časové náročnosti zakázky. Časová náročnost zakázky je počítána v „člověkodnech“ (dále jen MD). Jeden MD je brán jako klasický pracovní den, tedy 8 hodin. Všechny ceny uvedené v následujících podkapitolách jsou uvedeny bez DPH. Celková kalkulace obsahuje obvyklou marži pro EZÚ a její struktura dává prostor pro případná cenová vyjednávání ze strany klienta. V případě školení a osobní certifikace nelze o cenové výši vyjednávat. Níže uváděné ceny jsou navrhované, nejedná se o oficiální ceny stanovené EZÚ.

Úvodní informační školení

Úvodní informační školení je nabízeno za účelem informování zákazníka, vysvětlení jednotlivých částí produktu a jejich opodstatnění a realizovatelné přínosy pro organizaci. Z těchto důvodů je nabízeno bezplatně, a to jak pro potenciální zákazníky, tak pro potenciální partnerské organizace. Jeho časová náročnost je odhadována na 1 hodinu pro prezentaci a 1 až 2 hodiny pro řešení dotazů a diskuzi.

Situační analýza kybernetické bezpečnosti

Na situační analýzu jsou kladeny nižší nároky než na audit. Časová náročnost pro provedení situační analýzy ve velké míře závisí na konkrétním zákazníkovi. Do hry zde vstupuje několik faktorů stejných jako u auditu, zde však mají mnohem větší dopad (např. o míru vyspělosti systému, připravenost organizace na certifikaci, míru regulace). Obecně lze říci, že doba potřebná na provedení situační analýzy by měla dosahovat 25 – 50 % doby potřebné na provedení certifikačního auditu. Cena za 1 MD je stejná jako u auditů – 16 000 Kč.

Školení a osobní certifikace

Cena za 1 den školení se pohybuje okolo 8 000 Kč. Délka školení závisí na právním nebo normativním předpisu, na který je školení zaměřeno – zpravidla se jedná o jeden až tři dny. V případě osobní certifikace je cena za den vyšší – 10 000 Kč. Vyšší cena je způsobena certifikační zkouškou, která je součástí této části produktu. V obou uvedených cenách je reflektována i nutnost přípravy podkladů. Časový rozsah osobních certifikací je zpravidla 2 dny.

Certifikace kybernetické bezpečnosti

Výsledná časová náročnost je ovlivněna několika faktory. Mezi ně lze zařadit zejména:

- počet a druh vybraných komponent produktu,
    - to ovlivňuje také úroveň integrace (např. podobnost některých požadavků různých norem),
- úroveň integrace (např. zda je nastaven integrovaný přístup k interním auditům, bezpečnostní politice a cílům či procesům organizace),
- druh auditu – certifikační, dozorový nebo recertifikační,
- počet zaměstnanců v rozsahu auditu a
- počet poboček (včetně ústředí) v rámci rozsahu auditu.

Časová náročnost této části je dále ovlivněna spoustou méně významných faktorů, např. vyspělost zavedeného systému (managementu), připravenost organizace na certifikaci či míra regulace.

Tyto informace je potřeba od zákazníka získat před snahou o určení MD a přesné ceny. K tomu je využíván dotazník kybernetické bezpečnosti. Celkový počet MD zahrnuje jak dobu potřebnou pro přípravu podkladů (např. tvorba plánu auditu), přezkoumání dokumentace, posouzení provedené analýzy rizik, audit na místě, tak i vypracování závěrečné zprávy z auditu a případných dílčích auditních zpráv. Rozdělení MD mezi činnosti potřebné k realizaci auditu je závislé na konkrétní potřebě v rámci určité zakázky a řídí si ho vedoucí auditor.

Následný výpočet ceny spočívá v prostém vynásobení počtu určených MD cenou za 1 MD. Vzhledem k tomu, že všechny faktory tykající se zákazníka a tedy zakázky byly zohledněny již při výpočtu MD, cena za 1 MD je ve všech případech stejná – 16 000 Kč.

Bezpečnostní testy

Časová náročnost a od ní se odvíjející cena zavisí především na počtu poptávaných bezpečnostních testů, velikosti organizace, složitosti její infrastruktury a konkrétních přáních zákazníka vztahujících se k jejich provedení. Standardní cena za 1 MD je 15 000 Kč.

Zajištění bezpečnostní role auditora kybernetické bezpečnosti

U této služby se jedná o klasický outsourcing lidského kapitálu. Výsledná cena se tak odvíjí pouze od požadavků zákazníka – kolik MD bude poptávat. Cena za 1 MD je stanovena na 14 000 Kč.

6.3 Identifikace zdrojů potřebných k realizaci produktu

Vzhledem k charakteru produktu jsou nejvýznamnějším zdrojem potřebným pro realizaci produktu lidské zdroje a odborná znalost, tedy kvalifikace personálu. Finanční zdroje je potřeba alokovat převážně na příslušné zaměstnance kybernetické laboratoře. Technické vybavení není potřeba prakticky žádné, s výjimkou bezpečnostních testů (SW nástrojů) a standardního vybavení zaměstnanců – počítač, mobilní telefon, v případě auditorů automobil.

6.3.1 Personální zdroje

V případě personálních zdrojů je nutné identifikovat všechny zaměstnance, kteří jsou do realizace produktu zapojeni. Jedná se zejména o pracovníky kybernetické laboratoře a dále auditory, kteří nemusí patřit vyloženě pod kybernetickou laboratoř, přes to vstupují do realizace produktu tím, že provádí audit podle některých norem

zahrnutých v produktu. Laboratoř je označení klasického oddělení, které vychází ze stávající organizační struktury EZÚ a je s ní v souladu. Při realizaci produktu jsou využívány také externí personální zdroje – zejména auditoři. Zapojení externistů v rámci jednotlivých zakázek probíhá přes manažera produktu, který má na starost jednotlivé zakázky a je tedy de facto projektovým manažerem. Důležité je napojení laboratoře kybernetické bezpečnosti na obchodní úsek a úsek certifikace (CO EZÚ).

Oblast kybernetické bezpečnosti vyžaduje hlubokou odbornou znalost. Jelikož se jedná o vcelku nový a dynamicky se rozvíjející obor, je potřeba ji neustále prohlubovat pokračujícím vzděláváním a účastí na konferencích a školeních tak, aby člověk zachytil nejnovější trendy v této oblasti. Nutností je sledování aktuálnosti legislativních a normativních předpisů, podle kterých je audit a certifikace prováděna.

Tým tvořící laboratoř kybernetické bezpečnosti může být zpočátku tvořen také externisty (auditoři a technici), nicméně po zaběhnutí produktu by mělo být uvažováno o týmu, který bude složen z co největší části interními zaměstnanci společnosti, a to především z finančních důvodů. Využitím externích pracovníků jsou řešeny problémy týkající se nedostatku interních zdrojů (kapacit) EZÚ, popř. chybějící odbornost v dílčích komponentách produktu. Složení laboratoře kybernetické bezpečnosti vypadá následujícím způsobem:

- Vedoucí laboratoře kybernetické bezpečnosti
  - zodpovídá za řízení laboratoře kybernetické bezpečnosti, plánování práce a všechny další činnosti spojené s řízením laboratoře kybernetické bezpečnosti (přezkoumává požadavky zákazníka k technické a kapacitní způsobilosti laboratoře, kontroluje výstupy svých podřízených, zajišťuje a zodpovídá za odborný rozvoj svůj a svých podřízených, spolupracuje na normalizační činnosti a tvorbě předpisů a postupů, hospodárně vynakládá prostředky na spotřebu materiálu a nakupovaných služeb)
  - Tato role nemůže být zajištěna externím zaměstnancem.
- Manažer produktu kybernetické bezpečnosti
  - zodpovídá za obchodování a posuzování zakázek ve svěřené oblasti, získávání zakázek, obrat a péči o zákazníky, jakož i o rozvoj svěřené oblasti.

Zejména provádí akvizice u zákazníků, připravuje nabídky pro poptávky zákazníků, připravuje reakce pro objednávky, vyjednává o cenách a termínech zakázek a připravuje podklady pro jejich odvádění, spolupracuje s příslušnými pracovníky při řešení problémů ve svěřené oblasti.

- Tato role může, ale nemá být zajištěna externím zaměstnancem.

❖ Auditor kybernetické bezpečnosti

- zodpovídá za provádění auditů, inspekcí a posuzování shody s normativními a právními předpisy v oblasti kybernetické bezpečnosti. Vypracovává požadovanou dokumentaci a záznamy, prezentuje výsledky auditů/inspekcí a posuzování shody zákazníkům, zajišťuje svůj odborný rozvoj, školí a přednáší, spolupracuje na normalizační činnosti a tvorbě předpisů a postupů atd. Auditoři kybernetické bezpečnosti jsou nejčastějšími školiteli, protože jsou garanty za jednotlivé normativní předpisy, nejlépe je znají, mají nejvíce zkušeností z praxe a velmi dobré komunikační schopnosti.
- Tato role může být zajištěna externím zaměstnancem.

