Univerzita Hradec Králové
Fakulta informatiky a managementu

DIPLOMOVÁ PRÁCE

2018 **Adam Hübner**

Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Testování zabezpečení počítačové sítě s využitím standardů pro bezpečnost

Diplomová práce

Autor: Adam Hübner
Studijní obor: Aplikovaná Informatika

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Hradec Králové srpen 2018

Prohlášení:

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

V Hradci Králové dne: Adam Hübner

Poděkování:
Tímto bych rád poděkoval Mgr. Josefovi Horálkovi za poskytnuté rady, velkou míru trpělivosti, ochotu a pozitivní přístup při vedení mé diplomové práce a také mým blízkým za trpělivost, kterou se mnou měli během zpracovávání této diplomové práce.

Anotace

Diplomová práce je zaměřena na představení zásadních norem, standardů a metodik pro zavedení bezpečnostních opatření na úrovni zabezpečení dat a síťové komunikace. V teoretické části jsou představeny klíčové bezpečnostní normy a metodiky z oboru počítačových sítí a bezpečnosti dat a jsou porovnány vybrané metodiky. Praktická část se zaměřuje na realizaci bezpečnostních opatření na ochranu dat a komunikace a jejich testování včetně hodnocení důležitosti aktiv.

Annotation

Network security testing with usage of security standards

Main objective of diploma thesis is presentation of fundamental norms, standards and methodologies for creating security measures on the level of data security and network communication. Theory part introduces fundamental knowledge of network security and data security and comparison of selected methodologies. Research part is focused on realization security measures for data protection and communication, and testing with evaluation of assets importance.

Klíčová slova

síťová komunikace

řízení rizik

kybernetická bezpečnost

aktivum

bezpečnostní standard

OBSAH

ÚVOD

S vývojem informačních technologií roste i důležitost informačních systémů na běžný život. Většina organizací provozuje minimálně jeden informační systém, a to jak ve veřejném, tak státním sektoru. Tyto informační systémy a jejich infrastruktura hrají každodenní roli v životě každého z nás ať už jde o bankovnictví, online nakupování, či tak klíčové funkce jako jsou dodávky elektrického proudu.

S rostoucím využitím těchto technologií přímo úměrně roste i nebezpečí jejich případného zneužití, či vyřazení z provozu. Z toho důvodu je za potřebí vynaložit úsilí a prostředky pro ochranu takových systémů. V současnosti neexistuje žádné přímočaré řešení, které by systémy ochránilo před veškerými možnými útoky.

S novou Evropskou směrnicí o GDPR jsou kladeny vyšší požadavky na zabezpečení uživatelských informací i pro veřejný sektor, proto je vhodné uvážit nasazení bezpečnostních norem i nestátním organizacím. Standardní bezpečnostní normy a směrnice slouží především k nasazení směrnic na klíčové systémy státní infrastruktury. Zneužití či zcizení uživatelských informací je postihováno státem, proto by měly i organizace veřejného sektoru vynaložit úsilí pro zabezpečení jejich aktiv.

K zavedení bezpečnostních opatření však existuje mnoho bezpečnostních norem, které při jejich řádném plnění zajistí jistou úroveň zabezpečení. Účelem této práce je představit nejdůležitější bezpečnostní směrnice a normy a vytvořit model pro jejich nasazení v rámci organizační infrastruktury a zabezpečení aktiv organizací, a to především v rámci zabezpečení počítačových sítí a jejich provozu.

V rámci teoretické části budou představeny jednotlivé normy, směrnice a vládní ustanovení, jejich účel a využití. Bude provedena komparativní analýza k zhodnocení těchto norem. V rámci praktické části bude stanoven návrh zabezpečení, budou prozkoumána a zhodnocena klíčová aktiva organizací a bude stanovena jejich důležitost z pohledu dostupnosti, důvěrnosti a integrity. Budou představena konkrétní rizika a hrozby daných aktiv a budou navržena účinná bezpečnostní opatření negující tyto hrozby. V poslední řadě budou tato opatření testována a auditována, aby byla prozkoumána jejich dostatečnost a korektnost.

1. Bezpečnostní standardy a normy

V následující kapitole budou představeny zásadní požadavky na zabezpečení počítačových sítí dle vybraných nejpoužívanějších standardů norem. V každé kapitole budou popsány základní informace o jednotlivých normách a specifické informace pro jednotlivé normy.

1.1 ISO 15408-1, 15408-2, 15408-3

Série mezinárodních norem ISO/IEC 15408 byla vytvořena Mezinárodní organizací pro normalizaci ISO a Mezinárodní elektrotechnickou komisí IEC ve spolupráci s mezinárodními organizacemi. Norma vznikla z důvodu potřeby stanovit parametry a základy pro bezpečnost v oblasti IT. Skládá se ze tří částí, pod společným názvem Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT, jinak také známá pod pojmem Common Criteria (CC).

Soubor těchto tří norem vymezuje kritéria, která stanovují základ pro hodnocení bezpečnostních vlastností produktů a systémů IT. Tím je dosaženo, že výsledky hodnocení stanovují úroveň a jistou záruku kvality zabezpečení. Díky tomu je možné porovnat výsledky nezávislých hodnocení bezpečnosti. ISO/IEC 15408 poskytuje obecné množiny požadavků (PP – viz dále), které jsou použity v průběhu hodnocení, a s kterými jsou porovnávány konkrétní produkty a systémy. Tímto porovnáním je stanoven stupeň důvěry (Evaluation Assurance Level – EAL), který napomáhá spotřebitelům ke správnému výběru IT produktu, zejména zdali splňuje jimi kladené požadavky na bezpečnost a zdali neobsahuje bezpečnostní rizika neslučitelná s jejich používáním. Tato norma dále může posloužit jako návod k vývoji a tvorbě produktů a systémů v oblasti bezpečnosti IT.

Konkrétní produkt, který je vyvíjen podle normy ISO/IEC 15408 a zároveň je i podle těchto kritérií testován, je označován jako předmět hodnocení (Target of Evaluation – TOE). TOE jsou tedy konkrétní operační systémy, počítačové sítě, distribuované systémy, aplikace nebo například firewally.

Cílové produkty, pro které je tato norma tvořena, jsou: bezpečnostní opatření implementovaná v hardwaru, firmwaru nebo softwaru.

Hlavní rizika, která tato norma posuzuje, jsou: selhání bezpečnosti v oboru důvěrnosti, integrity a dostupnosti (confidentiality, integrity, availability – CIA).

Tato norma neklade obecné požadavky na chod organizace. Namísto toho předkládá bezpečnostní rizika, která výrobce produktů vyřeší svým vlastním způsobem. Slouží tedy především pro potenciální zákazníky, pro správný výběr produktů, pro jejich potřeby, se stanovenou určitou zárukou bezpečnostní kvality. ([1] Introduction, s. vi)

Target of Evaluation (TOE) – Je produkt nebo systém, který je standardem ISO 15408 předmětem hodnocení. ([1] kapitola 5.2)

Security Target (ST) – Je dokument popisující bezpečnostní vlastnosti TOE. Je vytvořen vývojářem TOE. Jedná se tedy o konkrétní produkt, na který jsou aplikované požadavky. ([1] příloha A.3.1)

Protection Profile (PP) – Popisuje typ TOE, jedná se o obecnější princip. Oproti ST se jedná o typ produktu. Specifikuje obecné požadavky na typ TOE. Obvykle je tvořen uživatelskou komunitou, která se snaží o zajištění požadavků na typ TOE. Další možností jsou vývojáři TOE nebo skupina vývojářů tvořících podobné produkty, jejichž cílem je stanovení společných minimálních výchozích požadavků pro typ TOE. Poslední možností jsou vlády a velké korporace specifikující své požadavky, jako součást jejich akvizice. ([1] kapitola 8.3)

1.1.1 ISO/IEC 15408-1

První část ISO 15408-1 stanovuje základní principy hodnocení bezpečnosti v oblasti IT. Nese název Úvod a všeobecný model. Jejím obsahem jsou návody a princip fungování hodnocení bezpečnosti. Dále stanovuje důležité pojmy a principy potřebné k určení úrovně zabezpečení a jeho hodnocení. Vytyčuje účel a cílovou audienci normy. Měla by sloužit jako návod pro vytvoření dokumentu pro hodnocení konkrétního produktu, případně tvorbu hodnotících kritérií. ([1] kapitola 1)

1.1.2 ISO/IEC 15408-2

ISO 15408-2 nese název Bezpečnostní funkční požadavky. Obsahuje výčet konkrétních stanovených požadavků, na které má být odkazováno ve vytvořených dokumentech pro hodnocení bezpečnosti. Zároveň je stanoveno, že funkční požadavky popsané v ISO 15408-2 by neměly být definitivní odpovědí na veškeré problémy bezpečnosti IT. Poskytuje naopak souhrn dobře známých bezpečnostních funkčních požadavků, které mohou být použity k výrobě důvěryhodných zařízení dle potřeb trhu. Tato část normy neobsahuje veškeré funkční požadavky, spíše obsahuje dobře známé požadavky, které byly komisí stanovující ISO 15408-2 stanoveny jako hodnotné v době vydání normy. Tvůrci produktů

mohou odkazovat i na požadavky, které tato norma neobsahuje. Jedná se pak o rozšířené požadavky, se kterými je nakládáno podle specifikace uvedené v první části normy. V neposlední řadě poskytuje určitý návod pro stanovené komise, jak jednotlivé produkty hodnotit. ([2] kapitola 4)

1.1.3 ISO/IEC 15408-3

ISO 15408-3 Stanovuje požadavky na zaručitelnost bezpečnosti. Určuje také stupně zabezpečení, které mohou jednotlivé produkty dosáhnout. ([3] kapitola 1)
Stupně zabezpečení (EALs – evaluation assurance levels):

- EAL1 – funkčně testován
- EAL2 – strukturně testován
- EAL3 – metodicky testován a zkontrolován
- EAL4 – metodicky navržen, testován a přezkoumán
- EAL5 – částečně formálně navržen a testován
- EAL6 – částečně formálně ověřený design a testován
- EAL7 – formálně ověřený design a testován

1.1.4 Proces hodnocení

Nejprve je nutné stanovit PP. PP obsahuje funkční i nefunkční požadavky bezpečnosti, které jsou předány ke schválení. V případě schválení, jsou označeny jako zhodnocená (evaluated) PP. Tyto zhodnocené PP jsou dále katalogizována.
Na základě zhodnocených PP jsou vytvořeny ST. ST musí splňovat všechny požadavky kladené v PP, nebo jejich striktnější varianty. Výjimka je možná pouze v ojedinělých případech, přičemž musí být zdůvodněno, proč není nutné dodržet původní požadavek PP, případně jaké jiné bezpečnostní opatření bylo stanoveno jako náhrada. Výsledky vyhodnocení ST jsou dále přímo použity k vyhodnocení TOE. ([1] kapitola 8.4).

1.1.5 Struktura evaluačního Dokumentu TOE

Každý evaluační dokument musí splňovat strukturu popsanou v ISO 15408-1. Struktura je popsána následovně:

- **Úvod ST** – Popisuje TOE na třech abstraktních úrovních:
    - Obsahuje odkaz na ST a TOE, který poskytuje identifikační materiály, na něž ST a TOE odkazuje.

- Přehled TOE – Stručně v několika odstavcích popisuje typ produktu, jak funguje a k čemu slouží. Dále specifikuje požadavky na hardware, software nebo firmware, který není součástí TOE, ale je potřebný k jeho správnému fungování.
- Popis TOE – popisuje architekturu a funkci TOE podrobněji nežli přehled. Obsahuje popis součástí TOE, seznam hardwaru, softwaru a firmwaru, který tvoří TOE. Dále by měl popis obsahovat logické bezpečnostní vlastnosti, které TOE nabízí, a to dostatečně podrobně, aby čtenář pochopil základy a účel těchto vlastností. Hlavním účelem je zajistit, aby byl popis dostatečně podrobný a čtenář měl jistotu co TOE zajišťuje a co již ne. To je zvláště důležité, pokud je TOE součástí většího celku a nemůže být snadno oddělena od ne-TOE subjektů. ([1] příloha A.4)

- **Nárok na shodu** – Obsahuje odkaz na verze dokumentů ISO/IEC 15408 a informaci, zda ST obsahuje rozšířené požadavky nebo ne. Dále shodu s existujícími PP, zda obsahuje veškeré balíčky, na které odkazuje. ([1] příloha A.5)
- **Definice bezpečnostních problémů** – Obsahuje definice hrozeb, které má negovat TOE nebo operační prostředí. Hrozby mají mít specifikovaného agenta hrozby (threat agent), jenž způsobuje nežádoucí akce, které mohou mít negativní vliv na aktiva. Agent hrozby může být popsán jako jednotlivá entita nebo v některých případech jako typ entity, nebo skupina entit. Příkladem může být hacker, uživatel nebo i počítačový proces. Může být dále specifikován dle aspektů, jako jsou schopnosti, zdroje, příležitost nebo motivace.

  Dále jsou v této podkapitole specifikovány **organizační bezpečnostní politiky** (OSPs), které je nutné prosadit pomocí TOE nebo operačního prostředí. Jedná se o bezpečnostní pravidla, procesy a pokyny, které musí být zajištěny organizací v operačním prostředí. Můžou být prosazovány organizací kontrolující operační prostředí nebo legislativou.

  V neposlední řadě tato kapitola obsahuje doporučení a předpoklady kladené na operační prostředí, aby mohlo být zajištěno správné fungování TOE. Pokud tyto požadavky a doporučení nejsou splněna, TOE nemusí zajišťovat veškerou bezpečnostní funkcionalitu.
- **Zabezpečovací úkoly** – Řeší, jakým způsobem má být docíleno odstranění bezpečnostních problémů a rizik. Nejprve má být stručně popsáno, jakým způsobem bude problém vyřešen. Následně jsou v podkapitolách specifikovány úkoly,

které má splnit TOE a operační prostředí. Požadavkem na TOE je například: Informace ze sekce vysokého stupně zabezpečení jsou důvěrné při přístupu ze sekce nízkého stupně zabezpečení. Požadavkem na operační prostředí pak může být například: TOE je jediným způsobem přístupu propojující sekci vysokého stupně zabezpečení a nízkého stupně zabezpečení. V poslední podkapitole je dokazována spojitost mezi zabezpečovacími úkoly a hrozbami, organizačními bezpečnostními politikami a doporučenými předpoklady. Je zde popsáno, který úkol zajišťuje řešení každé dané hrozbě. Následuje odůvodnění, které dokazuje že všechny hrozby, organizační bezpečnostní politiky a doporučené předpoklady byly efektivně adresované bezpečnostními úkoly. ([1] příloha A.7)

- **Definice rozšířených komponent** – Nepovinná část, je potřebná pouze v případě, je-li TOE založeno na komponentách nespecifikovaných v ISO/IEC – 15408-2 nebo 15408-3. ([1] příloha A.8)
- **Bezpečností požadavky –** Tato kapitola se skládá ze dvou částí. Z bezpečnostních funkčních požadavků (SFRs) a bezpečnostních garančních požadavků (SARs). SFRs je překlad zabezpečovacích úkolů pro TOE do standardizovaného jazyka. SARs je popis jakým způsobem je získána záruka, že TOE splňuje SFRs. Ve specifikacích SFRs není nutné uvádět specifikace vztahující se k aplikačnímu prostředí, poněvadž prostředí není hodnoceno. Naopak veškeré bezpečnostní úkoly musí být přiřazeny konkrétním SFRs. Každý SFR musí odkazovat na jeden či více bezpečnostních úkolů. Každý bezpečnostní úkol TOE musí mít nejméně jeden SFR, který na něj odkazuje. ([1] příloha A.9)
- **Souhrn specifikace TOE –** Úkolem této části je poskytnutí informací, jakým způsobem zajišťuje TOE splnění veškerých funkčních požadavků potenciálnímu uživateli. Tento souhrn by měl poskytovat hlavní technické mechanismy, které k tomuto účelu TOE využívá. Například zdali je přihlašování zprostředkováno pomocí hesla, tokenu nebo certifikátu. ([1] příloha A.10)

Ukázku tímto způsobem vytvořeného a schváleného dokumentu naleznete v příloze 1. této diplomové práce. Jedná se o hardwarovou datovou diodu od firmy FoxIT. (příloha 1)

1.2 Rodina ISO/IEC 27000

ISO/IEC mezinárodní standard řady 27000 pro řízení systémů poskytuje návod a přehled, jak připravit a provozovat systém řízení. Poskytuje vlastnosti a funkce, na kterých

se experti z praxe shodli a jsou považovány za klíčové. Série norem řady 2700 je zaměřena na vývoj standardu pro bezpečnost informací, rovněž známou pod pojmem Systém řízení bezpečnosti informací – Information Security Management Systém (dále již jen ISMS). ([4] kapitola 0.3)

Pomocí této řady norem mohou organizace vyvinout a nasadit souhrn postupů pro řízení zabezpečení jejich informačních aktiv. Pomocí nasazení ISMS tak mohou lépe chránit důležité informace, jako jsou finanční informace, duševní vlastnictví, informace o zaměstnancích nebo informace jim svěřené třetí stranou.

1.2.1 Princip ISMS

Klíčovým segmentem série norem 27000 je přijetí procesního přístupu PDCA (plan-do-check-act) neboli česky: Plánuj-Dělej-Kontroluj-Konej. Jedná se o přístup pro ustavení, zavedení, provozování, monitorování, udržování a zlepšování efektivnosti ISMS a tím i zaručení bezpečnosti celé organizace. Ke správnému fungování je třeba řídit vzájemně propojené činnosti. Pokud činnost využívá zdroje a využívá přeměnu vstupů na výstupy, může být považována za proces. Výstupy procesů mohou tvořit vstup pro další procesy. Organizace by pak měli přijmout takzvaný „procesní přístup“. Jedná se o aplikaci a identifikaci procesů a stanovení jejich vzájemného působení a řízení. ([4] kapitola 3.3)

- Plánování zahrnuje především pochopení požadavků na bezpečnost informací, stanovení cílů a plánů, analyzování stavu organizace a vytvoření plánů dosažení bezpečnostních cílů.
- Dělání zahrnuje aplikaci plánů a plnění cílů stanovených v předešlé fázi.
- Kontrolování zahrnuje měření výsledků, monitorování chodu organizace a cílů, které by měly být plněny.
- Konání následně obsahuje opravy chyb, a to jak v plánech, tak v případném výkonu bezpečnostních politik, zlepšení procesů k dosažení lepších výsledků.

