Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky



E-learningový kurz o kybernetické bezpečnosti

DIPLOMOVÁ PRÁCE

Studijní program: Aplikovaná informatika

Studijní obor: Informační management

Autor: Bc. Jakub Šalda

Vedoucí diplomové práce: prof. Ing. Petr Doucek, CSc.

Praha, duben 2019

Prohlášení

Prohlašuji, že jsem bakalářskou práci E-learningový kurz o kybernetické bezpečnosti vypracoval samostatně za použití v práci uvedených pramenů a literatury.

V Praze dne 26. dubna 2019 .....

Jakub Šalda

Poděkování

Rád bych poděkoval panu prof. Ing. Petru Douckovi, CSc. za cenné rady, věcné připomínky a vstřícnost při konzultacích a v průběhu zpracování diplomové práce. Také bych rád poděkoval zaměstnancům Národního úřadu pro kybernetickou a informační bezpečnost, kteří se mnou spolupracovali, za konzultace a pomoc při tvorbě kurzu.

Abstrakt

Práce se zabývá vytvořením školících materiálů pro manažera kybernetické bezpečnosti dle zákona o kybernetické bezpečnosti. Teoretická část se zabývá uvedením do kontextu v oblasti kybernetické bezpečnosti, její regulace legislativou pro určité organizace a systémem řízení bezpečnosti informací. Praktická část práce je vyhrazena samotnému školícímu kurzu. V úvodu kurzu se seznámíme se zákonem a vyhláškou kybernetické bezpečnosti a povinnostmi manažera se zaměřením na státní instituce. Pro vzdělávací účely je navržena fiktivní organizace ve státním sektoru vedoucí ke zvýšení informovanosti a možnosti simulování rozhodování dotčených rolí. Na tuto fiktivní organizaci je vytvořen školící materiál, který je obsahem kurzu. Po ukončení praktické části se tento kurz aplikuje na reálné subjekty a výsledky se vyhodnotí.

Klíčová slova

Kybernetická bezpečnost, zákon o kybernetické bezpečnosti, vyhláška o kybernetické bezpečnosti, systém řízení bezpečnosti informací, role kybernetické bezpečnosti, řízení rizik

JEL klasifikace

K240

Abstract

The thesis deals with the creation of training materials for the cyber security manager according to the Cyber Security Act. The theoretical part deals with the introduction into the context of cyber security, its regulation by legislation for certain organizations and the information security management system. The practical part is dedicated to the training course itself. At the beginning of the course we will become acquainted with the law and the decree of cyber security and the duties of a manager with a focus on state institutions. For educational purposes, a fictional organization in the state sector is designed to increase awareness and the ability to simulate the decisions of the roles involved. Training material which is part of the course, is created for the fictional organization. After the practical part, the course is applied to real subjects and the results are evaluated.

Keywords

Cyber Security, Cyber Security Act, Cyber Security Decree, Information Security Management System, Cyber Security Roles, Risk Management

JEL Classification

K240

Obsah

Úvod 11
1 Kybernetická bezpečnost 13
1.1 Pojmy 13
2 Legislativa kybernetické bezpečnosti 17
2.1 Zákon o kybernetické bezpečnosti 18
2.1.1 Předmět 18
2.1.2 Pojmy 19
2.1.3 Systém zajištění kybernetické bezpečnosti 19
2.1.4 Stav kybernetického nebezpečí 20
2.1.5 Výkon státní správy 21
2.1.6 Kontrola, nápravná opatření a přestupky 21
2.2 Vyhláška o kybernetické bezpečnosti 22
2.2.1 Předmět 23
2.2.2 Pojmy 23
3 Role kybernetické bezpečnosti 24
3.1 Manažer kybernetické bezpečnosti 24
3.2 Architekt kybernetické bezpečnosti 24
3.3 Garant aktiva 25
3.4 Auditor kybernetické bezpečnosti 25
3.5 Výbor kybernetické bezpečnosti 25
4 Řízení bezpečnosti informací 26
4.1 Systém řízení bezpečnosti informací 26
4.2 Základní normy řady 27000 26
4.2.1 ISO/IEC 27001 27
4.2.2 ISO/IEC 27002 28
4.2.3 ISO/IEC 27003 28
4.2.4 ISO/IEC 27004 28
4.2.5 ISO/IEC 27005 28
4.2.6 Další normy 29
4.3 Cybersecurity Framework 30
5 E-learning 31
6 Obsah e-learningového kurzu – teoretická část kurzu 32
6.1 Bezpečnost informací 32
6.1.1 Norma ISO/IEC 27001 33

6.1.2 Vyhláška o kybernetické bezpečnosti ... 33
6.2 Systém řízení bezpečnosti informací ... 34
6.3 Řízení aktiv ... 39
6.3.1 Primární a podpůrná aktiva ... 40
6.3.2 Identifikace a hodnocení aktiv ... 40
6.4 Řízení rizik ... 48
6.4.1 Metodika pro hodnocení rizik ... 48
6.4.2 Kritéria pro přijatelnost rizik ... 49
6.4.3 Zranitelnosti ... 49
6.4.4 Hrozby ... 49
6.4.5 Metoda výpočtu hodnoty rizika ... 50
6.4.6 Plán zvládání rizik ... 54
6.4.7 Prohlášení o aplikovatelnosti ... 54
6.5 Organizační bezpečnost ... 56
6.6 Bezpečnostní role ... 57
6.7 Řízení dodavatelů ... 59
6.7.1 Dodavatelské vztahy ... 59
6.7.2 Evidence významných dodavatelů ... 60
6.7.3 Řízení rizik spojených s dodavatelskými vztahy ... 60
6.7.4 Smlouvy uzavírané s dodavateli ... 61
6.8 Bezpečnost lidských zdrojů ... 62
6.9 Řízení změn ... 62
6.10 Řízení informačního a komunikačního systému ... 63
6.10.1 Akvizice, vývoj a údržba ... 63
6.10.2 Řízení provozu a komunikací ... 63
6.10.3 Řízení přístupu ... 64
6.10.4 Řízení kontinuity činností ... 65
6.11 Audit kybernetické bezpečnosti ... 66
6.12 Bezpečnostní politika a bezpečnostní dokumentace ... 67
6.13 Zvládání kybernetických bezpečnostních událostí a incidentů ... 67
6.13.1 Kybernetické bezpečností události ... 68
6.13.2 Kybernetické bezpečnostní incidenty ... 68
6.13.3 Detekce a vyhodnocování kybernetických bezpečnostních událostí a koordinaci zvládání kybernetických bezpečnostních incidentů ... 70
6.13.4 Detekce kybernetických bezpečnostních událostí ... 72

6.14 Bezpečnost HW 73
6.14.1 Fyzická bezpečnost 73
6.14.2 Bezpečnost komunikačních sítí 73
6.15 Uživatelé a oprávnění 75
6.15.1 Správa a ověřování identit 75
6.15.2 Řízení přístupových oprávnění 78
6.16 SW ochrana 79
6.17 Aplikační bezpečnost 81
6.18 Zajišťování úrovně dostupnosti informací 82
6.19 Průmyslové, řídící a obdobné specifické systémy 83
7 Obsah e-learningového kurzu – praktická část kurzu 84
7.1 Popis organizace 84
7.2 Organizační struktura 85
7.3 ISMS 86
7.4 Identifikace a evidence aktiv 87
7.5 Řízení rizik 87
8 Vyhodnocení e-learningového kurzu 88
8.1 Vyhodnocení teoretického testu 88
8.2 Vyhodnocení úkolů praktické části 88
8.3 Vyhodnocení dotazníku spokojenosti 89
Závěr 90
Literatura 91

Seznam obrázků

Obrázek 1: CIA 32

Obrázek 2: PDCA cyklus v ISMS (ČSN ISO/IEC 27001 2014) 35

Obrázek 3: Graf Přiměřené bezpečnosti za akceptovatelné náklady (Ondrák et al. 2013) 37

Obrázek 4: Model měření bezpečnosti informací (ČSN ISO/IEC 27004 2016) 39

Obrázek 5: Zjednodušený příklad katalogu aktiv 44

Obrázek 6: Zjednodušená analýza rizik 53

Obrázek 7: Zkrácený plán zvládání rizik 54

Obrázek 8: Zkrácené prohlášení o aplikovatelnosti 55

Obrázek 9: Hierarchie bezpečnostních rolí (NÚKIB 2019) 58

Obrázek 10: Schéma řízení kontinuity činností 65

Obrázek 11: Zvládání incidentů dle ZKB (Kintr a Široký 2019) 68

Obrázek 12: Model zabezpečené sítě (Ondrák et al. 2013) 75

Obrázek 13: Životní cyklus identit, Zdroj: icspraha.com 76

Obrázek 14: Vícefaktorová autentizace 77

Obrázek 15: Zjednodušené schéma přijetí pošty 80

Obrázek 16: Příklad asymetrické kryptografie 81

Obrázek 17: Obsah penetračního testování (tns.cz 2019) 81

Obrázek 18: Organizační struktura fiktivní organizace 86

Obrázek 19: Četnost správných odpovědí teoretického testu 88

Obrázek 20: Četnost správných odpovědí praktické části 89

Seznam zkratek

CERT – Computer Emergency Response Team

CIA – Confidentiality, Integrity, Availability

CSIRT – Computer Security Incident Response Team

ICT – informační a komunikační technologie

IS – informační systém

ISMS – Information Security Management Systém

KII – kritická informační infrastruktura

NBÚ – Národní bezpečnostní úřad

NCKB – Národní centrum kybernetické bezpečnosti

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

PDCA – Plan, Do, Check, Act

RTP – Risk Treatment Plan

SoA – Statement of applicability

VIS – významný informační systém

ZS – základní služba

NIST – National Institute of Standards and Technology

CSF – Cybersecurity Framework

IT – informační technologie

Úvod

Oblast kybernetické bezpečnosti jsem si zvolil proto, že toto téma je pro mne velmi zajímavé a v poslední době se stává stále více problematické. Dle mého názoru se bezpečnost informací bude v budoucnu prosazovat čím dál více. Myslím si, že je dobré rozšiřovat bezpečnostní povědomí mezi lidmi, obzvláště pak mezi těmi, kteří jsou součástí kritických částí.

Hlavní otázkou této práce je, zdali pracovníci zastávají bezpečnostní role v oblasti kybernetické bezpečnosti, především manažeři kybernetické bezpečnosti, mají dostatečné znalosti ohledně současných požadavků na bezpečnost udávaných legislativou, popřípadě nejlepší praxí. Problémem současné doby je málo kvalifikovaných lidí.

Hlavním cílem této práce je vytvoření obsahu pro e-learningový kurz. Tento kurz si klade za cíl seznámit účastníky, primárně manažery kybernetické bezpečnosti, se základními pojmy ze zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti. V praktické části tohoto kurzu bude možné si osvojit činnosti spojené s výkonem role manažera kybernetické bezpečnosti z prostředí veřejné sféry, které bude modelováno na vytvořené fiktivní organizaci.

Dalším cílem práce je seznámit čtenáře s kybernetickou bezpečností, legislativou a systémem řízení bezpečnosti informací. Přiblížit zákon i vyhlášku o kybernetické bezpečnosti a povinnosti z nich vyplývající se zaměřením na části týkajících se státních institucí. Dalším cílem práce je seznámit čtenáře s „nejlepší praxí“ v oblasti řízení bezpečnosti informací. Posledním, ale neméně důležitým, cílem je zpětná vazba získaná ať už výsledky z testů nebo dotazníkem spokojenosti s navrženým kurzem.

Předmětem e-learningového kurzu je vyhláška o kybernetické bezpečnosti. Kurz bude sloužit pro orgány veřejné moci, jež jsou správci významných informačních systémů nebo informačního nebo komunikačního systému kritické informační infrastruktury. Cílem kurzu je seznámení účastníků se základními pojmy vyhlášky o kybernetické bezpečnosti a vysvětlení opatření vyplývajících z této vyhlášky.

Metodikou k dosažení cílů této práce je analýza dokumentů pro získání informací. Jako metodika pro vyhodnocování výsledku kurzu a zjištění povědomosti kybernetické bezpečnosti je použito testování. Pro získání zpětné vazby bylo zvoleno dotazování formou dotazníku. Tvořením nejlepší praxe bylo dosaženo řízeným rozhovorem s pracovníky Národního úřadu pro kybernetickou a informační bezpečnost.

Teoretická část této práce se skládá ze čtyř kapitol. V kapitole 1 je krátký úvod do kybernetické bezpečnosti, vysvětlení základních pojmů a terminologie potřebné pro další čtení této práce. V kapitole 2 se budeme věnovat legislativě kybernetické bezpečnosti. Kapitola 3 je vyhrazena pro bezpečnostní role, neboť cílovou skupinou kurzu jsou zaměstnanci, jež je zastávají. Poslední kapitola teoretické části, kapitola 4, popisuje systém řízení bezpečnosti informací, jeho úpravu normami řady ISO 27000 a jeho možnou alternativu.

Praktická část obsahuje také čtyři kapitoly, první z nich, kapitola 5, pojednává o samotném kurzu jako celku. V kapitole 6 jsou předvedeny teoretické podklady pro e-learningový kurz,

tedy studijní materiály pro účastníky. V kapitole 7 je popsána vytvořená fiktivní organizace. V poslední kapitole, kapitola 8, se nachází interpretace získaných výsledků vytvořeného kurzu.

1 Kybernetická bezpečnost

Kybernetická bezpečnost se týká každého člověka, který využívá jakékoli prvky ICT. Kybernetická bezpečnost přestavuje soubor právních, organizačních a vzdělávacích opatření, která jsou přijata z důvodu ochrany počítačových systémů a dalších prvků ICT, aplikací, dat i uživatelů. Tedy stav, kdy dochází k ochraně před kriminální či neautorizovaným užitím reagováním na kybernetické hrozby či útoky a jejich následky.

1.1 Pojmy

Kybernetický prostor

Kybernetický prostor neboli kyberprostor, je virtuální realitou, který je tvořen prvky ICT, které vytváří globální sít. V rámci této sítě mezi sebou jednotlivé počítačové systémy interagují.

Aktivum

Jako aktivum se označuje veškerý hmotný a nehmotný majetek, vlastnost, lidé atd., všechno, co má pro určitou osobu hodnotu.

Primární aktivum je informace nebo služba, kterou zpracovává nebo poskytuje ICT a má hodnotu pro danou organizaci.

Podpůrné aktivum představuje technické aktivum, lokalitu, zaměstnance nebo prvek organizace podílející se na provozu, rozvoji, správě nebo bezpečnosti ICT.

Technickým aktivem se rozumí technické vybavení, komunikační prostředky a programové vybavení ICT. Také sem spadají i objekty, ve kterých jsou tato aktiva umístěna.

Bezpečnostní mechanizmus

Technika použitá pro implementaci bezpečnosti lze označit jako bezpečnostní mechanizmus.

Bezpečnost informací

Bezpečnost informací je definována jako zachování důvěrnosti, integrity a dostupnosti informací, také označováno jako CIA triáda (Confidentiality, Integrity, Availability)

Důvěrnost informací je vlastnost, která charakterizuje zajištění přístupu pouze pro osoby, které jsou k tomu oprávněné.

Integrita informací je vlastnost zajišťující správnost a úplnost dat. Je to jistota, že data nebyla změněna.

Dostupnost informací je vlastnost zajišťující přístupnost a použitelnost informací oprávněnému uživateli v požadovaný okamžik.

Zranitelnost a hrozba

Zranitelnost je slabé místo aktiva.

Hrozba je událost ohrožující bezpečnost a je schopná narušit běžný stav prvků. Hrozba potencionálně může vézt k incidentu.

Riziko, řízení rizik, hodnocení rizik a analýza rizik

Riziko je kombinace hrozby a zranitelnosti. Riziko lze vyjádřit jako možnost, že hrozba se uskuteční tím, že využije zranitelnosti aktiva. Riziko ukazuje, s jakou pravděpodobností může nechtěná událost nastat.

Řízení rizik je koordinace potřebná k řízení a kontrole organizace s ohledem na rizika

Hodnocení rizik je proces analýzy a vyhodnocení rizik. Z výsledku hodnocení rizik je určena významnost rizik a jejich přijatelná úroveň.

Analýza rizik je systematické používání informací pro odhad míry rizika a určení jeho zdrojů

Opatření

Opatření je aktivita umožňující snížení rizika.

Dopad

Dopad je vznik škody v důsledku působení hrozby.

Kybernetické útoky a Kyberkriminalita

Kybernetický útok je jakékoli úmyslné jednání útočníka v kybernetickém prostoru, které může negativně ovlivnit (poškodit) zájmy jiné osoby. V současné době jsou tyto útoky největší hrozbou v rámci kyberprostoru.

Zatímco kyberkriminalitou se rozumí jednání namířené proti počítačovému systému, síti, datům či uživatelům, které je v rozporu se zákonem.

Mezi kybernetické útoky patří například:

- DOS (Denial of Service) – zahlcení informačního kanálu,
- hacking – proniknutí do počítačového systému neautorizovaným způsobem (prolomení bezpečnostního systému),
- phishing – technika získávání citlivých údajů, která necílí na systém, ale na uživatele a klienty systému,
- sniffing – nelegální odposlech nebo záznam telekomunikačního provozu,
- spamming – zasílání nevyžádané pošty.

CERT/CSIRT

CERT (Computer Emergency Response Team) a CSIRT (Computer Security Incident Response Team) jsou týmy, které vznikají na úrovni jednotlivých organizací, které buď jsou poskytovateli Internetu nebo jeho prostředí využívají ke své hlavní činnosti. Tento tým má přesně vymezené pole působnosti, ve kterém jsou zodpovědní za řešení bezpečnostních incidentů a hrozeb.

Národní CERT/CSIRT je nejvyšší instance, kde je možné žádat o zásah, pomoc a intervenci. Primárně zprostředkovávají kontakt, případně koordinaci postupu jednotlivých řešitelů. Dalším úkonem Národního CERT/CSIRT je vzdělávání a spolupráce, tím podporuje vytváření dalších CERT/CSIRT týmů v zemi. Národním CERT/CSIRT v České Republice je CZ.NIC.

Vládní CERT/CSIRT se zaměřuje na oblast státní správy a samosprávy. V této oblasti řeší vzniklé incidenty, které ohrožují bezpečnost státu a jeho služeb. Vládní CERT/CSIRT má možnost přímého zásahu v případě problému a jeho existence je dána legislativou. Vládním CERT/CSIRT v České Republice je Národní centrum kybernetické bezpečnosti, které je výkonnou sekcí Národního úřadu pro kybernetickou a informační bezpečnost. (Kolouch a Bašta 2019)

Kritická informační infrastruktura

Kritická infrastruktura je prvek nebo systém prvků jehož narušení by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu. (Zákon č. 240/2000 Sb. 2000)

Kritická informační infrastruktura (KII) je definována nařízením vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. Aby prvek byl označen jako KII je nutné, aby splňoval průřezová a dopadová kritéria, která jsou uvedena v nařízení. (Nařízení vlády č. 432/2010 Sb. 2010)

Významný informační systém

Významný informační systém (VIS) se stanovuje podle vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. Pro zařazení systému mezi VIS je nutné splnit dopadová určující kritéria a oblastní určující kritéria, které jsou taktéž uvedena v této vyhlášce. Výjimku tvoří systémy, jejichž správcem je obec. Vyhodnocení těchto kritérií posuzuje správce IS. (Vyhláška č. 317/2014 Sb. 2014)

VIS je tedy informační systém spravovaný orgánem veřejné moci, při jehož narušení bezpečnosti může dojít k omezení, popřípadě ohrozit výkon působnosti orgánu veřejné moc. VIS není systém, který spadá do KII či ZS. Seznam všech VIS lze nalézt v příloze 1 této vyhlášky.

Základní služba

Základní služba (ZS) je služba, která je závislá na IS nebo sítích elektronických komunikací ve vybraných odvětvích. Sítě elektronických komunikací zajišťují přímé připojení ke KII.

Kritéria pro stanovení služby jako ZS jsou uvedena ve vyhlášce č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby. Určují se odvětvová a dopadová kritéria, která jsou

uvedená v příloze této vyhlášky. Odvětvová kritéria jsou určena druhem služby, druhem subjektu a speciálním kritériem druhu subjektu, tedy zohledněním významnosti subjektu v jednotlivém odvětví. (Vyhláška č. 437/2017 Sb. 2017)

PDCA cyklus

PDCA cyklus, Demingův cyklus, je iterativní metoda postupného zlepšování, na kterém také stojí i systém řízení bezpečnosti informací. Skládá se ze čtyř hlavních etap, plánování, realizace, ověření výsledku realizace a implementace zlepšení.

2 Legislativa kybernetické bezpečnosti

Ústředním orgánem státní správy v České republice, který mimo jiné zastával správu v oblasti kybernetické bezpečnosti byl Národní bezpečnostní úřad (NBÚ). NBÚ stále působí v oblastech ochrany utajovaných informací a bezpečnostní způsobilostí. (nbu.cz 2019)

Právní regulace kybernetické bezpečnosti stále prochází dynamickým vývojem. Legislativa musí reagovat na aktuální hrozby a kybernetické útoky a zavádět změny, což je jednou z příčin vzniku Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB), který po NBÚ převzal práva a povinnosti v oblasti kybernetické bezpečnosti, ochranu utajovaných informací v oblasti ICT a kryptografickou ochranu. NÚKIB zároveň vystupuje jako ústřední správní orgán v uvedených oblastech. Kromě těchto činností má NÚKIB na starosti také problematiku neveřejné služby v rámci družicového systému Galileo.

Hlavním zákonem v oblasti kybernetické bezpečnosti je Zákon o kybernetické bezpečnosti, nicméně dílčí aspekty ochrany České republiky před kybernetickými útoky je možné nalézt i v jiných právních předpisech.

Další zákony, které se dotýkají kybernetické bezpečnosti:

- zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů,
- zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů,
- zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů,
- zákon č. 240/2000 Sb., o krizovém řízení a změně některých zákonů (krizový zákon), ve znění pozdějších předpisů,
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů,
- zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů,
- zákon č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů,
- zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů,
- zákon č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů,
- zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů,
- zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů,
- zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů,
- zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim,
- zákon č. 89/2012 Sb., občanský zákoník,
- zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

Kybernetické bezpečnosti se týkají i následující ústavní zákony:

- Ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů
- Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů
- Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky

Kromě zákonů je kybernetická bezpečnost regulována i prováděcími předpisy, z nichž momentálně nejvýznamnějším je Vyhláška o kybernetické bezpečnosti.

Mezi další prováděcí předpisy zasahující do oblasti kybernetické bezpečnosti patří:

- nařízení vlády č. 522/2005 Sb., kterým se stanoví seznamy utajovaných informací, ve znění pozdějších předpisů,
- 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 pozdějších předpisů,
- vyhláška č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy),
- nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury,
- vyhláška 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů,
- vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích,
- vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby. (Kolouch a Bašta 2019)

2.1 Zákon o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti (ZKB) je zákon č.181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

Cílem tohoto zákona je zajištění bezpečného fungování české informační společnosti, tak že vytváří systém bezpečnostních opatření, která mají zajistit, že v případě incidentu se neohrozí celkové fungování informačních a komunikačních systémů. (Kolouch a Bašta 2019)

2.1.1 Předmět

Předmětem zákona o kybernetické bezpečnosti je:

- práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti,
- zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů. (Zákon č. 181/2014 Sb. 2014)

2.1.2 Pojmy

V zákoně o kybernetické bezpečnosti jsou definovány a využívány tyto pojmy:

- kybernetický prostor – digitální prostředí,
- kybernetická bezpečnost – souhrn právních, organizačních, technických a vzdělávacích prostředků k zajištění ochrany kybernetického prostoru,
- kritická informační infrastruktura – prvek nebo systém prvků kritické infrastruktury,
- bezpečnost informací – zajištění důvěrnosti, integrity a dostupnosti,
- správce IS – určují účel zpracování informací a podmínky provozování IS,
- správce ICT – účel a podmínky provozu ICT,
- provozovatel IS/ICT – zajišťují funkčnost technických a programových prostředků,
- významná síť – síť elektronických komunikacích k propojení do veřejné komunikační sítě nebo kritické infrastruktuře,
- základní služba – její poskytování je závislé na sítí elektronických komunikací a její narušení má významný dopad,
- IS základní služby – na jeho fungování je závislé poskytování základní služby,
- provozovatel základní služby – poskytuje základní službu a která je určena Národním úřadem pro kybernetickou a informační bezpečnost a
- digitální služba – služba informační společnosti (například on-line tržiště, vyhledávače, cloud). (Zákon č. 181/2014 Sb. 2014)

Orgány a osobami, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti, jsou:

a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací, pokud není orgánem nebo osobou podle písmene b),
b) orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem nebo provozovatelem komunikačního systému podle písmene d),
c) správce a provozovatel informačního systému KII,
d) správce a provozovatel komunikačního systému KII,
e) správce a provozovatel VIS,
f) správce a provozovatel informačního systému základní služby, pokud nejsou správcem nebo provozovatelem podle písmene c) nebo d),
g) provozovatel základní služby, pokud není správcem nebo provozovatelem podle písmene f), a
h) poskytovatel digitální služby. (Zákon 181/2014 Sb. 2014)

2.1.3 Systém zajištění kybernetické bezpečnosti

Bezpečnostní opatření

Souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v IS a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru. Zákon rozděluje tato opatření na organizační a technická. (Zákon č. 181/2014 Sb. 2014)

Organizační opatření se týkají především ustanovování systému řízení bezpečnosti informací, jeho plánování, kontroly, zlepšování atd. Tedy například odpovídají na otázku, proč vůbec

zavádět konkrétní technické opatření a řeší plánování jeho nasazení. Technická opatření jsou konkrétní technická řešení, která zajišťují požadované bezpečnostní funkce.

Jednotlivá opatření, jsou blíže specifikována a popsána ve Vyhlášce o kybernetické bezpečnosti.

