VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

DIPLOMOVÁ PRÁCE

Brno, 2023 Bc. Jaromír Štefánik

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

NÁSTROJ PRO PODPORU AUDITU KYBERNETICKÉ BEZPEČNOSTI

CYBERSECURITY AUDIT TOOL

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE

AUTHOR

Bc. Jaromír Štefánik

VEDOUCÍ PRÁCE

SUPERVISOR

JUDr. Mgr. Jakub Harašta, Ph.D.

BRNO 2023

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Bc. Jaromír Štefánik ***ID:*** 203436

Ročník: 2 ***Akademický rok:*** 2022/23

NÁZEV TÉMATU:

Nástroj pro podporu auditu kybernetické bezpečnosti

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je (i) identifikovat požadavky, které musí být splněny podle zákona č. 181/2014 Sb. a (ii) vytvořit nástroj, který umožní řízený a strukturovaný průchod těmito požadavky pro potřeby auditu. Nástroj umožní zástupci auditovaného subjektu odpovídat na otázky a nahrávat dokumenty, kterými prokáže splnění zákonných povinností. Na druhé straně nástroj umožní auditorovi splnění požadavků komentovat a z vložených dat vygenerovat předběžnou zprávu pro další fáze auditu. Nástroj musí umožnit editaci průchodu (auditních otázek a požadavků) v návaznosti na legislativní změny. Výstupem semestrálního projektu bude softwarová implementace nástroje pro podporu auditu v rozpracované formě se základní funkcionalitou. Výstupem diplomové práce bude kompletní nástroj včetně dokumentace.

DOPORUČENÁ LITERATURA:

dle pokynů vedoucího práce

Termín zadání: 6.2.2023 ***Termín odevzdání:*** 19.5.2023

Vedoucí práce: JUDr. Mgr. Jakub Harašta, Ph.D.

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

ABSTRAKT

Diplomová práca sa zaoberá problematikou auditov v oblasti kybernetickej bezpečnosti. V teoretickej časti sú priblížené náležitosti auditu kybernetickej bezpečnosti podľa rady noriem ISO/IEC 27000, požiadavky definované pre zákonom regulované subjekty podľa zákona č. 181/2014 Sb., bezpečnostné opatrenia vyplývajúce z vyhlášky č. 82/2018 Sb. a možné zmeny národnej legislatívy v oblasti kybernetickej bezpečnosti vyplývajúce zo smernice NIS2. V praktickej časti diplomovej práce bol zostavený nástroj (programovací jazyk Python), ktorý napomáha povinným subjektom štrukturovaných prechodom pri kontrole plnenia požiadaviek stanovených legislatívou a zároveň generuje súhrnnú správu plnenia požiadaviek do jedného celistvého dokumentu spolu s priloženou relevantnou dokumentáciou.

KĽÚČOVÉ SLOVÁ

audit, kybernetická bezpečnosť, ISO/IEC 27000, NIS, NIS2, pomôcka pre audity, Python, Vyhláška o kybernetickej bezpečnosti, Zákon o kybernetickej bezpečnosti

ABSTRACT

Master thesis deals with the issue of audits in the field of cybersecurity. The theoretical part presents the requirements of a cybersecurity audit according to the ISO/IEC 27000 series of standards, the requirements defined for legally regulated entities according to Act No. 181/2014 Coll., the security measures resulting from Decree No. 82/2018 Coll. and possible changes to national legislation in the field of cybersecurity resulting from the NIS2 Directive. In the practical part of the master thesis, a tool (Python programming language) has been compiled to assist the obliged entities structured by transitions in checking the compliance with the requirements set by the legislation and at the same time generating a summary report of the compliance with the requirements into one complete document together with the attached relevant documentation.

KEYWORDS

audit, audit aid, cybersecurity, Cybersecurity Act, Cybersecurity Decree, ISO/IEC 27000, NIS, NIS2, Python

Vysadené pomocou balíčku `thesis` verzie 4.07; `http://latex.feec.vutbr.cz`

ŠTEFÁNIK, Jaromír. *Nástroj pro podporu auditu kybernetické bezpečnosti*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2023, 88 s. Diplomová práca. Vedúci práce: JUDr. Mgr. Jakub Harašta, Ph.D.