❖ Technik kybernetické bezpečnosti

- zodpovídá za provádění bezpečnostních testů a jejich výsledky. Účastní se auditů/inspekcí a posuzování shody s normativními a právními předpisy v oblasti kybernetické bezpečnosti jako technický expert. Vypracovává protokoly o bezpečnostním testu, zpracovává testovací postupy, předtisky záznamů, využívá vhodné nebo předepsané testovací techniky, vybavení a prostor k provádění bezpečnostních testů, poskytuje a zodpovídá za odborná stanoviska a komentáře k průběhu bezpečnostních testů a jejich výsledkům.
- Tato role může být zajištěna externím zaměstnancem.

❖ Referent laboratoře kybernetické bezpečnosti

- zodpovídá za agendu zakázek (včetně reklamací) v oblasti kybernetické bezpečnosti, práci s programem auditů, přípravu smluv a fakturaci. Přijímá, připravuje a vyřizuje objednávky, připravuje jmenování auditního týmu, uzavírá a aktualizuje smlouvy a objednávky, odvádí a fakturuje

zakázky, aktualizuje a spravuje data o zakázkách a zákaznících v oblasti kybernetické bezpečnosti, připravuje podklady pro vymáhání pohledávek, organizuje školení.

- Tato role nemůže být zajištěna externím zaměstnancem.

6.3.2 Partnerské vztahy

V rámci realizace produktu se všemi jeho definovanými fázemi tak, aby bylo možné zajistit co nejkvalitnější službu a neustálé zlepšování, je nutné navázat partnerské vztahy. Důvody pro vytvoření těchto vztahů byly specifikovány v kapitole 5. Tento vztah je oboustranně výhodný, protože poskytované služby/produkty jsou navzájem komplementární. Stejně tak dochází k rozšíření obchodních sítí a zvýšení počtu obchodních příležitostí na obou stranách. Partnerské vztahy musí být vhodně smluvně zabezpečeny. Dodržení povinnosti zachování mlčenlivosti a vzájemná důvěra je v této oblasti naprosto nezbytná.

Využití služeb/produktů partnerů je potřebné zejména pro následující činnosti:

- tvorba, implementace a integrace systémů podle platných mezinárodních standardů a legislativních předpisů;
- optimalizace zavedených (integrovaných) systémů – vypořádání případných neshod a nedostatků zjištěných při auditech;
- poradenská činnost;
- spolupráce na školeních, workshopech, konferencích;
- dodávka hardwaru a softwaru podporujícího kybernetickou bezpečnost;
- spolupráce při realizaci bezpečnostních testů.

7 Shrnutí návrhu a realizace produktu

Tato diplomová práce se zaměřuje na návrh produktu, který najde uplatnění v oblasti kybernetické bezpečnosti, a na popis jeho realizace. Nejedná se o celistvý podnikatelský plán, nýbrž o jeho detailně rozepsané části. Podrobně jsou popsány všechny části produktu a nejdůležitější aspekty jeho realizace. Návrh produktu a jeho realizace v sobě odráží směr, kterým se chce EZÚ v této oblasti zabývat a prezentovat, uvažuje o současných a potřebných kapacitách a možnostech podniku, respektuje hodnoty, ke kterým se EZÚ hlásí a na kterých si zakládá.

Vzhledem k dynamickému vývoji v oblasti kybernetické bezpečnosti bude potřeba produkt a proces jeho realizace neustále vyhodnocovat a přizpůsobovat aktuálním potřebám. Důležitá bude i zpětná vazba od zákazníků a partnerů. Postupně tak vykrystalizuje struktura produktu a procesu jeho realizace, která bude pro zákazníka nejvhodnější a pro EZÚ nejefektivnější. Kromě zpětné vazby je vhodné neustále sledovat trh, tedy požadavky a potřeby zákazníků. Jelikož se jedná o nový produkt, je zapotřebí velkého marketingového úsilí (např. publikační činnost v podobě odborných článků, pořádání či účast na různých akcích, soutěžích a konferencích – zejména aktivní vystupování).

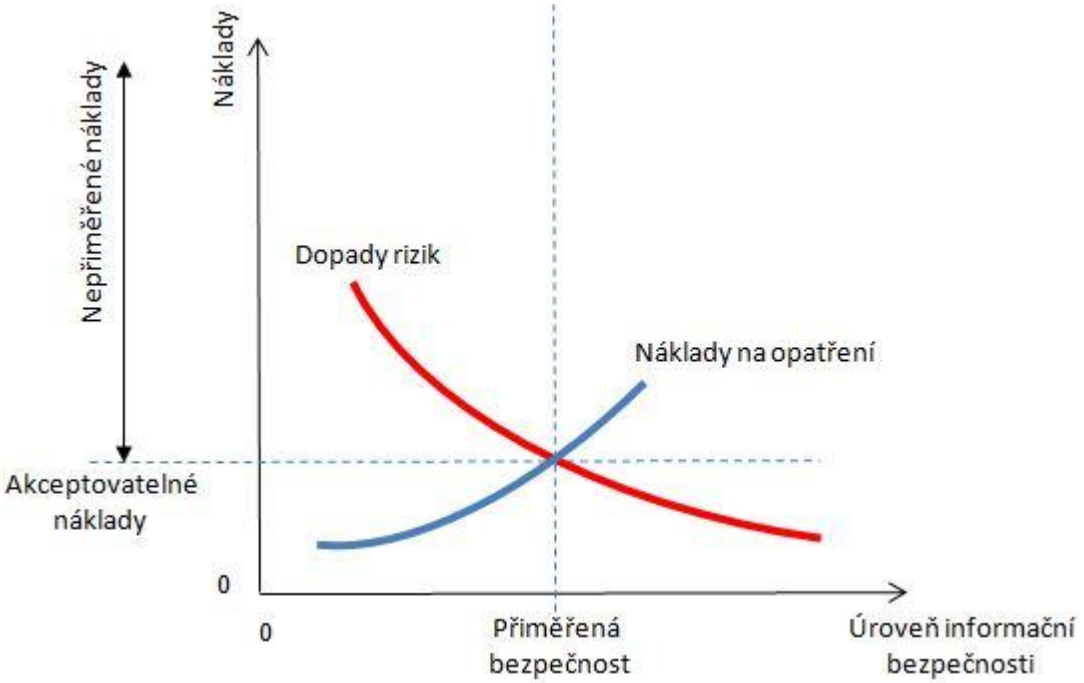
Z důvodu existence silné vazby na právní a normativní předpisy související s kybernetickou bezpečností ho budou nadále významně ovlivňovat veškeré změny týkající se těchto předpisů (vznik, vyřazení a veškeré aktualizace či korekce těchto předpisů). Směrem k rozvoji produktu bude působit zejména vznik nových předpisů souvisejcích s oblastí kybernetické bezpečnosti. Častá aktualizace a vydávání korekcí související s dynamickým rozvojem v této oblasti je z hlediska realizace produktu problematická a nese s sebou nustnost neustálého sledování veškerých změn v těchto předpisech. Nicméně častá a aktivní aktualizace příslušných předpisů je v této oblasti nezbytností a velkým přínosem pro jejich uživatele.

Další možnost rozvoje produktu a jeho realizace je spojena s rozšířením zacílení na další oblasti uvedené v kapitole 5.5 (střední a nižší priorita). Zejména v oblastech, u kterých je v současnosti bariérou vstupu neexistence příslušných právních či normativních předpisů, spočívá velká příležitost.

Realizace produktu sama o sobě nezajistí vhodnou úroveň kybernetické bezpečnosti. Té lze dosáhnout pouze při součinnosti zákazníka a především zapojení vrcholového managementu. Bez zájmu vrcholového vedení organizace a všech zaměstnanců budou všechny implementované systémy a technologie neefektivní, naopak budou spíše přítěží pro realizaci primárních činností organizace. V závislosti na tom, jaký přístup ke kybernetické bezpečnosti organizace a zejména její vrcholové vedení zvolí, se bude výsledná úroveň kybernetické bezpečnosti pohybovat mezi IV. a V. úrovní (v návaznosti na úrovně definované v kapitole 2.1).

V rámci realizace produktu je velmi důležité zachování a dodržování hodnot EZÚ – nezávistlost, nestrannost, partnerství, inovace a profesionalitu. Zachování a dodržování všech těchto hodnot je nezbytně nutné pro fungování podniku v oblasti kybernetické bezpečnosti a pro nabízení a poskytování kvalitních služeb s jistotou, že bude zachována mlčenlivost a důvěrnost. Důležitá je také aktivní komunikace se zákazníky a partnery. Ta by měla probíhat zejména formou přímého kontaktu, který je nejvhodnějším právě pro zachování a podporu výše zmíněných hodnot a důvěry.

Důležité je řádné provedení úvodních fází, jako jsou analýza rizik a situační analýza. Z výstupu analýzy rizik musí vyplývat, která rizika jsou akceptovatelná a kterými je naopak nutné se zabývat, tedy stanovit k nim opatření. Z analýzy by mělo být patrné, jak velké škody může způsobit realizace určité hrozby na jednotlivých aktivech a s jakou pravděpodobností může k takové realizaci dojít. To vše se prolíná s další důležitou činností - určením nepřiměřených nákladů na zajištění kybernetické bezpečnosti (viz Obrázek 5). Poměřovány jsou výsledné hodnoty rizik a náklady na jednotlivá opatření.