Kybernetická bezpečnostní událost a kybernetický bezpečnostní incident

Kybernetická bezpečnostní událost je událost, která může způsobit narušení bezpečnosti informací. Kybernetický bezpečnostní incident je narušení bezpečnosti informací, jejichž evidenci vede Úřad (NÚKIB).

Opatření jsou úkony, které se provádějí z důvodu ochrany před hrozbou, kybernetickým bezpečnostním incident nebo k řešení bezpečnostního incidentu. a patří sem varování, reaktivní opatření a ochranné opatření.

Národní CERT zajišťuje v rozsahu stanoveném ZKB sdílení informací na národní a mezinárodní úrovni v oblasti kybernetické bezpečnosti.

Provozovatel národního CERT provádí následující činnosti:

- Přijímá a uchovává oznámení kontaktních údajů.
- Přijímá a eviduje hlášení o kybernetických bezpečnostních incidentech.
- Vyhodnocuje kybernetické bezpečnostní incidenty.
- Poskytuje metodickou podporu, pomoc a součinnost při výskytu kybernetického bezpečnostního incidentu.
- Provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti.
- Plní roli týmu CSIRT podle příslušného předpisu Evropské unie.
- Spolupracuje s týmy CSIRT jiných členských států.

Vládní CERT jako součást Úřadu (NÚKIB):

- Přijímá oznámení kontaktních údajů.
- Přijímá hlášení o kybernetických bezpečnostních incidentech.
- Vyhodnocuje kybernetické bezpečnostní incidenty.
- Poskytuje metodickou podporu, pomoc a součinnost při výskytu kybernetického bezpečnostního incidentu.
- Přijímá údaje od provozovatele národního CERT a tyto údaje vyhodnocuje.
- Provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti.
- Plní roli týmu CSIRT podle příslušného předpisu Evropské unie.
- Spolupracuje s týmy CSIRT jiných členských států. (Zákon č. 181/2014 Sb. 2014)

2.1.4 Stav kybernetického nebezpečí

Stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost služeb elektronických komunikací anebo bezpečnost a integrita sítí elektronických komunikací, a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České

republiky ve smyslu zákona upravujícího ochranu utajovaných informací. O vyhlášení stavu kybernetického nebezpečí rozhoduje ředitel Úřadu. (Zákon č. 181/2014 Sb. 2014)

2.1.5 Výkon státní správy

Úřad

Správní úřad pro oblast kybernetické bezpečnosti a pro vybrané oblasti ochrany utajovaných informací podle zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti.

Úřad má za povinnost:

- stanovit bezpečnostní opatření,
- vydávat opatření,
- plnit stanovené úkoly ve vybraných oblastech ochrany utajovaných informací,
- vést evidence,
- ukládat správní tresty,
- působit jako koordinační orgán ve stavu kybernetického nebezpečí,
- zajišťovat mezinárodní spolupráci v oblasti kybernetické bezpečnosti,
- ověřovat každé 2 roky aktuálnost určení prvků KII,
- určovat provozovatele základní služby a informační systém základní služby,
- informovat veřejnost o kybernetickém bezpečnostním incidentu,
- provádět analýzu a monitoring kybernetických hrozeb a rizik a
- plnit další úkoly v oblasti kybernetické bezpečnosti stanovené ZKB a ve vybraných oblastech utajovaných informací podle zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti. (Zákon č. 181/2014 Sb. 2014)

2.1.6 Kontrola, nápravná opatření a přestupky

Kontrola plnění povinností stanovené zákonem o kybernetické bezpečnosti a opatřeními obecné povahy vydané Úřadem se provádí dle kontrolního řádu a vykonává ji Úřad. Kontrolu Úřadu vykonává Poslanecká sněmovna, která k tomuto účelu zřizuje zvláštní kontrolní orgán.

Při zjištěných nedostatcích během kontroly Úřad uloží odstranění, popřípadě určí jakým způsobem.

Poskytovatel služby se může dopustit například těchto přestupků:

- nesplnění za stavu kybernetického nebezpečí povinnost uloženou Úřadem v rozhodnutí nebo v opatření obecné povahy,
- nesplnění některé z povinností uloženou nápravným opatřením.

Správce nebo provozovatel se může dopustit například těchto přestupků:

- neprovedení bezpečnostních opatření anebo nevede bezpečnostní dokumentaci,
- neohlášení kybernetického bezpečnostního incidentu,
- nesplnění povinností uložené Úřadem,

- nepředání dat, provozních údajů a informací,
- Neoznámení kontaktních údajů nebo jejich změnu Úřadu.

Detailní přehled všech přestupků pro jednotlivé orgány a osoby jsou uvedeny v §25 ZKB. Za nejvážnější přestupky lze uložit pokutu až do výše 5 000 000 Kč. (Zákon č. 181/2014 Sb. 2014)

2.2 Vyhláška o kybernetické bezpečnosti

Vyhláška o kybernetické bezpečnosti (VKB) je vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). VKB obsahuje soubor opatření za účelem zvýšení bezpečnosti kybernetického prostoru. Vyhláška navazuje na §5 ZKB, který pojednává o bezpečnostních opatřeních.

Jak již bylo zmíněno bezpečnostní opatření se dělí na organizační a technická a stejně tak je postavena i struktura vyhlášky.

Paragrafy týkající se organizačních opatření jsou:

- § 3 - Systém řízení bezpečnosti informací,
- § 4 - Řízení aktiv,
- § 5 - Řízení rizik,
- § 6 - Organizační bezpečnost,
- § 7 - Bezpečnostní role,
- § 8 - Řízení dodavatelů,
- § 9 - Bezpečnost lidských zdrojů,
- § 10 - Řízení provozu a komunikací,
- § 11 - Řízení změn,
- § 12 - Řízení přístupu,
- § 13 - Akvizice, vývoj a údržba,
- § 14 - Zvládání kybernetických bezpečnostních událostí a incidentů,
- § 15 - Řízení kontinuity činností a
- § 16 - Audit kybernetické bezpečnosti.

Paragrafy týkající se technických opatření jsou:

- § 17 - Fyzická bezpečnost,
- § 18 - Bezpečnost komunikačních sítí,
- § 19 - Správa a ověřování identit,
- § 20 - Řízení přístupových oprávnění,
- § 21 - Ochrana před škodlivým kódem,
- § 22 - Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů,
- § 23 - Detekce kybernetických bezpečnostních událostí,
- § 24 - Sběr a vyhodnocování kybernetických bezpečnostních událostí,
- § 25 - Aplikační bezpečnost,

- § 26 - Kryptografické prostředky,
- § 27 - Zajišťování úrovně dostupnosti informací a
- § 28 - Průmyslové, řídicí a obdobné specifické systémy.

Obsah těchto opatření je podrobně popsán v podobné struktuře v kapitole 6.

2.2.1 Předmět

Předmětem vyhlášky o kybernetické bezpečnosti je:

- obsah a struktura bezpečnostní dokumentace,
- obsah a rozsah bezpečnostních opatření,
- typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů,
- náležitosti a způsob hlášení kybernetického bezpečnostního incidentu,
- náležitosti oznámení o provedení reaktivního opatření a jeho výsledku,
- vzor oznámení kontaktních údajů a jeho formu a
- způsob likvidace dat, provozních údajů, informací a jejich kopií. (Vyhláška č. 82/2018 Sb. 2018)

2.2.2 Pojmy

Ve vyhlášce o kybernetické bezpečnosti jsou definovány a využívány tyto pojmy:

- administrátor – zajišťuje správu, provoz, použití, údržbu, a bezpečnost technického aktiva,
- akceptovatelné riziko – není nutné jej zvládat s opatřeními,
- bezpečnostní politika – soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv,
- hodnocení rizik – proces identifikace, analýzy a vyhodnocení rizik,
- hrozba – potenciální příčina, která může způsobit škodu,
- podpůrné aktivum – technické aktivum, zaměstnanci a dodavatelé,
- primární aktivum – informace nebo služba, kterou zpracovává nebo poskytuje IS/ICT,
- riziko – možnost, že určitá hrozba využije zranitelnosti aktiva a způsobí škodu,
- řízení rizik – činnost zahrnující hodnocení rizik, výběr a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik,
- systém řízení bezpečnosti informací – způsob ustavení, zavádění, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací a dat,
- technické aktivum – vybavení, jejichž selhání může mít dopad na IS/ICT,
- uživatel – využívá aktiva,
- vrcholové vedení – řídí povinnou osobu,
- významný dodavatel – provozovatel IS/ICT,
- významná změna – může mít vliv na kybernetickou bezpečnost a představuje vysoké riziko a
- zranitelnost – slabé místo aktiva nebo opatření, které může být zneužito jednou nebo více hrozbami. (Vyhláška č. 82/2018 Sb. 2018)

3 Role kybernetické bezpečnosti

VKB definuje tyto bezpečnostní role – manažer kybernetické bezpečnosti, architekt kybernetické bezpečnosti, auditor kybernetické bezpečnosti a garant aktiva.

Mezi další role vystupující z hlediska bezpečnosti informací patří administrátor, uživatel a dodavatel.

Někdy se také můžeme setkat s rolemi analytik kybernetické bezpečnosti, který provádí analýzy zranitelností a dává doporučení pro implementace bezpečnostních opatření, nebo technik kybernetické bezpečnosti, jež vyvíjí SW bezpečnostní opatření, systémy, kontroly, protokoly atd. v oblasti bezpečnosti.

3.1 Manažer kybernetické bezpečnosti

Manažer kybernetické bezpečnosti je bezpečnostní role odpovědná za systém řízení bezpečnosti informací v omezeném rozsahu dle VKB na systémy, které spadají pod regulaci ZKB. Manažer kybernetické bezpečnosti je tedy zodpovědný za systém řízení bezpečnosti informací pouze u těchto systémů. Jedná se o zcela klíčovou roli pro správné nastavení fungování systému řízení bezpečnosti informací. Pro tuto činnost proto musí prokázat odbornou způsobilost a praxi. Délka praxe je stanovena na 3 roky a to proto, že za tuto dobu je možné získat dostatek zkušeností pro výkon této role. V případě absolvování vysokoškolského studia je délka požadované praxe zkrácena na 1 rok. Manažer kybernetické bezpečnosti má dále povinnost informovat vrcholové vedení o činnostech vyplývajících z rozsahu jeho odpovědnosti a stavu systému řízení bezpečnosti informací, cílem je, aby docházelo k usnadnění prosazování konceptu systému řízení bezpečnosti informací a k dobré informovanosti a zainteresovanosti vrcholového vedení do problematiky kybernetické bezpečnosti. Vzhledem k náplni práce manažera kybernetické bezpečnosti nesmí být osoba vykonávající tuto roli pověřena výkonem rolí odpovědných za provoz informačního a komunikačního systému. Organizační zařazení osoby zastávající roli manažera je na uvážení povinné osoby. V praxi bývá někdy problém, pokud manažer kybernetické bezpečnosti zároveň zastává některou z výkonných funkcí, například vedoucí ICT oddělení, auditor kybernetické bezpečnosti apod. V takových případech zpravidla nemůže nebo nechce prosazovat všechny aspekty systému řízení bezpečnosti informací napříč organizací. (Vyhláška č. 82/2018 Sb. 2018)

3.2 Architekt kybernetické bezpečnosti

Architekt kybernetické bezpečnosti je bezpečnostní role odpovědná za zajištění návrhu implementace bezpečnostních opatření tak, aby byla zajištěna bezpečná architektura informačního a komunikačního systému, až například po bezpečnost na aplikační úrovni. Výkonem této role může být pověřena osoba, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s navrhováním implementace bezpečnostních opatření a zajišťováním architektury bezpečnosti. Časové požadavky na praxi jsou stejné jako u role

manažer kybernetické bezpečnosti, tedy doba nejméně tří let nebo doba jednoho roku v případě, že osoba vykonávající tuto roli absolvovala studium na vysoké škole. Výkon této role je možné rozdělit mezi více osob při zohlednění jejich zaměření a vzhledem k využívaným technologiím u povinné osoby. Osoba vykonávající roli architekta kybernetické bezpečnosti nesmí být zároveň osobou odpovědnou za provoz informačního a komunikačního systému regulovaného zákonem o kybernetické bezpečnosti, a to ze stejného důvodu jako je tomu u role manažer kybernetické bezpečnosti. (Vyhláška č. 82/2018 Sb. 2018)

3.3 Garant aktiva

Garant kybernetické bezpečnosti je bezpečnostní role odpovědná za zajištění rozvoje, použití a bezpečnosti aktiva. Hlavním úkolem je zajištění důvěrnosti, dostupnosti a integrity aktiv. (Vyhláška č. 82/2018 Sb. 2018)

3.4 Auditor kybernetické bezpečnosti

Auditor kybernetické bezpečnosti je bezpečnostní role odpovědná za provádění auditu kybernetické bezpečnosti. Požadavky na odbornou způsobilost praxí jsou stejné jako u bezpečnostních rolí manažer kybernetické bezpečnosti a architekt kybernetické bezpečnosti. V případě auditora kybernetické bezpečnosti je klíčové, aby auditor vykonával svoji činnost nestranně, a nesmí být pověřen výkonem jiných bezpečnostních rolí. (Vyhláška č. 82/2018 Sb. 2018)

3.5 Výbor kybernetické bezpečnosti

Výbor kybernetické bezpečnosti je tvořen osobami s příslušnými pravomocemi a odbornou způsobilostí pro celkové a řízení a rozvoj systému řízení bezpečnosti informací a osobami významně se na systému řízení bezpečnosti informací a koordinaci souvisejících činnostech podílející. Alespoň jedním ze členů výboru kybernetické bezpečnosti musí být zástupce vrcholového vedení, nebo jím pověřená osoba, a manažer kybernetické bezpečnosti. Vzhledem k rozhodovací pravomoci vrcholového vedení by spolu měli vrcholové vedení a manažer kybernetické bezpečnosti úzce komunikovat. (Vyhláška č. 82/2018 Sb. 2018)

4 Řízení bezpečnosti informací

Obecně řízení bezpečnosti informací je spíše problém na úrovni organizace než samotné zavádění technických opatření, z toho vyplývá, že se hlavně bude jednat o zajištění na úrovni managementu. Pro zvládnutí této problematiky je vhodné implementovat systém řízení bezpečnosti informací.

4.1 Systém řízení bezpečnosti informací

Systém řízení bezpečnosti informací (angl. Information Security Management System, zkráceně ISMS) je součást řízení organizace založená na přístupu k rizikům. Činnosti ISMS jsou ustanovení, zavádění, provoz, monitorování, přezkoumání, údržba a zlepšování bezpečnosti informací.

ISMS lze také definovat jako rámec politik, postupů, směrnic a přidružených zdrojů k dosažení stanovených cílů. Cílem ISMS je eliminace možné ztráty nebo poškození informačních aktiv. Tím se dosáhne tak, že se určí ta aktiva, která mají být chráněna, jsou identifikována a řízena možná rizika bezpečnosti informací a také jsou zavedena opatření s požadovanou úrovní záruk, která jsou následně kontrolována.

ISMS se dotýká těchto základních okruhů:

- IT bezpečnost,
- Komunikační bezpečnost,
- Personální bezpečnost,
- Administrativní bezpečnost,
- Fyzická bezpečnost,
- Dokumentace a
- Bezpečnostní funkce a mechanizmy. (Ondrák et al. 2013)

Etapy zavádění a jednotlivé požadavky ISMS, které vyplývají z VKB jsou obsahem praktické části této práce a jsou stručně uvedeny v kapitole 6.2.

4.2 Základní normy řady 27000

Norma ISO/IEC 27000:2018 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Přehled a slovník obsahuje přehled systémů řízení bezpečnosti informací, které tvoří předmět rodiny norem ISMS a definuje pojmy a terminologický slovník pro další normy z této série.

Rodina norem ISMS zahrnuje normy, které definují požadavky na ISMS, normy, jež tyto požadavky certifikují, normy pro přímou podporu, podrobné pokyny pro všechny procesy PDCA cyklu, normy pro posuzování shody ve vztahu k ISMS a další.

4.2.1 ISO/IEC 27001

Hlavní normou této řady je norma ISO/IEC 27001:2013 (popř. v českém překladu ČSN ISO/IEC 27001:2014) Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky. První verze této normy vznikla v roce 2005 a nahradila tak britskou normu BS 7799-2.

Norma poskytuje doporučení, jak aplikovat vybraná opatření ISO/IEC 27002, díky niž si mohou organizace na základě hodnocení rizik vybrat ta opatření, která mohou aplikovat ve svém prostředí. (Ondrák et al. 2013)

Norma klade důraz na to, aby ISMS byl součástí procesů a celkové struktury řízení organizace. Dále je doporučeno, aby bezpečnost informací byla zvažována již při návrhu procesů, informačních systémů a opatřeních. Zároveň se předpokládá, že implementace ISMS bude přizpůsobena potřebám organizace. (ČSN ISO/IEC 27001 2014)

Základní požadavky na ISMS dle normy ISO/IEC 27001

Jako první požadavek je v této normě uveden kontext organizace.

Ten cílí na:

- porozumění organizace a jejímu kontextu,
- určení a zainteresovaných stran a jejich požadavků které jsou relevantní k ISMS a
- stanovení rozsahu ISMS a aspekty, které je třeba zvážit při jeho stanovení.

Rozsah systému ISMS musí být dostupný jako dokumentovaná informace.

Požadavek vůdčí role cílí na vrcholové vedení a jejich závazky vůči ISMS, například stanovení politiky bezpečnosti informací, zajištění integrace požadavků ISMS do procesu organizace, zajištění dostupnosti zdrojů potřebných pro ISMS, určení rolí, odpovědností a pravomoci v oblasti bezpečnosti informací atd. Politika bezpečnosti informací tyto závazky zahrnuje a také musí být dostupná jako dokumentovaná informace, komunikována v rámci organizace a přiměřeně dostupná zainteresovaným stranám.

Dalším požadavkem je plánování, myšleno jako plánování opatření, cílů bezpečnosti informací a jejich dosažení.

Požadavky na podporu obsahují:

- určení a zajištění zdrojů potřebných pro ISMS,
- určení a řízení nezbytných kompetencí osob,
- jejichž práce má vliv na bezpečnost informací,
- povědomí zaměstnanců politiky bezpečnosti informací, svého přínosu k efektivnosti ISMS a důsledků nepřizpůsobení se požadavkům ISMS a
- určení potřeby pro interní a externí komunikaci.

Při provozování ISMS se:

- posuzují rizika bezpečnosti informací v pravidelných intervalech
- implementuje plán ošetření rizik bezpečnosti informací

Při hodnocení výkonnosti probíhá:

- vyhodnocování výkonnosti bezpečnosti informací a efektivnost ISMS,
- interní audit v plánovaných intervalech a
- přezkoumávání vedením organizace v pravidelných intervalech pro zajištění jeho vhodnosti, přiměřenosti a efektivnosti.

Závěrem je zavádění potřebných opatření a požadované neustálé zlepšování ISMS. (ČSN ISO/IEC 27001 2014)

Norma obsahuje přílohu, ve které jsou uvedené cíle opatření a jednotlivá opatření, které jsou strukturovaná podle obsahu normy.

4.2.2 ISO/IEC 27002

Norma ISO/IEC 27002:2013 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací je sbírka nejlepších bezpečnostních praktik a lze ji využít jako kontrolní seznam správného zavedení bezpečnosti informací. Obsahuje 114 strukturovaných oblastí doporučení rozdělených do 11 kapitol, ve kterých je více než 5000 přímých a odvozených bezpečnostních opatření, které podporují dosažení podnikatelských cílů. (Ondrák et al. 2013; RiskAnalysisConsultants 2019)

4.2.3 ISO/IEC 27003

Norma ISO/IEC 27003:2017 Informační technologie - Bezpečnostní techniky - Směrnice pro implementaci systému řízení bezpečnosti informací poskytuje doporučení pro ustanovení a implementaci ISMS v souladu s požadavky normy ISO/IEC 27001. Norma vysvětluje proces návrhu a implementace ISMS a výsledkem je finální plán implementace projektu ISMS. Příloha normy obsahuje kontrolní seznam činností potřebných k ustanovení a implementaci ISMS, popis rolí a odpovědností bezpečnosti informací, informace o průběhu interního auditu, struktury politik a informace o monitorování a měření bezpečnosti informací. (Ondrák et al. 2013)

4.2.4 ISO/IEC 27004

Norma ISO/IEC 27004:2016 Informační technologie - Bezpečnostní techniky - Řízení bezpečnosti informací - Monitorování, měření, analýza a hodnocení nabízí doporučení pro vývoj a používání metrik. Obsahuje také měření účinnosti ISMS a účinnosti opatření uvedených v ISO/IEC 27001. V příloze jsou uvedeny příklady jednotlivých konceptů pro měření určitých opatření nebo procesů ISMS. (Ondrák et al. 2013)

4.2.5 ISO/IEC 27005

Norma ISO/IEC 27005:2018 Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací obsahuje doporučení pro řízení rizik bezpečnosti informací s ohledem

na požadavky dle ISO/IEC 27001. Činnosti uvedené v této normě nepodléhají žádné konkrétní metodice, tím pádem je na každé organizaci, aby si vybrala svůj přístup, a je aplikovatelná na všechny typy organizací, které mají v úmyslu řídit rizika potencionálně ohrožující bezpečnost informací organizace. (Ondrák et al. 2013)

4.2.6 Další normy

Další normy, které byly doposud publikovány jsou:

- ISO 27006 – specifikace požadavků a doporučení pro orgány provádějící audit a certifikaci ISMS.
- ISO 27007 – doporučení k provádění auditů ISMS.
- ISO 27008 - doporučení auditorům ISMS a doplňuje ISO 27007.
- ISO 27009 - definice požadavků pro používání ISO/IEC 27001 ve specifických odvětvích.
- ISO 27010 - doporučení pro řízení bezpečnosti informací při interní a mimo firemní komunikaci.
- ISO 27011 - doporučení a požadavky na řízení bezpečnosti informací v prostředí telekomunikačních operátorů.
- ISO 27013 - doporučení pro implementaci ISO/IEC 20000 a ISO/IEC 27001.
- ISO 27014 - doporučení při návrhu Information Security Governance.
- ISO 27016 - doporučení pro nastavení bezpečnostního programu s ohledem na předpokládané finanční výsledky.
- ISO 27017 - doporučení pro zabezpečení cloud computingu
- ISO 27018 - nabízí vhodná bezpečnostní opatření pro zabezpečení soukromí zákazníků poskytovatelům cloudových služeb.
- ISO 27019 – interpretace a aplikace normy ISO/IEC 27002 organizacím v energetickém průmyslu, aby byla zajištěna bezpečnost jejich systémů pro elektronické řízení procesů.
- ISO 27021 - požadavky na odbornou způsobilost specialistů z oblasti ISMS.
- ISO 27023 - srovnání posledních vydání norem ISO/IEC 27001 a ISO/IEC 27002 s předchozími vydáními.
- ISO 27031 - doporučení pro zajištění kontinuity činností organizace (business continuity).
- ISO 27032 - bezpečnostní doporučení týkající se kyberprostoru.
- ISO 27033 - doporučení pro implementaci protiopatření vztahujících se k bezpečnosti sítí.
- ISO 27034 - doporučení pro bezpečnou tvorbu, implementaci a užívání aplikačního softwaru.
- ISO 27035 - řízení incidentů bezpečnosti informací.
- ISO 27036 - doporučení pro hodnocení a řízení informačních rizik spojených s pořizováním zboží a služeb od dodavatelů.
- ISO 27037 - doporučení pro zjišťování, sběr, získávání a uchovávání digitálních důkazů.
- ISO 27038 - doporučení pro publikování digitálních dokumentů.

- ISO 27039 - doporučení pro výběr, nasazení a provoz systémů pro detekci a prevenci bezpečnostních průniků (Intrusion Detection and Prevention Systems - IDPS).
- ISO 27040 - doporučení pro bezpečné ukládání dat.
- ISO 27041 - doporučení pro výběr forenzních metod pro zajištění a zkoumání digitálních důkazů.
- ISO 27042 - doporučení pro analýzu a vyhodnocování digitálních důkazů.
- ISO 27043 - zásady a postupy při vyšetřování incidentů s využitím digitálních důkazů.
- ISO 27050 – problematika zkoumání elektronických stop (Electronic discovery).
- ISO 27799 - doporučení a požadavky na řízení bezpečnosti informací ve zdravotnických zařízeních. (RiskAnalysisConsultants 2019)

4.3 Cybersecurity Framework

Kromě ISMS jsou zde i jiné rámce pro zvládání řízení bezpečnosti informací, například Cybersecurity Framework (CSF), který pochází od Národního institutu standardů a technologie (angl. National Institute of Standards and Technology, zkráceně NIST).

CSF se zaměřuje na řízení činností v oblasti kybernetické bezpečnosti a stejně jako ISMS má přístup založený na rizikách. Jádrem rámce je soubor činností, výsledků a informativních referencí, které jsou společné napříč sektory a kritickou infrastrukturou. Tento soubor poskytuje detailní pokyny pro vývoj organizačních profilů. Pomocí organizačních profilů pomůže organizaci sjednotit a upřednostnit své aktivity v oblasti kybernetické bezpečnosti s byznys požadavky. CSF dále poskytuje mechanismus pro organizace, aby mohly nahlédnout a pochopit charakteristiky jejich přístupu při zvládání rizik, což následně pomůže ke stanovení priorit a dosažení cílů kybernetické bezpečnosti.