Vyhlásenie autora o pôvodnosti diela

Meno a priezvisko autora:	Bc. Jaromír Štefánik
VUT ID autora:	203436
Typ práce:	Diplomová práca
Akademický rok:	2022/23
Téma závěrečnej práce:	Nástroj pro podporu auditu kybernetické bezpečnosti

Vyhlasujem, že svoju záverečnú prácu som vypracoval samostatne pod vedením vedúcej/cého záverečnej práce, s využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej záverečnej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto záverečnej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákonníka Českej republiky č. 40/2009 Sb.

Brno ....

podpis autora*

*Autor podpisuje iba v tlačenej verzii.

POĎAKOVANIE

Týmto by som sa chcel srdečne poďakovať vedúcemu mojej diplomovej práce pánovi JUDr. Mgr. Jakubovi Haraštovi, Ph.D. za odborné vedenie, konzultácie, trpezlivosť a podnetné návrhy k práci.

Obsah

Zoznam obrázkov

Úvod

Veda, počítače, informatika, kybernetická bezpečnosť. So spomenutými slovami sa každý stretáva na dennej báze, či už pri otvorení novín alebo spustenia televízie. Za posledných pár desiatok rokov sa stali neoddeliteľnou súčasťou života počítače a informatizácia prakticky každého pracovného odvetvia. Podobne bez mobilných telefónov alebo smartfónov, bez okamžitého priameho spojenia s rodinou, priateľmi naprieč celým svetom, si nevieme dnešný svet predstaviť.

Každá minca má dve strany, obdobne aj výdobytky informačnej techniky. Pomáhajú nám každý deň, či už pri jednoduchých činnostiach, ale aj pri vedeckých výpočtoch. Nie všetci užívatelia počítača myslia na to, do akej miery sú vystavení riziku straty svojich vzácnych dát, informácií.

Presne z tohoto dôvodu vznikol odbor Informačná bezpečnosť nielen na Vysokom učení technickom v Brne na fakulte elektrotechniky a komunikačných technológií (akademický rok 2015/2016). V nie ďalekej minulosti (rok 2014) bol v Českej republike vydaný Zákon o kybernetické bezpečnosti (Zákon č. 181/2014 Sb.).

Na začiatku tejto diplomovej práce sú priblížené teoretické východiská a podklady pre kybernetickú bezpečnosť a jej audity.

Prvou vysvetlenou tematikou je práve kybernetická bezpečnosť, ktorej hlavné princípy sú vysvetlené pre netechnickú verejnosť.

Ďalšou neoddeliteľnou časťou sú práve audity v oblasti kybernetickej bezpečnosti. Spomenuté sú audity, kontroly podľa vyhlášky o kybernetickej bezpečnosti a audity vychádzajúce z rodiny noriem ISO 27000 (auditná a kontrolná činnosť Národního úřadu pro kybernetickou a informační bezpečnost sa opiera do veľkej miery práve o audity podľa ISO 27007). V podkapitole audity podľa ISO noriem sú vymenované techniky, ktoré sprevádzajú auditnú činnosť spred začiatku auditu až po úkony po vykonanom audite. Všetky tieto činnosti sú rozdelené do častí: zahájenie auditu, príprava činností, vykonávanie činností auditu, správa z auditu a ukončenie auditu.

Tretia kapitola sa týka právnej úpravy kybernetickej bezpečnosti (skr. KB) v Českej republike. Sú v nej spomenuté hlavné aj vedľajšie právne pramene, ktoré súvisia práve s právnou úpravou KB v Českej republike. Základným stavebným kameňom pre spomenutú právnu oblasť je zákon o kybernetickej bezpečnosti, ktorý určuje práva a povinnosti pre dôležité orgány, vymedzuje povinné orgány a osoby, ktorým v zápätí tiež určuje čo musia plniť a na čo majú právo. Po vymenovaní povinných subjektov nasleduje ich podrobný rozbor, konkrétnejšie ich povinnosti podľa zákona o kybernetickej bezpečnosti, bezpečnostné opatrenia vyplývajúce z vyhlášky o kybernetickej bezpečnosti. Ďalej sa pojednáva o možných legislatívnych zmenách v oblasti kybernetickej bezpečnosti reagujúcich na požiadavky smernice NIS2.