Obrázek 5 – Určení nepřiměřených nákladů na kybernetickou bezpečnost
Vlastní tvorba

Vzhledem k zařazení oblasti státní správy mezi oblasti s nejvyšší prioritou je důležité zmínit výzvu č. 10 s názvem „Kybernetická bezpečnost“, která je jednou z 22 aktuálních výzev v IROP a jejích celková alokace je 1 411 764 706 Kč. [46] Oprávněnými žadateli jsou především organizační složky státu, kraje, příspěvkové organizace organizačních složek státu a další státní organizace a podniky. Příjem žádostí o podporu byl zahájen 21. 10. 2015 a bude ukončen 30. 6. 2017. Výzva se týká zvýšení odolnosti VIS a KII veřejné správy proti kybernetickým hrozbám. Hlavní podporovanou aktivitou jsou technická opatření vedoucí k zabezpečení VIS a KII veřejné správy (např. kamerové systémy, protipožární opatření, nástroje pro ověřování identity uživatelů, nástroje pro zaznamenávání činnosti KII a VIS). Musí být dodržována zejména specifická pravidla této výzvy [47] a obecná pravidla výzev. [48]

[46] Další informace o výzvě č. 10 v IROP lze nalézt na: http://www.strukturalni-fondy.cz/getmedia/20ccaa3d-72de-4e94-a85a-932c3bcb90f7/Text-10-vyzvy_SC-3-2_kyberbezpecnost_1-1.pdf?ext=.pdf
[47] Specifická pravidla pro žadatele a příjemce lze nalézt na: http://www.strukturalni-fondy.cz/getmedia/0a1bdd2a-6892-412a-9061-57d4cc03541e/Pravidla-10-vyzvy_SC-3-2_kyberbezpecnost_1-1.pdf?ext=.pdf
[48] Obecná pravidla pro žadatele a příjemce lze nalézt na: http://www.strukturalni-fondy.cz/getmedia/12957ad9-bcac-4ad3-b45d-b46cd68ed5a0/Obecna-pravidla-IROP_vydani-1-2_02112015_final.pdf?ext=.pdf

Závěr

V současné době se pro ověřování a certifikaci v oblasti kybernetické bezpečnosti většina organizací uchyluje k certifikaci ISO/IEC 27001, popř. zákona č. 181/2014 Sb., o kybernetické bezpečnosti. V horším a bohužel častějším případě neřeší kybernetickou bezpečnost vůbec. Nicméně splnění požadavků zákona o kybernetické bezpečnosti a certifikaci ISO/IEC 27001 nelze vnímat jako jistotu důkladného zajištění kybernetické bezpečnosti, ale spíše jako první krok v tomto úsilí, na který je potřeba navázat kroky dalšími. To v práci navžený produkt zohledňuje a právě to je jeho největším přínosem. Navržený produkt je komplexní a adresuje hlavní výzvy v oblasti kybernetické bezpečnosti včetně zaměření na lidský faktor a edukaci. Popis důležitých aspektů realizace navrženého produktu a následné shrnutí dále rozvíjí přínos produktu a zaměřuje se na jeho možnou realizaci v praxi a jeho další rozvoj v budoucnosti.

Diplomová práce obsahuje návrh produktu a popis hlavních aspektů jeho realizace. Navržený produkt a popis jeho realizace je vztažen k činnosti Elektrotechnického zkušebního ústavu, s. p. Produkt i proces realizace bude nadále rozvíjen a upravován v závislosti na reakci trhu, zpětné vazbě od zákazníků a kapacitách podniku.

Na závěr práce bych rád zmínil známé prohlášení současného CEO bezpečnostního gigantu CISCO, Inc., se kterým nelze než souhlasit.

„There are two types of companies: those who have been hacked, and those who don´t yet know they have been hacked.“ [82]

John Chambers

Chief Executive Offier of Cisco

Seznam použité literatury

[1] POŽÁR, J. *Vybrané hrozby informační bezpečnosti organizace.* [online]. 2011. PA ČR. Dostupné na: http://www.cybersecurity.cz/data/Pozar2.pdf [Přístup získán 30. 12. 2015]

[2] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti*. Přel. K. Vavruška. 3. vyd. PA ČR, AFCEA. Praha. 2015. 242 s. ISBN 978-80-7251-436-6

[3] CyberSecurity, 2016. *Cyber security (Kybernetická bezpečnost).* [online]. Dostupné na: http://www.cybersecurity.cz/basic.html [Přístup získán 1. 1. 2016]

[4] i-SCOOP, 2016. *Information management and intelligence executive guide* [online]. Dostupné na: http://www.i-scoop.eu/information-management/ [Přístup získán 1. 1. 2016]

[5] HAGER, M.. *Návrh obchodního modelu poskytujícího služby v oblasti kybernetické bezpečnosti*. Technická univerzita v Liberci. Ekonomická fakulta. Liberec, 2014. 64 s. Bakalářská práce

[6] HALAMA, L. *Návrh vybraných služeb kybernetické bezpečnosti*. Technická univerzita v Liberci. Ekonomická fakulta. Liberec, 2015. 61 s. Bakalářská práce

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

[8] MVČR, Odbor bezpečnostní politiky, 2014. *Kybernetické hrozby.* [online]. Dostupné na: http://www.mvcr.cz/clanek/bezpecnostni-hrozby-337414.aspx?q=Y2hudW09Mw%3D%3D [Přístup získán 2. 1. 2016]

[9] ČSN ISO/IEC 27000. *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník*. ÚNMZ. 2014

[10] OWASP, 2012. *Attacks.* [online]. Dostupné na: https://www.owasp.org/index.php/Category:Attack [Přístup získán 2. 1. 2016]

[11] Icon Labs, 2016. *Security for the Smart Home – Who is Responsible?* [online]. Dostupné na: http://www.iconlabs.com/prod/security-smart-home-%E2%80%93-who-responsible [Přístup získán 2. 1 .2016]

[12] HAGER, M. *Ročenka ELEKTRO 2016*. FCC Public, s.r.o. Praha. 2016. s. 146-167. ISBN 978-80-86534-27-5

[13] ČÍŽEK, J. *Hackeři útočili na automobil. Přes web ovládli brzdy i motor*. [online]. 2015. Dostupné na: http://www.zive.cz/clanky/hackeri-utocili-na-automobil-pres-web-ovladli-brzdy-i-motor/sc-3-a-179080/default.aspx [Přístup získán 8. 1. 2016]

[14] Cisco, 2015. *Cisco 2015 Annual Security Report.* [online]. Dostupné na: http://www.cisco.com/web/offers/pdfs/cisco-asr-2015.pdf [Přístup získán 15. 1. 2016]

[15] Check Point, 2015. *Check Point – 2015 Security Report.* [online]. Dostupné na: http://www.checkpoint.com/resources/downloads/CheckPoint-2015-SecurityReport.pdf [Přístup získán 16. 1. 2016]

[16] Ponemon Institute, 2016. *Ponemon Institute's 2015 Global Cost of Data Breach Study Reveals Average Cost of Data Breach Reaches Record Levels.* [online]. Dostupné na: http://www.prnewswire.com/news-releases/ponemon-institutes-2015-global-cost-of-data-breach-study-reveals-average-cost-of-data-breach-reaches-record-levels-300089057.html
[Přístup získán 16. 1. 2016]
[17] SOPHOS, 2015. *Our cybersecurity predictions for 2016.* [online]. Dostupné na: https://blogs.sophos.com/2015/12/11/our-cybersecurity-predictions-for-2016/
[Přístup získán 16. 1. 2016]
[18] DOUCEK, P. *Řízení bezpečnosti informací.* 2. rozš. vyd. o BCM. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8
[19] CERT, 2012. *ČSN EN ISO 19011:2012. Směrnice pro auditování systémů managementu.* [online]. Dostupné na: http://www.cert.cz/download/ISO_19011_2012.pdf
[Přístup získán 17. 1. 2016]
[20] PDQM, 2016. *Interní nebo externí audit.* [online]. Dostupné na: http://www.pdqm.cz/Standards/Business-Excellence/interni-nebo-externi-audit.html
[Přístup získán 17. 1. 2016]
[21] EUROCHEM, 2009. *Metodika interních auditů (2): Rozdělení auditů.* [online]. Dostupné na: http://www.eurochem.cz/index.php?LA=CS&MN=Metodika+intern%EDch+audit%F9+(2)%3A+Rozd%EClen%ED+audit%F9&ProdID=000288060A347D860002E8C2&DT=4097&TXTID=2013&PHPSESSID=fa...
[Přístup získán 17. 1. 2016]
[22] NEŠETŘIL, V. *AKREDITACE – úvod do problematiky*. [online]. 2002. Dostupné na: http://katedry.fmmi.vsb.cz/639/qmag/pr01-cz.htm
[Přístup získán 17. 1. 2016]
[23] ISO. *Akreditační orgány.* [online]. Dostupné na: http://www.iso.cz/akreditacni-organy
[Přístup získán 17. 1. 2016]
[24] ÚNMZ, 2016. *O Úřadu.* [online]. Dostupné na: http://www.unmz.cz/urad/o-uradu
[Přístup získán 17. 1. 2016]
[25] ÚNMZ, 2016. *Úřad vykonává působnost státu v následujících oblastech.* [online]. Dostupné na: http://www.unmz.cz/urad/urad-vykonava-pusobnost-statu-v-nasledujicich-oblastech
[Přístup získán 17. 1. 2016]
[26] ČIA. *O nás.* [online]. Dostupné na: http://www.cia.cz/o-nas.aspx
[Přístup získán 17. 1. 2016]
[27] PURSER, S. Best Practices in Computer Network Defense: Incident Detection and Response. *Standards for Cyber Security*. M.E.Hathaway (Ed.). IOS Press. 2014. s. 97-106. DOI 10.3233/978-1-61499-372-8-97
[28] RAC, 2016. *ISO/IEC 27001:2013.* [online]. Dostupné na: http://www.iso27000.cz/rac/homepage.nsf/CZ/27001
[Přístup získán 22. 1. 2016]