Hlavním cílem CSF je zlepšit řízení rizik v oblasti kybernetické bezpečnosti pro kritickou infrastrukturu, ale může být využit jakoukoli organizací v jakémkoli sektoru. (National Institute of Standards and Technology 2018)

Kromě samotného rámce NIST dále nabízí příručku pro bezpečnost informací poskytující široký přehled prvků pro bezpečnost informací, které pomáhají manažerům pochopit, jak vytvořit a implementovat systém pro bezpečnost informací. Ta je publikována pod označením NIST 800-100. Příručka je určená pro bezpečností role, především pro manažery v oblasti bezpečnosti informací. Příručka využívá terminologii primárně pro vládní sektor a je na každé organizaci, aby si přizpůsobila uvedené návody podle svých potřeb. (Bowen et al. 2006)

Další důležitou publikací v této oblasti je NIST 800-50, který poskytuje návody pro vytváření a udržování programu pro zvyšování povědomí a školení v oblasti IT bezpečnosti organizace. Zdůrazňuje, že lidský faktor je zásadní při poskytování adekvátní úrovně zabezpečení a zároveň i také velkou slabinou. (Wilson a Hash 2003)

5 E-learning

Kurz slouží pro orgány veřejné moci, jež jsou správci významných informačních systémů nebo informačního nebo komunikačního systému kritické informační infrastruktury.

Cílem kurzu je seznámení účastníků se základními pojmy Vyhlášky o kybernetické bezpečnosti a vysvětlení opatření vyplývajících z této vyhlášky.

Celý e-learningový kurz se skládá z několika částí. Teoretická část je obsažena v kapitole 6 a praktický příklad najdete v kapitole 7. Po absolvování školení v podobě teorie kuru je nutné složit i teoretický test. Tento test obsahuje 31 otázek týkajících se pouze obsahu kurzu, tedy především vyhlášky o kybernetické bezpečnosti. Test je formou uzavřených otázek a všechny otázky jsou výběrové. Otázky byly vytvořeny tak aby byla dotčena všechna hlavní témata kuru. E-learning je vytvořen ve výukovém programu Moodle.

Na závěr byl sestaven dotazník spokojenosti pouze pro potřeby této práce, který by měl ohodnotit vytvořené materiály a testovací otázky. Dotazník se týká obsahu, srozumitelnosti, přínosnosti a obtížnosti jednotlivých částí. Také se dotazuje na splněná očekávání a získanou hodnotu. K ohodnocení je využito známkování jako ve škole na stupnici od jedné do pěti.

Vyhodnocení kurzu a výstup dotazníku spokojenosti je obsažen v kapitole 8.

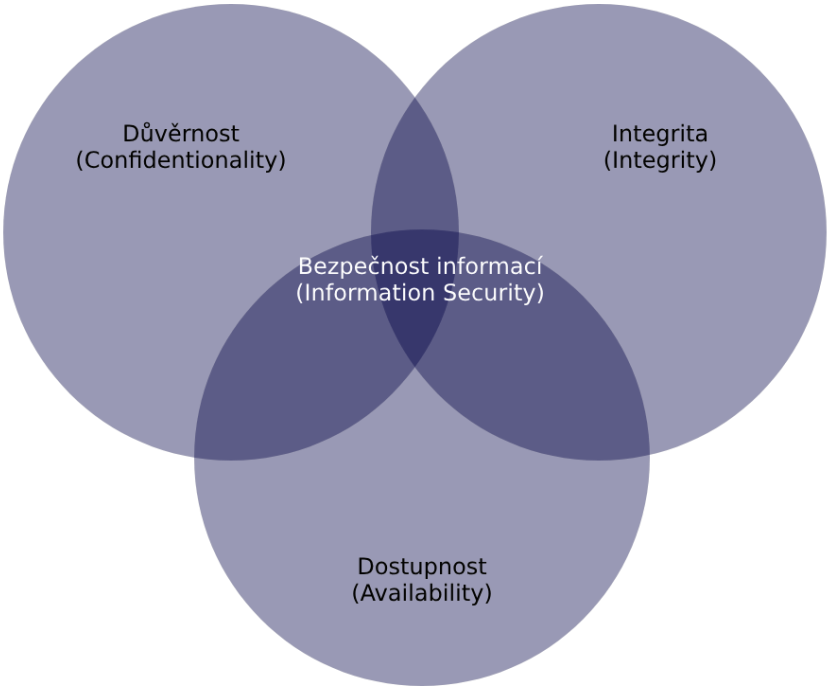
6 Obsah e-learningového kurzu – teoretická část kurzu

V této kapitole je uvedena upravená teoretická část kurzu.

6.1 Bezpečnost informací

V rámci bezpečnosti informací se řeší ochrana informací, tedy zajištění jejich důvěrnosti, dostupnosti a integrity.

- **Důvěrnost** je vlastnost, charakterizující, že informace není dostupná nebo není odhalena neautorizovaným jednotlivcům, entitám nebo procesům.
- **Dostupnost** je vlastnost přístupnosti a použitelnosti na žádost autorizované entity.
- **Integrita** je vlastnost ochrany přesnosti a úplnosti dat. Jistota, že data nebyla změněna.



Obrázek 1: CIA

Bezpečnost informací je takový stav, kdy jsou zajištěny tyto základních charakteristiky současně a v souladu s požadavky na míru jejich zajištění.

Je zřejmé, že i v oblasti zajišťování kybernetické bezpečnosti zahrnuje bezpečnost informací nejen bezpečnost IS/ICT, ale také s tím úzce související oblasti, jako je fyzická bezpečnost, ochrana osobních údajů, řízení lidských zdrojů, řízení vztahů s dodavateli atd.

6.1.1 Norma ISO/IEC 27001

Tato norma je součástí rodiny standardů ISO/IEC 27000 pro řízení informační bezpečnosti v organizacích a poskytuje komplexní přístup k informační bezpečnosti v organizaci, zahrnuje veškerá aktiva od dat, přes papírové dokumenty, informační a komunikační technologie až po znalosti.

- ✓ Zahrnuje též rozvoj kvalifikace zaměstnanců a technickou ochranu proti počítačovým podvodům.
- ✓ Využívá se při certifikaci k nezávislému posouzení schopnosti organizace vytvořit a udržovat komplexní systém informační bezpečnosti.
- ✓ Norma je propojena a harmonizována s jinými systémy řízení, jako ISO/IEC 9001 (řízení kvality a ISO/IEC 14001 (řízení životního prostředí). (Ondrák et al. 2013)

6.1.2 Vyhláška o kybernetické bezpečnosti

Vyhláška č. 82/2018 Sb., Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) (dále jen „Vyhláška“ nebo „VKB)“ definuje v § 3 až 27 nezbytná bezpečnostní opatření v oblasti kybernetické bezpečnosti, na základě kterých je dosaženo přiměřené bezpečnosti informací.

Bezpečnostní opatření dle VKB

Vyhláška rozděluje bezpečnostní opatření na organizační a technická.

Organizační opatření se týkají především ustanovování systému řízení bezpečnosti informací, jeho plánování, kontroly, zlepšování atd. Tedy například odpovídají na otázku, proč vůbec zavádět konkrétní technické opatření a řeší plánování jeho nasazení.

Paragrafy týkající se organizačních opatření jsou:

- § 3 - Systém řízení bezpečnosti informací,
- § 4 - Řízení aktiv,
- § 5 - Řízení rizik,
- § 6 - Organizační bezpečnost,
- § 7 - Bezpečnostní role,
- § 8 - Řízení dodavatelů,
- § 9 - Bezpečnost lidských zdrojů,
- § 10 - Řízení provozu a komunikací,
- § 11 - Řízení změn,
- § 12 - Řízení přístupu,

- § 13 - Akvizice, vývoj a údržba,
- § 14 - Zvládání kybernetických bezpečnostních událostí a incidentů,
- § 15 - Řízení kontinuity činností a
- § 16 - Audit kybernetické bezpečnosti.

Technická opatření jsou konkrétní technická řešení, která zajišťují požadované bezpečnostní funkce.

Paragrafy týkající se technických opatření jsou:

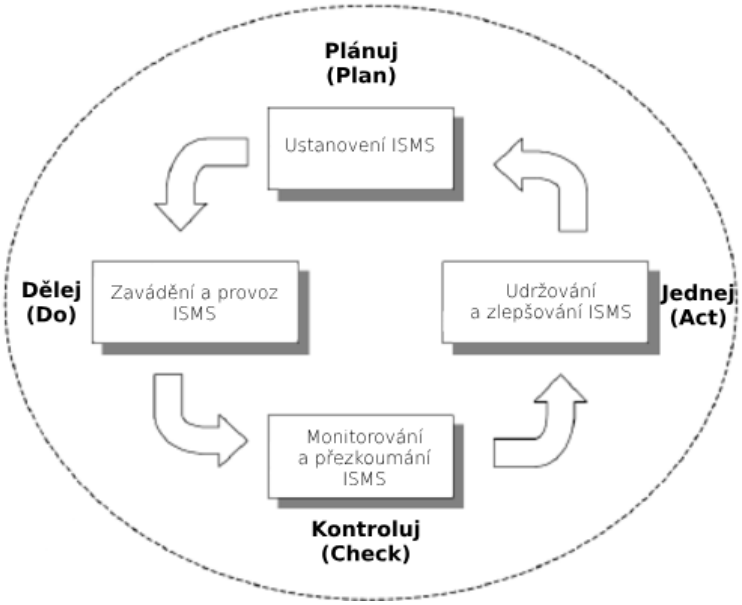
- § 17 - Fyzická bezpečnost,
- § 18 - Bezpečnost komunikačních sítí,
- § 19 - Správa a ověřování identit,
- § 20 - Řízení přístupových oprávnění,
- § 21 - Ochrana před škodlivým kódem,
- § 22 - Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů,
- § 23 - Detekce kybernetických bezpečnostních událostí,
- § 24 - Sběr a vyhodnocování kybernetických bezpečnostních událostí,
- § 25 - Aplikační bezpečnost,
- § 26 - Kryptografické prostředky,
- § 27 - Zajišťování úrovně dostupnosti informací a
- § 28 - Průmyslové, řídicí a obdobné specifické systémy.

6.2 Systém řízení bezpečnosti informací

- ISMS je rámec politik, postupů, směrnic a přidružených zdrojů k dosažení stanovených cílů organizace.

Systém řízení bezpečnosti informací podle VKB:

- Je postaven na iterativním PDCA cyklu (Plan – Do – Check – Act) a na přístupu k rizikům informačního a komunikačního systému.



Obrázek 2: PDCA cyklus v ISMS (ČSN ISO/IEC 27001 2014)

Stanovuje způsob ustavení, zavádění a provozování, monitorování a přezkoumání, udržování a zlepšování bezpečnosti informací a dat, po vzoru mezinárodní normy ISO/IEC 27001.

- ✓ Upozornění**:** Díky soustavnému a správnému vykonávání činností, které jsou v rámci této kapitoly obecně popsány níže a následně dále v textu rozpracovány do konkrétních požadavků VKB, dojde k dosažení kontinuálního zlepšování ISMS v organizaci, protože dojde k naplnění PDCA cyklu.

Stanovení rozsahu ISMS

Nezbytným krokem pro efektivní řízení bezpečnosti informací je stanovení adekvátního rozsahu ISMS v organizaci. Rozsah je třeba vymezit organizačními částmi a aktivy, kterých se ISMS týká.

Při stanovování rozsahu ISMS je nutné přihlédnout k požadavkům organizace a k požadavkům dotčených stran, např. k zákonným a jiným právním požadavkům (smluvním atd.).

V souladu s nejlepší praxí je stanovení rozsahu ISMS napříč celou organizací s minimem výjimek, tak aby bylo zajištěno, že jsou v rozsahu všechna klíčová aktiva, která je potřeba chránit.

- ✓ Poznámka: I při stanovení rozsahu ISMS na celou organizaci probíhá kontrola ze strany NÚKIB pouze v rozsahu určených systémů v souladu se ZKB.

V případě, kdy je rozsah stanoven pouze na část organizace, např. pouze na jeden systém spadající pod zákon o kybernetické bezpečnosti, je nutné definovat rozsah do takové míry detailu, aby bylo patrné, kterých organizačních částí a aktiv se rozsah ISMS týká.

- ✓ Doporučení: Je nutné definovat jednotlivé organizační části v rozsahu ISMS – např. sekce, odbory, oddělení apod.
- ✓ Aktiva patřící do rozsahu ISMS je přípustné definovat i seskupená – např. administrátoři, uživatelé, dodavatelé, lokality, aktivní prvky, záložní zdroje apod. Musí být ale zřejmé, kterých aktiv se rozsah ISMS týká a kterých nikoliv.
- ✓ Současně by měly být v organizaci známy hranice (perimetr) ISMS.

Stanovení cílů ISMS

V rámci ISMS je nezbytné vhodně stanovit jeho cíle. Tyto cíle je třeba nastavit tak, aby je bylo možné vyhodnocovat a sledovat tak jejich plnění. (Vyhláška č. 82/2018 Sb. 2018)

Pro definici cílů lze využít například metodiku SMART. Dle této metodiky by měl být cíl definován pěti charakteristikami:

- S – Specific – co nejpřesněji, aby bylo zřejmé, co je daným cílem myšleno.
- M – Measurable – měřitelný, aby bylo možné posoudit, do jaké míry byl cíl naplněn.
- A – Accepted – akceptovaný (přijatý) zodpovědnou osobou.
- R – Realistic – reálný, aby ho bylo možné v reálném čase dosáhnout.
- T – Timed – časově ohraničený.

- ✓ Příklad: procentuální snížení počtu řešení případů zavirování pracovní stanice vinou uživatele (antivirová řešení jak na stanicích, mailových serverech, tak poučení uživatelů), zabránění úniku informací (správné nasazení DLP), zrychlení doby obnovy systému po selhání (řešení kontinuity činností), zefektivnění a zrychlení řešení bezpečnostních incidentů (nasazení prostředí pro jejich řešení)

Analýza rizik

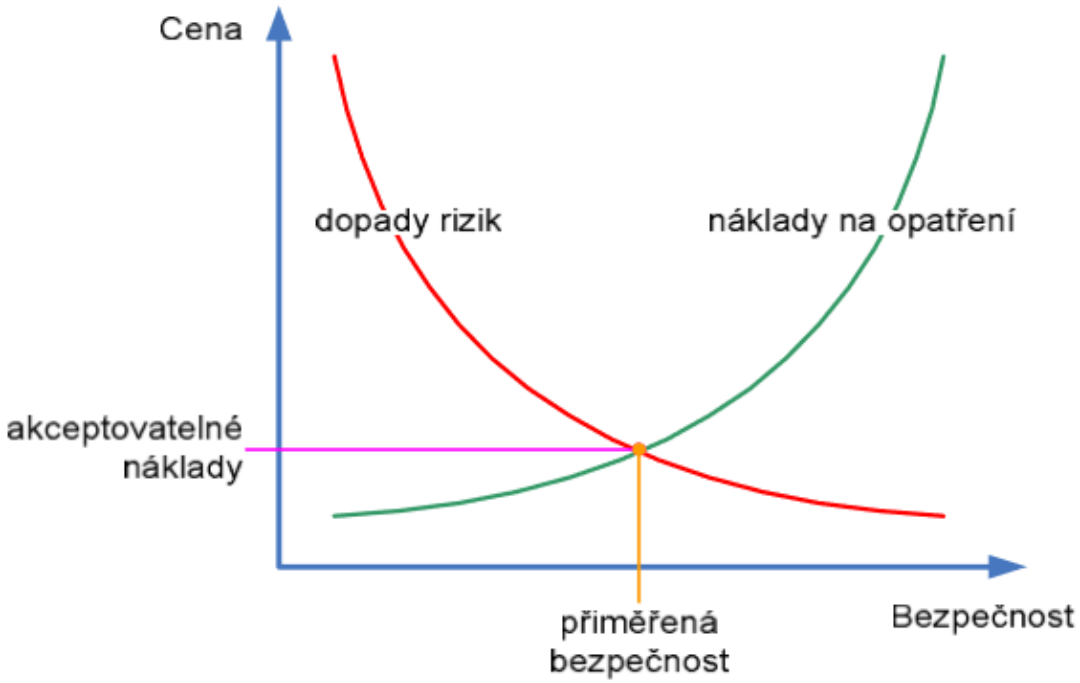
Je postup, na základě kterého dojde ke zjištění možných bezpečnostních rizik a stanovení jejich hodnot.

Hodnocení rizik je prováděno pro jednotlivá aktiva (případně skupiny aktiv) v rámci rozsahu ISMS. Prvním krokem je zjištění hodnoty daného aktiva a následně určení možných hrozeb a zranitelností a určení jejich hodnot. Kombinace hodnoty aktiva, hrozby a zranitelnosti pak určí výši rizika.

Bezpečnostní opatření

Konkrétní bezpečnostní opatření by měla vyplynout z provedené analýzy rizik a zaváděná opatření by vždy měla být přiměřená. Bezpečnostní opatření musí být zaváděna v souladu se stanovenými cíli ISMS, bezpečnostními potřebami a hodnocením rizik.

Jako přiměřená bezpečnost se označuje stav, kdy velikost úsilí a investic do bezpečnosti odpovídá hodnotě aktiv a míře možných rizik, viz graf přiměřené bezpečnosti za akceptovatelné náklady.



Obrázek 3: Graf Přiměřené bezpečnosti za akceptovatelné náklady (Ondrák et al. 2013)

Bezpečnostní politiky

Na základě bezpečnostních potřeb organizace a výsledků hodnocení rizik je v rámci ISMS nezbytné vytvořit a schválit bezpečnostní politiku pro jednotlivé oblasti ISMS obsahující hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací. (Vyhláška č. 82/2018 Sb. 2018)

Monitorování ISMS

Současně je třeba zajistit řízení provozu a zdrojů ISMS a zaznamenávat činnosti spojené s ISMS a řízením rizik.

- Příklad: zaznamenávání činností (logů) jednotlivých technologických zařízení, měření efektivity ISMS, sledování bezpečnostních událostí, zaznamenávání událostí ovlivňující výkon nebo efektivitu ISMS, schvalování rozpočtu na ISMS, uchovávání zápisů z jednání Výboru pro kybernetickou bezpečnost.

Řízení změn

Změny patřící do rozsahu ISMS je nutné průběžně identifikovat a v případě významných změn je následně i řídit. Významnou změnou se rozumí změna, která má nebo může mít vliv na kybernetickou bezpečnost a představuje vysoké riziko bez ohledu na již zavedená opatření. (Vyhláška č. 82/2018 Sb. 2018)

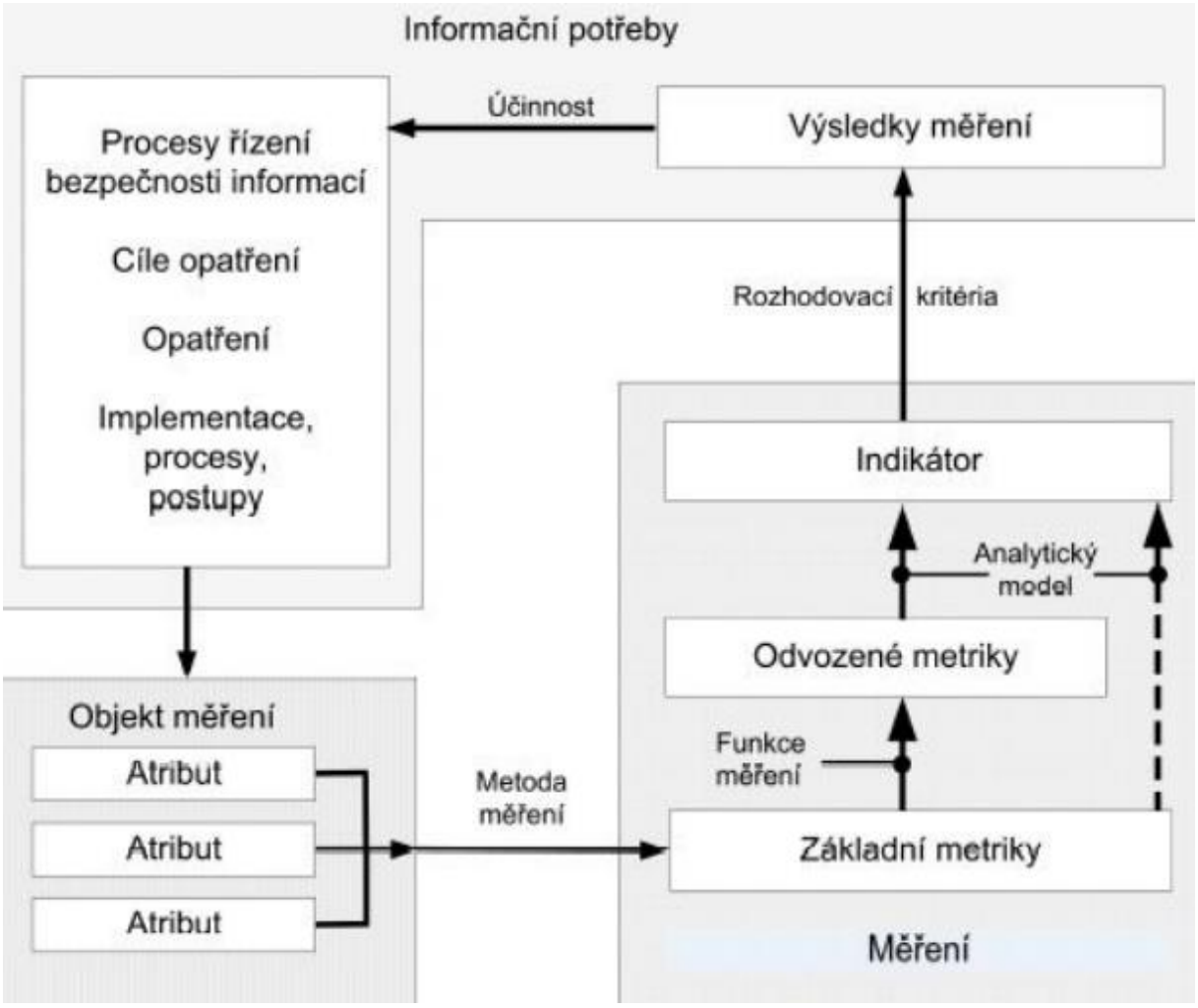
- ✓ Příklad: Za významnou změnu lze považovat například změnu konfigurace, funkčnosti ale i změnu významného dodavatele.

Kontrola a audit ISMS

Další klíčovou součástí je zajištění pravidelného provádění auditu systému řízení bezpečnosti informací/kybernetické bezpečnosti (dále jen „auditu“) v rámci rozsahu ISMS, který slouží jako nástroj pro zajištění efektivního zlepšování zavedeného ISMS a jako upozornění na případné odchylky od nejlepší praxe.

Vyhodnocování účinnosti ISMS

Dále je potřeba zajistit i pravidelné vyhodnocování účinnosti ISMS, které obsahuje hodnocení stavu ISMS včetně revize hodnocení rizik, posouzení výsledků provedených auditů a dopadů kybernetických bezpečnostních incidentů na stanovený rozsah ISMS.



Obrázek 4: Model měření bezpečnosti informací (ČSN ISO/IEC 27004 2016)

Aktualizace ISMS

Na základě výsledků vyhodnocení účinnosti ISMS, zjištění auditů a v souvislosti s významnými změnami je nutné aktualizovat ISMS a příslušnou dokumentaci. (Vyhláška č. 82/2018 Sb. 2018)

6.3 Řízení aktiv

Oblast řízení aktiv je významnou součástí ISMS a úzce souvisí se správně stanoveným rozsahem ISMS.

Na základě správného řízení aktiv je k dispozici aktuální přehled všech aktiv v rozsahu ISMS, aktiva jsou ohodnocena z hlediska jejich důležitosti a jsou jim přiřazeni garanti aktiv.

V rámci řízení rizik se stanovují i přiměřené bezpečnostní požadavky na ochranu aktiv během jejich životního cyklu, a to v souladu s jejich hodnocením.

Aktiva, potažmo jejich hodnota stanovená na základě hodnocení jejich důležitosti následně také slouží jako významný vstup pro analýzu rizik.

6.3.1 Primární a podpůrná aktiva

V rámci VKB jsou pro přehlednost aktiva dělena na primární a podpůrná.

Primární aktivum představuje informaci nebo službu, kterou zpracovává nebo poskytuje informační a komunikační systém, tato primární aktiva jsou současně často hodnototvorná pro fungování dané organizace. Jako příklady primárních aktiv lze uvést data, informace nebo poskytované služby.

Podpůrné aktivum představuje technické aktivum, zaměstnance a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému, například HW a SW technologie pro poskytování služeb. (Vyhláška č. 82/2018 Sb. 2018)

Aktiva je možné dále rozlišovat podle vlastních potřeb organizace. Podpůrná aktiva tedy příkladem jsou:

- HW (počítače, komunikační zařízení, média, odborné technické vybavení, …),
- SW (aplikační software, systémový software, vývojové nástroje, …),
- sítě (router, hub, switch, …),
- pracovníci (klíčoví zaměstnanci, administrátoři, …),
- lokalita (areál, budovy, místnosti, …) a
- organizace (řídící orgán, organizační struktura, dodavatelé, …). (ČSN ISO/IEC 27005 2013)

Bez podpůrných aktiv by nebylo možné provozovat ani aktiva primární a jde tedy sledovat jejich závislost.

6.3.2 Identifikace a hodnocení aktiv

Identifikace a evidence aktiv

Jedním ze základních požadavků na řízení aktiv je jejich identifikace. Ta by měla být prováděna v souladu se stanovenou metodikou pro identifikaci aktiv.

V souladu s identifikací aktiv je požadována i jejich evidence v dokumentované podobě a pravidelné přezkoumání aktuálnosti této evidence buď ve stanovené periodě, nebo v souladu s významnou změnou. (Vyhláška č. 82/2018 Sb. 2018)

Perioda pro přezkoumání evidence aktiv by měla být stanovena v souladu s potřebami organizace, např. jednou za rok, případně za dva roky. Důležité je přitom nezapomínat na významné změny, jako je například rozsáhlá změna technologií systému. V souvislosti s významnými změnami je nutné evidenci aktiv aktualizovat co nejdříve.

- ✓ Poznámka: U identifikovaných aktiv je nutné stanovit osobu, která je za dané aktivum odpovědná, tzv. garant aktiva. Garantem aktiva se rozumí bezpečnostní role odpovědná za zajištění rozvoje, použití a bezpečnost aktiva (bude dále v textu).