Jedná se tedy o nekonečný cyklus a koloběh. V prvním kroku se stanoví politiky cílů, procesů a postupů ISMS ke snížení rizik a zlepšení bezpečnosti organizace. V druhém kroku se tyto politiky, procesy a postupy nasadí do provozu. Ve třetím kroku se posuzuje, audituje a měří výkon procesů vzhledem ke stanoveným politikám. Výsledky jsou předávány vedení organizace k přezkoumání. Ve čtvrtém kroku vedení organizace stanoví preventivní opatření a případná opatření k nápravě. Cílem je neustálé zlepšování ISMS. ([5] kapitola 1.2)

1.2.2 Úkoly pro ISMS

1.2.2.1 Bezpečnostní politika

V rámci stanovení bezpečnostní politiky by měl být vedením organizace definován směr bezpečnosti informací v souladu s regulatorními požadavky, zákony a požadavky organizace. Měl by být vytvořen a schválen dokument bezpečnostní politiky informací. Všichni zaměstnanci a relativní třetí strany by měli mít k tomuto dokumentu přístup.
V plánovaných intervalech, nebo v případě, že nastanou významné změny, by měla být bezpečnostní politika organizace opětovně přezkoumávána a vylepšována. ([5] příloha A.5)

1.2.2.2 Organizace bezpečnosti

Organizace by měla řídit bezpečnost informací. Vedení organizace by mělo jednoznačně přiřadit a vymezit role v oblasti bezpečnosti informací. Mělo by stanovit jasný směr bezpečnosti a podporovat ho. Činnosti v tomto oboru by měly být koordinovány za pomoci zástupců odvětví celé organizace. Dále by měly být jednoznačně určeny odpovědnosti. Při zavádění nových zařízení pro zpracování informací by měl být stanoven jednoznačný postup schvalování vedoucími zaměstnanci. Dohody o ochraně důvěrných informací by měly být přezkoumávány, stejně tak veškeré dohody a povinnosti na zachování mlčenlivosti. Organizace by měla udržovat přiměřené vztahy s orgány veřejné zprávy, stejně tak i se zájmovými skupinami bezpečnostního zaměření a profesními sdruženími. Veškerá tato vytýčená bezpečnostní ustanovení a jejich nasazení by měla být v pravidelných intervalech a při závažných změnách v organizaci nezávisle přezkoumávána. ([5] příloha A.6)

1.2.2.3 Externí subjekty

Je třeba stanovit a zachovat bezpečnost informací, které jsou přístupné, zpracovávané, sdělované nebo spravované externími subjekty. Měla by být identifikována rizika a implementována opatření, nežli bude povolen přístup externích subjektů k informacím organizace a zařízením pro jejich zpracování. Veškeré požadavky na bezpečnost by měly být předem zajištěny, dříve než k nim bude povolen přístup klientům. Veškeré bezpečnostní požadavky by měly být stanoveny a dodržovány při přístupu, zpracování a šíření informací třetích stran. ([5] příloha A.6.2)

1.2.2.4 Klasifikace a řízení aktiv

Organizace by měla evidovat a aktualizovat seznam důležitých aktiv. Aktiva související se zařízeními pro zpracování informací by měla mít stanoveného vlastníka. Organizace by dále měla stanovit a zdokumentovat pravidla pro použití informací a aktiv, které souvisí se zařízeními pro zpracování informací. Dále by veškeré informace měly být klasifikovány dle jejich hodnoty, citlivosti, kritičnosti a právních požadavků. S tím souvisí značení informací. Pro značení by měly být zavedeny postupy dle klasifikačních schémat určených organizací. ([5] příloha A.7)

1.2.2.5 Bezpečnost lidských zdrojů

Hlavním účelem tohoto bodu je snížení rizik souvisejících s lidskými chybami, krádežemi, podvody nebo zneužitími prostředků organizace. To samozřejmě souvisí především se zaměstnanci, ale i s třetími stranami. Hlavním úkolem je tedy jednoznačně stanovit povinnosti a role. Tyto povinnosti a role by měly být zdokumentovány v souladu s bezpečnostní politikou organizace. Všichni zaměstnanci by měli být prověřeni dle v dané zemi platných zákonů, předpisů a v souladu s etikou. Tato prověření by měla být závislá na dané pozici, a to především s ohledem na klasifikaci informací, ke kterým by měli mít daní zaměstnanci přístup. Hlavním kritériem v hodnocení by měla být spolehlivost a případná potenciální rizika. Veškerá ustanovení o odpovědnostech za bezpečnost informací by měla být ustanovena v pracovních smlouvách.

Zaměstnanci a smluvní třetí strany by si měli být vědomi bezpečnostních rizik, hrozeb a problémů, svých odpovědností a povinností, dodržovat a podílet se na bezpečnostní politice organizace, a to během své běžné práce. O dodržování bezpečnosti v souladu se zavedenými politikami a směrnicemi by se měli starat vedoucí zaměstnanci, kteří by dodržování těchto směrnic a politik měli vyžadovat od uživatelů a třetích stran. Stejně tak by měli být zaměstnanci s ohledem na svou pracovní náplň opakovaně školeni v oblasti bezpečnosti informací, bezpečnostní politiky a směrnicím organizace. S ohledem napředešlé by se zaměstnanci, kteří porušili pravidla a bezpečnost informací, mělo být vedeno formalizované disciplinární řízení.

Při ukončování pracovního vztahu se zaměstnanci, případně se třetími stranami, je třeba stanovit a definovat odpovědnosti z toho vyplývající. Zaměstnanci a třetí strany by v případě rozvázání poměru (radši: ukončení vzájemné spolupráce) měli odevzdat veškeré předměty, které jsou majetkem organizace. Stejně tak by měli být zbaveni veškerých přístupových práv k informacím a zařízením pro zpracování informací. ([5] příloha A.8)

1.2.2.6 Fyzická bezpečnost a bezpečnost prostředí

Organizace by měla zajistit, aby nebyl umožněn neautorizovaný přístup do vymezených prostor z důvodu potenciálního poškození a zásahům do provozních budov a informací organizace. Veškeré informace a zařízení by se měly nacházet v prostorách, ve kterých jsou používány bezpečnostní perimetry. Osoby by do takovýchto míst měly být kontrolovány vstupní kontrolou a přístup do nich by měly mít pouze oprávněné osoby. Na kanceláře, místnosti a zařízení by měla být aplikována vhodná fyzická bezpečnostní zařízení. Dále by měla být zajištěna ochrana před hrozbami vnějšího prostředí. Jedná se o preventivní opatření proti přírodním a lidmi zapříčiněným katastrofám. Je tedy vhodné aplikovat prvky fyzické ochrany. Prvky fyzické ochrany by dále měly být navrženy a aplikovány v zabezpečených oblastech. Místa, kudy by se mohly neoprávněné osoby dostat do prostor organizace, by měla být kontrolována, ideálně by však měla být izolována od zařízení pro zpracování informací.

Aktiva by měla být umístěna ve vnitřním perimetru budovy a chráněna. Příležitosti k neoprávněnému přístupu by měly být omezeny. Zařízení by měla být chráněna před výpadky způsobenými selháním napájení a selháním podobných podpůrných služeb Veškeré kabelové rozvody sloužící pro přenos dat a podporu informačních služeb by měly být chráněny před odposlechem

a poškozením. U zařízení by měla být zajištěna stálá dostupnost a integrita. Pokud

je zařízení používané mimo prostory organizace, mělo by být náležitě zabezpečeno s ohledem na rizika vyplývající z jejího použití. Při likvidaci nebo znovupoužití paměťových zařízení by mělo být zajištěno odstranění citlivých dat a licencovaných programů. Veškeré přemísťování zařízení, informací a programového vybavení by mělo podléhat schválení. ([5] příloha A.9)

1.2.2.7 Řízení komunikací a provozu

Veškeré provozní postupy by měly být dostupné všem uživatelům, udržovány aktuální a zdokumentované. Změny v zařízeních pro zpracování informací by měly být kontrolovány a řízeny. Mělo by být zváženo oddělení procesů vývoje, testování a provozu z důvodu snížení rizika neoprávněného přístupu k provozním systémům.

Veškeré dodávky služeb od třetích stran by se striktně měly řídit smluvními podmínkami, a to především s ohledem na úroveň služeb týkajících se bezpečnosti informací. Organizace by měla monitorovat a pravidelně přezkoumávat služby, zprávy a záznamy

poskytované třetími stranami. Veškeré změny v poskytování služeb třetími stranami by měly být řízeny s ohledem na kritičnost systémů a procesů organizace.

Dalším cílem by mělo být minimalizování rizika selhání informačních systémů. Veškeré zdroje a kapacitní požadavky by měly být nastaveny, monitorovány a projektovány. Při přejímání nových informačních systémů by mělo být zajištěno dostatečné testování, a to v průběhu vývoje a před zavedením do ostrého provozu.

Integrita dat a programů by měla být chráněna před škodlivými programy a mobilními kódy. Měla by být implementována opatření na jejich detekci, prevenci a nápravu. Následně by mělo být zvyšování bezpečnostního povědomí uživatelů. Veškeré povolené mobilní kódy by měly být používány v souladu s bezpečnostní politikou. Nepovolené mobilní kódy by neměly být spuštěny vůbec.

Dále by mělo být zajištěno dostatečné zálohování. Organizace by měla zajistit pořízení a testování záložních kopií důležitých informací a programového vybavení v pravidelných intervalech.

Infrastruktura počítačových sítí a informace, které síť obsahuje, by měly podléhat ochranně. Počítačové sítě by měly být vhodným způsobem kontrolovány a spravovány z důvodu zamezení možným hrozbám a zaručení bezpečnosti systému a aplikací. Síťové služby by měly obsahovat bezpečnostní prvky, měla by být určena úroveň poskytovaných služeb. To vše by mělo být ukotveno v dohodách o poskytování síťových služeb, a to v případech jak interní, tak externí správy.

Veškerá média by měla být chráněna před prozrazením, modifikací, ztrátou nebo poškozením aktiv organizace. Z tohoto důvodu by měly být stanoveny postupy pro správu vyměnitelných počítačových médií. Pokud již nejsou média více použitelná či upotřebitelná, měla by být bezpečně a spolehlivě zlikvidována. Pro manipulaci a ukládání informací na médiích by měla být stanovena pravidla především z důvodu nebezpečí neautorizovaného přístupu a zneužití informací. Stejně tak veškerá systémová dokumentace by měla být chráněna před neautorizovaným přístupem.

Dále by měla organizace zajistit bezpečnost informací a programů při jejich výměně s externími subjekty i v rámci organizace. Organizace by měla zajistit, stanovit a zavést formální postupy, opatření a politiky na ochranu informací při jejich výměně pro všechny typy komunikačních zařízení. Výměna informací mezi organizací a třetími stranami by měla podléhat dohodám mezi těmito stranami. Při výměně a přepravě informací mimo organizace by měla být zajištěna dostatečná ochrana před neoprávněným přístupem, zneužitím a narušením. Informace přenášené elektronicky by měly být taktéž dostatečným

a vhodným způsobem chráněny. Pro výměnu informací mezi podnikovými informačními systémy by měla být vytvořena a zavedena politika a odpovídající směrnice.
Organizace by měla taktéž zajistit bezpečnost v oboru elektronického obchodu. Organizace by měla zajistit ochranu před podvodnými aktivitami, zpochybňováním smluv, modifikaci informací, či jejich prozrazením, především při přenosu informací ve veřejných sítích v rámci elektronického obchodování. Stejně je tomu tak i u On-line transakcí. Přenos by měl být zajištěn úplný a mělo by být zamezeno špatnému směrování, neoprávněnému prozrazení, duplikaci, opakování zpráv, či jejich změně. Veřejně přístupné informace by měly být chráněny před neoprávněnou modifikací.
Organizace by dále měla zajistit dostatečný monitoring, detekovat neoprávněné zpracování informací. Organizace by měla pořizovat a uchovávat bezpečnostně významné události, chybová hlášení a auditní záznamy pro případné vyšetřování a monitoring řízení přístupu. K monitorování by měly být stanoveny principy a pravidla pro použití zařízení pro zpracování informací, které by měla být pravidelně zkoumána. Tyto záznamy by měly být chráněny před zfalšováním a neoprávněným přístupem. Veškeré aktivity systémových operátorů a správců systému by měly být zaznamenávány. Veškeré chyby by měly být analyzovány a zaznamenávány a následně by měla být provedena opatření k jejich nápravě. V poslední řadě by měla být zajištěna synchronizace časů klíčových systémů pro zpracování informací se schváleným zdrojem přesného času. ([5] příloha A.10)

1.2.2.8 Řízení přístupů

K řízení přístupů by měla být v závislosti na aktuálních bezpečnostních požadavcích vytvořena politika, která bude dokumentována a průběžně přezkoumávána.
Organizace by měla předcházet a zamezit neoprávněnému přístupu k informačním systémům, a naopak kontrolovat oprávněné přístupy uživatelů. Za tímto účelem by měla být zajištěna formální registrace uživatelů, díky které bude možné zajistit autorizovaný přístup k víceuživatelským informačním systémům a službám. Stejně tak by mělo existovat inverzní řešení, kdy bude registrace zrušena. Přiřazování privilegií by mělo být striktně řízené a omezené. Veškerá hesla by měla být tvořena a přidělována na základě formálních procesů. Uživatelská práva a přístupy by měly být v pravidelných intervalech revidovány. Dále by mělo být zabráněno prozrazení, krádeži informací či neautorizovanému přístupu k informacím a zařízením pro jejich zpracování. Výběr uživatelských hesel by měl dodržovat stanovené bezpečnostní postupy. Neobsluhovaná zařízení by měla být přiměřeně

chráněna před neoprávněným přístupem. Dále by měla být dodržována zásada prázdné obrazovky a prázdného stolu u zařízení pro zpracování informací.
Síťové služby by měly podléhat regulacím a předcházet neautorizovanému přístupu. Uživatelé by měli mít přístup pouze k takovým síťovým službám, ke kterým mají přiřazené oprávnění. Vzdálení uživatelé by měli být vždy autentizováni. S ohledem na to by měla být zvážena automatická identifikace zařízení z vybraných lokalit a přenosných zařízení. Veškerý přístup k fyzickým i logickým portům by měl být řízen bezpečně. Organizace by měla v síťové infrastruktuře oddělit skupiny uživatelů, informačních služeb a systémů. Pokud používá organizace sdílené sítě přesahující hranice organizace, možnost připojení uživatelů by měla být omezena v souladu s politikou řízení přístupů a požadavky aplikací. Mělo by být zavedeno řízení směrování sítě, aby nebyla narušována politika řízení přístupů aplikací organizace.
Podobným kritériím podléhají i operační systémy. Přihlašování k operačním systémům by mělo být řízeno postupy bezpečného přihlášení. Každý uživatel by měl mít přiděleno své specifické uživatelské ID, které ho bude jednoznačně identifikovat a bude zajištěna vhodná autentizace k ověření jeho identity. Mělo by být zajištěno použití kvalitních hesel, k čemuž by měl sloužit interaktivní systém správy hesel. Dále by mělo být omezeno a přísně kontrolováno použití systémových nástrojů, které jsou schopné překonávat systémové nebo aplikační kontroly. Po stanovené době neaktivity či nečinnosti by měly být neaktivní relace samovolně ukončeny. U významných a rizikových aplikací by mělo být zváženo omezení doby spojení.
Přístup k informacím uložených v počítačových systémech by měl být také omezen. Vše by se mělo dít v souladu s definovanou politikou řízení přístupu. Přístup k informacím by měl být omezen v souladu s těmito politikami. Dále je vhodné oddělit a izolovat citlivé aplikační systémy do svého počítačového prostředí.
Mobilní informační zařízení by měla být používána dle ustanovených formálních pravidel na ochranu proti rizikům při použití mobilních výpočetních a komunikačních zařízení. Pro práci na dálku by organizace měla zavést zásady, postupy a opatření. ([5] příloha A.11)

1.2.2.9 Nákup, vývoj a údržba informačních systémů

Hlavním cílem je zajištění a zavedení bezpečnostních opatření do informačních systémů. Veškeré nové systémy či úpravy existujících systémů by měly obsahovat požadavky na bezpečnostní opatření. Organizace by měla předcházet ztrátě, modifikaci, chybám

či případnému zneužití uživatelských dat v aplikacích. Veškerá data přicházející do systémů by měla být kontrolována z hlediska jejich správnosti a adekvátnosti. Měla by být zvážena a případně zavedena kontrola platnosti dat pro detekci poškození či modifikace informací vzniklého úmyslnými zásahy či chybami při zpracování. Měla by být zajištěna opatření k zajištění integrity zpráv, autentizace a dalších požadavků na bezpečnost u jednotlivých aplikací. Platnost výstupních dat by měla být také náležitým způsobem ověřena. Důvěrnost, autentičnost a integrita informací organizace by měly být chráněny kryptografickými prostředky. Tyto kryptografické prostředky by měly být řízeny pravidly pro jejich použití. Dále by měl existovat systém správy klíčů pro podporu kryptografických technik.

Systémové soubory by měly být chráněny. Pro zavádění a instalaci programového vybavení na provozních systémech by měly být zavedeny postupy kontroly. Dále by měl být zajištěn pečlivý výběr, ochrana a kontrola testovacích dat organizace. Ke zdrojovým kódům a knihovnám systémů by měl být omezen přístup.

Dále by měla být v rámci aplikačních systémů udržována bezpečnost programů a informací. Veškeré změny by měly podléhat zavedeným formálním postupům. Pokud proběhne změna operačního systému, měly by být otestovány a přezkoumány kritické aplikace, aby byl zajištěn plynulý chod organizace a odhalily se případné změny, které mají nepříznivý dopad na provoz a bezpečnost organizace. Veškeré prováděné změny by měly být řízeny, a programové balíky modifikovány pouze je-li to nezbytně nutné. Organizace by měla zabránit úniku informací. Pokud organizace používá programové vybavení vyvíjené třetí stranou, její vývoj by měl být organizací monitorován.