[29] NIST, 2014. *Framework for Improving Critical Infrastructure Cybersecurity.* [online]. Version 1.0. Dostupné na: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf
[Přístup získán 22. 1. 2016]
[30] Systémy jakosti, *ISO/IEC 27001.* [online]. Dostupné na: http://systemyjakosti.cz/produkty/management-bezpecnosti-informaci-isoiec-27001-isms/
[Přístup získán 22. 1. 2016]
[31] ISO survey, 2014. *The ISO Survey of Management System Standard Certifications (2006-2014).* [online]. Dostupné na: http://www.iso.org/iso/iso-survey_2014.zip
[Přístup získán 23. 1. 2016]
[32] NBÚ, 2005. *Informace o hodnocení bezpečnosti informačních technologií. Common Criteria (CC)*. [online]. Dostupné na: https://www.nbu.cz/download/nodeid-757/
[Přístup získán 23. 1. 2016]
[33] Common Criteria. *Certificate Authorizing Members. Certificate Consuming Members.* [online]. Dostupné na: http://www.commoncriteriaportal.org/
[Přístup získán 23. 1. 2016]
[34] ISO, 2012. *ISO/IEC 19790:2012*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=52906
[Přístup získán 23. 1. 2016]
[35] ISO, 2014. *ISO/IEC 24759:2014*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=59142
[Přístup získán 23. 1. 2016]
[36] ISO, 2016. *ISO/IEC 17825:2016*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=60612
[Přístup získán 23. 1. 2016]
[37] CyberSecurity, 2016. *Legislativa v České republice*. [online]. Dostupné na: http://www.cybersecurity.cz/law.html
[Přístup získán 24. 1. 2016]
[38] MALÝ, J., VALENTOVÁ, H. *Závěrečná zpráva z hodnocení dopadů regulace (RIA)*. [online]. Národní bezpečnostní úřad – odbor právní a legislativní. Dostupné na: https://www.govcert.cz/download/nodeid-1304/
[Přístup získán 24. 1. 2016]
[39] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Sbírka zákonů České republiky. 2014. Částka 75. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181
[Přístup získán 24. 1. 2016]
[40] Prováděcí právní předpisy k zákonu č. 181/2014 Sb. Sbírka zákonů České republiky. 2014. Částka 127. Dostupné také z: https://www.nbu.cz/download/nodeid-1067/
[Přístup získán 24. 1. 2016]

[41] GovCERT. *Bezpečnostní role a jejich začlenění v organizaci*. [online]. Dostupné na: http://www.govcert.cz/download/nodeid-589/
[Přístup získán 24. 1. 2016]
[42] NBÚ. *Prováděcí právní předpisy*. [online]. Dostupné na: http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/
[Přístup získán 24. 1. 2016]
[43] Usnesení vlády České republiky č. 105 ze dne 16. 2. 2015 k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020. Dostupné také z: http://dataplan.info/img_upload/7bdb1584e3b8a53d337518d988763f8d/narodni-strategie-kyber.-bezpecnosti-cr-usneseni.pdf
[Přístup získán 24. 1. 2016]
[44] Usnesení vlády České republiky č. 382 ze dne 25. 5. 2015 k Akčnímu plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020. Dostupné také z: https://apps.odok.cz/attachment/-/down/VPRA9X3GGQ3K
[Přístup získán 24. 1. 2016]
[45] Usnesení vlády České republiky č. 781 ze dne 19. 10. 2011 o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. Dostupné také z: https://www.govcert.cz/download/nodeid-562/
[Přístup získán 24. 1. 2016]
[46] Usnesení vlády České republiky č. 624 ze dne 20. 6. 2001. Dostupné také z: http://ezu.cz/wp-content/uploads/2016/01/usneseni_vlady_624_2001.pdf
[Přístup získán 24. 1. 2016]
[47] ISO, 2012. *ISO/IEC 17024:2012*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=52993
[Přístup získán 24. 1. 2016]
[48] ISACA, 2016. *Certification*. [online]. Dostupné na: http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Pages/default.aspx
[Přístup získán 24. 1. 2016]
[49] ISO, 2015. *ISO/IEC TR 27023:2015*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61005
[Přístup získán 25. 1. 2016]
[50] ISO, 2015. *ISO/IEC 27017:2015*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43757
[Přístup získán 25. 1. 2016]
[51] ISO, 2014. *ISO/IEC 27018:2014*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61498
[Přístup získán 25. 1. 2016]

[52] ISO, 2013. *ISO/IEC TR 27019:2013*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43759
[Přístup získán 25. 1. 2016]
[53] ISO, 2015. *ISO/IEC 27033-1:2015*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63461
[Přístup získán 25. 1. 2016]
[54] ISO, 2012. *ISO/IEC 27033-2:2012*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51581
[Přístup získán 25. 1. 2016]
[55] ISO, 2010. *ISO/IEC 27033-3:2010*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51582
[Přístup získán 25. 1. 2016]
[56] ISO, 2014. *ISO/IEC 27033-4:2014*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51583
[Přístup získán 25. 1. 2016]
[57] ISO, 2013. *ISO/IEC 27033-5:2013*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51584
[Přístup získán 25. 1. 2016]
[58] ISO, 2016. *ISO/IEC FDIS 27033-6*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51585
[Přístup získán 25. 1. 2016]
[59] ISO, 2011. *ISO/IEC 27034-1:2011*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44378
[Přístup získán 25. 1. 2016]
[60] ISO, 2015. *ISO/IEC 27034-2:2015*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=55582
[Přístup získán 25. 1. 2016]
[61] ISO, 2016. *ISO/IEC CD 27034-3*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=55583
[Přístup získán 25. 1. 2016]
[62] ISO, 2016. *ISO/IEC CD 27034-5*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=55585
[Přístup získán 25. 1. 2016]
[63] ISO, 2015. *ISO/IEC PDTS 27034-5-1*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67741

[Přístup získán 25. 1. 2016]
[64] ISO, 2016. *ISO/IEC DIS 27034-6*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=60804
[Přístup získán 25. 1. 2016]
[65] ISO, 2016. *ISO/IEC CD 27034-7*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=66229
[Přístup získán 25. 1. 2016]
[66] ISO, 2011. *ISO/IEC 27035:2011*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44379
[Přístup získán 25. 1. 2016]
[67] ISO, 2014. *ISO/IEC 27036-1:2014*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=59648
[Přístup získán 25. 1. 2016]
[68] ISO, 2014. *ISO/IEC 27036-2:2014*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=59680
[Přístup získán 25. 1. 2016]
[69] ISO, 2013. *ISO/IEC 27036-3:2013*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=59688
[Přístup získán 25. 1. 2016]
[70] ISO, 2016. *ISO/IEC DIS 27036-4*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=59689
[Přístup získán 25. 1. 2016]
[71] ISO, 2012. *ISO/IEC 27037:2012*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44381
[Přístup získán 25. 1. 2016]
[72] ISO, 2014. *ISO/IEC 27038:2014*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44382
[Přístup získán 25. 1. 2016]
[73] ISO, 2015. *ISO/IEC 27039:2015*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56889
[Přístup získán 25. 1. 2016]
[74] ISO, 2015. *ISO/IEC 27040:2015*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44404
[Přístup získán 25. 1. 2016]
[75] ISO, 2015. *ISO/IEC 27041:2015*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumbe

r=44405
[Přístup získán 25. 1. 2016]
[76] ISO, 2015. *ISO/IEC 27042:2015*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44406
[Přístup získán 25. 1. 2016]
[77] ISO, 2015. *ISO/IEC 27043:2015*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44407
[Přístup získán 25. 1. 2016]
[78] ISO, 2016. *ISO/IEC DIS 27050-1*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63081
[Přístup získán 25. 1. 2016]
[79] ISO, 2016. *ISO/IEC WD 27050-2*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=66230
[Přístup získán 25. 1. 2016]
[80] ISO, 2016. *ISO/IEC CD 27050-3*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=66231
[Přístup získán 25. 1. 2016]
[81] ISO, 2014. *ISO/IEC NP 27050-4*. [online]. Dostupné na: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=66232
[Přístup získán 25. 1. 2016]
[82] CHAMBERS, J. *What does the Internet of Everything mean for security?* [online]. World Economic Forum. Dostupné na: https://www.weforum.org/agenda/2015/01/companies-fighting-cyber-crime/?utm_content=bufferb0881&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer
[Přístup získán 5. 3. 2016]
[83] ČSN ISO/IEC 27001. *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky*. ÚNMZ. 2014
[84] ČSN ISO/IEC 20000-1. *Informační technologie – Management služeb – Část 1: Požadavky na systém managementu služeb*. ÚNMZ. 2014
[85] ČSN ISO/IEC 15408-1. *Informační technologie – Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 1: Úvod a obecný model*. ÚNMZ. 2013
[86] ČSN ISO/IEC 15408-2. *Informační technologie – Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 2: Bezpečnostní funkční komponenty*. ÚNMZ. 2010
[87] ČSN ISO/IEC 15408-3. *Informační technologie – Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 3: Komponenty bezpečnostních záruk*. ÚNMZ. 2010
[88] ČSN EN ISO/IEC 17024. *Posuzování shody – Všeobecné požadavky na orgány pro certifikaci osob*. ÚNMZ. 2013