Hodnocení aktiv

Další důležitou součástí řízení aktiv je stanovení metodiky pro hodnocení aktiv.

- ✓ Informace: Metodika musí být přizpůsobená potřebám organizace a osob, které s ní pracují (ve většině případů manažer KB a garanti aktiv). Tyto osoby s ní musí umět pracovat a být schopny na základě metodiky hodnocení aktiv provést.

Při hodnocení aktiv je posuzováno, jaký dopad by mělo narušení bezpečnosti informací u jednotlivých aktiv z hlediska integrity, důvěrnosti a dostupnosti a následně jsou rozdělena je do jednotlivých úrovní v souladu se stanovenou metodikou pro hodnocení aktiv.

Minimální rozsah hodnocení důležitosti aktiv je uvedený v následujících tabulkách (viz Tabulka 1, Tabulka 2**Chyba! Nenalezen zdroj odkazů.** a Tabulka 3). (Vyhláška č. 82/2018 Sb. 2018)

Tabulka 1: Stupnice pro hodnocení důvěrnosti, Zdroj: 82/2018 Sb. Příloha č. 1

Úroveň	**Popis**	**Příklady požadavků na ochranu aktiva**
Nízká	Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy povinné osoby. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle tzv. traffic light protokolu (dále jen „TLP“) je využíváno označení TLP:WHITE.	Není vyžadována žádná ochrana. Likvidace/mazání aktiva na úrovni Nízká – viz Tabulka 4.
Střední	Aktiva nejsou veřejně přístupná a tvoří know-how povinné osoby, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:GREEN nebo TLP:AMBER.	Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu. Likvidace/mazání aktiva na úrovni Střední – viz Tabulka 4.
Vysoká	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (například obchodní tajemství, osobní údaje). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:AMBER.	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací komunikační sítí jsou chráněny pomocí kryptografických prostředků.

		Likvidace/mazání aktiva na úrovni Vysoká – viz Tabulka 4.
Kritická	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické obchodní tajemství, zvláštní kategorie osobních údajů). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:RED nebo TLP:AMBER.	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Dále metody ochrany zabraňující zneužití aktiv ze strany administrátorů. Přenosy informací jsou chráněny pomocí kryptografických prostředků. Likvidace/mazání aktiva na úrovni Kritická – viz Tabulka 4.

Tabulka 2: Stupnice pro hodnocení integrity, Zdroj: 82/2018 Sb. Příloha č. 1

Úroveň	**Popis**	**Příklady požadavků na ochranu aktiva**
Nízká	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy povinné osoby.	Není vyžadována žádná ochrana.
Střední	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů povinné osoby a může se projevit méně závažnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány standardní nástroje (například omezení přístupových práv pro zápis).
Vysoká	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů povinné osoby s podstatnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených komunikačními sítěmi je zajištěna pomocí kryptografických prostředků.
Kritická	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů povinné osoby s přímými a velmi vážnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (například pomocí technologie digitálního podpisu).

Tabulka 3: Stupnice pro hodnocení dostupnosti, Zdroj: 82/2018 Sb. Příloha č. 1

Úroveň	**Popis**	**Příklady požadavků na ochranu aktiva**

Nízká	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).	Pro ochranu dostupnosti je postačující pravidelné zálohování.
Střední	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů povinné osoby.	Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.
Vysoká	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za velmi důležitá.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv.
Kritická	Narušení dostupnosti aktiva není přípustné, a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za kritická.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.

- ✓ Poznámka: Pro hodnocení aktiv je přípustné rozšířit počet úrovní, či některé sloučit, nicméně je třeba dodržet jednoznačné vazby mezi vlastním hodnocením aktiv se způsobem uvedeným ve VKB.
- ✓ Hodnocení aktiv by měli provádět garanti aktiva, kteří by měli být schopni aktivum ohodnotit ve spolupráci s manažerem KB.
- ✓ Příklad: viz Obrázek 5 - Zjednodušený katalog aktiv uvedený bez vazeb mezi primárními a podpůrnými aktivy. Hodnota aktiva je vypočtena jako maximální hodnota z dostupnosti, integrity a důvěrnosti.

ID	Název	Typ aktiva	Popis	Správce aktiva	Garant aktiva	Hodnota aktiva			
						Dostupnost	Integrita	Důvěrnost	Hodnota aktiva
ICO1	Certifikace senzorů	primární	proces certifikace	Odbor certifikace	K. Hovorka	3	4	3	4
ICO2	Informace o senzorech	primární	typ senzoru, účel, technické parametry…	Sekce kontroly	S. Reichl	2	3	2	3
ICO3	Laboratorní výsledky	primární	výsledné hodnoty z laboratoře	Laboratoř	k. Škuta	2	4	2	4
ICO4	Informace o certifikátech	primární	platnost, datum, senzor,…	Odbor certifikace	E. Hejzlar	2	4	1	4
ICO5	Kontaktní údaje podavatele	primární	kontaktní osobní údaje,…	Kancelář úřadu	O. Vyhnálek	1	2	1	2
IDB01	Databáze certifikačního systému	podpůrné		Odbor IT	R. Široký	3	4	4	4
IDB02	Databáze webové prezentace	podpůrné		Odbor IT	R. Široký	3	3	3	3
IHW01	Server certifikačního systému	podpůrné		Odbor IT	M. Tichý	3	4	4	4
IHW02	Webový server	podpůrné		Odbor IT	M. Tichý	2	3	3	3
IHW03	Směrovače	podpůrné		Odbor IT	S. Pytlík	3	2	2	3
IHW04	Kabely	podpůrné		Odbor IT	S. Pytlík	3	2	2	3
IHW05	Osobní počítače	podpůrné		Odbor IT	J. Frydrych	2	3	3	3
IHW06	File server	podpůrné		Odbor IT	M. Tichý	3	3	3	3
ILC01	Serverovna	podpůrné		Odbor IT	M. Tichý	4	4	3	4
ILC02	Laboratoř	podpůrné		Laboratoř	k. Škuta	3	4	4	4
ISS01	Dodavatelé laboratorního vybavení	podpůrné		Laboratoř	k. Škuta	3	2	3	3
ISS02	Zaměstnanci laboratoře	podpůrné		Laboratoř	k. Škuta	3	3	4	4
ISS03	Administrátoři	podpůrné		Odbor IT	S. Reichl	3	3	3	3
ISW01	Firewall	podpůrné		Odbor IT	S. Pytlík	3	2	3	3
ISW02	Operační systém	podpůrné		Odbor IT	J. Frydrych	2	2	2	2
ISW03	Certifikační systém	podpůrné		Odbor IT	M. Vodák	3	4	4	4
ISW04	Webová prezentace	podpůrné		Odbor IT	S. Otruba	3	3	2	3

Obrázek 5: Zjednodušený příklad katalogu aktiv

Hodnocení důležitosti primárních aktiv

Při hodnocení důležitosti primárních aktiv je třeba posoudit především:

- rozsah a důležitost osobních údajů, zvláštních kategorií osobních údajů nebo obchodního tajemství,
- rozsah dotčených právních povinností nebo jiných závazků,
- rozsah narušení vnitřních řídicích a kontrolních činností,
- poškození veřejných, obchodních nebo ekonomických zájmů a možné finanční ztráty,
- dopady na poskytování důležitých služeb,
- rozsah narušení běžných činností,
- dopady na zachování dobrého jména nebo ochranu dobré pověsti,
- dopady na bezpečnost a zdraví osob,
- dopady na mezinárodní vztahy a
- dopady na uživatele informačního a komunikačního systému. (Vyhláška č. 82/2018 Sb. 2018)

✓ Informace: Tento výčet není absolutní, jsou uvedeny pouze nejdůležitější faktory. Každá organizace by si měla tento seznam rozšířit dle svých potřeb. V případě, že některý z faktorů uvedených na seznamu není pro dané aktivum relevantní, je tento faktor posouzen pouze ve smyslu nerelevantní.

Určení vazeb mezi primárními a podpůrnými aktivy

Mezi primárními podpůrnými aktivy existují vazby, které je nutné vzhledem ke složitosti systémů a správnému odhodnocení aktiv znát, evidovat a hodnotit důsledky těchto závislostí. Tyto vzájemné vazby je nutné zohledňovat při hodnocení podpůrných aktiv. (Vyhláška č. 82/2018 Sb. 2018)

- Příklad: V praxi se může snadno stát, že několik primárních aktiv je závislých na jednom podpůrném aktivu. Taková vazba pak může mít vliv na hodnotu daného podpůrného aktiva.

Klasifikace aktiv

Na základě hodnocení aktiv je dále nutné zavádět příslušná pravidla ochrany nutná pro jejich zabezpečení. Jedná se zejména o stanovení přípustných způsobů používání aktiv, pravidla pro manipulaci s těmito aktivy, včetně pravidel pro bezpečné elektronické sdílení a jejich fyzické přenášení, způsob likvidace dat, provozních údajů, informací a jejich kopií nebo likvidaci technických nosičů dat.

- Příkladem může být příloha č. 1 Vyhlášky (viz Tabulka 1, Tabulka 2 a Tabulka 3), která popisuje možné způsoby ochrany aktiv a dále příloha č. 4 Vyhlášky o likvidaci dat obsahující mimo jiné příklady možných způsobů likvidace pro jednotlivé úrovně důvěrnosti aktiva (viz níže).

Likvidace aktiv

Tato oblast se zabývá stanovením pravidel pro mazání dat a likvidaci technických nosičů dat. Je nutné zvolit adekvátní úroveň likvidace vzhledem k hodnotě a důležitosti aktiv.

Při sestavování pravidel je nutné zohlednit:

- hodnotu aktiva (zejména z pohledu důvěrnosti,
- technologii – typy a velikosti nosičů informace,
- zda se nosič informace nachází pod kontrolou organizace či nikoliv,
- zda jsou data součástí dedikovaného nebo multitenantního prostředí,
- kdo bude likvidaci dat provádět,
- dostupnost vybavení a nástrojů pro likvidaci,
- kapacitu likvidovaných nosičů,
- zda je k dispozici vyškolený personál,
- časovou náročnost likvidace,
- cenu likvidace s ohledem na nástroje, školení, validaci, opětovné využití nosiče informace,
- možné způsoby likvidace dat a
- použitelné způsoby likvidace dat vzhledem ke stavu nosiče informace. (Vyhláška č. 82/2018 Sb. 2018)

Způsoby likvidace dat mohou být:

- Odstranění (odstranění datového souboru, vyhození tištěného dokumentu, …).
    - Odstranění dat tak, aby byla pro systém nedostupná.
    - Nejméně bezpečné (lze obnovit).
    - Nosič musí podporovat opětovný zápis.
    - Použitelné pro nízkou úroveň důvěrnosti aktiva.
- ✓ Fyzické zničení nosiče (mechanicky, chemicky či tepelným způsobem).
    - Nejbezpečnější metoda likvidace dat (nelze znovu požít).
    - Použitelné pro střední až kritickou úroveň.
- ✓ Několikanásobné přepsání nosiče.
    - Přepsání nahodilými hodnotami.
    - Středně bezpečný způsob likvidace (volně dostupné nástroje neobnoví).
    - Není vhodné pro poškozená média nebo média s velkou kapacitou.
    - Nosič musí podporovat opětovný zápis.
    - Použitelné pro všechny úrovně důvěrnosti aktiva.
- ✓ Znečitelnění dat jejich šifrováním. (Vyhláška č. 82/2018 Sb. 2018)

- ✓ Příklad: Příklad možných způsobů likvidace podle úrovně důvěrnosti aktiva viz Tabulka 4.

Tabulka 4: Příklad možných způsobů likvidace aktiv, Zdroj: 82/2018 Sb. Příloha č. 4

<table>
<tr><th></th><th colspan="4">Přípustný způsob likvidace podle úrovně důležitosti aktiva</th></tr>
<tr><th>Nosič informace</th><th>1. Nízká</th><th>2. Střední</th><th>3. Vysoká</th><th>4. Kritická</th></tr>
<tr><td rowspan="2">Informace na lidsky čitelném nosiči (tištěné dokumenty, poznámky a podobně)</td><td rowspan="2">Odstranění: Vyhození do odpadu.</td><td>Přepsání: Začernění.</td><td colspan="2" rowspan="2">Fyzická likvidace: Znehodnocení nosiče informací použitím skartovacího stroje s podélným i příčným řezem, spálením nebo rozložením.</td></tr>
<tr><td>Fyzická likvidace: Znehodnocení nosiče informací použitím skartovacího stroje.</td></tr>
<tr><td>Mobilní zařízení (mobilní telefony, tablety)</td><td>Odstranění: Vymazání informací, reset zařízení do továrního nastavení.</td><td>Přepsání: Pro zařízení s šifrovaným úložištěm – odstranění informací a reset do továrního nastavení.</td><td colspan="2" rowspan="3">Fyzická likvidace: Rozebrání zařízení a zničení nosiče informací.</td></tr>
<tr><td>Síťová zařízení (router, switch, modem a podobně)</td><td rowspan="2">Odstranění: Vymazání informací, reset do továrního nastavení.</td><td rowspan="2">Přepsání: Odstranění a zahlcení umělými událostmi (umělý síťový provoz, testovací tiskové úlohy a podobně.).</td></tr>
<tr><td>Kancelářské vybavení (scanery, tiskárny, fax)</td></tr>
<tr><td>Magnetická média (magnetické pásky, disky, HDD [Hard Disk Drive])</td><td rowspan="2">Odstranění: Smazání dat na úrovni souborového systému.</td><td rowspan="2">Přepsání: Přepsání dat. V případě šifrovaného média je alternativou bezpečná likvidace kryptografických klíčů</td><td colspan="2" rowspan="2">Fyzická likvidace: Zničení nosiče informací.</td></tr>
<tr><td>Optická média (CD, DVD, HD-DVD, BLU-RAY)</td></tr>
</table>

<table>
<tr><td>Elektronická média (flash paměti)</td><td></td><td>Fyzická likvidace.</td><td colspan="2"></td></tr>
<tr><td rowspan="3">Outsourcing a cloud</td><td colspan="4">Přípustný způsob likvidace dat by měl být stanoven smluvním ujednáním.</td></tr>
<tr><td>Odstranění: Odstranění všech souborů včetně předchozích verzí.</td><td>Přepsání: Použití šifrování datových úložišť na úrovni paměťového média a bezpečná likvidace kryptografických klíčů.

Alternativně v případě dedikovaného paměťového média je možné data po ukončení služby

přepsat.</td><td>Přepsání: Použití šifrování datových úložišť na úrovni paměťového média a bezpečná likvidace kryptografických klíčů uložených v certifikovaném hardware security modulu (HSM) řízená zákazníkem (například podle standardu FIPS 140-2 Level 2). Při ukončení služby bude zlikvidován vrchní přístupový klíč a data jsou přepsána.</td><td>Přepsání/fyzická likvidace: Použit způsob viz úroveň “3. Vysoká” nebo použita dedikovaná paměťová kapacita úložiště. Při ukončení služby provedena celková sanitizace všech použitých paměťových médií podle výše uvedených řádků pro úroveň kritická.</td></tr>
</table>

6.4 Řízení rizik

ISMS v souladu s požadavky VKB je postaveno na přístupu orientovaném na rizika, řízení rizik je tedy klíčový proces přímo navazující na identifikaci aktiv. Řízení rizik představuje opakující se sled činností, jejichž cílem je odhalit a řídit potenciální rizika, omezit tak pravděpodobnost jejich výskytu a snížit jejich dopad na organizaci v případě, že nastanou.

Aby bylo řízení rizik účinné, je třeba jej v pravidelných intervalech aktualizovat, taktéž po každé významné změně.

6.4.1 Metodika pro hodnocení rizik

V rámci řízení rizik je nutné stanovit metodiku pro hodnocení rizik, a to včetně kritérií pro akceptovatelnost rizik. (Vyhláška č. 82/2018 Sb. 2018) Stejně jako u metodiky pro hodnocení aktiv je nezbytné, aby metodika byla přizpůsobená potřebám organizace a klíčové bezpečnostní role (manažer KB a garanti aktiv) byli schopní s touto metodikou pracovat.

Proces hodnocení rizik by měl totiž být formalizovaný, prokazatelný a opakovaně proveditelný bez závislosti na konkrétní osobě

6.4.2 Kritéria pro přijatelnost rizik

V rámci kritérií pro akceptovatelnost rizik by měla být rozlišena rizika, která jsou akceptovatelná a taková, která akceptovatelná nejsou a je třeba je snižovat.

Akceptovatelným rizikem se rozumí riziko, které přijatelné a se souhlasem vedení není nutné jej zvládat pomocí dalších bezpečnostních opatření. Přijatelné může být například z důvodu nízké pravděpodobnosti, nízkých možných následků nebo malého vlivu na míru bezpečí, případně z důvodu nepřiměřených nákladů viz Obrázek 3.

6.4.3 Zranitelnosti

Zranitelnost je slabé místo (nedostatek) aktiva, které může využít jedna či více hrozeb. V rámci ISMS je zranitelnost často vnímána jako vlastnost aktiva.

Příklady zranitelností (Příloha č. 3 VKB):

- nedostatečná údržba informačního a komunikačního systému,
- zastaralost informačního a komunikačního systému,
- nedostatečná ochrana vnějšího perimetru,
- nedostatečné bezpečnostní povědomí uživatelů a administrátorů,
- nedostatečná údržba informačního a komunikačního systému,
- nevhodné nastavení přístupových oprávnění,
- nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
- nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování,
- nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí,
- nedostatečná ochrana aktiv,
- nevhodná bezpečnostní architektura,
- nedostatečná míra nezávislé kontroly a
- neschopnost včasného odhalení pochybení ze strany zaměstnanců. (Vyhláška č. 82/2018 Sb. 2018)

✓ Doporučení: je vhodné uvažovat i další zranitelnosti relevantní pro daná aktiva a kontext organizace.

6.4.4 Hrozby

Hrozba je činnost ohrožující bezpečnost. Hrozba zneužívá zranitelnosti či překonává bezpečnostní opatření. Hrozbou mohou být např. živelné pohromy, havárie, společenské jevy, ekonomické jevy nebo také chování jednotlivců.

Příklady hrozeb (Příloha č. 3 VKB):

- porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů,
- poškození nebo selhání technického anebo programového vybavení,
- zneužití identity,
- užívání programového vybavení v rozporu s licenčními podmínkami,
- škodlivý kód (například viry, spyware, trojské koně),
- narušení fyzické bezpečnosti,
- přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie,
- zneužití nebo neoprávněná modifikace údajů,
- ztráta, odcizení nebo poškození aktiva,
- nedodržení smluvního závazku ze strany dodavatele,
- pochybení ze strany zaměstnanců,
- zneužití vnitřních prostředků, sabotáž,
- dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb,
- nedostatek zaměstnanců s potřebnou odbornou úrovní,
- cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik,
- zneužití vyměnitelných technických nosičů dat a
- napadení elektronické komunikace (odposlech, modifikace). (Vyhláška č. 82/2018 Sb. 2018)

✓ Doporučení: je vhodné uvažovat i další hrozby a zranitelnosti relevantní pro daná aktiva a kontext organizace.

6.4.5 Metoda výpočtu hodnoty rizika

Nezbytnou součástí hodnocení rizik je jednoznačné stanovení funkce pro určení rizika. Tato hodnota rizika je nejčastěji vyjádřena funkcí ovlivněnou dopadem, jakožto hodnotou aktiva z hlediska důležitosti, hrozbou a zranitelností. (Vyhláška č. 82/2018 Sb. 2018)

Může být použita například funkce:

$$Riziko = dopadová\ hodnota\ aktiva \times hrozba \times zranitelnost$$

Hodnocení rizik

Při hodnocení rizik je nutné hodnotit rizika alespoň v rozsahu dle následujících tabulek (viz Tabulka 5, Tabulka 6 a Tabulka 7) zohlednit relevantní hrozby a zranitelnosti a posoudit možné dopady na aktiva.

Hodnocené rizik lze zajistit i jinými způsoby, než jak je uveden zde, nicméně musí být zabezpečeno, že použitá metodika hodnocení rizik zajistí stejnou nebo vyšší úroveň procesu řízení rizik.

Výsledky provedené analýzy rizik musí být obsahem zprávy o hodnocení rizik.

- Správce a provozovatel informačního nebo komunikačního systému kritické informační infrastruktury provádí hodnocení rizik alespoň jednou ročně.

- Správce a provozovatel významného informačního systému provádí hodnocení rizik alespoň jednou za tři roky. (Vyhláška č. 82/2018 Sb. 2018)

Tabulka 5: Stupnice pro hodnocení hrozeb, Zdroj: 82/2018 Sb. Příloha č. 2

Úroveň	**Popis**
Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

Tabulka 6: Stupnice pro hodnocení zranitelností, Zdroj: 82/2018 Sb. Příloha č. 2

Úroveň	**Popis**
Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Jsou zavedena bezpečnostní opatření, která jsou schopna včas detekovat možné zranitelnosti nebo případné pokusy o jejich zneužití.
Střední	Zneužití zranitelnosti je málo pravděpodobné až pravděpodobné. Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné zranitelnosti nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.
Vysoká	Zneužití zranitelnosti je pravděpodobné až velmi pravděpodobné. Bezpečnostní opatření jsou zavedena, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
Kritická	Zneužití zranitelnosti je velmi pravděpodobné až víceméně jisté. Bezpečnostní opatření nejsou realizována nebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.

Tabulka 7: Stupnice pro hodnocení rizik, Zdroj: 82/2018 Sb. Příloha č. 2

Úroveň	Popis
Nízké	Riziko je považováno za akceptovatelné.
Střední	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko akceptovatelné.
Vysoké	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.
Kritické	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.

- ✓ Příklad: viz Obrázek 6 – zjednodušená analýza rizik. Hodnota rizika je určená podle vzorce: dopadová hodnota aktiva * hodnota hrozby * hodnota zranitelnosti. Akceptační linie pro tento příklad byla nastavena na hodnotu 32.

ID rizika	Popis rizika	Označení aktiva	Dopadová hodnota aktiva	Označení hrozby	Hodnota hrozby	Označení zranitelnosti	Hodnota zranitelnosti	Hodnota rizika	Akceptováno	ID bezpečnostního opatření
R001	Únik citlivých informací z důvodu nedodržení bezpečnostních pravidel uživatelem	ISW07 Certifikační systém	3	H-001 porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů	2	Z-004 nedostatečné bezpečnostní povědomí uživatelů a administrátorů	3	18	Ano	O001
R002	Útočník získá přístupové údaje uživatele	IHW06 Osobní počítače	3	H-003 zneužití identity	2	Z-004 nedostatečné bezpečnostní povědomí uživatelů a administrátorů	3	18	Ano	O002
R003	Vyzrazení citlivých informací či citlivých technických informací o systému	IDB01 Databáze certifikačního systému	4	H-017 cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik	4	Z-004 nedostatečné bezpečnostní povědomí uživatelů a administrátorů	3	48	Ne	O001
R004	Vyzrazení citlivých informací či citlivých technických informací o systému	IDB02 Databáze webové prezentace	3	H-017 cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik	3	Z-004 nedostatečné bezpečnostní povědomí uživatelů a administrátorů	3	27	Ano	O001
R005	Nevhodná manipulace zaměstnanců s primárními aktivy	ICO3 Laboratorní výsledky	4	H-013 pochybení ze strany zaměstnanců	2	Z-004 nedostatečné bezpečnostní povědomí uživatelů a administrátorů	3	24	Ano	O001
R006	Útočník překoná bezpečnost systému a získá neautorizovaný přístup k primárním aktivům	IHW02 Server certifikačního systému	4	H-005 kybernetický útok z komunikační sítě	3	Z-011 nevhodná bezpečnostní architektura	3	36	Ne	O003
R007	Útočník překoná bezpečnost systému a vyřadí z provozu podpůrné aktivum	ISW01 Firewall	3	H-005 kybernetický útok z komunikační sítě	3	Z-011 nevhodná bezpečnostní architektura	2	18	Ano	O003
R008	Omezení dostupnosti systému z důvodu nedostatného nastavení bezpečnosti	ISW07 Certifikační systém	3	H-007 narušení fyzické bezpečnosti	2	Z-011 nevhodná bezpečnostní architektura	1	6	Ano	O003
R009	Omezení dostupnosti systému z důvodu nedostatného nastavení bezpečnosti	ISW09 Webová prezentace	3	H-007 narušení fyzické bezpečnosti	2	Z-011 nevhodná bezpečnostní architektura	1	6	Ano	O004
R010	Útočník zneužije nedostatečně silné nastavení hesla pro přístup do systému	ISW07 Certifikační systém	3	H-001 porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů	2	Z-011 nevhodná bezpečnostní architektura	1	6	Ano	O004
R011	Administrátor zneužije svého přístupu k systému a provede neautorizovanou změnu	IHW06 Osobní počítače	3	H-010 zneužití nebo neoprávněná modifikace údajů	3	Z-010 nedostatečná ochrana aktiv	2	18	Ano	O005
R012	Administrátor zneužije svého přístupu k systému a provede neautorizovanou změnu	ICO3 Laboratorní výsledky	4	H-010 zneužití nebo neoprávněná modifikace údajů	3	Z-010 nedostatečná ochrana aktiv	3	36	Ne	O005
R013	Útočník získá neoprávněný přístup do fyzického bezpečnostního perimetru	ILC01 Serverovna	4	H-007 narušení fyzické bezpečnosti	4	Z-003 nedostatečná ochrana vnějšího perimetru	3	48	Ne	O006
R014	Útočník získá neoprávněný přístup do fyzického bezpečnostního perimetru	ILC02 Laboratoř	4	H-007 narušení fyzické bezpečnosti	3	Z-003 nedostatečná ochrana vnějšího perimetru	3	36	Ne	O006
R015	Špatné provádění a nedostatečná kontrola nad hlavním procesem organizace	IC01 Certifikace senzorů	4	H-020 trvale působící hrozby	4	Z-013 neschopnost včasného odhalení pochybení ze strany zaměstnanců	4	64	Ne	O007

Obrázek 6: Zjednodušená analýza rizik

6.4.6 Plán zvládání rizik

Navazujícím dokumentem na analýzu rizik je plán zvládání rizik (angl. Risk Treatment Plan, zkráceně RTP). Jedná se o dokument obsahující cíle a přínosy bezpečnostních opatření pro zvládání jednotlivých neakceptovaných rizik, určení osoby zajišťující prosazování bezpečnostních opatření pro zvládání rizik, potřebné finanční, technické, lidské a informační zdroje, termín jejich zavedení, popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními a způsob realizace bezpečnostních opatření. V souladu s tímto plánem zvládání rizik jsou zaváděna bezpečnostní opatření. (Vyhláška č. 82/2018 Sb. 2018)

- ✓ Upozornění: Dokumenty vycházející z analýzy rizik včetně samotného hodnocení rizik je nutné pravidelně aktualizovat a musí zohledňovat nejen významné změny, ale i změny v rozsahu ISMS, opatření podle § 11 ZKB a kybernetické bezpečnostní incidenty, včetně dříve řešených.