Pokud existuje veřejně publikovaná technická zranitelnost uvnitř provozovaného informačního systému, měla by tato informace být včasně získána a následně vyhodnocena úroveň ohrožení organizace. Následně by měla být přijata opatření na pokrytí souvisejících rizik. ([5] příloha A.12)

1.2.2.10 Zvládání bezpečnostních incidentů

Veškeré bezpečnostní události a slabiny informačních systémů by měly být včasně hlášeny pro zahájení kroků vedoucích k jejich nápravě, a to tak rychle, jak jen to je možné. Tyto slabiny a bezpečnostní události by měly být povinně hlášeny všemi zaměstnanci, smluvními stranami a dalšími uživateli informačních systémů, a to i v případě, že se jedná o pouhé podezření.

Odpovídající postupy pro zvládání takovýchto bezpečnostních incidentů by měly být zavedeny pro rychlé, účinné a systematické řešení bezpečnostních incidentů. Dále by měly být zavedeny mechanismy pro kvalifikování a monitorování bezpečnostních chyb a incidentů. Mělo by být možno určit rozsah a náklady. V případě že bezpečnostní incident vyústí v právní řízení vůči organizaci či osobě s organizací související, měly by být zajištěny, sbírány a uchovány potřebné důkazy s incidentem související. Následně by měly být předkládány soudu. ([5] příloha A.13)

1.2.2.11 Řízení kontinuity činností organizace

Organizace by měla chránit své kritické procesy před selháním informačních systémů nebo katastrofami, případně zajistit jejich včasnou obnovu. Organizace by měla vytvořit řízený proces pro rozvoj a udržování kontinuity činností organizace. Příčiny přerušení činností organizace by měly být identifikovány včetně velikosti dopadu, pravděpodobnosti a možných následcích na bezpečnost informací. Měly by existovat plány pro zprovoznění kritických procesů a dostupnosti informací po přerušení těchto procesů nebo kritickém selhání, a to v požadovaném čase a na požadovanou úroveň. Dále by organizace měla vytvořit jednotný systém plánů kontinuity činností organizace pro zajištění konzistentního plánu a priorit testování a údržby. Tyto plány by měly být pravidelně testovány a aktualizovány. ([5] příloha A.14)

1.2.2.12 Soulad s požadavky

Organizace by se měla vyvarovat porušení norem občanského nebo trestního práva, bezpečnostních požadavků nebo smluvních povinností. Veškeré zákonné a podzákonné a smluvní požadavky by měly být jednoznačně definovány, zdokumentovány a udržovány aktuální. Měly by být stanoveny a zavedeny vhodné postupy pro použití materiálů a aplikačního programového vybavení v souladu se zákony na ochranu duševního vlastnictví. Dodržování smluvních požadavků by mělo být aplikováno na ochranu důležitých záznamů organizace. Stejně tak veškeré osobní údaje by měly být spravovány v souladu s odpovídající legislativou a předpisy. Zařízení pro zpracování informací by neměla být použita jiným než autorizovaným způsobem. Kryptografická opatření by měla být používána dle zákonů, předpisů a příslušných úmluv.

Organizace by měla zajistit, aby její systémy odpovídaly bezpečnostním normám. To by mělo být v kompetencích vedoucích zaměstnanců. Ti by měli zajistit správné provádění bezpečnostních postupů v souladu s bezpečnostními politikami a normami. Organizace

by dále měla zajistit pravidelnou kontrolu informačních systémů, zda jsou v souladu s normami a politikami.

Bezpečnostní audity by měly být předem plánovány takovým způsobem, aby co nejméně narušili chod organizace. Aby se předešlo možnému zneužití a ohrožení auditních nástrojů, měly by být tyto nástroje náležitě chráněny. ([5] příloha A.15)

1.2.3 Doporučená opatření

Doporučená opatření budou rozepsána v kapitole „Komparativní Analýza“, a to z důvodu téměř devadesáti devíti procentní shody s českým zákonem o kybernetické bezpečnosti. Původní zákon z roku 2014 č. 181/2014 Sb., o kybernetické bezpečnosti vykazoval přibližně osmdesáti procentní shodu, po novele v roce 2017 již stanovuje téměř totožná, mnohdy i přísnější doporučená bezpečnostní opatření. Implementace jednotlivých požadavků a řešení organizační a technické stránky bezpečnosti pak v prostředí ČR definuje vyhláška o kybernetické bezpečnosti 82/2018 Sb. Národního úřadu pro kybernetickou ochranu.

1.3 RFC

RFC neboli „Request for Comment“ jsou na sobě víceméně nezávislé dokumenty řešící konkrétní doporučení, best practise řešení a normy. Tyto dokumenty jsou veřejně dostupné na stránce http://www.rfc-editor.org/. Jedná se o publikace technologické komunity zabývající se fungováním internetu. Hlavními tvůrci těchto dokumentů jsou IETF (Internet Engineering Task Force), IRTF (Internet Research Task Force), IAB (Internet Architecture Board) a nezávislí autoři. Systém RFC dokumentů je podporován americkou neziskovou organizací ISOC (Internet Society).

Hlavním účelem těchto dokumentů je popisování správných metod, chování, postupů a výzkumů pro správné a ucelené chování internetu a internetem propojených systémů. Z pohledu nezávislých uživatelů je dodržováním RFC standardů a doporučení docílena bezproblémová komunikace na internetu. RFC nám tedy říkají, jakým způsobem zacházet s jednotlivými protokoly, jak je správně nasadit a aplikovat. Jedná se především o praktické návody, rady či přehledy. Zpracováno podle stránek organizace IETF[7].

1.3.1 Struktura RFC dokumentů

RFC dokumenty mají v hlavičce souhrn informací. Každý RFC dokument má své specifické sériové číslo. Když je dokumentu přiděleno sériové číslo a je publikován, nemůže být nikdy pozměněn. V případě, že je zapotřebí pozměnit informace či případné doporučení, které dokument poskytuje, je vytvořen nový RFC dokument se svým novým „vyšším“ sériovým číslem a předešlý je kategorizován jakožto historický RFC dokument. Oproti standardům společnosti ISO či IEC, RFC dokumenty vznikají rozdílným způsobem a standardizační proces je rozdílný. Každé RFC nejdříve vzniká jako takzvaný Internet Draft (Internetový návrh) a může být navržen libovolnou organizací či komunitou. Tento návrh je publikován jako Standardní RFC po schválení IETF. Obvykle jsou tvořeny experty účastnícími se v pracovních skupinách. Návrhy jsou v několika kolech sdíleny a upravovány, než jsou vydány jako Standardizované RFC. RFC dokumenty používají standardizovaný jazyk uveřejněný v RFC 2119 a 8174 a jsou uveřejňovány jako čistý ASCII text se snadným převodem do jiných druhů dokumentů. Zpracováno podle stránek organizace IETF [8].

Dále je v hlavičce uveden vydavatel či tvůrce RFC, datum vydání, kategorie, případné číslo v podkategorii, pokud dané RFC do nějaké spadá. Kategorie a podkategorie budou popsány v následující kapitole. V případě, že daný RFC dokument tvoří novelu jiného staršího RFC, je v hlavičce uveden odkaz na dané RFC, které nahrazuje. V případě, že se naopak jedná o starší RFC, které bylo novelizováno, v hlavičce je taktéž k nalezení odkaz na novější RFC, které nahrazuje tento dokument.

V samotném dokumentu je vždy uveden celý název daného RFC a následující kapitoly:

- Status of this Memo – slouží k vysvětlení, za jakým účelem tento dokument vznikl a jakého je charakteru. Dále také například sděluje informaci, že je dokument volně šiřitelný.
- Abstract – Krátký a stručný popis obsahu dokumentu, důvod a účel dokumentu.
- Kapitolu o copyrightu.
- Table of Contents – Nese strukturovaný obsah dokumentu s odkazy na jednotlivé kapitoly.

Následně obvykle RFC dokumenty obsahují úvod či přehled. Zpracováno podle [9].

1.3.2 Kategorie a podkategorie RFC dokumentů

Krom toho, že každý RFC je kategorizován svým specifickým jednoznačným číslem, může být dále kategorizován podle typu dokumentu. V tom případě krom svého specifického RFC čísla obsahuje i název podkategorie a specifické číslo identifikující dokument v dané podkategorii. Kategorizace RFC dokumentů tímto způsobem přináší některé výhody. Jednou z hlavních výhod může být například pozměňování a vývoj standardů. Svět se vyvíjí a svět internetu často mnohem rychleji. Pokud se informace v RFC dokumentu stanou neplatnými a je dále kategorizován dle podkategorie, podkategorie zůstane stále stejná, v případě že řeší stále ten samý problém, a změní se pouze odkaz na novější RFC dokument, který tvoří revizi původního RFC dokumentu. Hlavní kategorie a podkategorie tedy jsou:

- STD (Internet Standard)
- Informational
- Experimental
- BCP (Best Current Practice)
- Historical
- Unknown nebo Uncategorized (dříve vzniklé RFC dokumenty)

STD dokumenty tvoří standardy a doporučení ke správnému působení na internetu. Příkladem můžem být například RFC 5000, které specifikuje používané protokoly na internetu.

Podkategorie Informationan (Informační) uvádí co je obsahem RFC dokumentu a jak s ním má být nakládáno.

Podkategorie Experimental vyjadřuje, že není jisté, zda návrh RFC bude fungovat tak jak bylo zamýšleno a zda bude přijat veřejností. V případě že bude přijat veřejností, bude funkční a stane se populárním může být následně standardizován jako STD.

BCP neboli „Best Current Practise“ obsahují doporučené a oficiální pravidla, které nejsou pouze informačního charakteru, ale zároveň nebudou ovlivňovat způsob šíření dat. Mezi BCP a STD je často jen tenká hranice. BCP by měly utvářet doporučení, avšak některé mohou obsahovat omezení. Mohou zahrnovat i technické doporučení, například jakým způsobem použít filtrování zdrojových dat k zajištění vyšší obtížnosti DoS útoků.

Historické RFC jsou kategorizovány jako „nedoporučené k dalšímu používání“, tedy jako nepodporované a neplatné standardy a doporučení. Zpracováno podle [10].

1.3.3 Příklady RFC dokumentů

RFC 2827 [9] nese název „Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing“ (Vstupní síťové filtrování: porážka DoS útoků, které jsou způsobeny zahlcováním zdrojovými IP adresami). Byl vydán skupinou Network Working Group v květnu 2000, je zařazen do podkategorie best current practice pod číslem 38. Tento RFC dokument specifikuje nejlepší současné praktiky pro internetovou komunitu v ohledu ochrany sítí před spoofingovými DoS útoky. Důvodem vzniku tohoto dokumentu byly výskytu DoS útoků, které byly způsobeny zahlcováním neexistujícími IP adresami. Tento RFC dokument představuje jednoduché a efektivní řešení pro používání filtrování vstupního provozu k docílení zamezení DoS útoků z oblastí mimo agregačních bodů internet service providerů. Tento dokument je dále rozšířen a aktualizován v RFC 3704, ale stále je platný a účinný. Hlavním účelem dokumentu je zvýšit povědomí a zabezpečovací praktiky internetové komunity a nabádat administrátory korporátních sítí a poskytovatelů internetu k nasazení vstupního filtrování IP adres. Při tomto postupu bude zamezeno příležitostem útočníků k využití falšovaných zdrojových adres k DoS útokům. Také bude tímto způsobem mnohem snadnější vystopovat útočníka, protože zdroj útoku bude pravděpodobně správný.

RFC 4962 [11] nese název „Guidance for Authentication, Authorization, and Accounting (AAA) Key Management“ (Návod pro management klíčů u AAA). Byl vydán skupinou Network Working Group v červenci roku 2007, je zařazen do podkategorie best current practice pod číslem 132. Tento RFC dokument poskytuje návod pro návrháře a výrobce AAA protokolů pro výměnu klíčů. Poskytuje také užitečné informace pro systémy pracující s těmito protokoly. Dává návody, jak zajistit dostatečnou složitost k vytvoření bezpečných, dlouhotrvajících AAA protokolů.

RFC 7100 [12] nese název „Retirement of the „Internet Official Procotol Standards, Summary Document“ (vyřazení souhrnu oficiálních internetových protokolových standardů). Byl vydán skupinou IETF v srpnu roku 2013, je zařazen do podkategorie best current practice pod číslem 9. Tento krátký RFC dokument shrnuje důvod vyřazení RFC dokumentu 5000 do historických, a tedy i neplatných a nedoporučených RFC. S ohledem na strukturu a vznik RFC dokumentů, není možné aktualizovat souhrnné informace v RFC dokumentech. Tedy seznam z RFC 5000 je považován za neplatný a místo tohoto dokumentu vznikl aktualizovaný seznam na stránkách https://www.rfc-editor.org/standards .

1.4 NIS

Směrnice NIS vznikla na základě ustanovení evropského parlamentu a rady 19.7. 2016. Hlavním důvodem vzniku této směrnice byl rostoucí vliv, který mají informační systémy a služby na chod společnosti. Jejich zabezpečení je tedy klíčové pro ekonomické a společenské fungování vnitřního trhu. S nárůstem tohoto vlivu se samozřejmě zvýšil i výskyt incidentů a hrozeb, které mají dopad na společnost. Mohou působit finanční ztráty, narušit důvěru uživatelů nebo bránit ve výkonu ekonomické činnosti. Z důvodu nadstátního rozměru a vlivu informačních technologií a systémů, a to především internetu, bylo zapotřebí stanovit bezpečnostní opatření k zajištění chodu systémů jak na národní, tak na nadnárodní úrovni. V první části dokument zmiňuje hlavní důvody k zavedení této směrnice. V první kapitole pak představuje obecná ustanovení.
Celá tato kapitola včetně podkapitol byla zpracována podle směrnice NIS [12].

1.4.1 Obecná ustanovení NIS

Obecná ustanovení ukládají členským státům povinnosti a doporučení, které musí zajistit pro řádné fungování. Obecná ustanovení jsou rozdělena do jednotlivých článků, dále budou všechny stručně popsány. Více se budu věnovat těm, které blízce souvisí s konkrétními požadavky či opatřeními.
Článek 1 stanovuje předmět a oblast působnosti směrnice NIS. Úkolem je stanovení vysoké společné úrovně bezpečnosti sítí a informačních systému v členských státech Evropské Unie a zlepšit tím fungování vnitřního trhu. Směrnice povinuje všechny členské státy přijetím národní strategie pro bezpečnost informačních systémů a sítí. Směrnice tvoří skupinu pro spolupráci pro budování vzájemné důvěry a strategické spolupráce v rámci EU v oboru informačních systémů. K tomuto účelu zavádí bezpečnostní tým typu CSIRT (Computer Security Incident Response Team), který zajišťuje podporu pro operativní spolupráci. Dále stanovuje povinnost hlásit bezpečnostní incidenty pro provozovatele základních a digitálních služeb, stejně tak jako bezpečnostní požadavky s tímto oborem souvisejícím. Členské státy by si dle směrnice měly určit vnitrostátní orgány, utvořit konkrétní týmy CSIRT, jež se budou starat o bezpečnost sítí a informačních systémů.
Článek 2 nese název Zpracování osobních údajů, jeho obsahem jsou pouze odkazy na další směrnice, které řeší tento problém podrobněji, a to jak na národní, tak mezinárodní úrovni.

Článek 3 uvádí, že směrnice stanovuje pouze minimální přijatá opatření a členské státy si mohou ponechat a využívat svá ustanovení a zákony, pokud splňují rozsah této směrnice nebo kladou striktnější požadavky nežli směrnice NIS.
Článek 4 stanovuje seznam zásadních pojmů, které jsou v dalších článcích použity.
Článek 5 určuje a stanovuje kritéria, podle kterých jsou kategorizovány systémy a provozovatelé takzvaných základních služeb. Provozovatelé základních služeb jsou tedy subjekty, které poskytují službu, která je kritická z hlediska zachování společenských ekonomických činností. Zároveň je tato služba závislá na informačních systémech a sítích a případný incident by mohl narušit poskytování této služby. Vzájemná spolupráce mezi členskými státy je navázána v případě, že poskytovatel dané služby jí poskytuje ve vícero členských státech. Bude vytvořen seznam poskytovatelů základních služeb a bude průběžně aktualizován. Státy jsou povinné poskytovat informace o těchto systémech komisi, která je bude kontrolovat a hodnotit. Mezi tyto poskytované informace patří přinejmenším: seznam poskytovatelů základních služeb, vnitrostátní opatření určující provozovatele základních služeb, počet provozovatelů základních služeb v každém odvětví a pokud existují, tak i mezní hodnoty ustanovující příslušné zásobovací úrovně dle počtu uživatelů závislých na dané službě, případně důležitost provozovatele základních služeb.
Článek 6 řeší významné narušení služeb. Klade doporučení, která by měly členské státy zvážit. Závažnost narušení služeb by měla být hodnocena dle počtu uživatelů závislých na poskytovaných službách. Dále by měla být hodnocena dle závislosti na ostatních odvětvích a službách, na délce dopadu možného incidentu, jeho intenzitě a závažnosti s ohledem na ekonomické a společenské činnosti či veřejnou bezpečnost. Rovněž by měla být hodnocena s ohledem na geografický rozsah, na který by měl incident vliv, podíl, který zaujímá subjekt na trhu a důležitost subjektu s ohledem volby možné náhrady.

1.4.2 Národní rámce pro bezpečnost sítí a informačních systémů

Každý členský stát Evropské Unie je dle článku 7 povinen stanovit národní strategii pro bezpečnost sítí a informačních systémů, stanovit strategické cíle a opatření s cílem dosažení vysoké úrovně bezpečnosti v oboru počítačových sítí a informačních systémů. Tato opatření musí být aplikována na odvětví energetiky, dopravy, bankovnictví, infrastruktury finančních trhů, zdravotnictví, dodávek a rozvodů pitné vody a digitální infrastruktuře. Hlavním úkolem je zajištění následujících cílů a opatření: Utvoření cílů a priority národní strategie k zajištění bezpečnosti sítí a informačních systémů. Utvoření rámců pro jejich plnění, stanovení úloh a povinností vládních orgánů a relevantních subjektů.