Štvrtá kapitola predstavuje čitateľom možné legislatívne zmeny pre oblasť kybernetickej bezpečnosti súvisiace s vydanou smernicou NIS2. V rámci tejto kapitoly sú priblížené jedny z najzaujímavejších úprav, ktoré prináša smernica NIS2. Ďalej sú priblížené zmeny v navrhovanom znení zákona o kybernetickej bezpečnosti a súvisiacich vyhlášok po transpozícii NIS2 do právnej úpravy kybernetickej bezpečnosti Českej republiky.

Piata kapitola tejto diplomovej práce je praktickou časťou, v ktorej bol navrhnutý nástroj pre podporu auditu kybernetickej bezpečnosti. V rámci tejto kapitoly je popísané členenie programu na jednotlivé časti, vysvetlená funkcionalita programu s priloženým vývojovým diagramom pre lepšie pochopenie, možnosti modifikácie nastavení a štruktúra výsledného súhrnného dokumentu s vyplnenými legislatívnymi požiadavkami.

1 Kybernetická bezpečnosť

Ako bolo uvedené v úvodných slovách diplomovej práce, s pojmom kybernetická bezpečnosť sa stretávajú ľudia súčasnej doby prakticky na dennom poriadku. Tento fakt utvrdili okolnosti za posledné roky, ako napríklad pandémia COVID-19 alebo vyhrotená vojnová situácia na neďalekej Ukrajine. Nielen v dôsledku spomenutých nepriaznivých okolností sa navýšili počty kybernetických incidentov (nahlásené počty kybernetických incidentov Národnímu úřadu pro kybernetickou a informační bezpečnost) z počtu 217 (rok 2019) na číslo 468. Od začiatku situácie na Ukrajine boli rovnako avizované útoky mieriace na okolité členské štáty Európskej únie, Česká republika nebola výnimkou. [1] [2]

Kybernetická bezpečnosť (angl. Cyber security) často zamieňaná s príbuzným odborom informačná bezpečnosť je odvetvím informačnej bezpečnosti v kybernetickom priestore. Pričom **kybernetická bezpečnosť** mieri na ochranu počítačových systémov pred neoprávneným prístupom, odcudzením dát, kompromitáciou systému a pred mnohými inými hrozbami. Inými slovami sa jedná o ochranu dát v kybernetickom priestore pred hrozbami zabezpečením systémových zraniteľností. Stále sa však jedná o ochranu aktív, aby bola zachovaná bezpečnosť informácií, ktoré majú pôvod v digitálnej podobe.[3] Podľa slovníka kybernetickej bezpečnosti je definovaná ako "Súhrn právnych, organizačných, technických a vzdelávacích prostriedkov smerujúcich k zaisteniu ochrany kybernetického priestoru". [4]

Snahou **informačnej bezpečnosti** je ochrana aktív v akejkoľvek podobe, nielen digitálnej ale aj v podobe fyzickej (napríklad tlačené dokumenty v archívoch). V minulosti existovali tiež citlivé informácie, ktoré bolo nutné ochrániť pred zneužitím, modifikáciou, alebo odcudzením. Mohli byť zabezpečené na fyzickej úrovni, teda fyzickou bezpečnosťou priestoru s uchovávanými informáciami. [3]

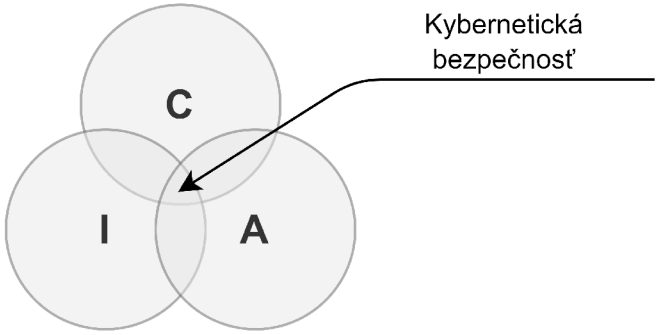
1.1 Triáda CIA

Triáda CIA je jednou z najznámejších a najčastejšie aplikovaných princípov pre dosiahnutie informačnej, ale aj kybernetickej bezpečnosti. Jej cieľom je zaistiť bezpečnosť informácií počas ich celého životného cyklu (vytvorenie, prenos, spracovávanie, úschova). [5]

Skratka CIA v sebe ukrýva tri posudzované oblasti pre docielenie bezpečnosti informácií:

- **C (Confidentiality)** - Dôvernosť,
- **I (Integrity)** - Celistvosť,
- **A (Availability)** - Dostupnosť.