- ✓ Příklad: viz Obrázek 7 – Zkrácený plán zvládání rizik, slouží pouze jako ukázka.

ID	Bezpečnostní opatření	Popis	Vazba na riziko	Cíle a přínosy	Zodpovídá	Termín zavedení opatření	Potřebné zdroje			Metrika pro vyhodnocení úspěšnosti
							Technické	Finanční (Kč)	Lidské (MD)	
O-001	Centralizovaná automatická aktualizace uživatelského software	Zavedení automatické centrální aktualizace uživatelského software ...	R-003, R-010, R-014, R-015	snížení pravděpodobnosti instalace škodlivého kódu způsobené neaktualizovaným software	Jan Komárek	18.4.2019	Softw001	100 000	4	Snížení počtu alertů na neaktuální software
O-002	Zvyšování bezpečnostního povědomí uživatelů	Sestavení plánu zvyšování bezpečnostního povědomí a následné proškolování uživatelů v souladu s tímto plánem	R-006, R-010, R-014, R-020	poučení uživatelů o kybernetické bezpečnosti, o způsobu tvorby bezpečného hesla a nakládání s ním	Jan Komárek	19.7.2019	Školící místnost a její vybavení	5 000	5	Snížení počtu lístečků s hesly u monitoru
O-003			R-013, R-014, R-015, R-020							

Obrázek 7: Zkrácený plán zvládání rizik

6.4.7 Prohlášení o aplikovatelnosti

V návaznosti na výsledky hodnocení rizik a s ohledem na bezpečnostní potřeby organizace je třeba zpracovat prohlášení o aplikovatelnosti (angl. Statement of Applicability, zkráceně SoA). Jedná se o dokument, jehož obsahem je přehled bezpečnostních opatření podle VKB, která nebyla aplikována včetně odůvodnění, a která byla aplikována, včetně způsobu jejich plnění.

- ✓ Příklad: viz Obrázek 8 – zkrácené prohlášení o aplikovatelnosti, slouží pouze jako ukázka možného vyplnění zavedených a nezavedených opatření.

ZDROJ	§	NÁZEV §	TEXT §	APLIKOVÁNO	ZPŮSOB, ZDŮVODNĚNÍ ZAVEDENÍ/NEZAVEDENÍ OPATŘENÍ	ODKAZ
VKB	**§ 3**	**Systém řízení bezpečnosti informací**	**Povinná osoba v rámci systému řízení bezpečnosti informací musí:**	-	-	-
VKB	§ 3	Systém řízení bezpečnosti informací	Stanovit s ohledem na požadavky dotčených stran a organizační bezpečnost rozsah systému řízení bezpečnosti informací, ve kterém určí organizační části a aktiva, jichž se systém řízení bezpečnosti informací týká.	ano	Je třeba vědět, čeho bezpečnost vlastně řídíme, co je pro organizaci důležité. K tomu využíváme metodiku pro určování aktiv. Seznam aktiv je vytvořen formou tabulky, která je umístěna ve složce Bezpečnost.	-
VKB	§ 3	Systém řízení bezpečnosti informací	Stanovit cíle systému řízení bezpečnosti informací.	ano	Organizace musí znát odpovědné osoby za jednotlivá aktiva. Zcela klíčová je tato osoba například při analýze rizik.	-
VKB	§ 3	Systém řízení bezpečnosti informací	Určit pro stanovený rozsah systému řízení bezpečnosti informací, na základě cílů systému řízení bezpečnosti informací, bezpečnostních potřeb a hodnocení rizik, a zavést přiměřená bezpečnostní opatření.	ne	Nedisponujeme žádnými průmyslovými, řídicími a obdobnými specifickými systémy.	-
VKB	§ 3	Systém řízení bezpečnosti informací	Řídit rizika podle § 5.	ano	Uplatňuje se přístup zaměřený na rizika	-
VKB	§ 3	Systém řízení bezpečnosti informací	Vytvořit a schválit bezpečnostní politiku v oblasti systému řízení bezpečnosti informací, která obsahuje hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací, a na základě bezpečnostních potřeb a výsledků hodnocení rizik stanovit bezpečnostní politiku v dalších oblastech podle § 30 a zavést přiměřená bezpečnostní opatření.	ano	Bezpečnostní politika je hlavním bezpečnostním dokumentem a byla schválena vedením organizace	-
VKB	§ 3	Systém řízení bezpečnosti informací	Zajistit provedení auditu kybernetické bezpečnosti u informačního a komunikačního systému (dále jen „audit kybernetické bezpečnosti[1]") podle § 16.	ano	Audit je naplánován a provádět dle stanovených pravidel	-
VKB	**§ 4**	**Řízení aktiv**	**Povinná osoba v rámci řízení aktiv musí:**	-	-	-
VKB	§ 4	Řízení aktiv	Stanovit metodiku pro identifikaci aktiv.	ano	Metodika pro evidenci aktiv byla stanovena	-
VKB	§ 4	Řízení aktiv	Stanovit metodiku pro hodnocení aktiv alespoň v rozsahu uvedeném v příloze č. 1 k této vyhlášce.	ano	Metodika pro hodnocení aktiv byla převzata z přílohy č.1 VKB	-
VKB	§ 4	Řízení aktiv	Identifikovat a evidovat aktiva.	ano	Aktiva IS jsou identifikována a evidována	-
VKB	§ 4	Řízení aktiv	Určit a evidovat vazby mezi primárními a podpůrnými aktivy a hodnotit důsledky závislosti mezi primárními a podpůrnými aktivy.	ne	v našem případě není nutné evidovat vazby mezi primárními a podpůrnými aktivy	

Obrázek 8: Zkrácené prohlášení o aplikovatelnosti

6.5 Organizační bezpečnost

Kybernetickou bezpečnost je nutné zajistit i organizačně s ohledem na rozsah ISMS. Organizace musí mít definované a přidělené odpovědnosti a pravomoci ve vztahu k ISMS. To se týká jak vrcholového vedení, tak výboru kybernetické bezpečnosti a bezpečnostních rolí, jejichž stanovení ukládá VKB.

Ze strany vedení organizace je vyžadována zejména aktivita popsaná níže.

Vedení organizace by mělo:

- zajistit stanovení bezpečnostní politiky a cílů ISMS slučitelných se strategickým směrováním organizace a integraci ISMS do všech souvisejících procesů v rámci organizace,
- zajistit dostupnost zdrojů (např. lidských, finančních),
- informovat zaměstnance o významu ISMS a významu dosažení shody s jeho požadavky se všemi dotčenými stranami,
- zajistit podporu k dosažení zamýšlených výstupů ISMS,
- vést zaměstnance k rozvíjení efektivity ISMS a podporovat je při tomto rozvíjení,
- prosazovat neustálé zlepšování ISMS,
- podporovat osoby zastávající bezpečnostní role při prosazování kybernetické bezpečnosti v oblastech jejich odpovědnosti,
- zajistit stanovení pravidel pro určení administrátorů a osob, které budou zastávat bezpečnostní role a zajistit, aby byla zachována mlčenlivost administrátorů a osob zastávajících bezpečnostní role,
- pro osoby zastávající bezpečnostní role zajistit příslušné pravomoci a zdroje včetně rozpočtových prostředků k naplňování jejich rolí a plnění souvisejících úkolů a
- zajistit testování plánů kontinuity činností, obnovy a procesů spojených se zvládáním kybernetických bezpečnostních incidentů. (Vyhláška č. 82/2018 Sb. 2018)

✓ Informace: Do testování plánů kontinuity činností, obnovy a procesů spojených se zvládáním kybernetických bezpečnostních incidentů by mělo být zapojeno i vrcholové vedení organizace. Hlavním důvodem zapojení vrcholového vedení do testování těchto plánů je především účast všech zainteresovaných stran proto, aby byla zajištěna úplná simulace průběhu nastalé krizové situace a její řešení aktivací plánů zpracovaných ke zvládání těchto situací. V rámci testů je nezbytné testovat také rozhodovací schopnosti, je tedy nezbytné, aby byly do testů zapojeny osoby s potřebnými pravomocemi. Proces zvládání kybernetických incidentů by měl být zautomatizovaný a všichni účastnící musí vědět, jaký je jejich úkol.

✓ Nedílným požadavkem je taktéž zajištění stanovení pravidel pro určení administrátorů a osob, které budou zastávat bezpečnostní role. Například do relevantních směrnic, organizačních řádů a smluv s konkrétními fyzickými osobami zapracovat ustanovení o bezpečnosti informací – dohody o mlčenlivosti, o zachování důvěrnosti apod.

Výbor kybernetické bezpečnosti

Výbor kybernetické bezpečnosti je tvořen osobami s příslušnými pravomocemi a odbornou způsobilostí pro celkové a řízení a rozvoj ISMS a osobami významně se na ISMS a koordinaci souvisejících činnostech podílející. Alespoň jedním ze členů výboru kybernetické bezpečnosti musí být zástupce vrcholového vedení, nebo jím pověřená osoba, a manažer kybernetické bezpečnosti. Vzhledem k rozhodovací pravomoci vrcholového vedení by spolu měli vrcholové vedení a manažer kybernetické bezpečnosti úzce komunikovat. Při sestavování výboru kybernetické bezpečnosti je vhodné přihlédnout k doporučením uvedeným v příloze 6. VKB. (Vyhláška č. 82/2018 Sb. 2018)

Bezpečnostní role

VKB definuje tyto bezpečnostní role – manažer kybernetické bezpečnosti, architekt kybernetické bezpečnosti, auditor kybernetické bezpečnosti a garant aktiva.

Povinné bezpečnostní role jsou stanoveny podle toho, o jaký orgán nebo osobu se jedná dle zákona o kybernetické bezpečnosti. Správce a provozovatel významného informačního systému (§ 3 písm. e zákona) určí minimálně bezpečnostní role manažera kybernetické bezpečnostní a garantů aktiv, přičemž zajistí zastupitelnosti bezpečnostní role manažer kybernetické bezpečnosti. Ostatní bezpečnostní role určí přiměřeně vzhledem k rozsahu a potřebám ISMS.

Správce a provozovatel informačního systému kritické informační infrastruktury, správce a provozovatel komunikačního systému kritické informační infrastruktury určí všechny bezpečnostní role, přičemž zajistí zastupitelnost bezpečnostních rolí manažer kybernetické bezpečnosti a architekt kybernetické bezpečnosti. (Vyhláška č. 82/2018 Sb. 2018)

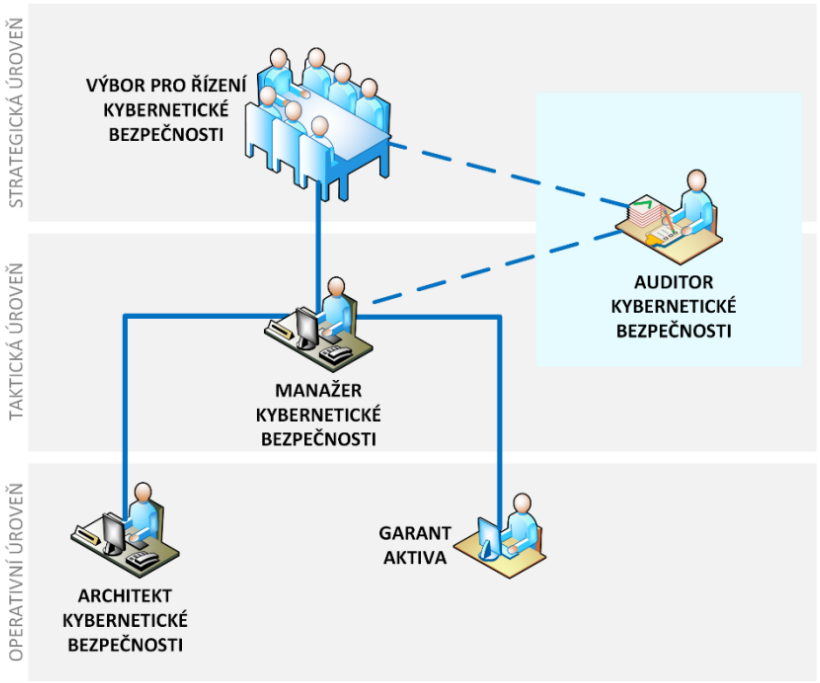
Zastupitelnost bezpečnostních rolí

Požadavek na zastupitelnost reaguje na poznatky z prováděných kontrol dodržování kybernetického zákona, kdy bylo zjištěno, že osoby zajišťující výkon povinných bezpečnostních rolí nemají v organizaci adekvátní zástup. Tato skutečnost může mít mimo jiné vliv na zajištění kontinuity některých činností organizace. Pro zajištění patřičné zastupitelnosti je možné rozložit povinnosti a kompetence mezi více osob. Pro zastupující osoby se požadavky kladené na odbornou způsobilost a praxi použijí přiměřeně. (Vyhláška č. 82/2018 Sb. 2018)

6.6 Bezpečnostní role

VKB definuje tyto bezpečnostní role – manažer kybernetické bezpečnosti, architekt kybernetické bezpečnosti, auditor kybernetické bezpečnosti a garant aktiva.

Při určování osob zastávajících bezpečnostní role je vhodné přihlédnout k doporučením vycházejícím z dobré praxe uvedených v příloze č. 6 VKB. V případě, že je v rámci jedné organizace v rozsahu ISMS více informačních a komunikačních systémů, není nutné jmenovat do jednotlivých rolí pro každý systém rozdílné osoby, tedy jedna bezpečnostní role může být odpovědná za více systémů.



Obrázek 9: Hierarchie bezpečnostních rolí (NÚKIB 2019)

Manažer kybernetické bezpečnosti

Manažer kybernetické bezpečnosti je bezpečnostní role odpovědná za ISMS. Jedná se o zcela klíčovou roli, zajišťující správné fungování ISMS.

Pro tuto činnost proto musí prokázat odbornou způsobilost a praxi. Délka praxe je stanovena na 3 roky a to proto, že za tuto dobu je možné získat dostatek zkušeností pro výkon této role. V případě absolvování vysokoškolského studia je délka požadované praxe zkrácena na 1 rok, a to vzhledem k tomu, že teoretické zkušenosti i praxe jsou získávány již během studia vysoké školy.

Mezi povinnosti Manažera kybernetické bezpečnosti například patří informovat vrcholové vedení o činnostech vyplývajících z rozsahu jeho odpovědnosti a stavu ISMS. Cílem je, aby docházelo k usnadnění prosazování konceptu ISMS a k dobré informovanosti a zainteresovanosti vrcholového vedení do problematiky kybernetické bezpečnosti.

Vzhledem k náplni práce manažera kybernetické bezpečnosti nesmí být osoba vykonávající tuto roli pověřena výkonem rolí odpovědných za provoz informačního a komunikačního systému. (Vyhláška č. 82/2018 Sb. 2018)

Organizační zařazení osoby zastávající roli manažera je na uvážení povinné osoby. Je doporučené, aby byl přímo pod nejvyšším orgánem organizace.

Architekt kybernetické bezpečnosti

Architekt kybernetické bezpečnosti je bezpečnostní role odpovědná za zajištění návrhu implementace bezpečnostních opatření tak, aby byla zajištěna bezpečná architektura informačního a komunikačního systému, až například po bezpečnost na aplikační úrovni.

Výkonem této role může být pověřena osoba, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s navrhováním implementace bezpečnostních opatření a zajišťováním architektury bezpečnosti. Časové požadavky na praxi jsou stejné jako u role manažer kybernetické bezpečnosti, tedy doba nejméně tří let nebo doba jednoho roku v případě, že osoba vykonávající tuto roli absolvovala studium na vysoké škole. (Vyhláška č. 82/2018 Sb. 2018)

Výkon této role je možné rozdělit mezi více osob při zohlednění jejich zaměření a např. vzhledem k využívaným technologiím.

Garant aktiva

Garant kybernetické bezpečnosti je bezpečnostní role odpovědná za zajištění rozvoje, použití a bezpečnosti aktiva. Garant aktiva by měla být současně osoba, která prosazuje zajišťování důvěrnosti, dostupnosti a integrity aktiva, jehož je správcem. (Vyhláška č. 82/2018 Sb. 2018)

Auditor kybernetické bezpečnosti

Auditor kybernetické bezpečnosti je bezpečnostní role odpovědná za provádění auditu kybernetické bezpečnosti.

Požadavky na odbornou způsobilost praxí jsou stejné jako u bezpečnostních rolí manažer kybernetické bezpečnosti a architekt kybernetické bezpečnosti.

V případě auditora kybernetické bezpečnosti je klíčové, aby auditor vykonával svoji činnost nestranně, a nesmí být pověřen výkonem jiných bezpečnostních rolí. (Vyhláška č. 82/2018 Sb. 2018)

6.7 Řízení dodavatelů

Veškeré dodavatelské vztahy by měly být řízeny na základě ošetření ve smlouvách. Smlouvy by měly vycházet z jasných a konkrétních požadavků zadavatele a měly by být vymahatelné, sankce za nedodržení smluvních ujednání by měly být dostatečně motivující. Požadavky v oblasti kybernetické bezpečnosti by měly být definovány na základě analýzy rizik.

6.7.1 Dodavatelské vztahy

V rámci řešení dodavatelských vztahů je nutné vytvořit bezpečnostní pravidla pro dodavatele, respektující systém řízení bezpečnosti informací. S relevantními pravidly v oblasti ISMS musí být dodavatelé prokazatelně seznámeni a musí být vyžadováno jejich plnění. (Vyhláška č. 82/2018 Sb. 2018)

- ✓ Mělo by dojít k informování dodavatele o zavedeném systému ISMS a o skutečnostech z toho vyplývajících (seznámení dodavatele s příslušnými relevantními bezpečnostními politikami např. způsob značení a nakládání s informacemi).

6.7.2 Evidence významných dodavatelů

Součástí řízení vztahů s dodavateli je i vedení evidence významných dodavatelů. Významný je takový dodavatel, který je významný z hlediska bezpečnosti informačního a komunikačního systému. Povinností je významného dodavatele informovat o tom, že je významný dodavatel. Seznámení musí být písemnou formou a prokazatelné. (Vyhláška č. 82/2018 Sb. 2018)

Prokazatelné informování dodavatele o jeho významnosti

Náležitosti prokazatelného informování jsou:

- identifikace správce nebo provozovatele,
- identifikace informačního a komunikačního systému,
- identifikace významného dodavatele,
- vyrozumění o skutečnosti, že dodavatel je pro správce významným dodavatelem, a popřípadě také o tom, že významný dodavatel je zároveň provozovatelem,
- obsah bezpečnostních pravidel pro dodavatele a
- provozovatel informačního nebo komunikačního systému, který byl prokazatelně informován správcem o tom, že je významný dodavatel, hlásí kontaktní údaje NÚKIB. (Vyhláška č. 82/2018 Sb. 2018)

6.7.3 Řízení rizik spojených s dodavatelskými vztahy

Součástí řízení dodavatelů je i řízení rizik s nimi spojenými.

V případech týkajících se řízení rizik spojených s významnými dodavateli je nezbytné, aby smlouvy uzavírané s významnými dodavateli obsahovaly relevantní oblasti uvedené níže a pravidelně přezkoumávat plnění uzavřených smluv s významnými dodavateli z hlediska ISMS. (Vyhláška č. 82/2018 Sb. 2018)

- ✓ Doporučení: Evidenci významných dodavatelů je vhodné přizpůsobit potřebám organizace. Měla by se zakomponovat do bezpečnostní politiky tak, aby byla stále k dispozici, snadno se přezkoumávala a mohla se využít v případě významné změny. Kromě evidence významných dodavatelů se dle potřeby evidují i ostatní dodavatelé.

V rámci výběrového řízení a před uzavřením smlouvy je nezbytné provést hodnocení rizik souvisejících s plněním předmětu výběrového řízení, stanovit způsoby a úrovně realizace bezpečnostních opatření a určit obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření.

Hodnocení rizik a pravidelná kontrola zavedených bezpečnostních opatření u poskytovaných plnění, a to buď pomocí vlastních zdrojů nebo pomocí třetí strany.

Zajistit reakci na rizika a zjištěné nedostatky a zajistit jejich řešení. (Vyhláška č. 82/2018 Sb. 2018)

6.7.4 Smlouvy uzavírané s dodavateli

V souvislosti s řízením rizik spojených s významnými dodavateli by mělo být zajištěno, aby smlouvy, tam kde je to relevantní, uzavírané s významnými dodavateli obsahovaly:

- ustanovení o bezpečnosti informací,
- ustanovení o oprávnění užívat data,
- ustanovení o autorství programového kódu, popřípadě o programových licencích,
- ustanovení o kontrole a auditu dodavatele,
- ustanovení upravující řetězení dodavatelů,
- ustanovení o povinnosti dodavatele dodržovat bezpečnostní politiky povinné osoby nebo ustanovení o odsouhlasení bezpečnostních politik dodavatele povinnou osobou,
- ustanovení o řízení změn,
- ustanovení o souladu smluv s obecně závaznými právními předpisy,
- ustanovení o povinnosti dodavatele informovat povinou osobu,
- specifikace podmínek z pohledu bezpečnosti při ukončení smlouvy (například přechodné období při ukončení spolupráce, kdy je třeba ještě udržovat službu před nasazením nového řešení, migrace dat a podobně),
- specifikace podmínek pro řízení kontinuity činností v souvislosti s dodavateli (například zahrnutí dodavatelů do havarijních plánů, úkoly dodavatelů při aktivaci řízení kontinuity činností),
- specifikace podmínek pro formát předání dat, provozních údajů a informací po vyžádání správcem,
- pravidla pro likvidaci dat,
- ustanovení o právu jednostranně odstoupit od smlouvy a
- ustanovení o sankcích za porušení povinností. (Vyhláška č. 82/2018 Sb. 2018)

Při řetězení dodavatelů musí být zajištěno, že poddodavatelé zaváží plnit v plném rozsahu smluvní povinnosti mezi povinnou osobou a dodavatelem. Subdodavatelé nesmí jednat v rozporu s požadavky povinné osoby.

Dodavatel by měl informovat o:

- kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy,
- způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním smlouvy,
- významné změně ovládání tohoto dodavatele podle zákona o obchodních korporacích,
- změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných tímto dodavatelem k plnění podle smlouvy se správcem.

Možnost jednostranně odstoupit od smlouvy je možné v případě významné změny kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy využívanými dodavatelem k plnění podle smlouvy. (Vyhláška č. 82/2018 Sb. 2018)

6.8 Bezpečnost lidských zdrojů

Pro oblast IS/ICT je vyžadováno řízení bezpečnosti lidských zdrojů, které je z větší části tvořené plánem rozvoje bezpečnostního povědomí.

Kromě plánu se zajistí kontrola dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávající bezpečnostní role.

Pokud dojde k ukončení smluvního vztahu s administrátory nebo osobami zastávající bezpečnostní role je nutné zajistit předání odpovědnosti těchto osob.

Dále je potřeba určit pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role. (Vyhláška č. 82/2018 Sb. 2018)

Plán rozvoje bezpečnostního povědomí

Plán rozvoje bezpečnostního opatření je realizován stanovením a následně dodržováním plánu rozvoje bezpečnostního povědomí, které má za cíl zajistit odpovídající vzdělání a zlepšování bezpečnostního povědomí, čímž by se měl snížit počet interních incidentů.

Součástí plánu je:

- určení odpovědných osob za realizaci tohoto plánu,
- poučení uživatelů, administrátorů, osob zastávající bezpečnostní role a dodavatelů o jejich povinnostech a bezpečnostní politice a
- stanovení odborných školení uživatelů, administrátorů a osob zastávající bezpečnostní role.

Účinnost plánu, provedených školení a další činnosti spojené se zlepšováním bezpečnostního povědomí se pravidelně hodnotí. (Vyhláška č. 82/2018 Sb. 2018)

- ✓ Doporučení: Školení by mělo odpovídat cílové skupině a být tak co nejvíce efektivní, tyto znalosti je třeba ověřovat a pravidelně obnovovat, tak aby byla zajištěná kontrola dodržování bezpečnostní politiky. Poučení zainteresovaných osob by mělo být prokazatelné. Plán je dobré optimalizovat a držet stále aktuální na základě hodnocení účinnosti plánu.

6.9 Řízení změn

V rámci řízení změn se provádí přezkoumávání možných dopadů změn a určování významných změn.

Významná změna je taková změna, která má nebo může mít vliv na kybernetickou bezpečnost a představuje vysoké riziko. Posouzení, zda se jedná o významnou změnu či nikoliv je tak na konkrétní organizaci.