Seznam použitých zkratek

AAAO	Asociace akreditovaných a autorizovaných organizací
AFCEA	Armed Forces Communication and Electronics Association
AO	Akreditační orgán
ARP	Address Resolution Protocol
BCM	Business Continuity Management
BS	British Standard
BSI	British Standards Institution
BYOD	Bring Your Own Device
CC	Common Criteria
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security
CD	Committee Draft
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CGEIT	Certified in the Governance of Enterprise IT
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CISO	Chief Information Security Officer
CO	Certifikační orgán
CRISC	Certified in Risk and Information Systems Control
CSIRT	Computer Security Incident Response Team
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
ČIA	Český institut pro akreditaci
ČR	Česká republika
ČSN	Česká technická norma
DDoS	Distibuted Denial of Service
DIS	Draft of International Standard
DLP	Data Loss Protection
DNS	Domain Name Server
DoS	Denial of Service
DPH	Daň z přidané hodnoty
EN	Evropská norma
EOQ	European Organization for Quality
ES	Evropské společenství
EU	Evropská unie
EZÚ	Elektrotechnický zkušební ústav
FDIS	Final Draft of International Standard
FIPS	Federal Information Processing Standard
GPS	Global Position System
IAF	International Accreditation Forum
IBM	International Business Machine
ICT	Information and Communication Technology
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission

ILAC	International Laboratory Accreditation Co-operation
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IRCA	International Risk Control Academy
IROP	Integrovaný regionální operační program
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISVS	Informační systém veřejné správy
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
KB	Kybernetická bezpečnost
KII	Kritická informační infrastruktura
M2M	Machine to Machine
MAC	Medium Access Control
MD	Man-day
MS	Microsoft
NBA	Network Behavior Analysis
NBÚ	Národní bezpečnostní úřad
NCKB	Národní centrum kybernetické bezpečnosti
NP	New Project
OS	Operační systém
OSSTMM	Open Source Security Testing Methodology Manual
PDF	Package Definition File
PP	Protection Profile
RAC	Risk Analysis Consultants
SLA	Service Level Agreement
SMM	Systém Management Mode
SQL	Structured Query Language
SSL	Secure Sockets Layer
ST	Security Target
TCSEC	Trusted Computer System Evaluation Criteria
TOGAF	The Open Group Architecture Framework
TR	Technical Report
ÚIŠ	Úvodní informační školení
ÚNMZ	Úřad pro technickou normalizaci, metrologii a státní zkušebnictví
USA	United States of America
UTM	Unified Threat Management
VIP	Very Important Person
VIS	Významný informační systém
VPN	Virtual Private Network
WD	Working Draft

Seznam obrázků

Seznam tabulek

Seznam příloh

Přílohy

Příloha A - Specifikace aktuálních dílčích norem rodiny ISO/IEC 27XXX

Aktuální verze normy [zdroj]	**Název**	**Předmět a účel**
Normy obsahující přehled a terminologii		
ISO/IEC 27000:2014 [9]	*Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník*	Norma poskytuje organizacím a jednotlivcům: a) přehled řady norem ISMS; b) úvod k ISMS a c) termíny a definice použité v řadě norem ISMS.
Normy specifikující požadavky		
ISO/IEC 27001 :2013 [9]	*Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky*	Norma specifikuje požadavky na ustavení, implementování, provozování, monitorování, přezkoumávání, udržování a zlepšování formalizovaných systémů řízení bezpečnosti informací (ISMS) v kontextu celkových rizik činnosti organizace. Definuje požadavky na implementaci opatření bezpečnosti informací upravených podle potřeb jednotlivých organizací nebo jejich částí. Tuto mezinárodní normu by měly používat všechny organizace bez ohledu na typ, velikost a povahu. Organizace provozující ISMS by měly mít příslušnou shodu doloženou auditem a certifikací.
ISO/IEC 27006 :2015 [9]	*Informační technologie – Bezpečnostní techniky – Požadavky na orgány poskytující audit a certifikaci systémů řízení bezpečnosti informací*	Norma specifikuje požadavky a poskytuje návod pro orgány poskytující audit a certifikaci ISMS v souladu s ISO/IEC 27001, vedle požadavků obsažených v ISO/IEC 17021. Je určena k podpoře akreditace certifikačních orgánů, poskytujících certifikaci ISMS podle ISO/IEC 27001.
Normy popisující obecné směrnice		
ISO/IEC 27002 :2013 [9]	*Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací*	Norma poskytuje seznam obecně akceptovaných cílů opatření a opatření pro doporučené postupy, které mají být použity jako návod k implementaci při výběru a provádění opatření, jejichž cílem je dosáhnout bezpečnosti informací.
ISO/IEC 27003 :2010 [9]	*Informační technologie – Bezpečnostní techniky – Směrnice pro implementaci systému řízení bezpečnosti informací*	Norma poskytuje praktický návod pro implementaci a dále informace pro ustavení, implementování, provozování, monitorování, přezkoumávání, udržování a zlepšování ISMS podle ISO/IEC 27001.

ISO/IEC 27004 :2009 [9]	*Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Měření*	Norma poskytuje návod a doporučení pro vývoj a použití měření, aby se posoudila efektivnost ISMS, cílů opatření a opatření použitých k implementaci a řízení bezpečnosti informací podle specifikace v ISO/IEC 27001.
ISO/IEC 27005 :2011 [9]	*Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací*	Norma poskytuje návod pro implementaci procesně orientovaného přístupu k řízení rizik, aby tak pomohla uspokojivě implementovat a splnit požadavky na řízení rizik bezpečnosti informací uvedené v ISO/IEC 27001.
ISO/IEC 27007 :2011 [9]	*Informační technologie – Bezpečnostní techniky – Směrnice pro audit systémů řízení bezpečnosti informací*	Norma poskytuje návod na provádění auditů ISMS a návod popisující kompetence auditorů systémů řízení bezpečnosti informací vedle návodu obsaženého v ISO 19011, který je obecně použitelný na systémy řízení.
ISO/IEC TR 27008 :2011 [9]	*Informační technologie – Bezpečnostní techniky – Směrnice pro audit opatření ISMS*	Technická zpráva poskytuje návod na přezkoumávání, implementování a provozování opatření včetně kontroly technické shody opatření informačních systémů podle norem bezpečnosti informací ustavených danou organizací. Není určena pro audity systémů řízení.
ISO/IEC 27013 :2015 [9]	*Informační technologie – Bezpečnostní techniky – Návod pro integrovanou implementaci ISO/IEC 27001 a ISO/IEC 20000-1*	Norma poskytuje návod pro integrovanou implementaci ISO/IEC 27001 a ISO/IEC 20000-1. Dává organizacím možnost lepšího pochopení charakteristik, podobností a odlišností ISO/IEC 27001 a ISO/IEC 20000-1 a pomůže tak při plánování integrovaného systému řízení.
ISO/IEC 27014 :2013 [9]	*Informační technologie – Bezpečnostní techniky – Správa bezpečnosti informací*	Norma poskytuje návod týkající se principů a procesů pro správu bezpečnosti informací, kterými může organizace hodnotit, usměrňovat a monitorovat řízení bezpečnosti informací.
ISO/IEC TR 27016 :2014 [9]	*Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Organizační ekonomika*	Technická zpráva poskytuje metody umožňující organizacím lépe ekonomicky rozumět tomu, jak přesněji oceňovat jejich informační aktiva, ohodnotit potenciální rizika, hrozící těmto informačním aktivům, uvědomit si hodnotu, kterou opatření na ochranu informací dodávají těmto informačním aktivům, a určit optimální výši zdrojů, které mají být použity při zabezpečení těchto informačních aktiv.
ISO/IEC TR 27023 :2015 [49]	*Informační technologie – Bezpečnostní techniky – Mapování revidovaných edicí ISO/IEC 27001 a ISO/IEC 27002*	Norma mapuje a srovnává poslední vydání norem ISO/IEC 27001 a ISO/IEC 27002. Účelem tohoto mapování je ukázat návaznost požadavků normy ISO/IEC 27001 na implementační doporučení v ISO/IEC 27002.
Normy popisující směrnice specifické pro jednotlivá odvětví		
ISO/IEC 27010 :2015 [9]	*Informační technologie – Bezpečnostní techniky – Směrnice pro řízení bezpečnosti informací pro meziodvětvové komunikace a komunikace mezi organizacemi*	Norma poskytuje směrnice pro implementaci řízení bezpečnosti informací v rámci komunit sdílejících informace a dodatečně poskytuje opatření a návod specificky souvisící s bezpečnosti informací v meziodvětvových komunikacích a komunikacích mezi organizacemi. Může být použitelná zejména pro výměny a sdílení informací souvisící se zajištěním, údržbou a ochranou kritické infrastruktury organizace nebo dané země.