Pre lepšiu predstavu je možné vymedzenie kybernetickej bezpečnosti pomocou prieniku všetkých troch princípov triády, ako je vyobrazené na obr. 1.1 [5]



Obr. 1.1: Kybernetická bezpečnosť a triáda CIA

1.1.1 Dôvernosť

Táto oblasť predstavuje zabezpečenie prístupu k dátam, informáciám či systému, ku ktorému pristupujú určené osoby s autorizovaným prístupom. Teda je neprístupná pre entity (osoby, procesy v informačnom systéme) s nepreukázateľným oprávnením prístupu k aktívam.

Pre dosiahnutie dôvernosti sú využívané rôzne metódy, ako napríklad riadenie prístupu. [5]

1.1.2 Celistvosť

Pod pojmom celistvosť je myslená vlastnosť presnosti, t.j. istota, že aktíva neboli pozmenené a sú v pôvodnej podobe. Predstavuje zabezpečenie znemožnením editácie súborov, informácií, dát entitou s neoprávneným prístupom. [5]

1.1.3 Dostupnosť

Poslednou oblasťou z triády CIA je dostupnosť. Význam tejto oblasti spočíva v garancii možnosti prístupu k aktívam pri nutnosti potreby. Príklad pre lepšiu predstavu reflektuje systém so zaistenou dôvernosťou a celistvosťou, ktorý je nepoužiteľným pokiaľ nebude možné k systému pristupovať podľa potreby používateľov. [5]

2 Audit kybernetickej bezpečnosti

V predchádzajúcej kapitole bol vysvetlený pojem kybernetickej bezpečnosti zo všeobecného hľadiska, ale v realite musia povinné subjekty plniť svoje záväzky nielen vo všeobecnej rovine.

Ďalšou časťou implementácie kybernetickej bezpečnosti je právny pohľad na danú tematiku. Vo výkladovom slovníku kybernetickej bezpečnosti je slovné spojenie vysvetľované ako súhrn právnych, organizačných, technických a vzdelávacích prostriedkov využitých pre docielenie ochrany kybernetického priestoru. [4] V nasledujúcich kapitolách tejto práce budú priblížené vymenované prostriedky k zaisteniu kybernetickej bezpečnosti.

Audit kybernetickej bezpečnosti predstavuje systematický a nezávislý proces vykonávaný poverenou osobou (auditorom), pri ktorom sú zaistené dôkazné materiály. Výsledkom je výstupný dokument s objektívnym ohodnotením dôkazov k určeniu rozsahu plnenia auditovaných kritérií.

Audity môžu byť rôzneho typu:

- **audit prvou stranou** - spravidla sa jedná o interný audit,
- **audit druhou stranou** - audit externého poskytovateľa alebo audit inej externej zainteresovanej strany,
- **audit treťou stranou** - typicky vykonávaný nezávislou organizáciou poskytujúcou auditorské služby (napríklad certifikačný audit pre certifikáciu zhody s niektorou z noriem alebo audit podľa zákonov vykonávaný štátnymi orgánmi).

[6] [7]

Medzi známe kritériá pri implementácii a auditoch kybernetickej bezpečnosti patrí česká norma ČSN EN ISO/IEC 27000, alebo pri zákonom vymedzených subjektoch vyhláška č. 82/2018 Sb., Vyhláška o kybernetické bezpečnosti (skr. VKB). Podľa názvu normu a vyhlášku nemožno spájať do jedného celku, avšak sú si podobnejšie, ako sa zdá na prvý pohľad. Súvislosť medzi radou noriem ISO/IEC 27000 a vyhláškou o kybernetické bezpečnosti je evidentný. Pri vytváraní VKB tvorili normy ISO/IEC 27000 základný stavebný kameň, od čoho sa autori inšpirovali. Na rozdiel od normy je Vyhláška o kybernetické bezpečnosti záväzná a aj prípadná certifikácia povinného subjektu podľa normy ISO/IEC 27000 nič nemení na tom, že musí subjekt spĺňať právne určené požiadavky. [8]