U významných změn je třeba:

- dokumentovat jejich řízení,
- provádět analýzu rizik,
- přijmou opatření za účelem snížení všech nepříznivých dopadů spojených s významnými změnami,
- aktualizovat bezpečnostní politiku a příslušnou dokumentaci.,
- zajistit jejich testování,
- a zajistit možnost navrácení do původního stavu a
- rozhodnut (v případě správců a provozovatelů významných informačních systémů rozhodnout „přiměřeně“) o případném provedení penetračního testování nebo testování zranitelností (v rozsahu aktiv dotčených významnou změnou). (Vyhláška č. 82/2018 Sb. 2018)

✓ Příklad: Za významnou změnu lze považovat například změnu konfigurace, funkčnosti ale i změnu významného dodavatele.

6.10 Řízení informačního a komunikačního systému

6.10.1 Akvizice, vývoj a údržba

V souvislosti s plánovanou akvizicí, vývojem a údržbou informačního a komunikačního systému je třeba:

- řídit rizika (viz řízení rizik),
- řídit případné významné změny (viz řízení změn),
- stanovit bezpečnostní požadavky,
- zahrnout bezpečnostní požadavky do projektu akvizice, vývoje a údržby,
- zajistit bezpečnost vývojového a testovacího prostředí
- zajistit ochranu používaných testovacích dat,
- provádět bezpečnostní testování významných změn před jejich zavedením do provozu a
- je-li cílem provedení akvizice nebo vývoje nástroj pro správu a ověřování identity, pak zajistit plnění požadavku na více-faktorouvou autentizaci. (Vyhláška č. 82/2018 Sb. 2018)

6.10.2 Řízení provozu a komunikací

V rámci řízení provozu a komunikací se zajišťuje bezpečný provoz informačního a komunikačního systému za pomocí stanovení pravidel a postupů. V případě změn je nezbytné tato pravidla a postupy aktualizovat.

Provozní pravidla a postupy

Součástí provozních pravidel a postupů se definují:

- práva a povinnosti administrátorů, uživatelů a osob zastávající bezpečnostní role,
- postupy pro ukončení, restart, obnovu chodu systému a ošetření chybových stavů,
- postupy pro sledování kybernetických bezpečnostních událostí a opatření pro ochranu přístupu k záznamům o těchto událostech,
- pravidla a postupy pro ochranu před škodlivým kódem,
- spojení na kontaktní osoby, které jsou pověřeny výkonem systémové a technické podpory,
- postupy řízení a schvalování provozních změn,
- postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů,
- pravidla a postupy pro ochranu informací a dat v průběhu celého životního cyklu,
- pravidla a postupy pro instalaci technických aktiv,
- provádění pravidelného zálohování a kontroly použitelnosti provedených záloh a
- pravidla a postupy pro zajištění bezpečnosti síťových služeb. (Vyhláška č. 82/2018 Sb. 2018)

Dle ISMS se zajistí oddělení vývojového, testovacího a provozního prostředí.

- ✓ Doporučení: Vývojové a provozní programové vybavení provozovat na různých počítačích, doménách a adresářích. Provozní a testovací systémy by měly používat různé uživatelské profily. Testovací prostředí má simulovat provozní, ale testovací data anonymizovat.

- ✓ Doporučení: Provozní pravidla je vhodné pravidelně kontrolovat a aktualizovat

6.10.3 Řízení přístupu

Přístup k informačnímu a komunikačnímu systému se řídí na základě provozních a bezpečnostních potřeb. K řízení přístupu musí být přijata taková opatření, která zajistí ochranu přihlašovacích údajů. K tomu jsou využívány i technické nástroje pro správu a ověřování identit a pro řízení přístupových oprávnění.

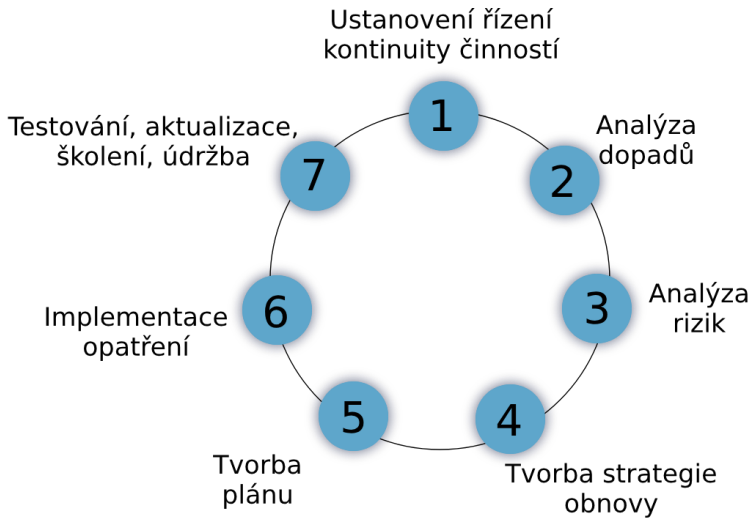
V rámci řízení přístupu ke komunikačnímu a informačnímu systému je nezbytné zajistit že:

- Řízení přístupu je prováděno za pomocí skupin a rolí.
- Každý uživatel a administrátor má unikátní identifikátor.
- Každý uživatel a administrátor získá práva a oprávnění (nezbytně nutné k výkonu práce) v souladu s politikou řízení přístupu.
- Jsou řízeny identifikátory, přístupová práva a oprávnění aplikací a technických účtů.
- Jsou zaváděna potřebná bezpečnostní opatření pro řízen přístupu zařízen k prostředkům informačního a komunikačního systému.
- Jsou přijata bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení a jiných technických zařízení, popřípadě i bezpečnostní opatření spojená s využitím technických zařízení, která nejsou ve správě organizace.
- Role a oprávnění jsou pravidelně přezkoumávány a při změně pozice nebo ukončení vztahu musí být ihned zrušeny.
- Je omezeno přidělování privilegovaných oprávnění na nezbytnou nutnou úroveň

- Je prováděno pravidelné přezkoumání nastavení veškerých přístupových oprávnění včetně rozdělení do přístupových skupin a rolí.
- Je omezeno a kontrolováno používání programových prostředků, které mohou být schopné překonat systémové nebo aplikační kontroly.
- Je prosazováno, aby uživatelé při používání privátních autentizačních informací dodržovali stanovené postupy.
- Je zajištěno odebrání nebo změnu přístupových oprávnění při změně pozice nebo zařazení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role.
- Přidělování a odebírání přístupových oprávnění je dokumentováno.
- Řízení přístupu ze všech zařízení.
- Kontrola prostředků pro překonání kontrol.
- Je využíván nástroj správy a ověřování identity podle kapitoly 6.15.1 a nástroje pro řízení přístupových oprávnění podle kapitoly 6.15.2. (Vyhláška č. 82/2018 Sb. 2018)

6.10.4 Řízení kontinuity činností

Cílem řízení kontinuity činností je přizpůsobit systém a vytvořit postupy, podle kterých bude možné zajistit funkčnost a obnovu klíčových procesů a činností organizace na předem stanovené minimální úrovni poskytovaných služeb v případě kybernetických bezpečnostních událostí (viz Kapitola 6.13.1). Životní cyklus řízení kontinuity činností viz Obrázek 10.



Obrázek 10: Schéma řízení kontinuity činností

Pro řízení kontinuity činností je nezbytné zajistit:

- Stanovit práva a povinností administrátorů a osob zastávajících bezpečnostní role.
- Posouzení možných rizik a dopadů kybernetických bezpečnostních incidentů ohrožujících kontinuitu činností (ohrožení dostupnosti), které vycházejí z hodnocení rizik a analýzy dopadů.
- Stanovení politiky řízení kontinuity činností.

- Provádět pravidelné testování a aktualizaci plánů kontinuity činností a havarijních plánů.
- Realizovat opatření pro zvýšení odolnosti informačního a komunikačního systému. (Vyhláška č. 82/2018 Sb. 2018)

Politika řízení kontinuity

Na základě výstupu hodnocení rizik a analýzy dopadů je třeba stanovit cíle řízení kontinuity činností jako:

- minimální úroveň poskytovaných služeb,
- dobu obnovení chodu,
- bod obnovení dat. (Vyhláška č. 82/2018 Sb. 2018)

Minimální úroveň poskytovaných služeb označuje stav, při kterém je užívaní, provoz a správa informačního a komunikačního systému na přijatelné úrovni,

Doba obnovení chodu označuje časový úsek, během kterého je nezbytné po kybernetickém bezpečnostním incidentu obnovit minimální úroveň poskytovaných služeb. Označuje se taktéž jako RTO (z angl. Recovery Time Objection).

Bod obnovení dat se definuje jako časové období, za které musí být data zpětně obnovena a označuje se jako RPO (angl. Recovery Point Objection).

6.11 Audit kybernetické bezpečnosti

Požadavkem na audit kybernetické bezpečnosti je provádění pravidelné kontroly dodržování:

- bezpečnostní politiky a jejího souladu s nejlepší praxí, a to včetně technické shody,
- relevantních právních předpisů, smluvních závazků a další předpisů,

V případě, že audit nalezne nedostatky, musí být na tyto nedostatky reagováno a určena a přijata taková nápravná opatření, která zajistí jejich odstranění, a tedy soulad s požadavky.

Audit je prováděn:

- při významných změnách, v rámci jejich rozsahu (pouze oblasti dotčené změnou) a
- v pravidelných intervalech alespoň jednou za tři roky v celém rozsahu požadavků v případě správce a provozovatele významného informačního systému a jednou za dva roky v případě správce nebo provozovatele systému kritické informační infrastruktury.

V případech, kdy audit kybernetické bezpečnosti nelze provést v plném rozsahu ve stanovené lhůtě (zejm. z důvodu časové náročnosti), je možné audit rozdělit systematicky na dílčí části. Takovýto postup je nutné zdůvodnit a postupovat tak, aby vždy po ukončení všech částí auditu byl výsledkem audit kybernetické bezpečnosti v celém rozsahu požadavků prováděcího právního předpisu, nejpozději v 5letém intervalu.

Organizace, která je současně provozovatelem, předkládá výsledky auditu kybernetické bezpečnosti správci daného informačního a komunikačního systému. (Vyhláška č. 82/2018 Sb. 2018)

Pravidelné posouzení stavu (audit či kontrola) celého systému řízení bezpečnosti informací je nezbytnou součástí procesu zlepšování. Během posouzení dojde k ujištění, zda je ISMS plně funkční a nalezení případných nedostatků, na které musí být adekvátně reagováno.

6.12 Bezpečnostní politika a bezpečnostní dokumentace

V rozsahu ISMS musí být v organizaci zavedena příslušná bezpečnostní politika a dokumentace. Obsah bezpečnostní dokumentace je uveden v příloze č.5 VKB. U jednotlivých dokumentů není potřeba dodržovat názvosloví ani strukturu, nicméně, jejich obsah by měl být součástí bezpečnostních dokumentů organizace, pokud je to relevantní (je aplikováno bezpečnostní opatření).

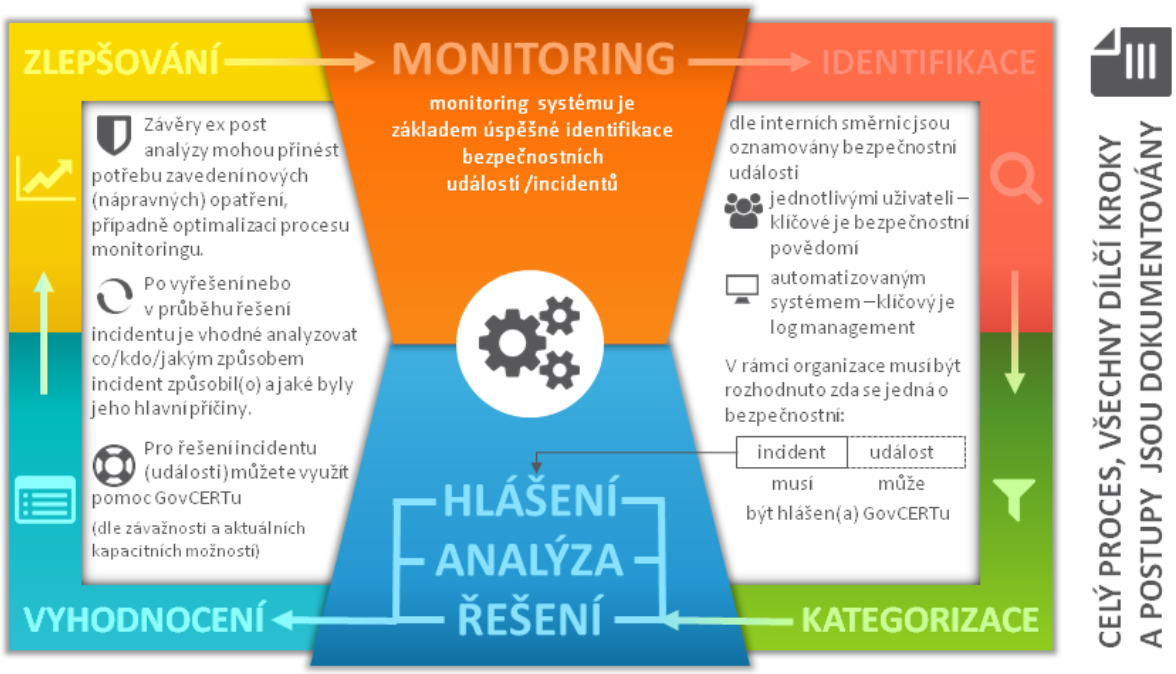
Bezpečnostní politika a bezpečnostní dokumentace:

- musí být aktuální,
- pravidelně přezkoumávána a podle potřeby revidována,
- dostupná v listinné nebo elektronické podobě,
- zpřístupněná relevantním osobám,
- vedena tak, že obsažené informace jsou úplné, čitelné, snadno identifikovatelné a snadno vyhledatelné,
- řízená,
- komunikována napříč organizací a
- chráněná z pohledu důvěrnosti, dostupnosti a integrity. (Vyhláška č. 82/2018 Sb. 2018)

✓ Doporučení: Vyvarovat se opakování stejných informací napříč různými dokumenty, dodržovat jednotou terminologii, pro snadnou vyhledatelnost využívat např. obsahy, indexování.

6.13 Zvládání kybernetických bezpečnostních událostí a incidentů

Správně nastavený proces zvládání incidentů zahrnuje velké množství dílčích činností. Kompletní proces je zachycen na obrázku.



Obrázek 11: Zvládání incidentů dle ZKB (Kintr a Široký 2019)

6.13.1 Kybernetické bezpečností události

Kybernetická bezpečnostní událost je stav, při kterém je ohrožena bezpečnost informací, nicméně nedojde k jejímu narušení. Není prokázán vliv z hlediska důvěrnosti, dostupnosti nebo integrity.

- ✓ Příklad: Neúspěšný pokus o nelegitimní přístup do systému, uživatel stáhne škodlivou přílohu e-mailu, nicméně ta je rozpoznána a zachycena antivirovým systémem

6.13.2 Kybernetické bezpečnostní incidenty

Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události. (Zákon č. 181/2014 Sb. 2014)

- ✓ Příklad: výpadek systému s vlivem na jeho dostupnost, neoprávněný přístup do systému, úmyslné porušení bezpečnostní politiky.

Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů

Organizace musí zaznamenávat bezpečnostní a potřebné provozní události důležitých aktiv informačního a komunikačního systému. Identifikaci důležitých aktiv, kterých se zaznamenávání událostí bude týkat, provede organizace podle potřeb ISMS.

Bezpečnostní událost je jakákoliv událost, která může mít přímý vliv na bezpečnost informací. Například zašifrování pevného disku, nastavení firewallu, instalace antiviru, Data Loss Prevention atd.

Provozní událostí se rozumí například snížení rychlosti připojení k internetu, docházení místa na disku, zvyšování odezvy zákaznického systému atd.

Zaznamenává se jednoznačná síťová identifikace zařízení původce, je-li v komunikační síti použit nástroj, který mění jeho síťovou identifikaci. (Vyhláška č. 82/2018 Sb. 2018) Požadavek cílí na skutečnost, aby použité bezpečnostní nástroje zcela nepřepisovaly identifikátory původců (např. IP adresy), ale aby je zachovávaly. To zejména z důvodů správného vyhodnocování událostí i pro případy vyšetřování incidentů.

- ✓ Příkladem je předcházení situacím jako např. použití nástroje typu "web application firewall" (dále "WAF"), který je nasazen nad webový server. Přičemž logy na webovém serveru poukazují, že veškeré dotazy přicházejí z IP adresy WAF, IP adresa skutečného původce dotazu, např. pomocí HTTP metod POST nebo GET, je v tomto případě zahazována.

U bezpečnostních a provozních událostí se zaznamenává:

- datum a čas (včetně časového pásma),
- typ činnosti,
- identifikace technického aktiva (které zaznamenávalo),
- identifikace účtu (kdo činnost provedl) a
- úspěšnost (popř. neúspěšnost) činnosti.

Datum a čas technických aktiv se synchronizuje nejméně jednou denně. Zaznamenaným informacím se zajistí ochrana před neoprávněným čtením a změnou.

Dále je nutné zaznamenávat:

- přihlašování a odhlašování k účtu (včetně neúspěšných pokusů),
- činnosti administrátorů,
- manipulace s účty,
- manipulace s oprávněními a právy,
- neprovedené činnosti (z důsledku nedostatečných práv a oprávnění),
- činnosti uživatelů,
- zahájení a ukončení činností technických aktiv,
- kritická a chybová hlášení technických aktiv,
- přístupy k záznamům o událostech,
- pokusy o manipulaci se záznamy o událostech a
- změny nastavení nástrojů pro zaznamenávání událostí.

Které událostí se budou zaznamenávat a následně uchovávat, by mělo být rozhodnuto v souladu s hodnocením důležitosti aktiv.

Záznamy událostí by se měly uchovávat nejméně po dobu 12 (pro významné informační systémy) nebo 18 měsíců (pro kritickou informační infrastrukturu) z důvodu, že pořizování tyto záznamy mohou sloužit pro případné vyhodnocování nebo vyšetřování bezpečnostního incidentu. (Vyhláška č. 82/2018 Sb. 2018)

6.13.3 Detekce a vyhodnocování kybernetických bezpečnostních událostí a koordinaci zvládání kybernetických bezpečnostních incidentů

Nezbytnou součástí částí zvládání kybernetických a bezpečnostních událostí a incidentů je zavedení procesu detekce a vyhodnocování kybernetických bezpečnostních událostí a koordinaci zvládání kybernetických bezpečnostních incidentů.

V rámci zvládání kybernetických bezpečnostních událostí a incidentů je nutné minimálně:

- nastavit jednoznačné odpovědnosti a definovat postupy,
- zajistit prostředí pro oznamování neobvyklého chování informačního a komunikačního systému a pro hlášení podezření na jakékoliv zranitelnosti,
- poučit uživatele, administrátory, osoby zastávající bezpečnostní role, další zaměstnance a dodavatele o existenci prostředí pro oznamování neobvyklého chování informačního a komunikačního systému a o důležitosti hlásit neobvyklé chování,
- zajistit detekci kybernetických bezpečnostních událostí (viz Kapitola 6.13.4),
- zajistit posuzování kybernetických bezpečnostních událostí, při kterém musí být rozhodnuto, zda mají být klasifikovány jako kybernetické bezpečnostní incidenty (viz Kapitola 0),
- stanovit postupy pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu,
- zajistit zvládání kybernetických bezpečnostních incidentů podle stanovených postupů a přijímat opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu,
- hlásit kybernetické bezpečnostní incidenty NÚKIB (viz Kapitola 0),
- vést záznamy o kybernetických bezpečnostních incidentech a o jejich zvládání,
- prošetřit a určí příčiny kybernetického bezpečnostního incidentu a
- vyhodnotit účinnost řešení kybernetického bezpečnostního incidentu a na základě vyhodnocení stanovit nutná bezpečnostní opatření, popřípadě aktualizovat stávající bezpečnostní opatření k zamezení opakování řešeného kybernetického bezpečnostního incidentu.

Správce a provozovatel kritické informační infrastruktury dále při detekci kybernetických bezpečnostních událostí používá nástroj pro sběr a vyhodnocování kybernetických bezpečnostních událostí. (Vyhláška č. 82/2018 Sb. 2018)

Kategorizace kybernetických bezpečnostních incidentů

Kybernetické bezpečnostní incidenty lze kategorizovat podle významnosti nebo podle dopadu.

Při kategorizování podle významnosti je třeba zohlednit dopady (dle dopadových určujících kritérií), počet dotčených osob, způsobené nebo předpokládané škody, důležitost dotčených aktiv, dopady na poskytované služby, délku trvání incidentu, zeměpisný rozsah a další dopady.

Při zohlednění se incidenty zařadí do následujících kategorií:

- **Kategorie III** – velmi významný kybernetický bezpečnostní incident, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých i potenciálních škod.

- **Kategorie II** – významný kybernetický bezpečnostní incident, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod.

- **Kategorie I** – méně významný kybernetický bezpečnostní incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod. (Vyhláška č. 82/2018 Sb. 2018)

Typ kybernetického bezpečnostního incidentu se určí podle dopadu, které způsobí narušení některé z charakteristik bezpečnosti informací:

- důvěrnost aktiv,
- integritu aktiv,
- dostupnost aktiv,
- kombinace předchozích. (Vyhláška č. 82/2018 Sb. 2018)

Forma a hlášení kybernetických bezpečnostních incidentů

Kybernetický bezpečnostní incident se Úřadu (popř. provozovateli národního CERT) hlásí na elektronickém formuláři zveřejněném na internetových stránkách Úřadu (popř. provozovatele národního CERT) zaslaném na adresu elektronické pošty Úřadu (popř. provozovateli národního CERT), do datové schránky Úřadu (popř. provozovateli národního CERT) nebo prostřednictvím datového rozhraní (pokud je používáno).

Náležitosti hlášení kybernetického bezpečnostního incidentu jsou:

- identifikace odesilatele,
- identifikace informačního a komunikačního systému,
- datum a čas zjištění incidentu a
- popis incidentu.

V případě, kdy nelze využít žádný ze způsobů hlášení, je možné jej zaslat i v listinné podobě. (Vyhláška č. 82/2018 Sb. 2018)

- ✓ Doporučení: V případě nahlašování kybernetického bezpečnostního incidentu je dobré postupovat podle zveřejněných návodů na internetových stránkách Úřadu/provozovatele národního CERT.

6.13.4 Detekce kybernetických bezpečnostních událostí

V rámci detekce kybernetických bezpečnostních událostí je nutné pomocí nástroje zajistit:

- ověření a kontrolu přenášených dat v rámci komunikační sítě, na perimetru komunikační sítě a mezi nimi jednotlivými komunikačními sítěmi a
- blokování nevyžádané komunikace.

Správce a provozovatel kritické informační infrastruktury provádí přiměřeně detekci kybernetických bezpečnostních událostí u:

- koncových stanic,
- mobilních zařízení,
- serverů,
- datových uložišť,
- výměnných datových nosičů,
- aktivních síťových prvků (router, switch) a
- obdobných aktiv. (Vyhláška č. 82/2018 Sb. 2018)

Sběr a vyhodnocení kybernetických bezpečnostních událostí

Správce a provozovatel kritické informační infrastruktury využívá nástroj pro sběr a nepřetržité vyhodnocování kybernetických bezpečnostních událostí.

Nástroj mimo sběr a vyhodnocování událostí umožní:

- sběr a vyhodnocování zaznamenaných bezpečnostních a provozních událostí,
- vyhledávání a seskupování souvisejících záznamů,
- poskytování informací pro určené bezpečnostní role o detekovaných kybernetických bezpečnostních událostech,
- identifikaci kybernetických bezpečnostních incidentů včasné varování určených bezpečnostních rolí,
- pravidelnou aktualizaci nastavení pravidel pro omezení případů nesprávného vyhodnocení událostí při vyhodnocování kybernetických bezpečnostních událostí a včasného varování a
- využívání informací pro optimální nastavení bezpečnostních opatření. (Vyhláška č. 82/2018 Sb. 2018)

Pravidla pro nesprávné vyhodnocení událostí se pravidelně aktualizují, aby se taky omezili případy jejich vniku.

6.14 Bezpečnost HW

6.14.1 Fyzická bezpečnost

K zajištění fyzické bezpečnosti je nutné nastavit přiměřená pravidla pro ochranu aktiv, tedy areálů, budov, místností a jakéhokoli vybavení, které může být překonáno, ukradeno, poškozeno nebo zničeno. K tomu je nezbytné stanovit fyzický bezpečnostní perimetr, který ohraničuje oblast pro zpracovávání informací a umístění technických aktiv ICT k předcházení neoprávněné manipulace s aktivy.

Uplatňují se následující prostředky fyzické bezpečnosti:

- zamezení neoprávněného vstupu,
- zamezení poškození,
- zamezení neoprávněných zásahů,
- zajištění ochrany na úrovni objektů a
- zajištění ochrany v rámci objektů. (Vyhláška č. 82/2018 Sb. 2018)

Za tímto účelem souží tyto bezpečnostní prvky:

- mechanické zábranné prostředky,
- zařízení elektrické zabezpečovací signalizace,
- prostředky omezující působení požárů,
- prostředky omezující působení projevů živelních událostí,
- systémy pro kontrolu vstupu,
- kamerové systémy,
- zařízení pro zajištění ochrany před selháním dodávky elektrického napájení a
- zařízení pro zajištění optimálních provozních podmínek.

6.14.2 Bezpečnost komunikačních sítí

Informační a komunikační systémy je nutné chránit na úrovni:

- Segmentace komunikační sítě.
- Řízení komunikace v rámci komunikační sítě a perimetru komunikační sítě.
- Zajištění důvěrnosti a integrity dat při přístupu mimo perimetr komunikační sítě (pomocí kryptografie).
- Aktivní blokování nežádoucí komunikace.
- Nástroj pro ochranu integrity komunikační sítě (pro segmentaci sítě a pro řízení komunikace mezi segmenty). (Vyhláška č. 82/2018 Sb. 2018)

Segmentace sítě

Segmentace sítě je rozdělení sítě organizace do jednotlivých zón (segmentů), které lze samostatně řídit, sledovat a chránit. Rozdělení lze provádět například podle organizačních jednotek, důvěrnosti dat, jednotlivých komponent infrastruktury apod. Rozdělení může být provedeno jak fyzicky, tak logicky (softwarově). Mělo by být možné řídit jak jednotlivé

segmenty, tak i samostatné komunikační sítě. Základem je vhodně navržená topologie sítě (adresace, VLAN). (Lynt services s.r.o. 2013)

- ✓ Poznámka: VLAN (Virtual Local Area Network) je logicky nezávislá síť vytvořená v rámci funkční sítě.