Stanovení opatření nutných pro připravenost, rychlou reakci a obnovu a spolupráce veřejného a soukromého sektoru. Vymezení výzkumných a rozvojových plánů a vzdělávacích, školících a informačních programů souvisejících s bezpečností sítí a informačních systémů. Utvoření plánu na posuzování rizik, utvoření seznamu subjektů, které jsou do tohoto odvětví zapojeny. Státy mají možnost požádat agenturu ENISA pro pomoc s vypracováním těchto úkolů a cílů. Členské státy mají oznamovací povinnost vůči Komisi, a to s lhůtou 3 měsíců od přijetí strategie pro národní bezpečnost.

Dle článku 8 mají členské státy povinnost určit jeden či více vnitrostátních příslušných orgánů pro klíčová odvětví v oblasti bezpečnosti sítí a informačních systémů. Dále musí určit jednotné kontaktní místo pro tuto oblast, který bude sloužit k zajištění přeshraniční spolupráce s ostatními členskými státy. Stát zajistí zdroje pro kontaktní místa, aby mohly účinně plnit svěřené úkoly. Státy mají povinnost oznámit tyto výše zmíněné orgány Komisi.

Článek 9 nařizuje členským státům utvořit jeden či více bezpečnostních týmů typu CSIRT pro pokrytí důležitých odvětví státní infrastruktury, které budou řešit rizika a incidenty dle určených postupů a zajistí dostatečné zdroje k zvládání těchto úkolů. Jednotlivé týmy musí spolupracovat jak na národní, tak na mezinárodní úrovni. Státy těmto týmům zajistí bezpečnou a odolnou komunikační a informační infrastrukturu. Státy mají povinnost oznámit působnost svých týmů Komisi. V případě potřeby mohou státy požádat agenturu ENISA (European Network and Information Security Agency) pro pomoc s budováním týmů.

Dle článku 10 státy zajistí, aby týmy dostávaly hlášení o incidentech dle směrnice NIS. Jednotlivé týmy dále předávají informace jednotným kontaktním místům.

1.4.3 Spolupráce

Článek 11 [13] řeší skupinovou spolupráci členských států. Skupina řeší své zadané úkoly na základě dvouletých období. Tato skupina je tvořena evropskou Komisí, agenturou ENISA a jednotlivými členskými státy. Komise zajišťuje služby sekretariátu. Úkoly této skupiny jsou především: strategické vedení pro síť CSIRT, výměna postupů, informací, hlášení incidentů, jednání o schopnostech a připravenosti členských států, hodnocení národních strategií, jednání o normách a specifikacích s normalizačními organizacemi, shromažďování informací o rizicích a incidentech, posuzování souhrnných zpráv, jednání o způsobech hlášení incidentů.

Článek 12 se zabývá samotnou sítí CSIRT. Síť je tvořena jednotlivými národními týmy, Agentura ENISA síti zajišťuje služby sekretariátu a podporuje spolupráci. Komise je zde pouze v roli pozorovatele. Úkolem sítě CSIRT je: zajišťování výměny informací o službách a schopnostech jednotlivých týmů CSIRT, výměna ne-obchodně citlivých informací ohledně incidentů, výměna a zpřístupnění nedůvěrných informací o incidentech, koordinování reakcí na incidenty, podpora při řešení přeshraničních incidentů, předávání včasných varování, vzájemné výpomoci, projednávání poznatků z testů a cvičení, jedná o schopnostech a připravenosti jednotlivých týmů, vydávání pokynů k usnadnění a sbližování operativních postupů.
Článek 13 řeší mezinárodní spolupráci se zeměmi mimo EU ohledně úpravy jejich účasti v činnostech pro spolupráci skupiny. Klade tím i povinnost zajištění dostatečné ochrany údajů.

1.4.4 Bezpečnost sítí a informačních systémů provozovatelů základních služeb

Tato kapitola klade obecná doporučení a opatření na bezpečnostní požadavky a případné hlášení incidentů provozovatelů základních služeb. Dle článku 14 musí členské státy zajistit přijetí vhodných a přiměřených technických a organizačních opatření k řízení bezpečnostních rizik provozovatelů základních služeb. Jedná se o opatření provozu sítí a informačních systémů, které provozovatelé používají pro výkon jejich činnosti. Tato opatření mají být odpovídající míře rizika a závažnosti případného incidentu. Incidenty musí být bez zbytečného prodlení hlášeny příslušným orgánům nebo týmu CSIRT. Tato hlášení zahrnují informace umožňující posouzení případných přeshraničních dopadů incidentů týmem CSIRT. Na významnost incidentu mají vliv především: počet uživatelů ovlivněných narušením služby, délka trvání a geografický rozsah incidentu. Po nahlášení a posouzení týmem CSIRT tým doporučí provozovateli základní služby relevantní informace následných opatření, které by mohly účinně vyřešit incident. Pokud je nutné při incidentu informovat veřejnost, může po konzultaci tuto roli zastat tým CSIRT.
Článek 15 dále řeší provádění a vymáhání. Členské státy musí zajistit všechny nezbytné pravomoci a prostředky pro posouzení, zda provozovatelé základních služeb dodržují své povinnosti ohledně bezpečnosti sítí a informačních systému. Příslušné státní orgány pak musí mít pravomoci a prostředky k vynucení sdělování informací od poskytovatelů základních služeb, podstatných pro posouzení bezpečnosti sítí a informačních systémů. Sdělované informace musí dle požadavku státních orgánů obsahovat i údaje o bezpečnosti

a o účinném provádění bezpečnostních politik a bezpečnostních auditů. V případě vyžádání těchto informací je příslušný orgán povinen uvést účel a důvod žádosti a upřesnit a specifikovat, jaké konkrétní informace jsou požadovány. Po posouzení těchto informací může příslušný orgán vydat závazné pokyny k nápravě zjištěných nedostatků provozovatelům základních služeb.

1.4.5 Bezpečnost sítí a informačních systémů poskytovatelů digitálních služeb

Článek 16 klade požadavky na bezpečnost digitálních služeb a včasné hlášení incidentů. Členské státy musí zajistit přijetí vhodných technických a organizačních opatření k řízení bezpečnostních rizik digitálních služeb. Především se jedná o sítě a informační systémy. Tato opatření musí zajišťovat určitou úroveň bezpečnosti dle rizik, která případný incident může způsobit. Hlavní kritéria pro posouzení této úrovně jsou: bezpečnost systémů a zařízení, monitorování, auditování a testování, řízení a zajištění kontinuity provozu, řešení případných incidentů a soulad s mezinárodními normami. Státy dohlíží na to, aby poskytovatelé digitálních služeb přijali potřebná opatření k minimalizaci dopadů incidentů a k zajištění kontinuity služeb. Dále musí být zajištěno, aby byly případné incidenty neprodleně hlášeny příslušným orgánům či týmům CSIRT v případě významného dopadu incidentu na poskytování služeb. Platí téměř totožné povinnosti a kritéria hodnocení jako pro poskytovatele základních služeb vysvětlených v článku 14. Změnou je to, že hlášení incidentu je povinné pouze pokud má poskytovatel digitální služby přístup k potřebným informacím k posouzení dopadu incidentu. Stejně jako u základních služeb pro mezistátní incidenty je příslušný orgán nebo tým CSIRT, kterému byl tento incident nahlášen, povinen ohlásit tento incident zasaženým členským státům. Tato nařízení se nevztahují na malé podniky a mikropodniky.

Dle článku 17 by měly státy zajistit kontrolní opatření, pokud mají důkazy, že poskytovatelé digitálních služeb neplní požadavky stanovené v předešlém článku. Státy poskytnou správním orgánům nezbytné pravomoci a prostředky. Od poskytovatelů digitálních služeb by mělo být možno požadovat poskytnutí nezbytných informací k posouzení informačních systémů a sítí včetně bezpečnostních politik a případnou nápravu při neplnění požadavků. Pokud poskytovatel digitálních služeb operuje ve vícero členských státech, měly by si být jednotlivé státy navzájem nápomocny při poskytování dostatečného zabezpečení.

Poskytovatel dle článku 18 podléhá pravomoci členského státu, v němž je primárně usazen. Je usazen primárně ve státě, kde má své sídlo. Pokud poskytovatel nemá sídlo uvnitř žádného členského státu, určí si svého zástupce, který má sídlo v některém ze členských států. V tom případě podléhá poskytovatel pravomocím státu, ve kterém je usazen jeho zástupce. V případě zastoupení poskytovatele je stále možné vést právní řízení se samotným poskytovatelem služeb.

1.4.6 Standardizace a dobrovolné hlášení

Dle článku 19 by měly členské státy podporovat používání evropských a mezinárodních norem a specifikací ohledně bezpečnosti sítí a informačních systémů, aniž by při tom diskriminovaly konkrétní druhy technologií. Doporučení a pokyny technických oblastí by měly být vydány členskými státy ve spolupráci s agenturou ENISA.

Dle článku 20 může kdokoliv, ačkoli není poskytovatelem základních či digitálních služeb, dobrovolně hlásit incidenty se závažným dopadem na kontinuitu služeb, které sami poskytují. Členské státy mají pravomoc upřednostňovat povinná hlášení před dobrovolnými a dobrovolná jsou vyřizována pouze v případech, ve kterých nepředstavují pro členské státy nepatřičnou a nepřiměřenou zátěž. V případě dobrovolných hlášení nemůže výkonný orgán ukládat takové povinnosti hlásícímu subjektu, které by mu nebyly uloženy, kdyby takovéto hlášení neučinil.

1.4.7 Závěrečná ustanovení

Článek 21 řeší sankcionování subjektů. Členské státy by měly stanovit přesné a adekvátní sankce za porušení vnitrostátních právních předpisů zavedených dle směrnice NIS. Tyto sankce by měly být účinné, přiměřené a odrazující. Tyto sankce pak musí být oznámeny Komisi, stejně tak jako jakékoli další změny těchto opatření.

Článek 22 řeší postup projednávání ve výboru. Pro případnou pomoc Komisi při posuzování a projednávání je nápomocen Výbor pro bezpečnost sítí a informačních systémů.

Dle článku 23 je Komise povinna předložit do 9. května 2019 zprávu Evropskému parlamentu a Radě, ve které vyhodnotí přístupy jednotlivých členských státu ohledně procesu určování provozovatelů základních služeb. Komise má povinnost pravidelně přezkoumávat fungování této směrnice.

Přechodná opatření jsou obsahem článku 24, který stanovuje termín, od kterého nejpozději započne síť CSIRT plnit své úkoly. Na žádosti členských států může CSIRT v přechodném období projednávat návrhy konkrétních vnitrostátních opatření umožňujících

určit provozovatele základních služeb. V přechodném období členské státy zajistí zastoupení ve skupině pro spolupráci v sítí CSIRT.

Článek 25 řeší provedení této směrnice ve vnitrostátním právu. Členské státy mají povinnost přijmout a zveřejnit právní a správní předpisy v souladu se směrnicí NIS do 9. května 2018. Přesné znění těchto předpisů musí být komisi neprodleně sděleno. Takto přijaté předpisy musí nabýt platnost od 10. května 2018. Předpisy musí obsahovat odkaz na směrnici NIS, nebo musí být odkaz učiněn při jejich úředním vyhlášení. Jakým způsobem bude tento odkaz stanoven je na posouzení členských států. Členské státy dále předloží znění hlavních ustanovení vnitrostátních právních předpisů v souladu s touto směrnicí.

Články 26 a 27 [13] řeší vstup v platnost této směrnici a cílovou skupinu určení. Směrnice platí pro všechny členské státy a je platná po uplynutí dvaceti dnů od vyhlášení v Úředním věstníku Evropské unie.

2. Komparativní analýza

V rámci systému a správy sítě by měla být zajištěna správa a ověřování identit. Měl by být použit nástroj pro správu a ověřování identit administrátorů, uživatelů a aplikací komunikačních a informačních systémů. Tento nástroj by měl zajišťovat ověření identity před tím, nežli je možné provádět činnosti v informačním a komunikačním systému. Měl by být stanoven limit pro neúspěšné pokusy o přihlášení. Měl by být dostatečně robustní a odolný před neoprávněným odcizení či zneužití přenášených a uložených autentizačních údajů. Autentizační údaje by měly být ukládány ve formě odolné proti offline útokům. Po určené době nečinnosti by měl požadovat znovu zadat autentizační údaje k ověření identity. Při obnově přístupu by měl dodržovat důvěrnost autentizačních údajů a tento systém řízení a ověřování identit by měl umožňovat centralizovanou správu identit. Autentizační mechanismus by měl být založen na větším množství faktorů, identifikátor účtu a heslo nejsou dostatečným zabezpečovacím mechanismem. Dokud není splněn požadavek na větší množství faktorů autentizace, musí nástroj pro ověření identity používat autentizaci pomocí kryptografických klíčů, aby byla zajištěna podobná úroveň zabezpečení. Pokud není nasazeno ani bezpečnostní opatření formou kryptografických klíčů, jsou dána další kritéria pro autentizaci pomocí identifikátoru účtu a hesel. Uživatelská hesla musí obsahovat nejméně 12 znaků, administrátorská hesla 17. Systém musí umožňovat zadání hesla o minimální délce 64 znaků. Musí umožňovat zadání velkých a malých písmen, číslic a speciálních znaků při tvorbě hesla. Musí umožňovat změnu uživatelských hesel, avšak ne častěji nežli jednou za 30 minut. Systém nesmí umožnit volbu nejčastěji používaných hesel, mnohonásobné opakování stejných znaků, použití přihlašovacího jména, e-mailu, názvu systému či jiných snadno odhadnutelných hesel. Dále musí zakázat volbu dříve používaných hesel s minimální pamětí pro 12 předchozích hesel. Uživatelé musí povinně měnit svá hesla nejméně jednou za 18 měsíců, mimo účty sloužící k obnově systémů v případě havárie. Dále pokud je používána pouze autentizace účtem a heslem je požadováno vynucení změny výchozího hesla po prvním použití, zneplatnění hesla sloužícího k obnovení přístupu po jeho prvním použití či uplynutí nejvýše 60 minut od jeho vytvoření a pravidla tvorby hesel musí být zahrnuty do plánu rozvoje bezpečnostního povědomí.

V rámci řízení přístupových oprávnění by měl být používán centralizovaný nástroj. Tento nástroj by měl zajistit řízení oprávnění pro umožnění přístupu k aktivům komunikačních a informačních systémů, zápis a čtení dat, nebo změnu oprávnění.

Doporučená opatření však nejsou plně konkretizovaná. Použijeme-li například doporučení ohledně hesel dle kapitoly 11.3.1 v normě ISO/IEC 27002 [6], uživatelé by měli dodržovat společností stanovené bezpečnostní postupy k tvorbě a používání hesel. Jsou kladena doporučení, která by měla být dodržena, avšak mohou existovat nejasnosti.
K zajištění nejadekvátnějšího zabezpečení je však ideální využití nejnovější české novely zákona o kybernetické bezpečnosti. Ten je zpracován v souladu s evropskou směrnicí NIS, a klade mnohdy striktnější omezení či požadavky na zabezpečení počítačových sítí a informačních systémů.

2.1 Vyhláška o Kybernetické bezpečnosti – VoKB- č. 82/2018 Sb.

Tato vyhláška klade legislativní bezpečnostní a reaktivní opatření, určuje povinné postupy při kybernetických bezpečnostních incidentech. Vychází ze směrnice NIS a dalších doplňujících materiálů. Je určena pro kritické informační a komunikační systémy, systémy poskytující základní služby a informační systémy a sítě poskytovatelů digitálních služeb. Stanovuje, jakým způsobem má vypadat obsah a struktura bezpečnostní dokumentace, bezpečnostních opatření, jakým způsobem jsou hodnoceny kybernetické bezpečnostní incidenty, jakým způsobem mají být tyto incidenty hlášeny, jakým způsobem mají být oznámeny reaktivní opatření a jeho výsledky, jakým způsobem mají být předávány kontaktní údaje, jakým způsobem mají být likvidována data, provozní údaje a veškeré informace a jejich kopie.
V první hlavě této vyhlášky jsou řešena organizační opatření. S ohledem na zaměření této práce bude tato opatření vynechána nebo využita pouze částečně. Požadavky v této hlavě jsou víceméně totožné se směrnicí ISO/IEC 27001. Mnohem významnější pro tuto diplomovou práci bude Hlava druhá, zabývající se technickými opatřeními. Tato kapitola včetně podkapitol byla zpracována dle aktuální vyhlášky o kybernetické bezpečnosti České republiky [14].

2.1.1 Technická opatření

V rámci fyzického zabezpečení by mělo být předcházeno možnému poškození, zneužití či krádeži aktiv, stejně tak přerušení poskytování služeb informačními a komunikačními systémy. Měl by být stanoven fyzický bezpečnostní perimetr, který bude určovat oblast, v niž budou uložena a zpracovávána technická aktiva komunikačních a informačních systémů. Tento perimetr by měl by měl být následně zabezpečen takovým způsobem, aby

bylo zamezeno neoprávněnému přístupu, poškozením, neoprávněným zásahům a aby byla zajištěna dostatečná ochrana jak na úrovni objektů, tak i uvnitř.

V rámci bezpečnosti komunikačních sítí je kladen důraz na nutnost segmentace sítě, zajištění řízení komunikace v rámci komunikační sítě a jejím perimetru, zavést kryptografická opatření k zajištění důvěrnosti a integrity dat při vzdáleném přístupu, vzdálené správě nebo při použití bezdrátových technologií pro přístup do komunikační sítě. Veškerá nežádoucí komunikace by měla být aktivně filtrována a blokována. Mezi segmenty sítě a při řízení komunikace by měl být využit nástroj, který zajistí ochranu integrity této sítě.