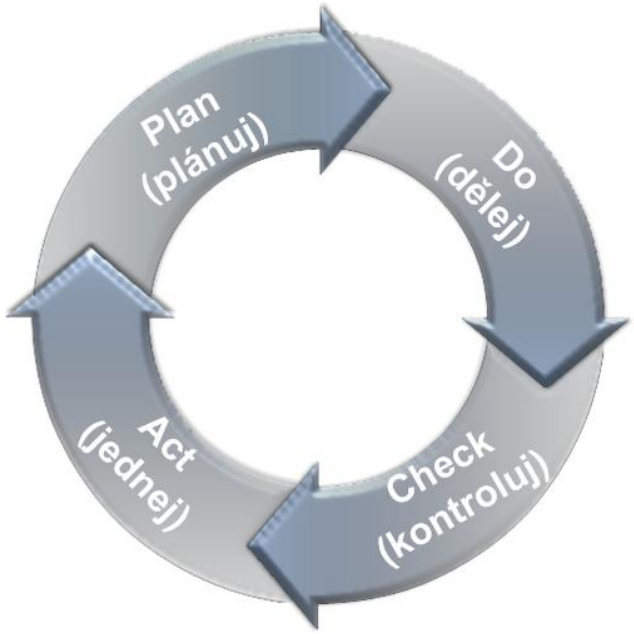
ISO/IEC 27011 :2008 [9]	*Informační technologie – Bezpečnostní techniky – Směrnice pro řízení bezpečnosti informací pro telekomunikační organizace na základě ISO/IEC 27002*	Norma poskytuje směrnice podporující implementaci řízení bezpečnosti informací v telekomunikačních organizacích. Poskytuje telekomunikačním organizacím úpravu směrnic ISO/IEC 27002, týkající se výhradně jejich průmyslového odvětví.
ISO/IEC TR 27015 :2012 [9]	*Informační technologie – Bezpečnostní techniky – Směrnice pro řízení bezpečnosti informací pro finanční služby*	Technická zpráva poskytuje směrnice pro iniciaci, implementaci, udržování a zlepšování bezpečnosti informací v organizacích poskytujících finanční služby. Představuje odborný dodatek k mezinárodním normám ISO/IEC 27001 a ISO/IEC 27002.
ISO/IEC 27017 :2015 [50]	*Informační technologie – Bezpečnostní techniky – Soubor zásad pro kontroly bezpečnosti informací založené na ISO/IEC 27002 pro cloudové služby*	Norma poskytuje doporučení pro zabezpečení cloud computingu. Norma je určena především pro poskytovatele cloudových služeb a jejich zakázníky.
ISO/IEC 27018 :2014 [51]	*Informační technologie – Bezpečnostní techniky – Soubor zásad pro ochranu osobně identifikovatelných informací (PII) ve veřejných cloudech zpracovávajících PII*	Norma obsahuje doporučení ohledně ochrany osobních údajů v cloud computingu. Norma je určena především pro poskytovatele cloudových služeb a jejich zákazníky.
ISO/IEC TR 27019 :2013 [52]	*Informační technologie – Bezpečnostní techniky – Směrnice pro řízení bezpečnosti informací dle ISO/IEC 27002 pro systémy řízení procesů specifických pro energetický průmysl.*	Technická zpráva je určena pro organizace působící v energetickém průmyslu, které implementují ISMS dle ISO/IEC 27002. Pomáhá organizacím v energetickém průmyslu zajistit bezpečnost jejich systémů pro elektronické řízení procesů.
ISO/IEC 27799 :2008 [9]	*Zdravotnická informatika – Řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002*	Norma poskytuje směrnice podporující implementaci řízení bezpečnosti informací ve zdravotnických organizacích. Poskytuje zdravotnickým organizacím úpravu směrnic ISO/IEC 27002, týkající se výhradně jejich odvětví.
Normy popisující směrnice specifické podle oblasti řízení		
ISO/IEC 27031 :2011 [9]	*Informační technologie – Bezpečnostní techniky - Směnice pro připravenost informačních a komunikačních technologií pro kontinuitu podnikání*	Norma popisuje celkový koncept a jednotlivé principy připravenosti informačních a komunikačních technologií na mimořádné události.
ISO/IEC 27032 :2012 [9]	*Informační technologie – Bezpečnostní techniky – Směrnice pro kybernetickou bezpečnost*	Norma poskytuje doporučení pro efektivní sdílení informací a koordinaci řízení incidentů mezi organizacemi, uživateli, vládami a poskytovateli služeb. Zaměřuje se na klíčové hrozby týkající se kyberprostoru, sociální inženýrství, malware, odcizení identity, řízení rizik v kyberprostoru v rámci organizací a poskytování bezpečných a zabezpečených služeb poskytovateli služeb.
ISO/IEC 27033 -1:2015 [53] **-2:2012** [54]	*Informační technologie – Bezpečnostní techniky – Bezpečnost sítě* *- Část 1:Přehled a koncepty* *- Část 2: Směrnice pro návrh a implementaci zabezpečení sítě*	Soubor norem obsahující doporučení pro implementaci protiopatření, které se vztahují k bezpečnosti sítí. Prozatím bylo vydáno prvních pět částí normy, šestá část je ve fázi registrace pro formální odsouhlasení.

-3:2010 [55] **-4:2014** [56] **-5:2013** [57] **ISO/IEC FDIS 27033-6**[58]	*- Část 3: Referenční síťové scénáře - Hrozby, vývojové techniky a otázky tykající se kontrol* *- Část 4: Zabezpečení komunikace mezi sítěmi pomocí bezpečnostních bran* *- Část 5: Zabezpečení komunikace napříč sítěmi využitím virtuálních privátních sítí (VPN)* *- Část 6: Zabezpečení přístupu do bezdrátových sítí*	
ISO/IEC 27034 **-1:2011** [59] **-2:2015** [60] **ISO/IEC CD 27034-3**[61] **ISO/IEC CD 27034-5**[62] **ISO/IEC PDTS 27034 -5-1** [63] **ISO/IEC DIS 27034-6**[64] **ISO/IEC CD 27034-7**[65]	*Informační technologie – Bezpečnostní techniky – Bezpečnost aplikací* *- Část 1: Přehled a koncepty* *- Část 2: Normativní rámec organizace* *- Část 3: Proces řízení bezpečnosti aplikací* *- Část 5: Protokoly a datová struktura kontrol bezpečnosti aplikací* *- Část 5-1: Protokoly a datová struktura kontrol bezpečnosti aplikací - XML schémata* *- Část 6: Případové studie* *- Část 7: Predikce záruk bezpečnosti aplikací*	Jedná se o návod pro manažery, vývojáře, auditory a v neposlední řadě také uživatele ICT poskytující doporučení pro tvorbu, implementaci a užívání aplikačního softwaru. Třetí a pátá část (včetně 5-1) je nyní ve fázi uzavření hlasování/komentování. Šestá část je ve fázi zahájení hlasování o návrhu. Část 7 je ve fázi studování návrhu.
ISO/IEC 27035 :2011 [66]	*Informační technologie – Bezpečnostní techniky – Řízení incidentů bezpečnosti informací*	Norma se zaměřuje na řízení incidentů bezpečnosti informací. Věnuje se postupům včasné detekce incidentů, jejich hlášení, vyhodnocení závažnosti a následné reakce. Dává doporučení pro identifikaci existujících zranitelností, posouzení jejich závažnosti a přijetí odpovídajících opatření.
ISO/IEC 27036 **-1:2014** [67] **-2:2014** [68] **-3:2013** [69] **ISO/IEC DIS 27036-4**[70]	*Informační technologie - Bezpečnostní techniky - Bezpečnost informací pro dodavatelské řetězce* *- Část 1: Přehled a koncepty* *- Část 2: Požadavky* *- Část 3: Směrnice pro bezpečnost dodavatelského řetězce informačních a komunikačních technologií* *- Část 4: Směrnice pro zabezpečení cloudových služeb*	Norma se soustředí na bezpečnost informací pro dodavatelsko-odběratelské vztahy. Normy obsahují doporučení organizacím pro hodnocení a snižování rizik týkajících se outsourcovaných služeb. Prozatím byly vydány první tři části. U čtvrté části bylo zahájeno hlasování o návrhu.
ISO/IEC 27037	*Informační technologie – Bezpečnostní techniky – Směrnice pro identifikaci, sběr, akvizici a uchování digitálních důkazů*	Norma obsahuje především doporučení pro zjišťování, sběr, získávání a