Zajištění důvěrnosti a integrity dat při přístupu mimo perimetr komunikační sítě

Zajištění důvěrnosti a integrity dat při přístupu mimo perimetr komunikační sítě se provádí za pomocí kryptografie, resp. zabezpečených protokolů pro komunikaci (HTTPS, SSH, CCMP, …). Pro bezpečnou komunikaci lze využít VPN, popřípadě autentizaci a šifrování pomocí certifikátu (S/MIME, PGP).

- ✓ Poznámky:
    - HTTPS (Hypertext Transfer Protocol Secure) je protokol, který umožňuje zabezpečenou komunikaci, především mezi webovým serverem a prohlížečem. (ManagementMania 2016)
    - SSH (Secure Shell) je zabezpečený komunikační protokol (zároveň i program) pro přenos dat nebo bezpečné používání vzdáleného počítače (např. používání určitých programů) přes nedůvěryhodnou počítačovou síť. Využívá se také k administraci serverů. (dsl.cz 2018)
    - CCMP (CCM Protocol) je šifrovací protokol pro bezdrátovou komunikaci, který je součástí 802.11i standardu pro bezdrátové LAN. Základem je algoritmus postavený na šifře AES. (TechTarget 2008)
    - VPN (Virtual Private Network) umožňuje zařízením (v nedůvěryhodné počítačové síti) vzdálenou komunikaci, jako by se vyskytovaly v lokální síti. (TechTarget 2019)
    - S/MIME (Secure/Multipurpose Internet Mail Extensions) je certifikát k zabezpečení elektronické pošty. Je standardem pro podepisování obsahu a šifrování veřejným klíčem a je využívána většinou poskytovatelů emailových služeb. (Techopedia Inc. 2019d)
    - PGP (Pretty Good Privacy) je metodika založená na algoritmu RSA používaná pro podepisování a šifrování. (Techopedia Inc. 2019c)

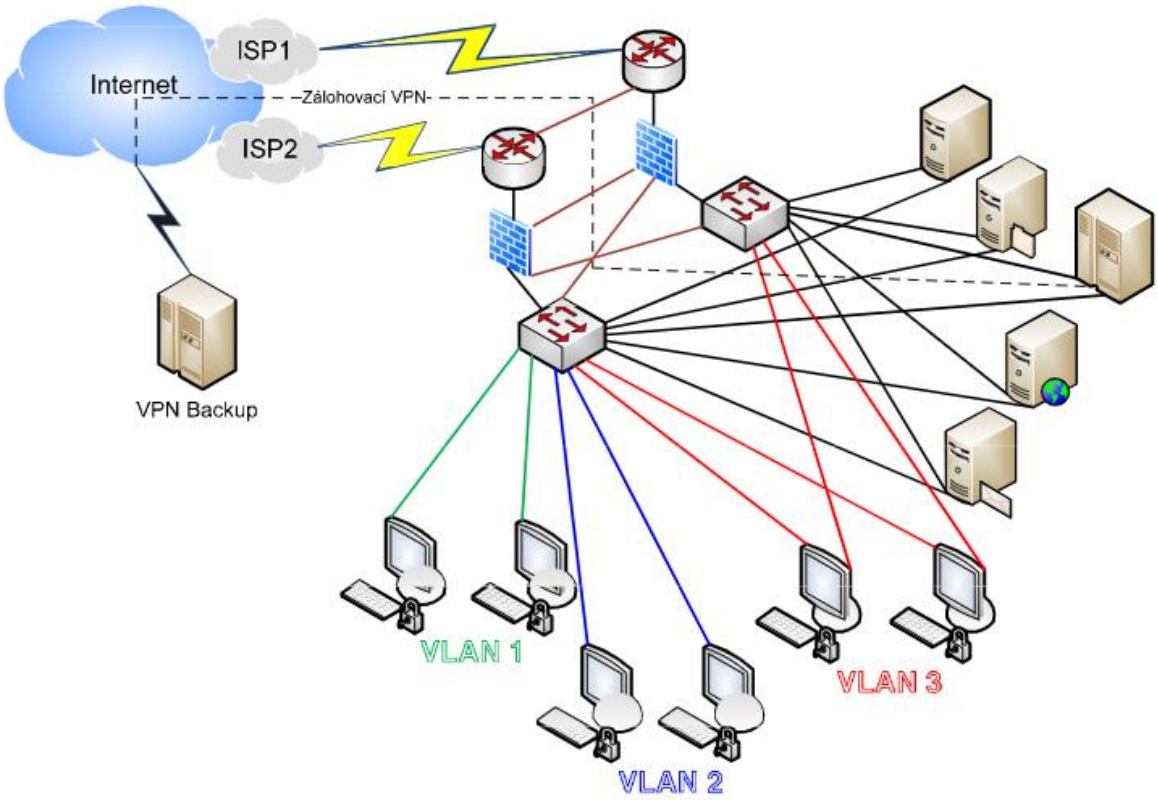
Blokování nežádoucí komunikace

Blokování nežádoucí komunikace spočívá v monitorování komunikace. Na základě vyhodnocovaných pravidel je pak blokována nežádoucí komunikace.

Lze použít nástroje typu IDS, IPS, Firewall a spoustu dalších. Současně je vhodné využívat i restrikce, typu blacklist, tedy seznam blokovaných adres (nepovolená, nežádoucí komunikace), se kterými nepůjde komunikovat a whitelist, tedy seznam povolených adres (povolená, žádoucí komunikace).

✓ Poznámky:

- IPS (Intrusion Prevention Systems) je obranný systém, který identifikuje škodlivé činnosti a následně se je snaží zablokovat. (Varonis 2018)
- IDS (Intrusion Detection Systems) je obranný systém detekující neobvyklé (podezřelé) aktivity monitorováním síťového provozu. (Varonis 2018)
- Firewall je software pro zabezpečení privátní sítě a využívá se pro zabezpečení síťového provozu mezi různými sítěmi. Firewall může být implementován i jako hardware. (Techopedia Inc. 2019a)



Obrázek 12: Model zabezpečené sítě (Ondrák et al. 2013)

6.15 Uživatelé a oprávnění

6.15.1 Správa a ověřování identit

Nástroj pro správu a ověření identit

Další oblastí bezpečnostních opatření je využívání nástroje pro správu a ověření identit (angl. Identity and Access Management, zkr. IAM) u uživatelů, administrátorů a aplikací informačního a komunikačního systému. Životní cyklus identit IAM viz Obrázek 13.

Tento nástroj musí zajistit:

- ověření identity ještě před samotným zahájením akcí v informačním a komunikačním systému,
- znovu ověření identity po určené době nečinnosti,
- řízení počtu neúspěšných pokusů o přihlášení (ochrana proti útoku hrubou silou, kdy dojde např. k prodlevě mezi možností o další pokus o zadání hesla, případně k dočasnému zablokování účtu – nutné nastavit přiměřeně vzhledem k případnému DDOS útoku na uživatelské účty),
- odolnost uložených nebo přenášených autentizačních údajů proti neoprávněnému odcizení a zneužití (nepřenášet a neukládat hesla v nezašifrované podobě)
- ukládání autentizačních údajů ve formě odolné proti offline útokům (ochrana nejen samotných hesel ale i databáze hesel),
- dodržení důvěrnosti autentizačních údajů při obnově přístupu (generovat jednorázová hesla, nezasílat hesla e-mailem atd.),
- centralizovanou správu identit. (Vyhláška č. 82/2018 Sb. 2018)



Obrázek 13: Životní cyklus identit, Zdroj: icspraha.com

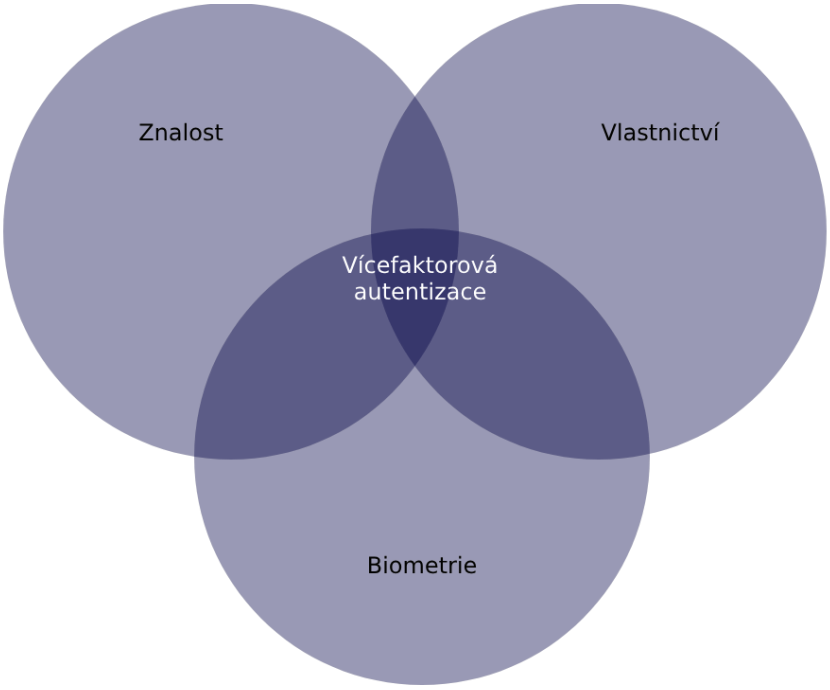
Vícefaktorová autentizace

Organizace musí, pokud tomu nebrání jiné objektivní důvody, pro ověření identity uživatelů, administrátorů a aplikací, využívat autentizační mechanizmus, který není založený pouze na použití identifikátoru účtu a hesla, nýbrž na vícefaktorové autentizaci (angl. Multi Factor Authentication, zkráceně MFA) s nejméně dvěma různými typy faktorů. (Vyhláška č. 82/2018 Sb. 2018)

Typy faktorů jsou:

- znalostní (něco, co uživatel zná nebo je mu sděleno)
    - např.: PIN, heslo, …
- vlastnický (něco co uživatel vlastní)
    - např.: Token, mobilní telefon, …
- biometrický (fyziologická vlastnost samotného uživatele)
    - Např.: Otisk prstu, oční sítnice, … (SystemOnLine.cz 2016)

Z pohledu finanční náročnosti a nároků na systém je pořízení a implementace tohoto způsobu autentizace stále často nejobtížnější a v některých případech by se při implementaci tohoto řešení u již existujících systémů mohlo jednat o nepřiměřené náklady. Na druhou stranu, při vhodné implementaci tohoto řešení se jedná v současné době o jeden z nejbezpečnějších způsobů autentizace.



Obrázek 14: Vícefaktorová autentizace

Kryptografické klíče

V případě, kdy není možné používat vícefaktorovou autentizaci, musí nástroj pro ověřování identity uživatelů, administrátorů a aplikací využívat alespoň autentizaci pomocí kryptografických klíčů, s tím, že je nutné zajistit minimálně obdobnou výši úrovně zabezpečení jako v případě využití vícefaktorové autentizace (využitím bezpečných algoritmů, bezpečným procesem správy klíčů atd.). (Vyhláška č. 82/2018 Sb. 2018)

Identifikátor účtu a heslo

Za předpokladu využívání autentizace pomocí pouze identifikátoru účtu a hesla k autentizaci, která zajišťuje nejnižší míru zabezpečení, je nutné technologicky vynucovat následující pravidla:

- Minimální délka hesel alespoň 12 znaků u uživatelů a 17 u administrátorů a aplikací.
- Možnost vytvořit a zapsat heslo o délce alespoň 64 znaků.
- Neomezené použití malých a velkých písmen, číslic a speciálních znaků.
- Možnost změnit heslo, přičemž mezi dvěma změnami musí být minimální interval 30 minut.
- Zakázat používání nejčastěji používaných hesel (kontrola proti slovníku).
- Zakázat mnohonásobně opakující se znaky.
- Zakázat využívání identifikačních údajů, identifikátorů osoby, e-mailů v hesle (kontrola řetězce hesla na shodu s identifikátorem účtu, příjmením, jeho e-mailem atd.).
- Omezit opětovné využívání dříve používaných hesel s pamětí pro alespoň 12 dříve používaných hesel.
- Povinná změna hesla v maximálním intervalu 18 měsíců (toto pravidlo se nevztahuje na účty sloužící k obnově systému v případě havárie).

Za předpokladu, že je využívání identifikátoru účtu a hesla je jediným způsobem autentizace, musí se dále dodržovat tato pravidla:

- Vynucení změny výchozího hesla po jeho prvním použití.
- Zneplatnění hesla sloužícího k obnovení přístupu po jeho prvním použití nebo po uplynutí nejvýše 60 minut od jeho vytvoření. (Vyhláška č. 82/2018 Sb. 2018)

6.15.2 Řízení přístupových oprávnění

Pro řízení přístupových oprávnění je vymezen požadavek na používání centralizovaného nástroje.

- S tímto nástrojem lze snáze řídit změny, které se následně promítají do dílčích částí systému. (Centralizovaná správa přístupových oprávnění napojená na AAA server zajistí jednotnou konfiguraci napříč celým systémem).

Je třeba zajistit řízení oprávnění na úrovni

- přístupu k jednotlivým aktivům systému
- pro čtení a zápis dat. (Vyhláška č. 82/2018 Sb. 2018)

Pro definici práv se nejčastěji využívá ACL (Access Control List), který určuje práva uživatelů na úrovni souborů, také se implementují práva na úrovni aplikací a operačního systému. Objektem oprávnění je přístup k jednotlivým aktivům informačního a komunikačního systému

- ✓ Poznámky:
    - AAA (authentication, authorization, and accounting) Server se stará o požadavky uživatelů pro připojení k počítači a poskytuje autentizaci, autorizaci a účtování. (TechTarget 2007)
    - ACL (Access Control List) je seznam oprávnění, které zajišťují přístup k libovolnému objektu. Může být jak na síťové úrovni (objektem jsou nejčastěji aktivní síťové prvky), tak i na systémové úrovni (objektem je nejčastěji soubor).

6.16 SW ochrana

Ochrana před škodlivým kódem

Ochrana před škodlivým kódem je důležitou součástí bezpečnosti kybernetického prostředí vzhledem k faktu, že množství škodlivého kódu neustále narůstá a je stále sofistikovanější. Je proto vyžadováno, aby správci a provozovatelé kritické informační infrastruktury za účelem ochrany před škodlivým kódem používaly vhodné nástroje, které zajišťují nepřetržitou automatickou ochranu a aby tyto nástroje byly pravidelně aktualizovány. Správce a provozovatel významného informačního systému toto opatření zavádí přiměřeně.

Do této kategorie patří nástroje pro detekci škodlivého kódu a skenery zranitelností (např. antivirové programy, nástroje pro detekci/prevenci průniku, nástroje pro síťovou analýzu, behaviorální nástroje atp.).

Nasazení konkrétního nástroje a způsob jeho implementace by vždy měly vycházet z výsledků analýzy rizik a z bezpečnostních potřeb organizace.

Nepřetržitá automatická ochrana probíhá s ohledem na důležitost aktiv u:

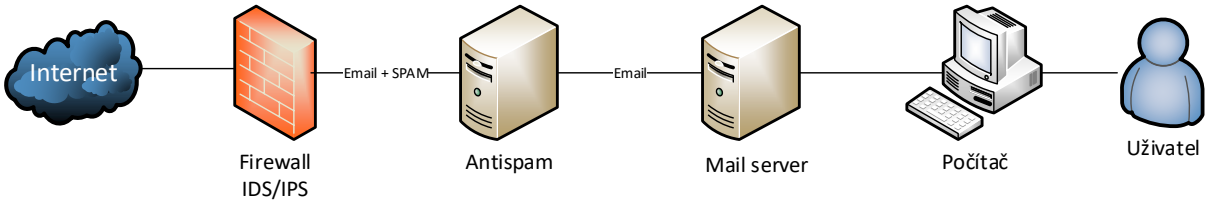
- koncové stanice,
- mobilní zařízení,
- servery,
- datová uložiště,
- výměnné datové nosiče,
- komunikační sítě a jejich prvky a
- obdobná zařízení.

U výměnných zařízení a datových nosičů je třeba monitorovat a řídit jejich používání a řídit automatické spouštění obsahu.

Dále je vhodné řídit oprávnění ke spouštění kódu a provádět pravidelnou a účinnou aktualizaci nástroje pro ochranu před škodlivým kódem. (např. tím, že ke spouštění kódu se váží oprávnění, aby se zamezilo náhodnému spuštění nekvalifikovaným uživatelem). (Vyhláška č. 82/2018 Sb. 2018)

Nástroji pro ochranu před škodlivým kódem mohou být antivir, HIPS/HIDS (Host-based Intrusion Protection/Detection System), Antispam, Applocker atd. Zapojení Antiviru a Antispamu v síti při přijetí pošty viz Obrázek 15Obrázek 12.

- ✓ Poznámky:
    - Antivirový program je software, který identifikuje a eliminuje počítačové viry na základě virové databáze. Sleduje vstupní a výstupní místa a porovnává je s virovou databází. (Archer 2016)
    - HIPS (Host-based Intrusion Protection System) je řešení, které detekují nežádoucí aktivitu na počítači uživatele. Na rozdíl od antiviru HIPS slouží jako ochrana proti známým i neznámým útokům. (Techopedia Inc. 2019b)
    - Antispam je systém, který se snaží identifikovat spam a poté odstranit ze schránky. Nezaručuje úplnou ochranu proti phishingu. (Archer 2016)
    - Applocker aplikace založená na whitelistu, tedy určuje, které programy mohou být spuštěny.



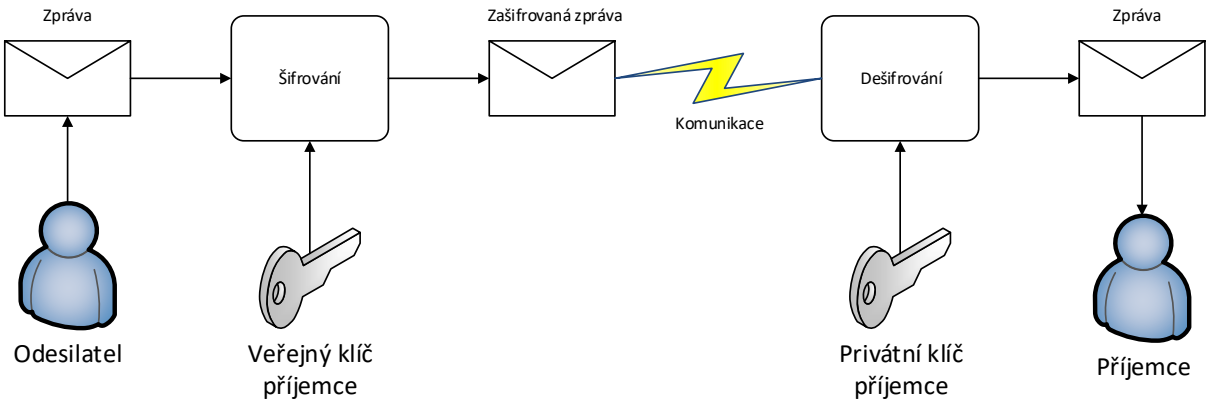
Obrázek 15: Zjednodušené schéma přijetí pošty

Kryptografické prostředky

Pro ochranu aktiv informačního a komunikačního systému se využívají kryptografické prostředky (kryptografická algoritmy a kryptografické klíče) a je velmi důležité používat pouze ty, které jsou aktuálně odolné pro zajištění potřebné kvality a nezbytné ochrany a správy šifrovacích klíčů a certifikátů. S kryptografickými prostředky je třeba bezpečně nakládat a při jejich užívání zohledňovat doporučení Úřadu, který je zveřejňuje na webových stránkách (úřední deska NÚKIB).

Systém správy klíčů a certifikátů zajišťuje generování, distribuci, ukládání, změny, omezení platnosti, zneplatnění certifikátů a likvidaci klíčů. Systém musí umožnit i kontrolu a audit. (Vyhláška č. 82/2018 Sb. 2018)

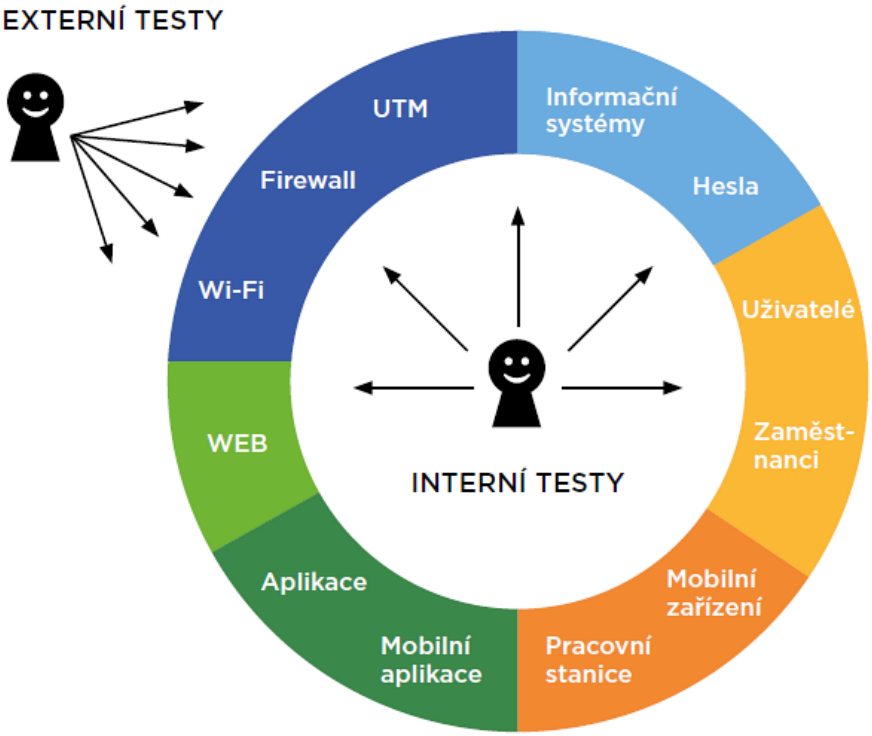
Kryptografie se dělí na symetrickou a asymetrickou. Při symetrickém šifrování se využívá jeden klíč, které znají pouze obě strany. U asymetrického šifrování máme dva klíče, jeden je a veřejný (pro šifrování) a druhý soukromý (pro dešifrování viz Obrázek 16. Zatímco veřejný klíč je dostupný každému, privátní klíč má pouze vlastník klíče.



Obrázek 16: Příklad asymetrické kryptografie

6.17 Aplikační bezpečnost

Součástí aplikační bezpečnosti je provádění penetračních testů informačního a komunikačního systému se zaměřením na důležitá aktiva. Penetrační testy se provádějí před uváděním aktiva do provozu a v souvislosti s významnou změnou. Penetrační testy je nutné spouštět za účelem nalezení případných slabých míst (zranitelnosti) z pohledu bezpečnosti a tato slabá místa odstranit, aby nemohla být ohrožena bezpečnost celého systému. (Vyhláška č. 82/2018 Sb. 2018)



Obrázek 17: Obsah penetračního testování (tns.cz 2019)

Aplikační bezpečnost dále zahrnuje trvalou ochranu pro aplikace, informace a transakce před neoprávněnou činností (např. kompromitace, neautorizovaná změna) a popřením neprovedených činností (nepopiratelnost). (Vyhláška č. 82/2018 Sb. 2018)

Kromě penetračních testů se dále provádí aplikační testy, WAF a skenování zranitelností.

- ✓ Poznámky:
    - Aplikační testy se provádějí na webových aplikacích za účelem zjištění zranitelností.
    - WAF (Web Application Firewall) zavádí souhlas pravidel na HTTP konverzaci (mezi klientem a webovou aplikací). Podle obsahu tyto dotazy filtruje nebo blokuje. (OWASP 2016)
    - Skenování zranitelností je proces analýzy systému z pohledu známých chyb.

6.18 Zajišťování úrovně dostupnosti informací

Pro zajištění úrovně dostupnosti se zavedou opatření, kterými se zajistí:

- Dostupnost informačního a komunikačního systému pro splnění cílů podle Kapitoly 6.10.4.
- Odolnost informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům.
- Dostupnost důležitých technických aktiv informačního a komunikačního systému.
- Redundanci aktiv nezbytných pro zajištění dostupnosti informačního a komunikačního systému. (Vyhláška č. 82/2018 Sb. 2018)

Způsoby a nástroje pro zajištění úrovně dostupnosti a odolnosti proti kybernetickému bezpečnostnímu incidentu se využívají HA clustery, HA Proxy, robustní návrh sítě, antiDDoS.

Doporučuje se vytvořit Disaster Recovery Plan, který shromažďuje postupy pro zajištění obnovy IT služeb po živelných pohromách a jiných zásadních událostech. Jeho cílem je v nejkratší době obnovit chod kritických aplikací a skládá se z řetězce konkrétních kroků vedoucích k obnově.

- ✓ Poznámky:
    - HA cluster (High Availability cluster) je skupina hostitelů, kteří společně vytváří jeden systém a tím průběžně zajišťují maximální dostupnost.
    - HA Proxy (High Availability Proxy) je zařízení, které distribuuje síť, popř. aplikační provoz mezi několik clusterů.
    - Robustní návrh sítě zaručí vysokou spolehlivost a odolnost vůči poruchám funkčnosti kritických služeb.

- AntiDDoS chrání proti útokům typu DDoS (přehlcení služby za pomocí velkého počtu zařízení).