V rámci systému a správy sítě by měla být zajištěna správa a ověřování identit. Měl by být použit nástroj pro správu a ověřování identit administrátorů, uživatelů a aplikací komunikačních a informačních systémů. Tento nástroj by měl zajišťovat ověření identity před tím, nežli je možná provádět činnosti v informačním a komunikačním systému. Měl by být stanoven limit pro neúspěšné pokusy o přihlášení. Měl by být dostatečně robustní a odolný před neoprávněným odcizení či zneužití přenášených a uložených autentizačních údajů. Autentizační údaje by měly být ukládány ve formě odolné proti offline útokům. Po určené době nečinnosti by měl požadovat znovu zadat autentizační údaje k ověření identity. Při obnově přístupu by měl dodržovat důvěrnost autentizačních údajů a tento systém řízení a ověřování identit by měl umožňovat centralizovanou správu identit. Autentizační mechanismus by měl být založen na větším množství faktorů, identifikátor účtu a heslo nejsou dostatečným zabezpečovacím mechanismem. Dokud není splněn požadavek na větší množství faktorů autentizace, musí nástroj pro ověření identity používat autentizaci pomocí kryptografických klíčů, aby byla zajištěna podobná úroveň zabezpečení. Pokud není nasazeno ani bezpečnostní opatření formou kryptografických klíčů, jsou dány další kritéria pro autentizaci pomocí identifikátoru účtu a hesel. Uživatelská hesla musí obsahovat nejméně 12 znaků, administrátorská hesla 17. Systém musí umožňovat zadání hesla o minimální délce 64 znaků. Musí umožňovat zadání velkých a malých písmen, číslic a speciálních znaků při tvorbě hesla. Musí umožňovat změnu uživatelských hesel, avšak ne častěji nežli jednou za 30 minut. Systém nesmí umožnit volbu nejčastěji používaných hesel, mnohonásobné opakování stejných znaků, použití přihlašovacího jména, e-mailu, názvu systému či jiných snadno odhadnutelných hesel. Dále musí zakázat volbu dříve používaných hesel s minimální pamětí pro 12 předchozích hesel. Uživatelé musí povinně měnit svá hesla nejméně jednou za 18 měsíců, mimo účty sloužící k obnově systémů v případě havárie. Dále pokud je používána pouze autentizace účtem a heslem je

požadováno vynucení změny výchozího hesla po prvním použití, zneplatnění hesla sloužícího k obnovení přístupu po jeho prvním použití či uplynutí nejvýše 60 minut od jeho vytvoření a pravidla tvorby hesel musí být zahrnuty do plánu rozvoje bezpečnostního povědomí.

V rámci řízení přístupových oprávnění by měl být používán centralizovaný nástroj. Tento nástroj by měl zajistit řízení oprávnění pro umožnění přístupu k aktivům komunikačních a informačních systémů, zápis a čtení dat, nebo změnu oprávnění.

Dle paragrafu 21 by měla být zajištěna ochrana před škodlivým kódem s ohledem na důležitost aktiv. Měly by být zajištěny nástroje pro nepřetržitou automatickou ochranu veškerých serverů, mobilních zařízení, koncových stanic, výměnných datových nosičů a datových uložišť, komunikačních sítí, jejich prvků a obdobných zařízení. Mělo by být monitorováno a řízeno používání datových nosičů a výměnných zařízení jako jsou externí disky, veškeré automatické spouštění obsahu výměnných zařízení a datových nosičů by mělo být řízeno. Oprávnění ke spouštění kódu by mělo být také řízeno. Nástroje pro ochranu před škodlivým kódem by měly být pravidelně a účinně aktualizovány.

Dle paragrafu 22 by měly být bezpečnostní a provozní události důležitých aktiv systémově zaznamenávány, rozsah aktiv, u kterých je prováděn bezpečnostní záznam, by měl být pravidelně aktualizován s ohledem na důležitosti aktiv. Ke správnému zaznamenávání bezpečnostních a provozních událostí je zapotřebí použití průvodce k zajištění jednoznačné síťové identifikace, pokud je používán nástroj měnící síťovou identifikaci. Informace o událostech by měly obsahovat informaci o datu a čase včetně časového pásma události, typu činnosti, identifikaci technického aktiva, kterým byla činnost zaznamenána, jednoznačnou identifikaci účtu, který je zodpovědný za provedenou činnost, jednoznačnou síťovou identifikaci průvodce, který činnost způsobil a zda byla činnost úspěšná či neúspěšná. Takto zaznamenaná data i informace by měly být chráněna před neoprávněným čtením a změnami. Dále by mělo být zaznamenáváno přihlašování -i neúspěšné a odhlašování k účtům, veškeré činnosti provedené administrátory, veškeré manipulace s účty a oprávněními, záznam při zamezení činností z důvodu nedostatečných přístupových práv a oprávnění, veškeré činnosti uživatelů u kterých hrozí vliv na bezpečnost komunikačních a informačních systémů, zahájení a ukončení veškerých činností technických aktiv, chybové a kritické hlášení těchto aktiv a přístupy k záznamům o událostech a pokusy o jejich libovolnou změnu, a změny provedené v nástrojích pro jejich zaznamenávání. Veškerá technická aktiva musí synchronizovat svůj čas alespoň každých

24 hodin. Klíčové informace musí být uchovávány po dobu nejméně 18 měsíců, u auditování 12 měsíců.

Pro správné zajištění detekce kybernetických útoků je dle paragrafu 23 třeba zajistit a používat nástroj pro detekci kybernetických bezpečnostních událostí. Tento systém by měl zajišťovat blokování nežádoucí komunikace, kontrolu veškerých dat a jejich ověření v rámci perimetru komunikační sítě a taktéž v rámci samotné komunikační sítě a mezi nimi. Tato detekce by měla být zajištěna přiměřeně s ohledem na důležitost aktiv, a to v rámci serverů, mobilních zařízení, koncových stanic, výměnných datových nosičů, datových uložišť, aktivních síťových prvků a obdobných aktiv.

Kybernetické bezpečnostní události by měly být dle paragrafu 24 důkladně sbírány a zaznamenávány. Pro tento účel by měl být zřízen nástroj pro sběr takovýchto událostí, který je bude nepřetržitě vyhodnocovat. Systém bude zaznamenávat kybernetické bezpečnostní události ze všech prvků infrastruktury, bude je vyhledávat a seskupovat do kategorií dle jejich souvislostí. Bude poskytovat informace o detekovaných kybernetických událostech zodpovědných bezpečnostním pracovníkům. Ty bude také včasně varovat v případě, že hrozí vznik kybernetického bezpečnostního incidentu vlivem události. Měl by také dostatečně omezit planá volání, vyhodnocených kybernetických událostí a jejich včasná varování. Toho by mělo být dosaženo pravidelnou aktualizací nastavení systému pro sběr bezpečnostních událostí. Informace z tohoto systému by měly být použity pro optimální nastavení bezpečnostních opatření informačních a komunikačních systémů.

V rámci nasazování aplikací by měly být prováděny penetrační testy v rámci informačních a komunikačních systémů před nasazením aplikace či při její významné změně. Veškeré aplikace, informace a transakce by měly být trvale chráněny před neoprávněnými činnostmi nebo jejich popřením.

Dále by měly být zavedeny a používány kryptografické prostředky, které budou používat aktuálně odolné kryptografické algoritmy a klíče. S tím souvisí i systém správy klíčů a certifikátů. Ten by měl zajistit možnost kontroly a auditování, generování klíčů, jejich následnou distribuci, ukládání, jejich obměňování, omezení jejich platnosti, zneplatnění certifikátů a likvidaci klíčů. Dále by měl zajistit bezpečné nakládání s kryptografickými prostředky zohledňovat doporučení v oblasti kryptografických prostředků vydanými Úřadem pro kybernetickou bezpečnost, dostupnými z webových stránek úřadu.

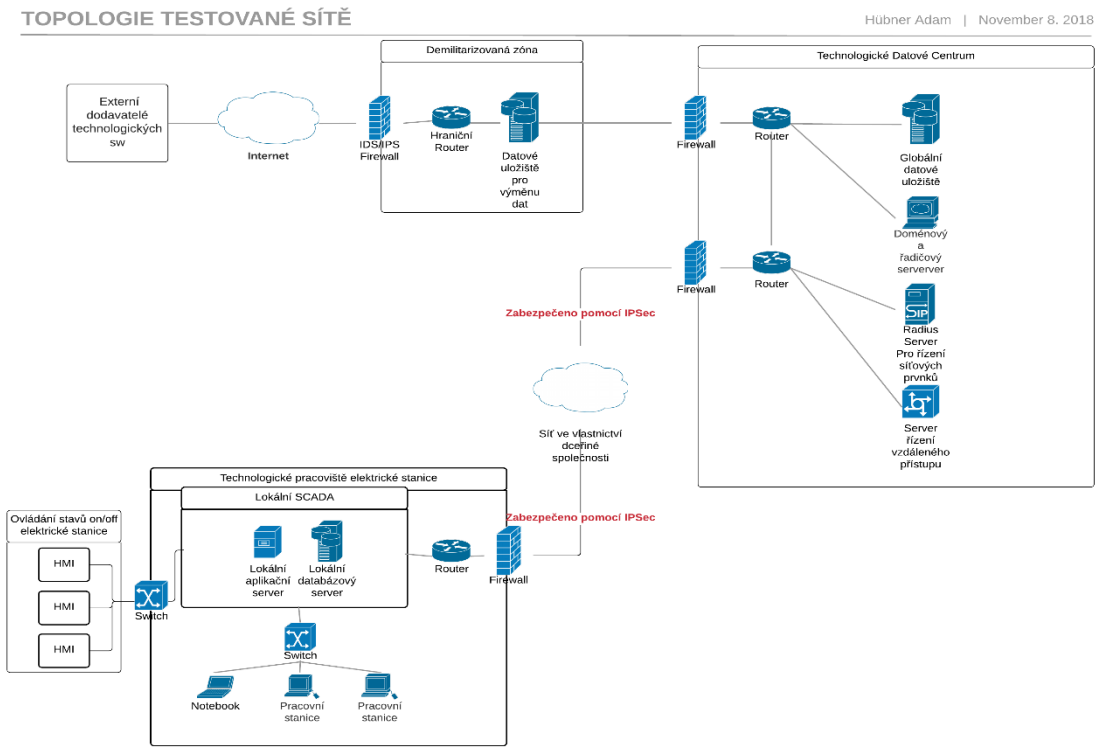
Dle paragrafu 27 by měla být zajištěna úroveň dostupnosti informačních a komunikačních systémů v dostatečné míře. Systémy musí být odolné vůči kybernetickým útokům týkajících se snížení či zamezení jejich dostupnosti. Důležitá aktiva těchto systémů musí být

taktéž dostupná, případně musí být zajištěna redundance nezbytných aktiv k zajištění dostupnosti systémů.

U průmyslových, řídících a dalších specifických systémů by měly být použity nástroje a opatření. Tato opatření se týkají použití specifických technických a programových prostředků, souvisejících s daným oborem. Omezení fyzického přístupu k těmto systémům a ke komunikační síti. Tyto systémy by měly být vyčleněny z klasické komunikační sítě a odloučeny do své specifické sítě. K těmto systémům by měl být omezen a řízen vzdálený přístup. Technická aktiva těchto systémů by měla být chráněna před využitím známých zranitelností. U těchto klíčových systémů by měly existovat opatření k rychlému obnovení po případném kybernetickém bezpečnostním incidentu.

Z podrobného prozkoumání vyhlášky o kybernetické bezpečnosti a normy ISO/IEC 27001 vyplývá velká shoda ve většině bodů. Jak vyhláška, tak norma kladou totožné požadavky na zabezpečení organizace krom bodů o digitálních službách, služeb elektronického obchodu a výměny informací s externími subjekty. V příloze číslo 2 je podrobná tabulka porovnání všech bezpečnostních požadavků vyhlášky a normy.

3. Topologie testované sítě



Obrázek 1 – Ukázka zjednodušené topologie testované sítě

Praktická část pracuje se zjednodušeným modelem komunikační části distribuční soustavy elektrické sítě. Zjednodušení je vztaženo na model technické stanice elektrické soustavy (ES) a technologického datového centra. Z pohledu vyhlášky o kybernetické bezpečnosti se je jedná o „součást kritické infrastruktury (KI)“ [14].

3.1 Technologické datové centrum

Technologické datové centrum slouží k centralizované správě jednotlivých technologických pracovišť elektrických stanic. Obsahuje globální datové uložiště a podpůrné aplikační servery, včetně serverů určených pro bezpečnost. Jedná se o srdce celého systému. V současnosti běží RADIUS dle RFC 2865 [15] protokol na jednotlivých stanicích i centru zvlášť, v námi navrhovaném řešení bude jeho správa centralizována přímo do datového centra. Doménový a řadičový server bude sloužit pro centralizovanou správu uživatelů a jejich přístupů, a dalších důležitých věcí týkajících se Active Directory (AD) a komunikace pomocí LDAP dle RFC 4511[16]. V současnosti je stanoven pouze na lokální úrovni jednotlivých stanic.

3.2 Technologická pracoviště elektrických stanic

Technologická pracoviště elektrických stanic jsou lokální ústředny, sloužící k ovládání „human machine interface“ (HMI), jejichž účelem je ovládání stavů on/off jednotlivých elektrických vedení. Takovýchto technologických pracovišť je velké množství, technici obvykle spravují x technologických pracovišť najednou. V současnosti neexistuje centralizovaná správa uživatelů, tedy každá stanice má řešenou správu uživatelů zvlášť, jednotlivě pro každou stanici. Každá ES obsahuje lokální systém „Supervisory Control And Data Acquisition (SCADA)“, neboli lokální dispečing ovládání HMI. K tomu jsou připojeny pracovní stanice, případně notebooky. Technici ES se vždy přihlašují ke konkrétní ES, která spadá pod jejich správu.

Síťovou infrastrukturu poskytuje dceřiná společnost, veškerá komunikace běží přes IP Security (IPSec). IPSec je konfigurován dle RFC 2401 [17] a RFC 2411 [18]. IPSec je soubor protokolů sloužící k ochraně důvěrnosti a integrity dat, která putují po síti. Funguje na síťové vrstvě ISO/OSI modelu a zpracovává pakety pomocí předdefinovaných skupin. Dále slouží k jednoduché implementaci virtuálních privátních sítí a vzdálenému přístupu uživatelů. K tomu používá dvě metody, autentizační hlavičku (AH – Authentication Header) a Encapsulating Security Payload (ESP). AH poskytuje autentizační služby a způsob, jak ověřit identitu odesílatele paketu. ESP naopak slouží k ověření obsahu paketu, stejně jako k šifrování dat [19].

3.3 Demilitarizovaná zóna

Demilitarizovaná zóna slouží k výměně a ukládání softwarových ovladačů HMI, jelikož HMI jsou dodávány od externích dodavatelů. Jedná se o zónu mezi privátní a veřejnou sítí. Je tedy zapotřebí, aby byla dostupná i pro veřejnost, přičemž by veřejnost neměla mít přímý přístup do vlastní vnitřní sítě. Je zabezpečena pomocí firewallů na obou stranách. V současnosti probíhá zasílání ovladačů pomocí emailu, což však není příliš bezpečný model. V navrhovaném řešení bude v Demilitarizované zóně umístěn File Trasnfer server, který bude sloužit k ukládání jednotlivých ovladačů od externích dodavatelů SW. Na vnějším perimetru (směr k internetu) bude zřízen IDS/IPS firewall [20], který bude filtrovat veškerou komunikaci směřující z a do internetu. Přímo na serveru proběhne automatická antivirová kontrola přijímaných dat. K antivirové kontrole bude použit program ESET na všech serverech i jednotlivých pracovních stanicích.

4. Návrh bezpečnostních opatření

V rámci zabezpečení bude počítačová síť rozdělena na vnitřní a vnější perimetr. Vnitřní perimetr bude dále rozdělen do sekcí dle jejich specifického použití. Tato kapitola včetně podkapitol byla zpracována za pomoci skript Pavla Šenovského [21].

4.1 Zabezpečení vnějšího perimetru

Jedná se o zabezpečení rozhraní mezi podnikovou sítí a ostatními sítěmi, především tedy Internetem. Jedná se o klíčovou část systému, přes toto rozhraní bude směřovat většina útoků z vnějšku. K zabezpečení poslouží především routery, firewally a systémy IDS a IPS. Router poslouží k směrování síťového provozu pomocí firewallů následně můžeme tento provoz účinněji filtrovat. Firewally jsou základním stavebním kamenem ochrany síťové infrastruktury. Díky nim je možné nastavit, která zařízení a které porty mohou komunikovat jejich prostřednictvím. Pomocí firewallů je možné nastavit přísná kritéria a pravidla komunikace. Nejbezpečnější variantou je filtrování veškerého provozu, který není povolen. To si však nese jistá úskalí. Pracovní stanice či jejich aplikace často potřebují využívat řadu služeb. Samozřejmě je možné tyto služby jednotlivě povolovat, nicméně udržování aktuálního a bezpečného seznamu může být často složité. Je tedy zapotřebí vyřešit rozpor mezi bezpečností a požadavky koncových uživatelů. Uživatelé potřebují přístup k síťovým službám bez ohledu na to, zda pracují ze vzdálených lokací nebo z kanceláře. Povolení těchto síťových služeb odkudkoliv by mělo negativní vliv na bezpečnost, protože by byly přístupné všem. To je obvykle řešeno různými formami autentizace, nicméně již je zde vytvořen přístup pro případný útok.

Jedním z možných v praxi využívaných řešení je použití VPN (Virtual Private Network). To zajišťuje bezpečnou komunikaci mezi vzdálenými koncovými zařízeními a počítačovou sítí. Uživatel mimo počítačovou síť využívá VPN klienta ke své autentizaci do sítě. VPN koncentrátor pak zajistí šifrované spojení mezi podnikovou sítí a vzdáleným autentizovaným zařízením. Tento koncentrátor zprostředkovává veškeré šifrování komunikace se specifickým klíčem pro každého externě připojeného uživatele. Jsou tedy kladeny vysoké požadavky na jeho výkon. Uživatelé by naopak měli využívat služeb VPN jen v případě, že potřebují síťové služby organizace, a to v co nejmenším měřítku. Uživatelé by měli omezit své činnosti na čistě pracovní a udržovat délku spojení po co nejkratší nutnou dobu.