:2012 [71]		uchovávání digitálních důkazů.
ISO/IEC 27038 :2014 [72]	*Informační technologie – Bezpečnostní techniky – Specifikace pro digitální redakci*	Norma poskytuje doporučení pro publikování digitálních dokumentů.
ISO/IEC 27039 :2015 [73]	*Informační technologie – Bezpečnostní techniky – Výběr, nasazení a provoz systémů detekce narušení bezpečnosti (IDPS)*	Norma obsahuje doporučení pro výběr, nasazení a provoz systémů pro detekci a prevenci bezpečnostních průniků (Intrusion Detection and Prevention Systems - IDPS).
ISO/IEC 27040 :2015 [74]	*Informační technologie – Bezpečnostní techniky – Bezpečnost úložišť*	Norma poskytuje doporučení ohledně bezpečného ukládání dat. Standard pomáhá uživatelům, kteří používají počítačové technologie pro ukládání dat, identifikovat a řídit související bezpečnostní rizika.
ISO/IEC 27041 :2015 [75]	*Informační technologie – Bezpečnostní techniky – Směrnice pro zajištění vhodnosti a přiměřenosti incidenty vyšetřujících metod*	Norma poskytuje doporučení pro zajištění důkazů pro digitální metody vyšetřování.
ISO/IEC 27042 :2015 [76]	*Informační technologie – Bezpečnostní techniky – Směrnice pro analýzu a interpretaci digitálních důkazů*	Norma obsahuje doporučení pro analýzu a interpretaci digitálních důkazů.
ISO/IEC 27043 :2015 [77]	*Informační technologie – Bezpečnostní techniky – Principy a procesy vyšetřování incidentů*	Norma definuje doporučené zásady a postupy při vyšetřování digitálních důkazů.
ISO/IEC DIS 27050-1[78] **ISO/IEC WD 27050-2**[79] **ISO/IEC CD 27050-3**[80] **ISO/IEC NP 27050-4**[81]	*Informační technologie – Bezpečnostní techniky – Electronic discovery* *- Část 1: Přehled a koncepty* *- Část 2: Směrnice pro správu a řízení electronic discovery* *- Část 3: Kodex pro electronic discovery* *- Část 4: Připravenost ICT pro electronic discovery*	Čtyřdílná norma by se měla zabývat problematikou zkoumání elektronických stop. První část je ve fázi hlasování o návrhu. Druhá část byla schválena pro registraci na CD. Třetí část prochází studiem a zahajuje se hlasování o CD. Čtvrtá část byla schválena jako nový projekt.

Tabulka 5 - Specifikace aktuálních dílčích norem rodiny ISO/IEC 27XXX
Vlastní tvorba

Příloha B - Kroky prováděné ve smyslu ISO/IEC 27001 v jednotlivých částech PDCA cyklu

<table>
<tr>
<td>Plan (plánuj)
Vymezení rozsahu ISMS
Definování politiky ISMS
Analýza a vyhodnocení rizik
Identifikace a vyhodnocení variant pro zvládání rizik
Výběr cílů opatření a jednotlivých opatření pro zvládání rizik
Získání souhlasu vedení k zavedení a provozu ISMS
Příprava Prohlášení o aplikovatelnosti</td>
<td rowspan="2"> 

Obrázek 6 – PDCA
Vlastní tvorba</td>
<td>Do (dělej)
Formulace plánu zvládání rizik
Implementace plánu zvládání rizik
Implementace bezpečnostních opatření
Implementace školení a vzdělávacích programů
Řízení provozu ISMS
Řízení zdrojů ISMS</td>
</tr>
<tr>
<td>Act (jednej)
Implementace identifikovaných zlepšení ISMS
Provedení nápravných a preventivních akcí
Projednání výsledků a návrhů na zlepšení se zainteresovanými stranami
Zajištění zlepšování dosažených cílů</td>
<td>Check (kontroluj)
Provedení monitorovacích procedur
Provedení pravidelných přezkoumání účinnosti ISMS
Měření účinnosti zavedených opatření
Přezkoumání úrovně zbytkového a akceptovatelného rizika
Provedení interního auditu ISMS
Pravidelná analýza řízení ISMS
Aktualizace bezpečnostních plánů
Zaznamenání činností a událostí s vlivem na ISMS</td>
</tr>
</table>

Tabulka 6 - Kroky prováděné ve smyslu ISO/IEC 27001 v jednotlivých částech PDCA cyklu
Vlastní tvorba

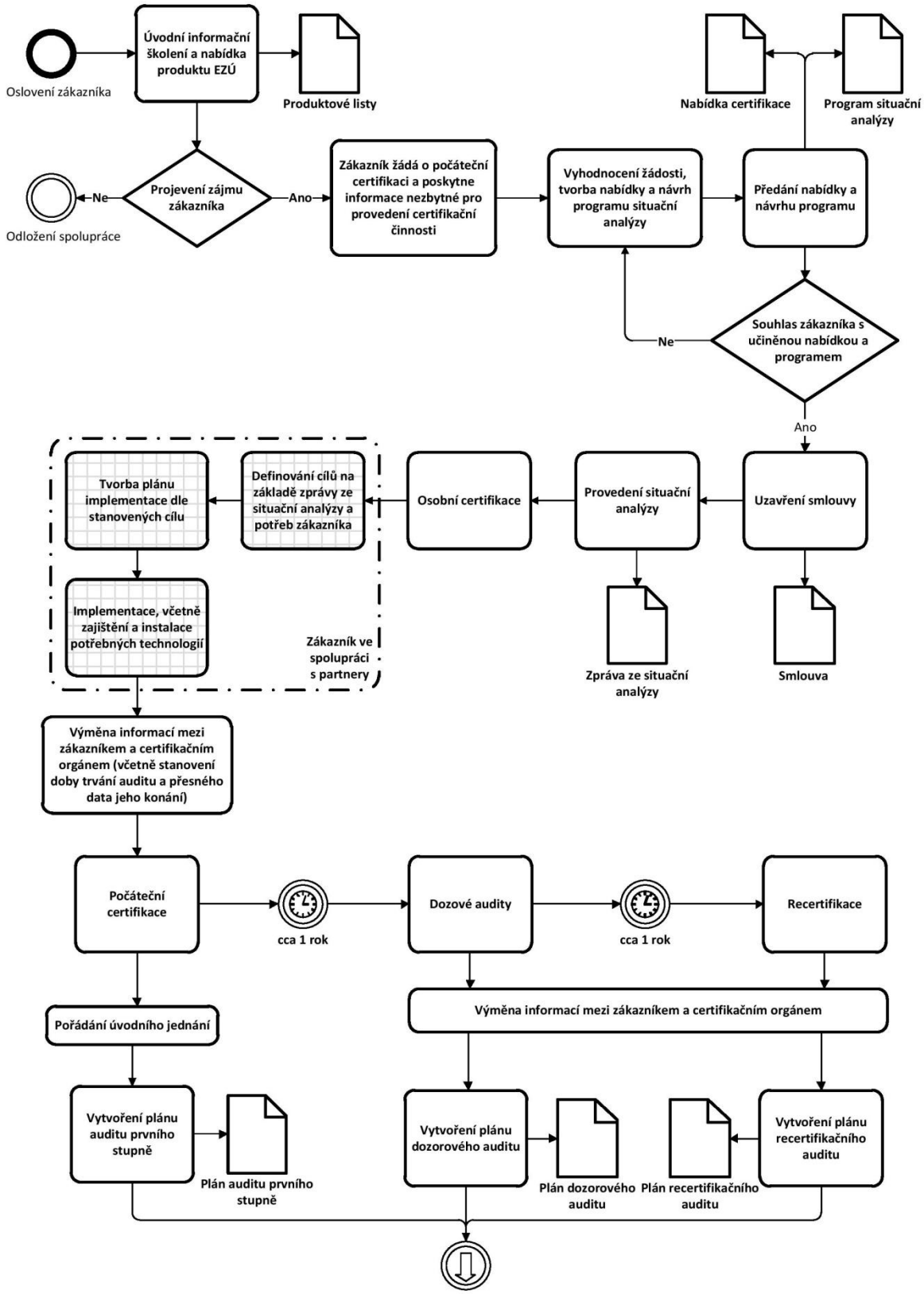
Příloha C – Přehled aktuálních právních a normativních předpisů zahrnutých v návrhu produktu (oblast statní správy)