6.19 Průmyslové, řídící a obdobné specifické systémy

Organizace pro zajištění kybernetické bezpečnosti průmyslových, řídicích a obdobných specifických systémů používá nástroje a opatření, které zajistí:

- Použití technických a programových prostředků, které jsou určeny do specifického prostředí.
- Omezení fyzického přístupu k zařízením těchto systémů a ke komunikační síti.
- Vyčlenění komunikační sítě určené pro tyto systémy od ostatní infrastruktury.
- Omezení a řízení vzdáleného přístupu k těmto systémům.
- Ochranu jednotlivých technických aktiv těchto systémů před využitím známých zranitelností.
- Obnovení chodu těchto systémů po kybernetickém bezpečnostním incidentu. (Vyhláška č. 82/2018 Sb. 2018)

✓ Poznámka: Používání těchto nástrojů a opatření by mělo vyplývat i ze správně provedené analýzy rizik pro tyto systémy

7 Obsah e-learningového kurzu – praktická část kurzu

Pro praktickou část kurzu byl zvolen příklad, který je demonstrován na fiktivní organizaci. Fiktivní organizace slouží jako testovací prostředí pro plnění úkolů souvisejících se zavedením ISMS. V jednotlivých částech je vždy zadáno několik úkolů, kterými účastník musí projít.

7.1 Popis organizace

Pro tyto účely se vymyslel menší úřad, nazvaný jako Úřad pro kontrolu senzorů (dále ÚKS). ÚKS je stručně popsán v několika bodech. Jedná se o úřad, který provádí měření a odbornou certifikaci senzorů na měření srdeční činnosti. Je dán tím, že dodavatelé těchto senzorů musí získat certifikát před uvedením produktu na trh, který je vydán po kontrole v odborné laboratoři, jež je součástí úřadu. Mimo jiné ÚKS kontroluje dodržování podmínek pro udržení certifikace a je povinen si vést evidenci neveřejných informací o všech senzorech, na kterých provádí testování. ÚKS je jediným orgán provádějící tuto certifikaci na území České Republiky a zaměstnává celkem 110 osob.

Přehled základních systémů, které ÚKS používá:

- Personální systém
- Ekonomický systém
- Spisová služba
- Webová prezentace
- Intraportál
- Emailová služba
- Certifikační systém
- Docházkový systém

Zjednodušený pohled na vybrané klíčové procesy úřadu je dán tabulkou Tabulka 8.

Tabulka 8: Klíčové procesy fiktivní organizace

Činnost	Popis	Zodpovědný útvar	Způsob vedení agendy
Řešení personálních otázek	Životní cyklus zaměstnanců od jejich náboru po ukončení spolupráce. Dále např. řešení zvyšování kvalifikace a školení zaměstnanců, změny zařazení zaměstnanců v organizaci, hlídání nároků a čerpání dovolených atd.	Personální oddělení	Převážně v elektronické podobě v rámci personálního systému

Správa financí úřadu	Kontrola čerpání financí, vyplácení mezd atd.	Ekonomické oddělení	V elektronické podobě.
Certifikace zařízení	Certifikace probíhá na základě testování v laboratoři, která je majetkem úřadu. Pokud laboratoř schválí produkt k certifikaci, certifikace je udělena.	Oddělení certifikace	Elektronicky
Vedení spisů	Zajištění správného životního cyklu dokumentů a spisů, a to od jejich vzniku, oběh, vyřízení až po skartační řízení v souladu se zákonem.	Kancelář úřadu	Elektronicky i papírovou formou.

7.2 Organizační struktura

Poté, co se účastník kurzu seznámí s činností ÚKS se jeho první úkol týká „správného“ zařazení oddělení kybernetické bezpečnosti v rámci organizace, své vysvětlení musí odůvodnit.

Následně je předvedena zjednodušená organizační struktura, která se nadále používá, jako možné správné řešení, viz Obrázek 18.

Přiložen je také krátký popis některých organizačních úseků.

Kancelář úřadu:

- Tiskový mluvčí úřadu.
- Mezinárodní spolupráce.
- Koordinace projektů.
- Je zde celkem 8 osob.

Laboratoř:

- Nezávislá laboratoř pro testování a měření kvality přístrojů.
- Je zde celkem 20 osob.
- K práci využívají speciální ICT technologie, určené a vyvinuté pro měření kvality snímačů tepové frekvence, výsledky měření následně předávají oddělení certifikace.
- Kompletní provoz a správu ICT technologií provádí Oddělení informačních technologií.

Oddělení certifikace

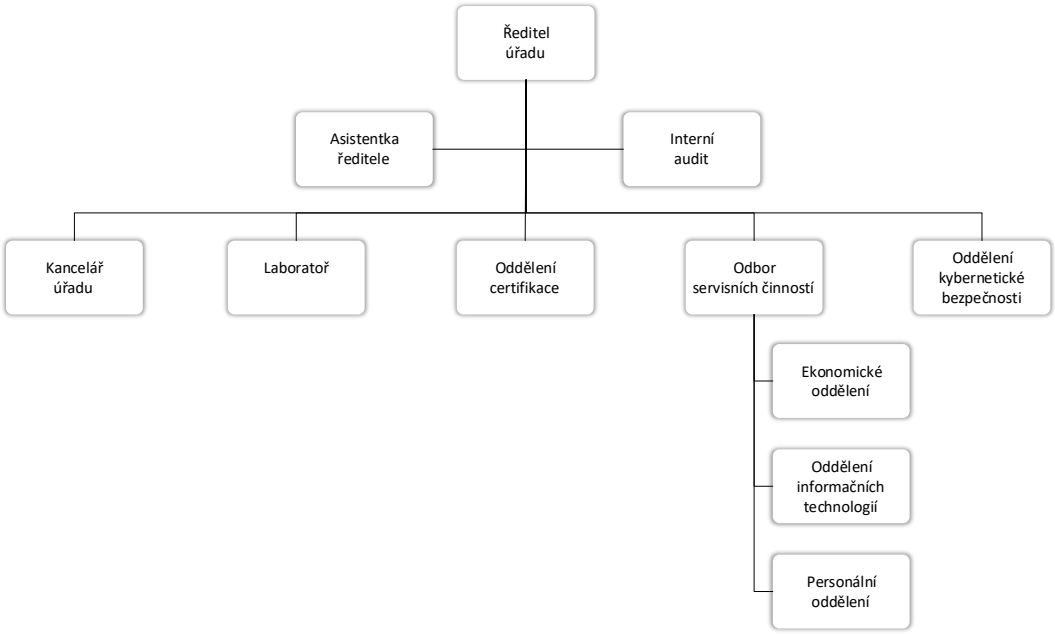
- Na základě výsledků z Laboratoře vystavují informaci o výsledku certifikace, které následně zasílají zájemci o certifikaci a vydávají do databáze, která je veřejně dostupná na webových stránkách úřadu.
- Je zde celkem 12 zaměstnanců.

Odbor servisních činností:

- Ekonomické oddělení:
    - Řeší ekonomické záležitosti.
    - Celkem 8 osob.
- Oddělení informačních technologií:
    - Řeší pro úřad kompletně zajištění provozu a správy ICT technologií.
    - Celkem 10 osob.
- Personální oddělení:
    - Řeší personální záležitosti.
    - Celkem 8 osob.

Oddělení kybernetické bezpečnosti:

- Odpovědná za kybernetickou bezpečnost úřadu.
- Manažer kybernetické bezpečnosti a auditor kybernetické bezpečnosti.
- Celkem 2 osoby.



Obrázek 18: Organizační struktura fiktivní organizace

7.3 ISMS

V následujících úkolech se účastník setká se samotnou problematikou ISMS.

V první řadě je nutné stanovení rozsahu ISMS, dále určení cílů ISMS a navrhnout pro výbor kybernetické bezpečnosti úkony pro manažera kybernetické bezpečnosti v rámci zavádění ISMS.

ÚKS si dále musí stanovit dokument Vrcholová bezpečnostní politika (ISMS). Účastník rámcově vypíše závazky, které tento dokument musí obsahovat.

Součástí je také rozeznávání významných změn.

Na závěr této podkapitoly se projednává, jakým způsobem se ISMS bude monitorovat.

7.4 Identifikace a evidence aktiv

Další částí je identifikace a evidence aktiv. Nyní účastník vystupuje už jen pouze jako manažer kybernetické bezpečnosti. Získaný seznam aktiv musí rozdělit na primární a podpůrná aktiva. Následně musí být schopen určit garanta aktiv pro vybraná aktiva.

Podpůrná aktiva je třeba dále roztřídit podle normy ISO/IEC 27005 na hardware, software, sítě, lokalitu, pracovníky a organizaci.

7.5 Řízení rizik

Po tom, co máme upřesněný katalog primárních a podpůrných aktiv přijde na řadu řízení rizik. Nejdřív se požaduje definice hrozby a zranitelnosti, které se následně vyzkouší na příkladu, je třeba tyto vlastnosti roztřídit.

Při výpočtu rizik se zohlední vhodný výpočet rizika. V této fázi je analýza rizik hotová, známe hodnotu rizik, jejich hrozby a zranitelnosti.

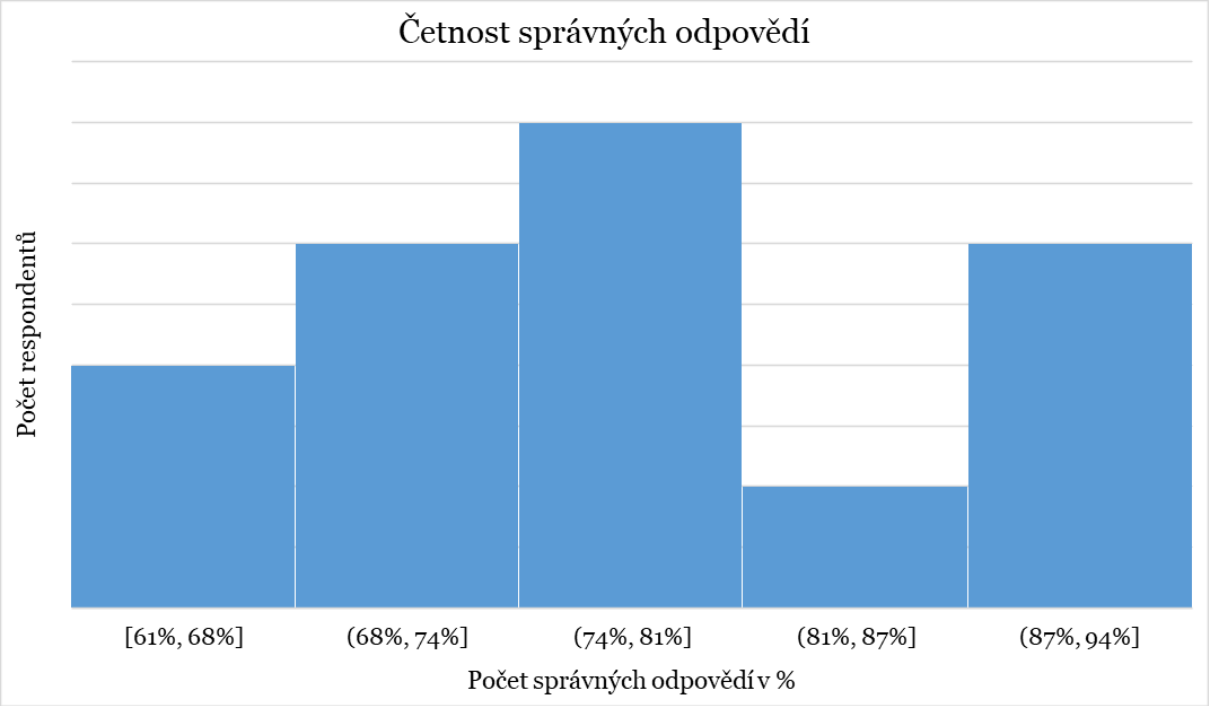
Začne se tvořit plán zvládání rizik a prohlášení o aplikovatelnosti. Po specifikaci těchto dvou dokumentů praktický příklad končí.

8 Vyhodnocení e-learningového kurzu

Výsledky se získávají ze třech různých zdrojů, z teoretického testu, z úkolů praktické části a z dotazníku spokojenosti.

8.1 Vyhodnocení teoretického testu

Výsledky teoretického testu dopadly lépe, než bylo předpokládáno, nicméně i tak celková úspěšnost nebyla dostačující. Procento správných odpovědí se pohybovalo v rozpětí od 61 % do 94 %, přičemž průměrný výsledek je 78 %. Histogram úspěšnosti podle počtu správných odpovědí, vyjádřené v procentech, je uveden na Obrázek 19. Pro úspěšné zvládnutí kurzu se počítá minimální hranice 74 % správně zodpovězených otázek, tedy alespoň 23 správně zodpovězených otázek, což se podařilo více než 75 % všech tázaných.



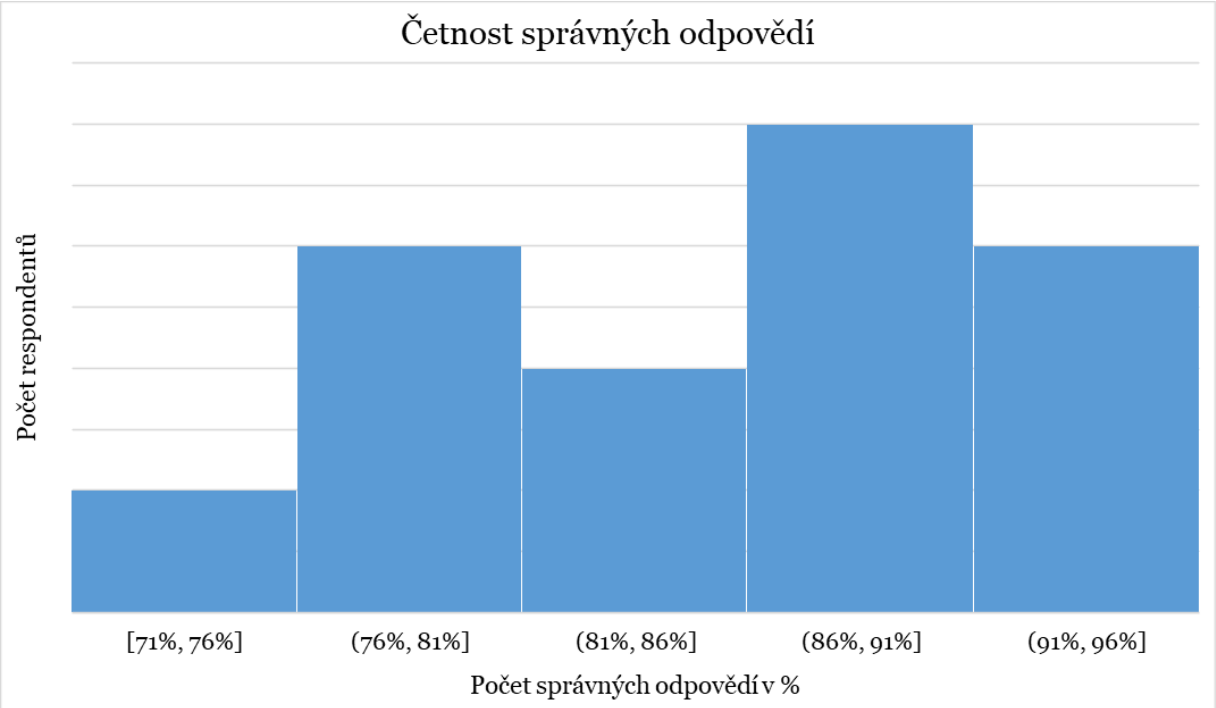
Obrázek 19: Četnost správných odpovědí teoretického testu

Nejvíce problematickým tématem byly otázky ohledně rolí kybernetické bezpečnosti. Při rozdělení na organizační a technické otázky byla chybovost téměř totožná.

8.2 Vyhodnocení úkolů praktické části

Celá praktická část byla přizpůsobena tak, aby při jejím hodnocení velkého množství účastníků nezabral každý test více než deset minut.

Prvním výstupem je počet správných odpovědí, zde se úspěšnost správně zodpovězených otázek pohybovala kolem 85 %. Procento správných odpovědí se pohybovalo v rozpětí od 71 % do 96 %. Obdobně jako u předchozí části se předpokládala minimální hranice pro úspěšné absolvování této části 75 %, jež překročilo více než 90 % zúčastněných. Histogram úspěšnosti podle počtu správných odpovědí, vyjádřené v procentech, je uveden na Obrázek 20.



Obrázek 20: Četnost správných odpovědí praktické části

Nejvíce problematickým tématem byla práce s výstupem analýzy rizik. Dalšími obtížnějšími tématy bylo stanovení a odůvodnění rozsahu ISMS a určování významných změn. Překvapivě oproti teoretickému testu zde nebyl téměř žádný problém s určováním bezpečnostních rolí, speciálně určování garanta příslušného aktiva.

8.3 Vyhodnocení dotazníku spokojenosti

Z celkového vyhodnocení dotazníku spokojenosti vyplývá, že praktický příklad byl pro účastníky kurzu velmi užitečný z pohledu všech zkoumaných aspektů. Celkové hodnocení praktického příkladu se pohybuje v průměru okolo 2,1, zatímco teorie byla ohodnocena průměrem 1,9. Z pohledu všech vlastností byl kurz jako celek ohodnocen známkou 2.

Závěr

Cílem této práce bylo vytvoření obsahu pro e-learningový kurz. Cíl byl splněn a popis kurzu je popsán v kapitole 5.Teoretická část kurzu je v kapitole 6 a praktická část kurzu je v kapitole 7. Byl vytvořen e-learningový kurz v oblasti kybernetické bezpečnosti pro reálné subjekty, především orgány veřejné moci, jež jsou správci významných informačních systémů nebo informačního nebo komunikačního systému kritické informační infrastruktury. E-learning je vytvořen ve výukovém programu Moodle. Předmětem e-learningového kurzu je vyhláška o kybernetické bezpečnosti.

Na prvních testovaných subjektech se ukázalo zlepšení oproti výsledkům dosažených před absolvováním tohoto e-learningu. Kurz také šetří čas pracovníků Národního úřadu pro kybernetickou a informační bezpečnost a jiných orgánů zainteresovaných v tomto tématu a je možné provádět tato školení s větší intenzitou.

Z jednotlivých výsledků kurzu se ukázalo, že teoretický test je pro účastníky složitější, jeho úspěšnost se pohybovala v průměru okolo 75 %. Praktický příklad uvedený na fiktivní organizaci byl výrazně úspěšnější, kde minimální hranici splnilo více než 90 % účastníků. Z výsledků testu je patrné, že je zapotřebí provádět školení v této oblasti i mezi manažery.

Kurz byl kladně ohodnocen dotazníkem spokojenosti a byly získány převážně pozitivní reakce na jeho obsah.

Výsledky této práce jsou limitovány nízkým počtem získaných odpovědí, které mohou zkreslovat finální výstupy. Obsah kurzu by se v budoucnosti mohl dále rozvíjet, aby přinesl vyšší přínos osobám zastávající bezpečnostní role a nadále zvyšoval informovanost v oblasti kybernetické bezpečnosti.

Práce může být využita k získání základního přehledu legislativy kybernetické bezpečnosti, kybernetické bezpečnosti ve státním sektoru, řízení bezpečnosti informací, popřípadě také může sloužit k detailnímu vysvětlení vyhlášky o kybernetické bezpečnosti.

Literatura

ARCHER, Peter, 2016. What's the difference between anti-spam and anti-virus IT protection? *Q2Q* [online] [vid. 2019-04-14]. Dostupné z: https://www.q2q-it.com/q2q-blog/item/188-what-s-the-difference-between-anti-spam-and-anti-virus-it-protection

BOWEN, Pauline, Joan HASH a Mark WILSON, 2006. Information Security Handbook: A Guide for Managers. 178.

ČSN ISO/IEC 27001, 2014. *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky*. září 2014. B.m.: únmz.

ČSN ISO/IEC 27004, 2016. *Informační technologie - Bezpečnostní techniky - Řízení bezpečnosti informací - Monitorování*. 2016. B.m.: ICS.

ČSN ISO/IEC 27005, 2013. *Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací*. srpen 2013. B.m.: ICS.

DSL.CZ, 2018. *SSH – bezpečné používání vzdáleného počítače a kopírování dat | DSL.cz* [online] [vid. 2019-04-14]. Dostupné z: http://www.dsl.cz/jak-na-to/jak-na-ssh#co-je-ssh

KINTR, Lukáš a Libor ŠIROKÝ, 2019. *Kybernetické bezpečnostní incidenty a jejich hlášení*.

KOLOUCH, Jan a Pavel BAŠTA, 2019. *CyberSecurity* [online]. 1. Praha: CZ.NIC, z. s. p. o [vid. 2019-04-13]. ISBN 978-80-88168-34-8. Dostupné z: https://knihy.nic.cz/files/edice/cybersecurity.pdf

LYNT SERVICES S.R.O., 2013. *Zabezpečení firemní sítě* [online] [vid. 2019-04-14]. Dostupné z: https://lynt.cz/infrastruktura/zabezpeceni

MANAGEMENTMANIA, 2016. HTTPS (Hypertext Transfer Protocol Secure). *ManagementMania.com* [online] [vid. 2019-04-14]. Dostupné z: https://managementmania.com/cs/https-hypertext-transfer-protocol-secure

NAŘÍZENÍ VLÁDY Č. 432/2010 SB., 2010. *Nařízení vlády o kritériích pro určení prvku kritické infrastruktury*. 30. prosinec 2010.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2018. *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* [online]. NIST Cybersecurity White Paper. Gaithersburg, MD: National Institute of Standards and Technology [vid. 2019-04-21]. Dostupné z: doi:10.6028/NIST.CSWP.04162018

NBU.CZ, 2019. O NBÚ. *Národní bezpečnostní úřad* [online] [vid. 2019-04-13]. Dostupné z: https://www.nbu.cz/cs/o-nas/

NÚKIB, 2019. *Bezpečnostní role* [online]. Dostupné z: https://www.govcert.cz/download/kii-vis/VKB/bezpe%C4%8Dnostn%C3%AD-role_v1.1.pdf

ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK, 2013. *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM. ISBN 978-80-7204-872-4.

OWASP, 2016. Web Application Firewall. *The OWASP™ Foundation* [online] [vid. 2019-04-14]. Dostupné z: https://www.owasp.org/index.php/Web_Application_Firewall

RISKANALYSISCONSULTANTS, 2019. RAC - Řada norem ISO/IEC 27000. *RiskAnalysisConsultants* [online] [vid. 2019-04-13]. Dostupné z: http://www.iso27000.cz/

SYSTEMONLINE.CZ, 2016. *Bezpečnostní politika hesel a vícefaktorová autentizace* [online] [vid. 2019-04-14]. Dostupné z: http://www.systemonline.cz/it-security/bezpecnostni-politika-hesel-a-vicefaktorova-autentizace.htm?mobilelayout=false

TECHOPEDIA INC., 2019a. What is a Firewall? - Definition from Techopedia. *Techopedia.com* [online] [vid. 2019-04-14]. Dostupné z: https://www.techopedia.com/definition/5355/firewall

TECHOPEDIA INC., 2019b. What is a Host-Based Intrusion Prevention System (HIPS)? - Definition from Techopedia. *Techopedia.com* [online] [vid. 2019-04-14]. Dostupné z: https://www.techopedia.com/definition/4290/host-based-intrusion-prevention-system-hips

TECHOPEDIA INC., 2019c. What is Pretty Good Privacy (PGP)? - Definition from Techopedia. *Techopedia.com* [online] [vid. 2019-04-14]. Dostupné z: https://www.techopedia.com/definition/4062/pretty-good-privacy-pgp

TECHOPEDIA INC., 2019d. What is Secure MIME (S/MIME)? - Definition from Techopedia. *Techopedia.com* [online] [vid. 2019-04-14]. Dostupné z: https://www.techopedia.com/definition/9245/secure-mime-smime

TECHTARGET, 2007. What is AAA server (authentication, authorization, and accounting)? - Definition from WhatIs.com. *SearchSecurity* [online] [vid. 2019-04-14]. Dostupné z: https://searchsecurity.techtarget.com/definition/AAA-server

TECHTARGET, 2008. What is CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)? - Definition from WhatIs.com. *SearchSecurity* [online] [vid. 2019-04-14]. Dostupné z: https://searchsecurity.techtarget.com/definition/CCMP-Counter-Mode-with-Cipher-Block-Chaining-Message-Authentication-Code-Protocol

TECHTARGET, 2019. What is a VPN? - Definition from WhatIs.com. *SearchNetworking* [online] [vid. 2019-04-14]. Dostupné z: https://searchnetworking.techtarget.com/definition/virtual-private-network

TNS.CZ, 2019. Penetrační testy. *Trusted Network Solutions, a.s.* [online] [vid. 2019-04-24]. Dostupné z: https://tns.cz/it-produkty-a-sluzby/penetracni-testy/

VARONIS, Jeff Petters, 2018. IDS vs. IPS: What is the Difference? *Inside Out Security* [online] [vid. 2019-04-14]. Dostupné z: https://www.varonis.com/blog/ids-vs-ips/

VYHLÁŠKA Č. 82/2018 SB., 2018. *Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)*. 28. květen 2018.

VYHLÁŠKA Č. 317/2014 SB., 2014. *Vyhláška o významných informačních systémech a jejich určujících kritériích*. 19. prosinec 2014.

VYHLÁŠKA Č. 437/2017 SB., 2017. *Vyhláška o kritériích pro určení provozovatele základní služby*. 15. prosinec 2017.

WILSON, M a J HASH, 2003. *Building an Information Technology Security Awareness and Training Program* [online]. NIST SP 800-50. Gaithersburg, MD: National Institute of Standards and Technology [vid. 2019-04-14]. Dostupné z: doi:10.6028/NIST.SP.800-50

ZÁKON Č. 181/2014 SB., 2014. *Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*. 29. srpen 2014.

ZÁKON Č. 240/2000 SB., 2000. *Zákon o krizovém řízení a o změně některých zákonů (krizový zákon)*. 9. srpen 2000.