VPN tedy slouží k šifrování samotného datového přenosu, ale již nezabezpečuje jeho obsah. K tomu je nutné stanovit ochranná opatření pro zařízení nacházející se mimo organizaci. Disky těchto zařízení by měly být šifrovány, uživatelé proškoleni o nutnosti zabezpečení a zařízení by měla být řádně konfigurována pro ochranu před škodlivým kódem a měla by obsahovat zásadní zabezpečení, jako jsou softwarové firewally a antiviry.
Pokud bude organizace používat Wi-fi (Wireless LAN), bude třeba zabezpečit i ji, poněvadž její dosah často přesahuje bezpečnostní perimetr budovy. K tomu by bylo vhodné použít rozšíření pro autentizaci síťového provozu WPA2 (Wi-Fi Protected Access II). Například EAP (Extensible Authentication Protocol) nebo PEAP (Protected EAP). EAP zajišťuje autentizační metody a další činnosti jako je například TTLS. EAP-TTLS následně zajišťuje autentizaci a vytvoření chráněného tunelu pro komunikaci (RFC 5281).

4.2 Zabezpečení Vnitřního perimetru

V této kapitole budou vysvětleny důležité bezpečnostní složky na vnitřním perimetru, tedy na vnitropodnikové síti. Jak bylo výše napsáno, jedná se především o servery a úložiště dat. Zde můžeme mít bezpečnost značně pod kontrolou, protože přesně víme, jaká zařízení důvěryhodná zóna obsahuje. Z toho důvodu můžeme tato zařízení snadněji konfigurovat co se bezpečnosti týče, stejně tak můžeme filtrovat síťový provoz, který do nich putuje. K tomuto účelu můžeme použít IDS/IPS senzory. Úkolem je zajistit, aby tato zóna byla opravdu bezpečná. Měla by být oddělena od ostatního síťového provozu, na rozhraní od zbytku podnikové sítě by měl být zaveden firewall či hardwarové diody filtrující provoz. Těmito zařízeními můžeme nastavit způsob komunikace mezi důvěryhodnými zařízeními, můžeme povolit číst, modifikovat či ukládat data pouze konkrétním zařízením z demilitarizované zóny, či zamezit poskytování služeb v důvěryhodné zóně jen na žádoucí služby.
S tím souvisejí i další bezpečnostní opatření, jako je zálohování. V předem utvořené bezpečnostní politice ISMS by měla organizace stanovit klíčová aktiva a informace, která mají být zálohována, média, na která mají být informace zálohována, jak často mají být data zálohována, jakým způsobem budou data chráněna a jakým způsobem budou data případně obnovována, v případě selhání.
S ohledem na požadavky kladené českou legislativou je ideální a dostupné zálohovací médium běžné HDD na bázi magnetického pole. Jeho životnost z důvodu demagnetizace může být přibližně 20 let, kdy legislativa klade povinnost udržovat bezpečnostní záznamy po dobu minimálně 12 nebo 18 měsíců. Zálohování by mělo probíhat po síti

na zabezpečené místo. Tím bude zajištěna ochrana zdrojů před lidskými chybami, může být proveden takzvaný rollback a zároveň je záloha zabezpečena před hardwarovými selháními jako je přepětí v síti či selhání zdroje. Další možností je volba SSD disků místo HDD. Mají vyšší zápisovou rychlost, netrpí na demagnetizaci, ale jsou omezené na určitý počet zápisů. Další možností zálohy je zápis na magnetické pásky, vhodné na zálohování velkého množství dat. Dále také existuje možnost zálohovat data v cloudu. Takto zálohovaná data jsou chráněná před fyzickým poškozením, na druhou stranu je třeba zvolit dobře zabezpečeného a důvěryhodného poskytovatele cloudových služeb. Případně lze využít možnost pronajmu prostoru v datových centrech a mít v nich vlastní zálohovací systém.
Dále je nutné zvolit typ zálohy, jakou budeme používat. Volba úplné zálohy je vždy bezpečnější, avšak její nevýhodou je dlouhá doba zálohování. Dále také při častém provádění úplných záloh bude nutné vynaložit větší prostředky na kapacitu zálohovacích zařízení. Další možností je inkrementální zálohování. Ta během zvolených časových intervalů zálohuje chráněná data. Zřizovatel specifikuje, která data projdou úplnou zálohou, a která pouze inkrementální. Inkrementální záloha pak obsahuje pouze taková data, která se změnila od doby poslední zálohy. Takto zálohované změny v souborech jsou identifikovány pomocí metaúdaje času modifikace. Při obnovně dat ze zálohy se nejprve provede obnovení dat z úplné zálohy a následně jsou obnoveny změny z inkrementálních záloh.
Aby bylo možné uchránit zálohovaná data před neoprávněnou manipulací a čtením, je třeba využít šifrovací schémata. Dále je nutné mít šifrovací klíče uložené na bezpečném místě, abychom mohli takovouto zálohu použít i v případě hardwarového selhání zálohovaného média.
Dále je dobré vzít v úvahu oddělení datové a programové části. Datovou část postačí zálohovat tradičním způsobem, pro programovou lze využít klonování disků. To zajistí, že po obnovení systému z obrazu na klonovaném disku bude systém opět plně funkční, protože není zálohován jen veškerý obsah souborů, ale jejich pozice na disku.
Samotná disková pole by měla být chráněna před hardwarovými selháními. K tomu poslouží různé druhy RAIDů. Jejich účel je ochrana dat před selháním jednotlivých disků. Z toho důvodu jsou disky uspořádány do diskových polí, jak anglický název napovídá (Redundant Array of Independent Discs). Kromě samotných dat jsou na disky alokovány paritní informace. Tyto informace slouží k rekonstrukci údajů z disků při jejich selhání. Existuje hned několik druhů RAIDů, v některých případech je možné použít i jejich kombinace. RAID-0 neslouží k redundanci dat, slouží především ke zrychlení zápisu, protože využívá obrácený princip. Data jsou rozdělena na části a každá část se zapisuje na jiný

disk. RAID-1 je považován za jeden z nejbezpečnějších, ale nejnákladnějších, tvoří úplný obraz dat na druhém disku. Ještě lepší bezpečnosti a rychlosti zápisu a čtení je docíleno pomocí RAID-10. Jedná se o kombinaci RAID 0 a RAID-1. Dvě disková pole typu RAID-0 jsou zapojena do RAID-1. V tomto případě je nutné vynaložit vysoké náklady na disková pole. Dále je možné využít RAID-5, který je použitelný při zapojení minimálně tří disků, kde kapacita jednoho disku je využita k záloze. Na všechny disky se ukládá část informací a při selhání jednoho z disků je možné použít data z ostatních disků k rekonstrukci disku, který selhal. Dále je možné selháním předcházet využitím disků s technologií S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology), které mohou při správném nastavení včasně informovat o potřebě výměny.
Dále by měly být veškeré porty zabezpečeny a vázány pouze na dané zařízení.

4.2.1 Systém fyzické ochrany C4

V rámci fyzické ochrany bude zaveden systém C4 [22]. To zahrnuje centralizovanou ochranu budov a jednotlivých aktiv organizace. K přístupu do budov organizace bude zaveden systém čipových karet. Toto opatření bylo zvoleno z důvodu požadované dvoufázové autentizace. Kvůli zákonu o ochraně osobních údajů nebyla zvolena autentizace pomocí oční sítnice nebo otisku prstů. Čtečkou karet budou vybaveny veškeré vstupní dveře a pracovní stanice. Zaměstnancům tak bude umožněn přístup pouze do míst, které jsou potřebné k výkonu jejich pracovních činností.
Budovy budou dále vybaveny kamerovými systémy na jednotlivých pracovištích. Stejně tak budou kamerami vybavena důležitá aktiva. Kamery budou spouštěny pouze při manipulaci s uvedenými aktivy (například otevření serverového racku).
V rámci systému C4 budou zapojena i požární čidla a další zařízení potřebná pro zabezpečení budov před přírodními katastrofami. Systém bude logován a bude upozorňovat odpovědnou osobu při jakékoliv změně či hrozbě. Pomocí předdefinovaných akcí systém automaticky vyřeší problém bez nutnosti lidského zásahu.

4.2.2 Systém managementu bezpečnostních informací a událostí

Security Information and Event Management (SIEM) [20] je dalším z nasazených systémů v rámci zabezpečení organizace. Takovéto systémy slouží ke snadnější a automatizované analýze a případnému hlášení problémů. Hlavními úkoly SIEM jsou:

- Včasná varování před útoky.
- Zálohování/Logování dat z reportů.

- Identifikace událostí a jejich vztažení ke správné příčině/cíli.
- Seskupování dat z jednotlivých prvků systému (firewally, servery, routery, switche, databáze, IDS/IPS.

K tomu poslouží centralizovaný Systém záznamu událostí Zabbix. Server bude umístěn v datovém centru organizace. Klient Zabbixu je nenáročný a je možné jej provozovat na veškerých zařízeních organizace. Tím bude docíleno centralizovaného monitoringu síťového provozu i jednotlivých zařízení.

Zabbix k tomuto účelu poskytuje sběr dat z SNMP (Simple Network Management Protocol) a pro kontrolu HW stavu zařízení IPMI (Intelligent Platform Management Interface). Dále zajišťuje kontrolu provozu na síťových portech. Odpovídající funkčnost je zajištěna u následujících služeb:

- FTP (File Transfer Protocol)
- IMAP (Internet Message Access Protocol)
- HTTP (Hypertext Transfer Protocol)
- HTTPS (Hypertext Transfer Protocol Secure)
- LDAP (Lightweight Directory Access Protocol)
- NNTP (Network News Transfer Protocol)
- POP3 (Post Office Protocol 3)
- SMTP (Simple Mail Transfer Protocol)
- SSH (Secure Shell) TCP (Transmission Control Protocol)
- Telnet (teletype network)

Dále také umožňuje kontrolu dostupnosti služeb přes TCP porty, kontrolu ICMP (Internet Control Message Protocol) pingu k ověření dostupnosti serverů a případnou kontrolu ztráty paketů, dále přístup ke službám monitoringu přes SSH nebo Telnet [23].

5. Realizace bezpečnostních opatření

V organizaci bude zaveden systém ISMS dle vyhlášky o kybernetické bezpečnosti [14] a všichni zaměstnanci budou o tomto kroku informováni. V rámci toho bude vydán dokument, který bude pravidelně každý rok a při každé významné změně systémů, které mají vliv na bezpečnost organizace, aktualizován. Bude obsahovat bezpečnostní dokumentaci, bezpečnostní opatření uvedená v této kapitole, hodnocení kybernetických incidentů a jakým způsobem takovéto incidenty hlásit, oznámení o provádění reaktivních opatření a informaci o způsobu likvidace dat, informací a jejich kopií.

Dále budou stanoveny role a odpovědnosti pracovníků, kteří budou zajišťovat koordinaci nasazení a funkčnosti ISMS, a budou odpovědni za bezpečnost organizace v daných sektorech.

V rámci organizace budou stanovena aktiva a způsob hodnocení jejich důležitosti a možných rizik. Hodnota aktiv bude vypočítána dle součinu možného dopadu bezpečnostního incidentu, hrozby a zranitelnosti aktiva. V rámci hodnocení rizik budou stanoveny 4 kategorie:

- nízké riziko – přijatelné riziko,
- střední riziko – v případě že je řešitelné nepříliš náročnými opatřeními, případně pokud je náročnost vysoká, je považováno za přijatelné,
- vysoké riziko – dlouhodobě nepřípustné riziko, mělo by být systematicky odstraněno,
- kritické riziko – akutní riziko, které musí být neprodleně odstraněno.

Typy aktiv budou stanovena na:

- datová,
- hardwarová,
- softwarová,
- informační služby.

V rámci stanovení hodnocení integrity aktiv budou stanoveny 4 typy hodnocení:

- nízká – není vyžadována ochrana integrity,
- střední – může být vyžadována ochrana integrity,
- vysoká – vyžaduje ochranu integrity,
- kritická – vyžaduje ochranu integrity, jedná se o klíčový prvek.

Stejně tak bude na úrovně stanoveno hodnocení u dostupnosti a důvěrnosti, a to konkrétně dostupnost:

- nízká – dostupnost aktiva není klíčová, výpadek je možno tolerovat v rámci dnů,
- střední – výpadek dostupnosti aktiva by neměl překročit jeden den,
- vysoká – výpadek dostupnosti by neměl překročit několik hodin, výpadek je nutné akutně řešit,
- kritická – výpadek daného aktiva není přípustný v rámci zachování zájmu organizace,

a důvěrnost:

- nízká – veřejně přístupná aktiva, neohrožující zájmy organizace,
- střední – soukromá aktiva, jejichž ochrana není vyžadována legislativou,
- vysoká – neveřejná aktiva jejichž ochrana je vyžadována právními předpisy nebo smluvními ujednáními, například osobní údaje,
- kritická – neveřejná aktiva jejichž ochrana je vyžadována právními předpisy nebo smluvními ujednáními, například citlivé osobní údaje.

S důvěrností blízce souvisí způsob likvidace dat. Data jsou likvidována s ohledem na typ aktiva a hodnocení důvěrnosti.

Dále jsou stanoveny kategorie pro hodnocení hrozeb:

- Nízké – jsou neexistující hrozby či málo časté hrozby. Výskyt takovéto hrozby není častější nežli jednou za 5 let.
- Střední – jsou málo pravděpodobné až pravděpodobné hrozby. Výskyt takovéto hrozby je obvyklý v rámci 1 až 5 let.
- Vysoké – jsou pravděpodobné až velmi pravděpodobné hrozby. Obvyklý výskyt takovéto hrozby je obvykle od 1 do 12 měsíců.
- Kritické – jsou velmi pravděpodobné až jisté hrozby. Obvyklý výskyt je častější nežli jednou za měsíc.

V poslední řadě jsou stanoveny následující kategorie pro hodnocení zranitelností:

- Nízká – neexistující či málo pravděpodobné zranitelnosti, případně jsou zavedena bezpečnostní opatření, která včasně detekují zranitelnosti a jejich případné zneužití.
- Střední – málo pravděpodobné až pravděpodobné zranitelnosti. Existují funkční bezpečnostní opatření, která jsou pravidelně kontrolována. Bezpečnostní opatření

jsou schopná zranitelnost detekovat nebo omezit případné pokusy o překonání bezpečnostních opatření. Dosavadní opatření nebyla doposud překonána.

- Vysoká – pravděpodobné až velmi pravděpodobné zranitelnosti. Dosavadní bezpečnostní opatření nepokrývají potřebné aspekty a nejsou pravidelně kontrolována. Je možné, že proběhly úspěšné dílčí pokusy o překonání bezpečnostních opatření.
- Kritická – pravděpodobné až téměř jistě zneužitelné zranitelnosti. Bezpečnostní opatření neexistují, nebo nefungují dostatečně účinně. Jejich kontrola není prováděna. Jsou známé případy překonání bezpečnostních opatření.

V rámci hodnocení aktiv byla stanovena následující aktiva a jejich hodnocení. Pro snadnější výpočet rizik jsou slovní hodnocení ze stupnic hodnocení převedena na číselnou řadu (1 – nízká, 2 – střední, 3 – vysoká, 4 – kritická). Stejná číselná řada je použita i u hodnocení konkrétních hrozeb a zranitelností. Tato kritéria vychází z vyhlášky o kybernetické bezpečnost [14].

Aktiva:	Důvěrnost:	Dostupnost:	Integrita:	Dopad:
Mobilní zařízení	2	1	2	4
Lokální SCADA ES	3	3	4	36
Pracovní stanice	2	2	3	12
Demilitarizovaná zóna	3	2	2	12
Technologické datové centrum	3	4	3	36

Tabulka 1 - hodnocení aktiv

V následujících tabulkách jsou uvedeny hrozby a zranitelnosti jednotlivých aktiv organizace. Dopad značí významnost aktiva pro organizaci. Je vypočítán pomocí součinu hodnot důvěrnosti, dostupnosti a integrity aktiva. Čím vyšší číslo, tím důležitější je aktivum pro organizaci. Hrozba označuje, jak moc je pravděpodobné, že dojde k incidentu. Čím vyšší číslo je, tím je incident pravděpodobnější a jeho výskyt častější. Zranitelnost značí aktuální ochranu aktiva před konkrétní hrozbou. Aktuálně nechráněná aktiva jsou značena nejvyšší hodnotou 4. Při provádění bezpečnostních opatření se bude tato hodnota snižovat v závislosti na účinnosti provedených bezpečnostních opatření. Naopak hodnota hrozby zůstane vždy stejná. Riziko je dáno součinem hrozby a zranitelnosti, a značí míru zneužitelnosti. Celkové riziko je součinem rizika a dopadu. Zohledňuje tedy nejen samotné riziko vzniku hrozby, ale i to, jaký vliv může mít případný incident na chod organizace. Čím vyšší číslo, tím kritičtější je stav a nutnost ochrany daného aktiva.