Identifikace předpisu	Název normy	Oblast použití
ČSN ISO/IEC 27001	Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací	Systémy řízení
Zákon č. 181/2014 Sb.	Zákon o kybernetické bezpečnosti	Systémy řízení
Usnesení vlády č. 624/2001	Usnesení vlády České republiky č. 624/2001	Software
Zákon č. 365/2000 Sb.	Zákon o o informačních systémech veřejné správy	Software
ISO/IEC 19790	Informační technologie - Bezpečnostní techniky - Bezpečnostní požadavky na kryptografické moduly	Bezpečnostní testy
ČSN ISO/IEC 15408-2	Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 2: Bezpečnostní funkční komponenty	Software, Hardware, Přenos dat
ČSN ISO/IEC 15408-3	Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 3: Komponenty bezpečnostních záruk	Software, Hardware, Přenos dat
ČSN ISO/IEC 12207	Informační technologie - Procesy v životním cyklu softwaru	Software
ISO/IEC 27040	Informační technologie - Bezpečnostní techniky - Bezpečnost úložišť	Úložiště dat
ISO/IEC TR 24748-1	Systémové a softwarové inženýrství - Řízení životního cyklu - Část 1: Návod k řízení životního cyklu	Software
ISO/IEC TR 24748-3	Systémové a softwarové inženýrství - Řízení životního cyklu - Část 3: Návod k aplikaci normy ISO/IEC 12207	Software
ISO/IEC 27033-2	Informační technologie - Bezpečnostní techniky - Bezpečnost sítí - Část 2: Pokyny pro návrh a implementaci síťové bezpečnosti	Přenos dat
ČSN ISO/IEC 20000-1	Informační technologie - Management služeb - Část 1: Požadavky na systém managementu služeb	Systémy řízení
ČSN ISO/IEC 20000-2	Informační technologie - Management služeb - Část 2: Pokyny pro použití systémů managementu služeb	Systémy řízení
ČSN ISO/IEC 20000-3	Informační technologie - Management služeb - Část 3: Pokyny pro vymezení rozsahu a použitelnosti ISO/IEC 20000-1	Systémy řízení
ČSN ISO 22301	Ochrana společnosti - Systémy managementu kontinuity podnikání	Systémy řízení
ČSN EN 28000	Specifikace pro systémy managementu bezpečnosti dodavatelských řetězců	Systémy řízení
ISO/IEC 18045	Informační technologie - Bezpečnostní techniky - Metodologie pro ohodnocení bezpečnosti IT	Software, Hardware, Přenos dat
ISO/IEC 14764	Softwarové inženýrství - Procesy životního cyklu softwaru	Software
ISO/IEC 15288	Systémové inženýrství - Procesy životního cyklu systému	Software
ISO/TR 20004	Informační technologie - Bezpečnostní techniky - Vylepšování analýzy zranitelnosti softwaru v rámci ISO / IEC 15408 a ISO / IEC 18045	Software, Hardware, Přenos dat
ISO/IEC TR/19791	Informační technologie - Bezpečnostní techniky - Hodnocení bezpečnosti operačních systémů	Software
ČSN ISO/IEC 27002	Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací	Systémy řízení
ČSN ISO/IEC 27003	Informační technologie - Bezpečnostní techniky - Směrnice pro implementaci systému řízení bezpečnosti informací	Systémy řízení
ČSN ISO/IEC 27005	Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací	Systémy řízení
ISO/IEC 27010	Informační technologie - Bezpečnostní techniky - Řízení informační bezpečnosti pro komunikaci mezi obory a mezi organizacemi	Systémy řízení
ISO/IEC 27016	Informační technologie - Bezpečnostní techniky - Řízení informační bezpečnosti - Ekonomika organizace	Systémy řízení
ISO/IEC 27035	Informační technologie - Bezpečnostní techniky - Řízení incidentů informační bezpečnosti	Systémy řízení
ISO/IEC 27036-2	Informační technologie - Bezpečnostní techniky - Informační bezpečnost pro dodavatelské vztahy - Část 2: Požadavky	Systémy řízení
ISO/IEC 27036-3	Informační technologie - Bezpečnostní techniky - Informační bezpečnost pro dodavatelské vztahy - Část 3: Pokyny pro bezpečnost dodavatelského řetězce informačních a komunikačních technologií	Systémy řízení
ISO/IEC 27013	Informační technologie - Bezpečnostní techniky - Návod pro integrovanou implementaci ISO/IEC 27001 and ISO/IEC 20000-1	Systémy řízení
ISO/IEC 27031	Informační technologie - Bezpečnostní techniky - Pokyny pro připravenost informační a komunikační technologie na kontinuitu podnikání	Systémy řízení
ISO/IEC 27014	Informační technologie - Bezpečnostní techniky - Řízení informační bezpečnosti (Governance)	Systémy řízení

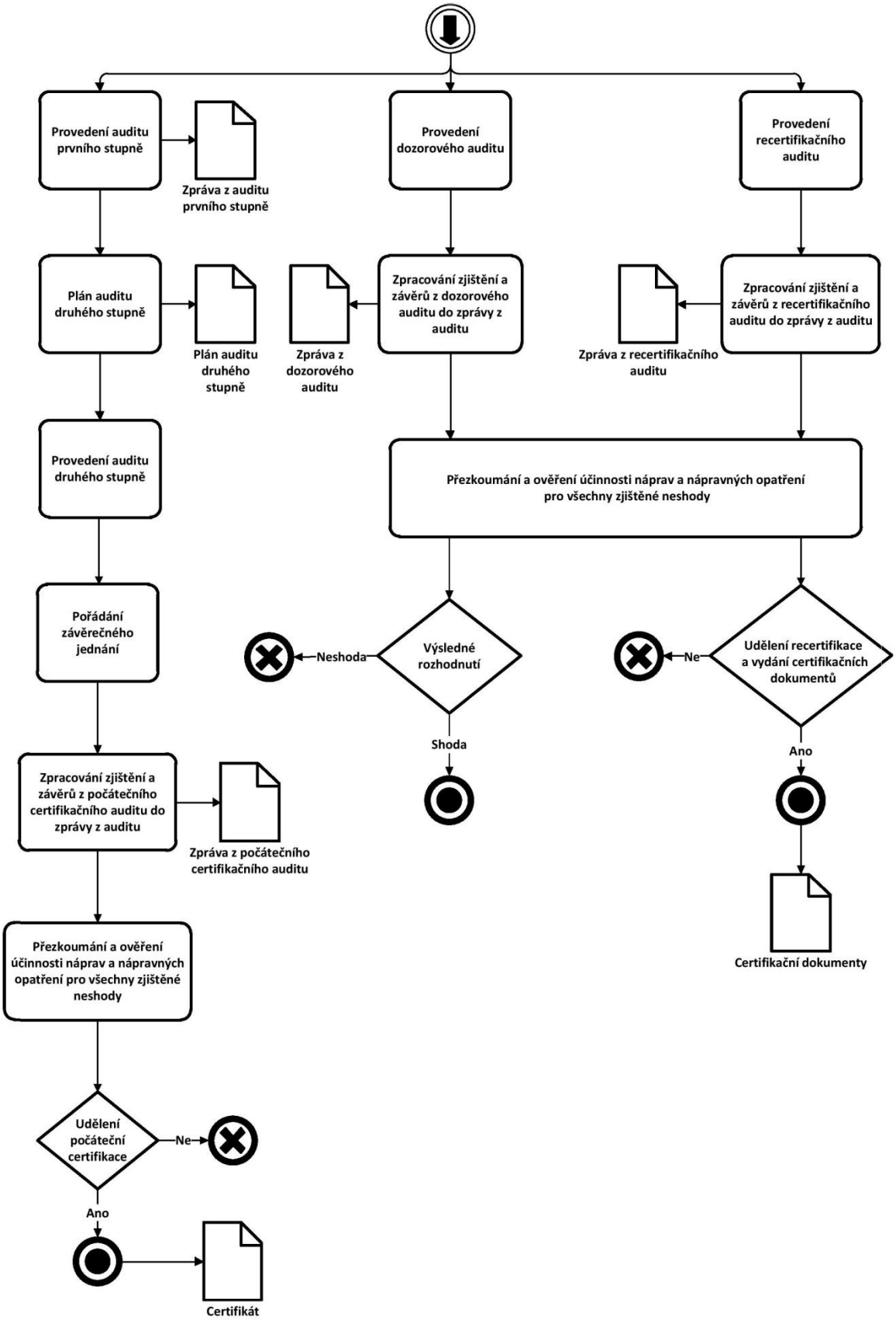
Obrázek 7 - Přehled aktuálních právních a normativních předpisů zahrnutých v návrhu produktu (oblast statní správy)

Vlastní tvorba

Příloha D – Modelový diagram datových toků



Obrázek 8 – Modelový diagram datových toků – část 1
Vlastní tvorba



Obrázek 9- Modelový diagram datových toků – část 2
Vlastní tvorba

Univerzita Hradec Králové
Fakulta informatiky a managementu

Zadání diplomové práce

Autor: **Bc. Michal Hager**

Studium: I14257

Studijní program: N6209 Systémové inženýrství a informatika

Studijní obor: Informační management

Název diplomové práce: **Návrh a realizace produktu za účelem ověřování a certifikace v oblasti kybernetické bezpečnosti dle platných mezinárodních standardů a legislativy České republiky**

Název diplomové práce AJ: Design and realization of a product for the purpose of verification and certification in the field of cyber security in accordance with applicable international standards and legislation of the Czech Republic

Cíl, metody, literatura, předpoklady:

Teoretická část 1. Kybernetická bezpečnost 2. Ověřování (audit) a certifikace v oblasti kybernetické bezpečnosti Praktická část 3. Návrh produktu 4. Realizace produktu 5. Zhodnocení návrhu a realizace produktu

KALAMÁR, Š. - POŽÁR, J. Vybrané aspekty informační bezpečnosti. 1. vyd. Praha: Policejní akademie České republiky, 2010. 190 s. ISBN 978-80-7251-339-0. DOUČEK, P. NOVÁK, L. SVATÁ, V. NEDOMOVÁ, L. Řízení bezpečnosti informací. 1. vyd. Professional Publishing, 2008, 239 s. ISBN 978-80-7431-079-3. HAGER, M. Návrh obchodního modelu poskytujícího služby v oblasti kybernetické bezpečnosti [online]. Technická univerzita v Liberci, Ekonomická fakulta, 2014. Dostupné z: http://theses.cz/id/rn8i8e/. ČSN ISO/IEC 27001. Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. 2014 Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. Sbírka zákonů ČR, 2014, částka 75.

Garantující pracoviště: Katedra informačních technologií,
Fakulta informatiky a managementu

Vedoucí práce: Ing. Agáta Milanov, Ph.D.

Datum zadání závěrečné práce: 21.10.2014