Lokální SCADA ES:

Hrozba:	Zranitelnost:	Dopad:	Hrozba:	Zranitelnost:	Riziko:	Celkové riziko:
Zneužití oprávnění	Nevhodné nastavení přístupových oprávnění	36	2	3	6	216
Ztráta, odcizení nebo poškození aktiva	Nedostatečné fyzické zabezpečení perimetru	36	2	4	8	288
Napadení elektronické komunikace (odposlech, modifikace)	Přenos odkrytých hesel	36	2	2	6	216
Napadení elektronické komunikace (odposlech, modifikace)	Nedostatečná kryptografická opatření	36	2	3	6	216
Napadení elektronické komunikace (odposlech, modifikace)	Nedostatečné zabezpečení portů	36	2	4	8	288
Napadení elektronické komunikace (odposlech, modifikace)	Nedostatečný systém pro detekci kybernetických útoků	36	3	3	9	324
Poškození dat	Nedostatečná kryptografická opatření	36	2	3	6	216
Zneužití nebo neoprávněná modifikace údajů	Nedostatečná kryptografická opatření	36	2	3	6	216
Zneužití vnitřních prostředků, sabotáž	Nedostatek kontrolních mechanizmů	36	2	4	8	288
Zneužití vnitřních prostředků, sabotáž	Nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování	36	2	4	8	288
Zneužití vnitřních prostředků, sabotáž	Nedostatečný systém pro detekci kybernetických útoků	36	2	3	6	216
Ztráta, odcizení nebo poškození aktiva	Nedostatečná údržba	36	3	2	6	216
Narušení fyzické bezpečnosti	Nedostatečné fyzické zabezpečení perimetru	36	2	4	8	288

Tabulka 2 - zranitelnosti a hrozby síťové infrastruktury před zavedením navržených bezpečnostních opatření

Demilitarizovaná zóna:

Hrozba:	Zranitelnost:	Dopad:	Hrozba:	Zranitelnost:	Riziko:	Celkové riziko:
Poškození dat	Nedostatečná ochrana vnějšího perimetru	12	2	4	8	96
škodlivý kód (například viry, spyware, trojské koně)	Nedostatečná automatická ochrana před škodlivým kódem	12	3	3	9	108
Zneužití vnitřních prostředků, sabotáž	Nedostatek kontrolních mechanizmů	12	2	4	8	96
Zneužití vnitřních prostředků, sabotáž	Nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování	12	2	4	8	96
Napadení elektronické komunikace (odposlech, modifikace)	Nedostatečný systém pro detekci kybernetických útoků	12	3	4	12	144
DoS útok	Nedostatečná ochrana vnějšího perimetru	12	3	4	12	144

Tabulka 3 - zranitelnosti a hrozby serverové farmy před zavedením navržených bezpečnostních opatření

Mobilní zařízení:

Hrozba:	Zranitelnost:	Dopad:	Hrozba:	Zranitelnost:	Riziko:	Celkové riziko:
Ztráta, odcizení nebo poškození aktiva	Nedostatečné bezpečnostní školení	4	2	3	6	24
Zneužití oprávnění	Špatná správa hesel	4	2	4	8	32
Zneužití oprávnění	Nevhodné nastavení přístupových oprávnění	4	3	3	9	36
škodlivý kód (například viry, spyware, trojské koně)	Nedostatečná automatická ochrana před škodlivým kódem	4	3	3	9	36

Tabulka 4 - zranitelnosti a hrozby mobilních zařízení před zavedením navržených bezpečnostních opatření

Technologické datové centrum:

Hrozba:	Zranitelnost:	Dopad:	Hrozba:	Zranitelnost:	Riziko:	Celkové riziko:
Ztráta, odcizení nebo poškození aktiva	Nedostatečné fyzické zabezpečení perimetru	36	2	3	6	216
Nezákonné zpracování dat	Špatná správa hesel	36	2	4	8	288
Zneužití nebo neoprávněná modifikace údajů	Špatná správa hesel	36	2	4	8	288
Škodlivý kód (například viry, spyware, trojské koně)	Nedostatečná automatická ochrana před škodlivým kódem	36	2	3	6	216
Zneužití vnitřních prostředků, sabotáž	Nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování	36	2	4	8	288
Napadení elektronické komunikace (odposlech, modifikace)	Nedostatečný systém pro detekci kybernetických útoků	36	3	4	12	432

Tabulka 5 - zranitelnosti a hrozby datových uložišť před zavedením navržených bezpečnostních opatření

Pracovní stanice:

Hrozba:	Zranitelnost:	Dopad:	Hrozba:	Zranitelnost:	Riziko:	Celkové riziko:
Ztráta, odcizení nebo poškození aktiva	Nedostatečné fyzické zabezpečení perimetru	12	2	3	6	72
Zneužití oprávnění	Špatná správa hesel	12	2	3	6	72
Zneužití oprávnění	Nevhodné nastavení přístupových oprávnění	12	3	3	9	108
Zneužití vyměnitelných technických nosičů dat	Nedostatečná automatická ochrana před škodlivým kódem	12	3	3	9	108
Cílený kybernetický útok pomocí sociálního inženýrství	Nedostatečné bezpečnostní školení	12	2	3	6	72
škodlivý kód (například viry, spyware, trojské koně)	Nedostatečná automatická ochrana před škodlivým kódem	12	3	3	9	108

Tabulka 6 - zranitelnosti a hrozby koncových stanic před zavedením navržených bezpečnostních opatření

Následně můžou být nasazena bezpečnostní opatření ke všem zranitelnostem:

- **Nevhodné nastavení přístupových oprávnění** – Každý zaměstnanec bude mít nastavena přístupová oprávnění na minimální možné, s ohledem na potřeby jeho pracovní činnosti. Veškeré změny v oprávněních budou pečlivě přezkoumávány a logovány. Stejná pravidla budou platit při využívání serverů, datových uložišť, klientských stanic a mobilních zařízení. Veškeré programové vybavení bude umožněno instalovat pouze odpovědným pracovníkům. V rámci sítě bude zřízeno Active Directory a komunikace pomocí LDAP [16].
- **Nedostatečné fyzické zabezpečení perimetru** – Budova organizace bude dostatečně zabezpečena, vstup do budovy bude kontrolován a přístup bude povolen pouze zaměstnancům podniku. K tomu bude nasazen systém fyzické ochrany C4 [22]. Přístup na jednotlivá pracoviště bude umožněn pouze pomocí čipové karty, stejným způsobem budou odděleny serverové místnosti od zbytku budovy. Kamerové systémy budou umístěny u klíčových aktiv organizace i uvnitř serverových racků, automaticky spouštěné při jejich otevření. Veškerá správa fyzické bezpečnosti bude centralizovaná a logovaná.
- **Nedostatečná ochrana vnějšího perimetru** – Na vnějším perimetru počítačové sítě bude zřízen firewall, který bude filtrovat veškerou škodlivou a nedůvěryhodnou komunikaci. Bude postupováno dle RFC 6092 [24] a RFC 4890 [25][25]. Firewallem bude také zabezpečena serverová a datová část infrastruktury od zbytku podnikové sítě. Mobilní zařízení budou moci přistupovat k ostatním aktivům pouze pomocí EAP-TTLS dle RFC 5281 [26]. Tyto služby zajistí jeden ze serverů. DoS útokům bude předcházeno dle RFC 2827 [9].
- **Přenos odkrytých hesel** – K přenosu hesel a dalších důležitých dat bude nasazen AAA protokol [19] RADIUS. Centrální RADIUS [15] server bude umístěn v technologickém datovém centru. Ten zajišťuje veškeré potřeby, šifruje jak hesla, tak celé pakety a využívá transportní protokol TCP.
- **Nedostatečná kryptografická opatření** – Souvisí s předešlým bodem. Provoz po vnitropodnikové síti je dále zajištěn pomocí IPSeC [17].
- **Nedostatečné zabezpečení portů** – Veškeré porty budou fyzicky zajištěny, případně zaslepeny, aby byl zamezen možný přístup k síťové infrastruktuře. Veškerá komunikace po nepovolených internetových portech bude zamezena firewally.

Povolené porty budou pouze ty, které jsou potřebné pro provoz komunikační části distribuční soustavy elektrické sítě.

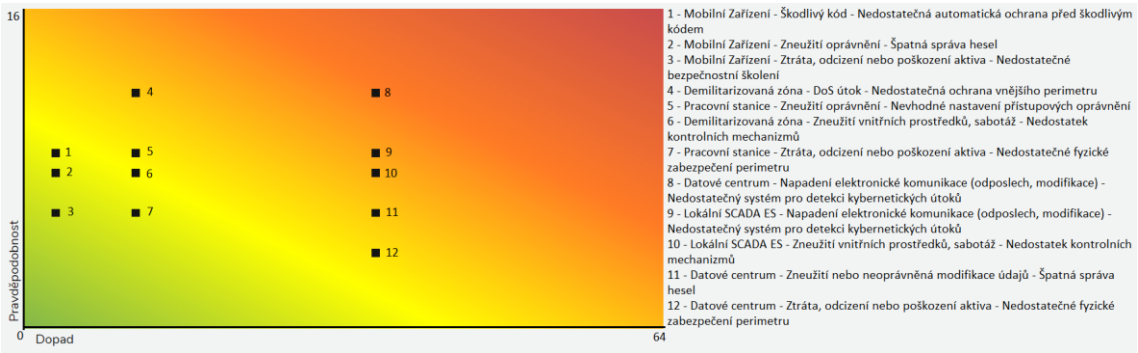
- **Nedostatečný systém pro detekci kybernetických útoků** – K detekci kybernetických útoků bude zřízen IDS dle RFC 4766 [27] , který bude spravován vyškoleným pracovníkem zodpovědným za jeho chod, případné hlášení a provádění ochranných opatření. Kromě toho bude veškerý provoz monitorován pomocí nástroje Zabbix. Dalším bodem je provoz antivirového programu Eset který zajišťuje automatickou ochranu před malwerem.
- **Nedostatek kontrolních mechanizmů** – Viz předešlé bezpečnostní opatření. Dále také bude zajištěno šifrování disků mobilních zařízení a externích uložišť.
- **Nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování** – Veškerý síťový provoz bude monitorován pomocí nástroje Zabbix [23]. Měl by zajistit dostatečnou úroveň monitoringu a zabezpečit tak včasná protiopatření. Dále budou prováděny pravidelné fyzické kontroly činnosti uživatelů a administrátorů.
- **Nedostatečná automatická ochrana před škodlivým kódem** – K ochraně před škodlivým kódem budou veškeré servery, klientské stanice a mobilní zařízení zabezpečena softwarem pro automatickou ochranu. Dle nezávislého testování [28] byl jakožto nejlepší kandidát zvolen Eset, který by měl zajistit dostatečnou úroveň zabezpečení ve všech ohledech vyhlášky č. 82/2018 Sb,
- **Špatná správa hesel** – V rámci správy hesel budou vytvořena softwarová opatření znemožňující volbu slabých hesel. Hesla budou povinně obsahovat minimálně 12 znaků, velká a malá písmena, speciální znaky a systém bude kontrolovat, zda se znaky příliš neopakují. Povinná změna hesla proběhne každé tři měsíce, resetované heslo bude možné použít pouze jednou, a to v rámci 30 minut od jeho aktivace. To bude zajištěno pomocí firemního správce hesel ManageEngine Password Manager Pro [29].
- **Nedostatečná údržba** – V rámci zajištění údržby bude veškerý hardware fyzicky kontrolován a monitorován. Obzvláště pak budou kontrolovány a monitorovány serverové zařízení a datová uložiště. Veškerá data budou zálohována každý den úplnou zálohou a každých třicet minut zálohou inkrementální. Data na datových uložištích budou uchovávána po dobu minimálně tří let. Disková pole budou

chráněna technologií S.M.A.R.T. Softwarová zařízení budou podléhat údržbě a pravidelným revizím.

- **Nedostatečné bezpečnostní školení** – Veškerý personál bude vyškolen v obecných bezpečnostních opatřeních, v systému ISMS a dále v bezpečnosti v konkrétních zaměření pracovních odvětví. Součástí obecných bezpečnostních opatření je i poučení o sociálním inženýrství. Zaměstnanci budou školeni při vstupu do zaměstnání, při zavedení systému ISMS a při každé významné změně bezpečnostních opatření.

6. Testování bezpečnostních opatření

K testování zabezpečení byl použit auditovací nástroj pro správu bezpečnostních hrozeb dle vyhlášky č. 82/2018 Sb o Kybernetické bezpečnosti vytvořený jakožto diplomová práce Jakuba Janši [30] nalezený na stránkách Národního Úřadu pro Kybernetickou Bezbečnost, dostupný z webu: http://kubikuv.cloud/audit/ [31]. V předchozí kapitole byly představeny jednotlivé zranitelnosti a hrozby aktiv organizace, před zavedením a nasazením navržených bezpečnostních opatření. Online auditovací nástroj poskytuje i grafické znázornění rizik s ohledem na význam jednotlivých aktiv. Takto nezabezpečená síť je znázorněna na obrázku číslo 1.



Obrázek 2 - Grafické znázornění rizik bez nasazených bezpečnostních opatření

Zde je možné vidět rizika v závislosti na pravděpodobnosti a možném způsobeném dopadu nedostatečných bezpečnostních opatření na chod organizace. Zelené hodnoty jsou ideální, žluté přijatelné, oranžové značí významnější riziko, které vyžaduje řešení, červené hodnoty značí kritický stav ohrožující chod podniku. Hodnota pravděpodobnosti je rovna riziku v tabulkách. Návrh grafického znázornění mapy rizik byl převzat od Vlasty Svaté z knihy Audit informačního systému [32].

V následujících tabulkách jsou nasazena bezpečnostní opatření. Rizika se značným způsobem zmenšila oproti předešlým tabulkám.

Lokální SCADA ES:

Hrozba:	Zranitelnost:	Dopad:	Hrozba:	Zranitelnost:	Riziko:	Celkové riziko:
Zneužití oprávnění	Nevhodné nastavení přístupových oprávnění	36	2	1	2	72
Ztráta, odcizení nebo poškození aktiva	Nedostatečné fyzické zabezpečení perimetru	36	2	1	2	72
Napadení elektronické komunikace (odposlech, modifikace)	Přenos odkrytých hesel	36	2	1	2	72
Napadení elektronické komunikace (odposlech, modifikace)	Nedostatečná kryptografická opatření	36	2	1	2	72
Napadení elektronické komunikace (odposlech, modifikace)	Nedostatečné zabezpečení portů	36	2	1	2	72
Napadení elektronické komunikace (odposlech, modifikace)	Nedostatečný systém pro detekci kybernetických útoků	36	3	1	3	108
Poškození dat	Nedostatečná kryptografická opatření	36	2	1	2	72
Zneužití nebo neoprávněná modifikace údajů	Nedostatečná kryptografická opatření	36	2	1	2	72
Zneužití vnitřních prostředků, sabotáž	Nedostatek kontrolních mechanizmů	36	2	1	2	72
Zneužití vnitřních prostředků, sabotáž	Nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování	36	2	1	2	72
Zneužití vnitřních prostředků, sabotáž	Nedostatečný systém pro detekci kybernetických útoků	36	2	1	2	72
Ztráta, odcizení nebo poškození aktiva	Nedostatečná údržba	36	3	1	3	108
Narušení fyzické bezpečnosti	Nedostatečné fyzické zabezpečení perimetru	36	2	1	2	72

Tabulka 7 - zranitelnosti a hrozby síťové infrastruktury bez zavedených bezpečnostních opatření

Demilitarizovaná zóna:

Hrozba:	Zranitelnost:	Dopad:	Hrozba:	Zranitelnost:	Riziko:	Celkové riziko:
Poškození dat	Nedostatečná ochrana vnějšího perimetru	12	2	2	4	48
škodlivý kód (například viry, spyware, trojské koně)	Nedostatečná automatická ochrana před škodlivým kódem	12	3	1	3	36
Zneužití vnitřních prostředků, sabotáž	Nedostatek kontrolních mechanizmů	12	2	1	2	24
Zneužití vnitřních prostředků, sabotáž	Nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování	12	2	2	4	48
Napadení elektronické komunikace (odposlech, modifikace)	Nedostatečný systém pro detekci kybernetických útoků	12	3	1	3	36
DoS útok	Nedostatečná ochrana vnějšího perimetru	12	3	2	6	72

Tabulka 8 - zranitelnosti a hrozby serverové farmy bez zavedených bezpečnostních opatření

Mobilní zařízení:

Hrozba:	Zranitelnost:	Dopad:	Hrozba:	Zranitelnost:	Riziko:	Celkové riziko:
Ztráta, odcizení nebo poškození aktiva	Nedostatečné bezpečnostní školení	4	2	2	4	16
Zneužití oprávnění	Špatná správa hesel	4	2	1	2	8
Zneužití oprávnění	Nevhodné nastavení přístupových oprávnění	4	3	1	3	12
škodlivý kód (například viry, spyware, trojské koně)	Nedostatečná automatická ochrana před škodlivým kódem	4	3	1	3	12

Tabulka 9 - zranitelnosti a hrozby mobilních zařízení bez zavedených bezpečnostních opatření

Technologické datové centrum:

Hrozba:	Zranitelnost:	Dopad:	Hrozba:	Zranitelnost:	Riziko:	Celkové riziko:
Ztráta, odcizení nebo poškození aktiva	Nedostatečné fyzické zabezpečení perimetru	36	2	1	2	72
Nezákonné zpracování dat	Špatná správa hesel	36	2	1	2	72
Zneužití nebo neoprávněná modifikace údajů	Špatná správa hesel	36	2	1	2	72
Škodlivý kód (například viry, spyware, trojské koně)	Nedostatečná automatická ochrana před škodlivým kódem	36	2	1	2	72
Zneužití vnitřních prostředků, sabotáž	Nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování	36	2	1	2	72
Napadení elektronické komunikace (odposlech, modifikace)	Nedostatečný systém pro detekci kybernetických útoků	36	3	1	3	108

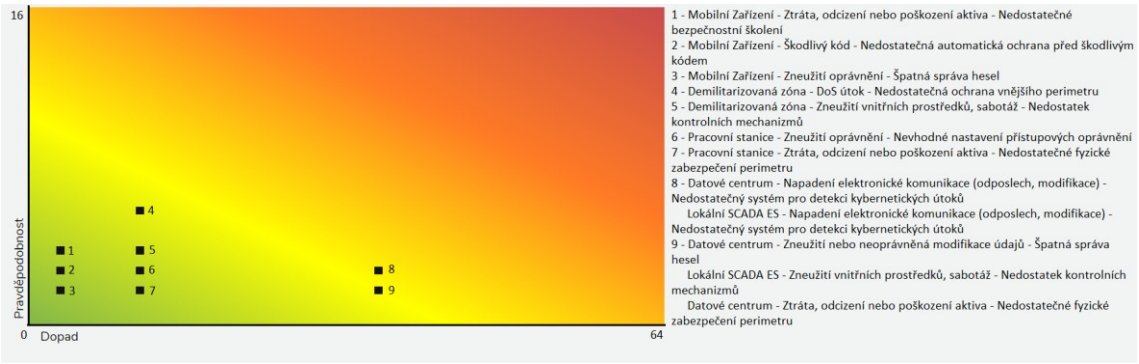
Tabulka 10 - zranitelnosti a hrozby datových uložišť bez zavedených bezpečnostních opatření

Pracovní stanice:

Hrozba:	Zranitelnost:	Dopad:	Hrozba:	Zranitelnost:	Riziko:	Celkové riziko:
Ztráta, odcizení nebo poškození aktiva	Nedostatečné fyzické zabezpečení perimetru	12	2	1	2	24
Zneužití oprávnění	Špatná správa hesel	12	2	1	2	24
Zneužití oprávnění	Nevhodné nastavení přístupových oprávnění	12	3	1	3	36
Zneužití vyměnitelných technických nosičů dat	Nedostatečná automatická ochrana před škodlivým kódem	12	3	1	3	36
Cílený kybernetický útok pomocí sociálního inženýrství	Nedostatečné bezpečnostní školení	12	2	2	4	48
škodlivý kód (například viry, spyware, trojské koně)	Nedostatečná automatická ochrana před škodlivým kódem	12	3	1	3	36

Tabulka 11 - zranitelnosti a hrozby koncových stanic bez zavedených bezpečnostních opatření

Jak je možné vidět z tabulek, rizika výrazně poklesla. Ještě lépe je to však vidět v následujícím grafu:



Obrázek 3 - Grafické znázornění rizik s nasazenými bezpečnostními opatřeními

Veškerá aktiva organizace jsou chráněna s ohledem na pravděpodobnost a možný dopad na chod organizace. Můžeme si povšimnout, že pravděpodobnost vzniku bezpečnostního problému je vyšší u mobilních zařízení a demilitarizované zóny. Přesto se jedná v rámci organizace o přijatelné riziko. Naopak i po zavedení bezpečnostních opatření na Datovém centru a Lokální SCADA se nám sice podařilo minimalizovat rizika, nicméně případný incident by měl mnohem vyšší dopad a vliv na chod organizace (nachází se ve žlutém poli na grafickém znázornění mapy rizik). To značí přijatelné riziko, nicméně je zapotřebí pravidelná kontrola bezpečnostních opatření. Činnosti bodů 8 a 9 by měly být znovu přezkoumány v budoucích krocích ISMS, aby byla zajištěna náležitá ochrana.

Pokud porovnáme mapu před a po zavedení nových bezpečnostních opatření, můžeme si povšimnout, nulového posunu po ose dopadu. To je z důvodu, že samotná aktiva se v průběhu nasazování nemění. Dopad jednotlivých aktiv byl určen již před testem. Hrozby samotné zůstávají také stejné. Jsou dány aktuální situací a možnostmi subjektů, které by se mohly pokusit o poškození aktiv organizace. Jediné, co tedy z pohledu organizace můžeme měnit, je zmírnění zranitelností jednotlivých hrozeb pomocí nasazování adekvátních bezpečnostních opatření.

Následuje tabulka, ve které je srovnáno dosažení požadovaných bezpečnostních opatření dle vyhlášky č. 82/2018 Sb o Kybernetické bezpečnosti a normy ISO/IEC 27001:

Bezpečnostní požadavky:	**VoKB č.82/2018 Sb.**	**ISO/IEC 27001**
Systém řízení bezpečnosti informací	Ano	Ano
Řízení aktiv	Ano	Ano
Řízení rizik	Ano	Ano
Organizační bezpečnost	Ano	Ano
Bezpečnostní role	Částečně	Částečně
Řízení dodavatelů	Částečně	Částečně
Bezpečnost lidských zdrojů	Částečně	Částečně
Řízení provozu a komunikací	Ano	Ano
Řízení změn	Ano	Ano
Řízení přístupu	Ano	Ano
Akvizice, vývoj a údržba	Ano	Ano
Zvládání kybernetických bezpečnostních událostí a incidentů	Ano	Ano
Řízení kontinuity činností	Ano	Ano
Audit kybernetické bezpečnosti	Ano	Ano
Fyzická bezpečnost	Ano	Ano
Bezpečnost komunikačních sítí	Ano	Ano
Správa a ověřování identit	Ano	Ano
Řízení přístupových oprávnění	Ano	Ano
Ochrana před škodlivým kódem	Ano	Ano
Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	Ano	Ano
Detekce kybernetických bezpečnostních událostí	Ano	Ano
Sběr a vyhodnocování kybernetických bezpečnostních událostí	Ano	Ano
Aplikační bezpečnost	Ano	Ano
Kryptografické prostředky	Ano	Ano
Zajišťování úrovně dostupnosti informací	Ano	Ano
Průmyslové, řídicí a obdobné specifické systémy	Ano	Ano
Digitální služby	Nevyžaduje	Nevyžaduje
Bezpečnostní politika a bezpečnostní dokumentace	Částečně	Částečně
Služby elektronického obchodu	Nevyžaduje	Neřešeno
Výměny informací	Nevyžaduje	Neřešeno

Tabulka 12 - plnění bezpečnostních požadavků dle VoKB Sb.86/2018 a ISO/IEC 20001

ZÁVĚR

V rámci této diplomové práce byly prostudovány a zpracovány veřejně dostupné i placené bezpečnostní normy, které byly následně v rámci komparativní analýzy zhodnoceny. Na základě této analýzy zaujímá klíčovou roli série norem ČSN/ISO 27000, která klade nejstriktnější a nejobsáhlejší požadavky a doporučení na zajištění dostatečné úrovně bezpečnosti počítačových sítí a dalších aktiv organizace.

Byly prostudovány směrnice, zákony a legislativní ustanovení, z nichž bylo vzato to nejlepší a podle jejich doporučení byla zpracována dostatečná bezpečnostní opatření organizační infrastruktury. Dne 28.05.2018 vyšla v platnost vyhláška o kybernetické bezpečnosti č. 82/2018 Sb., která vychází ze Evropské směrnice NIS a která splňuje její požadavky. V rámci komparativní analýzy bylo zjištěno, že tato vyhlášky klade téměř totožné požadavky a doporučení jako série norem ČSN/ISO 27000. Vyhláška oproti této normě klade požadavky na zabezpečení ohledně poskytování digitálních služeb, naopak neřeší zabezpečení služeb elektronického obchodu a výměny informací.

V rámci návrhu zabezpečení a jeho realizace byla pečlivě prostudována důležitá aktiva organizace spadající pod zařazení KI (kritická infrastruktura) dle VoKB č. 82/2018 Sb., byla určena jejich důležitost z pohledu dostupnosti, důvěrnosti a integrity. Byly prostudovány možné bezpečnostní hrozby a způsoby kybernetických útoků, které by mohly aktiva organizace negativně ovlivnit. Tyto hrozby a rizika byly zhodnoceny a přiřazeny jednotlivým aktivům organizace dle jejich pravděpodobnosti výskytu.

Následně byla navržena a nasazena bezpečnostní opatření minimalizující rizika těchto hrozeb, například využití služeb Active-Directory, zabezpečení fyzického perimetru pomocí bezpečnostního systému C4, nasazení firewallů na hranici perimetru počítačové sítě organizace a jejich konfigurace, využití centralizovaného AAA protokolu RADIUS pro šifrování síťové komunikace a zabezpečení hesel, nasazení monitorovacích zařízení vnitropodnikové sítě pomocí systému Zabbix, stanovení zálohovacích postupů a kritérií, využití disků s technologií S.M.A.R.T. v datových uložištích a využití ochrany před škodlivým kódem dle aktuálních hodnocení nezávislých testů. Všechna tato opatření byla navržena za použití aktuálních best-practice řešení a pokud možno za použití platných RFC dokumentů.

Byla stanovena kritéria testování hrozeb, způsob výpočtu rizik, a to jak v rámci hodnocení samotných hrozeb, tak i ve vztahu na důležitost jednotlivých aktiv, aby bylo možné provést samotné testování. V rámci testování nasazených bezpečnostních opatření byl použit auditovací nástroj, vytvořený dle vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb.
Ten prokázal dostatečnost nasazených bezpečnostních opatření. Nasazená opatření splňují kritéria a organizace by měla být dostatečně zabezpečena. Některé detaily nemohly být uveřejněny z důvodu možného ohrožení zájmů organizace.
Dále byl v rámci testování kontrolován soulad se samotnou vyhláškou a bezpečnostní normou ISO/IEC 27001. Nasazená opatření splňují klíčové body v zajištění bezpečnosti, mimo body, které nespadají do rozsahu práce z hlediska jejího tématu. Tato diplomová práce je zaměřena především na technická opatření a ochranu počítačových sítí a klíčových systémů organizační infrastruktury, z toho důvodu byla témata týkající se řízení lidských zdrojů zmíněna pouze okrajově. Stejně tak právní prvky typu smluvních pokut při nedodržení plnění smluv třetích stran.

Seznam zdrojů

[1] *ISO/IEC 15408-1:2009: Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model*. Třetí vydání. Švýcarsko: ISO/IEC, 2009.

[2] *ISO/IEC 15408-2:2008: Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components*. Třetí vydání. Švýcarsko: ISO/IEC, 2008.

[3] *ISO/IEC 15408-3:2008: Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components*. Třetí vydání. Švýcarsko: ISO/IEC, 2008.

[4] *ISO/IEC 27000:2018: Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary*. Páté vydání. Švýcarsko: ISO/IEC, 2018.

[5] *ISO/IEC 27001:2013: Information technology -- Security techniques -- Information security management systems -- Requirements*. Druhé vydání. Švýcarsko: ISO/IEC, 2013.

[6] *ISO/IEC 27002:2013: Information technology -- Security techniques -- Code of practice for information security controls*. Druhé vydání. Švýcarsko: ISO/IEC, 2013.

[7] IETF | RFCs. IETF | Internet Engineering Task Force [online]. Dostupné z: https://www.ietf.org/standards/rfcs/ .

[8] IETF | Internet-Drafts. IETF | Internet Engineering Task Force [online]. Dostupné z: https://www.ietf.org/standards/ids/ .

[9] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, DOI 10.17487/RFC2827, May 2000, Dostupné z: https://www.rfc-editor.org/info/rfc2827.

[10] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, DOI 10.17487/RFC2026, October 1996, Dostupné z: https://www.rfc-editor.org/info/rfc2026.

[11] Housley, R. and B. Aboba, "Guidance for Authentication, Authorization, and Accounting (AAA) Key Management", BCP 132, RFC 4962, DOI 10.17487/RFC4962, July 2007, Dostupné z: https://www.rfc-editor.org/info/rfc4962.

[12] Resnick, P., "Retirement of the "Internet Official Protocol Standards" Summary Document", BCP 9, RFC 7100, DOI 10.17487/RFC7100, December 2013, Dostupné z: https://www.rfc-editor.org/info/rfc7100.

[13] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii In: Úřední věstník, L 194/1, 19.7.2016, s. 1—30. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN .

[14] ČESKO. Část 2 vyhlášky 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). In: ČES Zákony pro lidi.cz [online]. © AION CS 2010-2018 [cit. 7. 8. 2018]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82#cast2.

[15] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, DOI 10.17487/RFC2865, June 2000, Dostupné z: https://www.rfc-editor.org/info/rfc2865.

[16] Sermersheim, J., Ed., "Lightweight Directory Access Protocol (LDAP): The Protocol", RFC 4511, DOI 10.17487/RFC4511, June 2006, Dostupné z: https://www.rfc-editor.org/info/rfc4511.

[17] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, DOI 10.17487/RFC2401, November 1998, Dostupné z: https://www.rfc-editor.org/info/rfc2401.

[18] Thayer, R., Doraswamy, N., and R. Glenn, "IP Security Document Roadmap", RFC 2411, DOI 10.17487/RFC2411, November 1998, Dostupné z: https://www.rfc-editor.org/info/rfc2411.

[19] ORIYANO, Sean-Philip. CEHv8: Certified Ethical Hacker version 8. Hoboken: Sybex, a Wiley brand, [2014]. ISBN 111864767X.

[20] HSU, D. Advances in cyber security: technology, operations, and experiences. First edition. New York: Fordham University Press, 2013. ISBN 9780823244577.

[21] ŠENOVSKÝ, Pavel. Počítače a ochrana dat - Návody do cvičení [online]. VŠB-TU Ostrava, Ostrava 2006, 35 str., dostupné z: https://fbiweb.vsb.cz/~sen76/data/uploads/skripta/pocitacove-site-a-ochrana-dat-navody-do-cviceni.pdf [cit. 30.7. 2018].

[22] Gamanet a. s.,C4 Portal [online]. Copyright © 2009 [cit. 14.11.2018]. Dostupné z: https://www.c4portal.com/Product/WhatIsC4.aspx?area=open-architecture

[23] Zabbix :: The Enterprise-Class Open Source Network Monitoring Solution [online]. Copyright © 2001 [cit. 14.11.2018]. Dostupné z: https://www.zabbix.com/features.

[24] Woodyatt, J., Ed., "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service", RFC 6092, DOI 10.17487/RFC6092, January 2011, Dostupné z: https://www.rfc-editor.org/info/rfc6092.

[25] Davies, E. and J. Mohacsi, "Recommendations for Filtering ICMPv6 Messages in Firewalls", RFC 4890, DOI 10.17487/RFC4890, May 2007, Dostupné z: https://www.rfc-editor.org/info/rfc4890.

[26] Funk, P. and S. Blake-Wilson, "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)", RFC 5281, DOI 10.17487/RFC5281, August 2008, dostupné z: https://www.rfc-editor.org/info/rfc5281.

[27] Wood, M. and M. Erlinger, "Intrusion Detection Message Exchange Requirements", RFC 4766, DOI 10.17487/RFC4766, March 2007, Dostupné z: https://www.rfc-editor.org/info/rfc4766.

[28] The Best Malware Removal and Protection Software of 2018 | PCMag.com. PCMag.com - Technology Product Reviews, News, Prices & Tips

[online]. Copyright © Bram Stein. License [cit. 09.08.2018]. Dostupné z: https://www.pcmag.com/roundup/354226/the-best-malware-removal-and-protection-tools.
[29] Password Manager for Enterprise Password Management, Secure Password Vault Software. ManageEngine - IT Operations and Service Management Software [online]. Dostupné z: https://www.manageengine.com/products/passwordmanagerpro/
[30] JAKUB, Janša. Audit kybernetické bezpečnosti. Praha, 2018. Diplomová práce. Vysoká škola ekonomická v Praze. Vedoucí práce Svatá Vlasta.
[31] Audit kybernetické bezpečnosti . workflow [online]. [cit. 09.08.2018]. Dostupné z: http://kubikuv.cloud/audit/
[32] SVATÁ, Vlasta. Audit informačního systému. Praha: Professional Publishing, 2011. ISBN 978-80-7431-034-8.

Seznam Tabulek

Seznam Obrázků

Seznam příloh

Příloha 1

Ukázka Security Target pro Fox Data Diode

Tato příloha nemohla být do práce vložena napřímo, protože podléhá autorským právům, a z toho důvodu jsou u tohoto pdf dokumentu stanovena ochranná opatření, která zabraňují jeho úpravy a vkládání do jiných dokumentů. Stále je ale dostupný pomocí hypertextového odkazu z webové stránky Ukázka Security Target pro Fox Data Diode.https://www.commoncriteriaportal.org/files/epfiles/%5BST_Public%5D_Fox_DataDiode_Security_Target.pdf

Příloha 2

Tabulka porovnání požadavků na zabezpečení VoKB Sb.86/2018 a ISO/IEC 20001

Bezpečnostní požadavky:	**VoKB č.82/2018 Sb.**	**ISO/IEC 27001**
Systém řízení bezpečnosti informací	Ano	Ano
Řízení aktiv	Ano	Ano
Řízení rizik	Ano	Ano
Organizační bezpečnost	Ano	Ano
Bezpečnostní role	Ano	Ano
Řízení dodavatelů	Ano	Ano
Bezpečnost lidských zdrojů	Ano	Ano
Řízení provozu a komunikací	Ano	Ano
Řízení změn	Ano	Ano
Řízení přístupu	Ano	Ano
Akvizice, vývoj a údržba	Ano	Ano
Zvládání kybernetických bezpečnostních událostí a incidentů	Ano	Ano
Řízení kontinuity činností	Ano	Ano
Audit kybernetické bezpečnosti	Ano	Ano
Fyzická bezpečnost	Ano	Ano
Bezpečnost komunikačních sítí	Ano	Ano
Správa a ověřování identit	Ano	Ano
Řízení přístupových oprávnění	Ano	Ano
Ochrana před škodlivým kódem	Ano	Ano
Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	Ano	Ano
Detekce kybernetických bezpečnostních událostí	Ano	Ano
Sběr a vyhodnocování kybernetických bezpečnostních událostí	Ano	Ano
Aplikační bezpečnost	Ano	Ano
Kryptografické prostředky	Ano	Ano
Zajišťování úrovně dostupnosti informací	Ano	Ano
Průmyslové, řídicí a obdobné specifické systémy	Ano	Ano
Digitální služby	Ano	Ne
Bezpečnostní politika a bezpečnostní dokumentace	Ano	Ano
Služby elektronického obchodu	Ne	Ano
Výměny informací	Ne	Ano

Univerzita Hradec Králové
Fakulta informatiky a managementu
Akademický rok: 2015/2016

Studijní program: Aplikovaná informatika
Forma: Prezenční
Obor/komb.: Aplikovaná informatika (ai2-p)

Podklad pro zadání DIPLOMOVÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Bc. Hübner Adam	Na Studánkách 404, Jaroměř - Pražské Předměstí	I1500860

TÉMA ČESKY:

Testování zabezpečení počítačové sítě s využitím standardů pro bezpečnost

TÉMA ANGLICKY:

Computer network security testing and best practise

VEDOUCÍ PRÁCE:

Mgr. Josef Horálek, Ph.D. - KIT

ZÁSADY PRO VYPRACOVÁNÍ:

Cílem práce je podrobně popsat normy, standardy a best parctice řešení pro zabezpečení počítačové sítě. Tyto metodiky porovnat a na jejich základě provést praktickou komparativní analýzy zavedení bezpečnosti a jejích praktického testování.

V teoretické části autor představí zásadní normy, standardy a metodiky pro zavedení bezpečnostních opatření na úrovni zabezpečení dat a síťové komunikace. Autor provede komparativní analýzu relevantních řešení a matodik.

V praktické části autor realizuje bezpečností opratření na ochranu dat a komunikace. Tato řešeí otestuje na základě vybraých best practice řešení.

SEZNAM DOPORUČENÉ LITERATURY:

ORIYANO, Sean-Philip. CEHv8: Certified Ethical Hacker version 8. Hoboken: Sybex, a Wiley brand, 2014. ISBN 111864767X.

HSU, D. Advances in cyber security: technology, operations, and experiences. First edition. New York: Fordham University Press, 2013. ISBN 9780823244577.

Podpis studenta: ..... **Datum:** .....

Podpis vedoucího práce: ..... **Datum:** .....