2.1 Rada noriem ISO/IEC 27000

V rade noriem ISO/IEC 27000 je definovaný systematický prehľad systémov riadenia bezpečnosti informácií (Information Security Management System - skr. **ISMS**). V dokumente ČSN ISO/IEC 27001 sú stanovené požiadavky pre správne zavedenie a

udržovanie ISMS v organizácii. V prílohách dokumentu sú formulované ciele aj jednotlivé opatrenia pre ich dosiahnutie, ako sú napríklad bezpečnosť ľudských zdrojov, riadenie aktív, riadenie prístupu, kryptografické prostriedky, fyzická bezpečnosť a iné. Táto norma vyčleňuje požiadavky v duchu Demingovho cyklu. [9] [10]

Demingov cyklus nie je exaktne spomenutý v norme ČSN ISO/IEC 27001, ale príbuznosť je značná, nakoľko špecifikuje požiadavky pre ustanovenie, implementovanie, udržovanie a stále zlepšovanie ISMS. Demingov iteračný cyklus, známy tiež pod názvom PDCA cyklus, sa skladá zo štyroch základných krokov. Vychádzajúc zo skratky PDCA sú kroky: naplánovanie (plan - **P**), vykonávanie (do - **D**), overovanie (check - **C**) a jednanie (act - **A**). Pre vysvetlenie krok plánovania slúži na stanovenie cieľov a navrhnutie plánov pre dosiahnutie cieľov. V časti vykonávanie sa uskutočňujú a premieňajú do praxe plánované činnosti. Pri overovaní sa kontrolujú výsledky a overuje splnenie dosiahnutých cieľov. Napokon v poslednom kroku jednania sa má organizácia poučiť z chýb pre vylepšenie činností a vyvarovať sa im v ďalšej iterácii PDCA cyklu. [9] [11]

Audit priamo v normách ISO/IEC 27000 je vysvetlený len z významového hľadiska ako systematický, nezávislý a dokumentovaný proces pre získanie dôkazov z auditu a ich objektívne hodnotenie pre určenie rozsahu, v ktorom sú auditované kritériá splnené. Norma ISO/IEC 27000 odkazuje na smernicu pre auditovanie systémov managementu ČSN EN ISO 19011. [9]

2.1.1 Audit podľa noriem ISO

Ako bolo vyššie spomenuté, audit kybernetickej bezpečnosti je možné uskutočňovať podľa noriem rodiny ISO/IEC 27000, avšak tá odkazuje na smernicu pre auditovanie systémov managementu ČSN EN ISO 19011. Základnú terminológiu a princípy pre auditovanie systémov je možné nájsť v rámci normy ČSN EN ISO 9000.

Popis vykonávania auditu je možné rozdeliť do niekoľkých častí ako je zahájenie auditu, príprava činností, vykonávanie činností, správa z auditu, ukončenie auditu a nasledujúci audit. [6] [7]

Kategórie opatrení a ich ciele podľa ISO/IEC 27001 je možné nájsť aj v prílohe A tejto práce.

Zahájenie auditu

V časti **zahájenie auditu** je nutné nadviazať prvotný kontakt s auditovanou organizáciou a predbežne sa dohodnúť na priebehu auditu. Vedúci tímu auditorov má na starosti kontaktovanie organizácie za účelom potvrdenia kompetencie uskutočniť audit, predstaviť ciele auditu, teda za akým účelom bude vykonávaný, čo bude predmetom auditu, vybrané metódy auditu, zloženie tímu auditorov. Nemenej

podstatné je vyžiadanie si a sprístupnenie relevantných dokumentácií, týkajúcich sa auditovanej organizácie. [6] [7]

Predmetom auditu je vymedzené, čoho sa bude týkať nastávajúci audit. Po vecnej stránke má obsahovať popis fyzických ale aj virtuálnych miest (napr. online prostredie, v ktorom organizácia vykonáva svoju prácu), funkcie, organizačné jednotky, alebo aj činnosti a procesy. [6] [7]

Metódy auditovania sa členia na základe miesta, kde sa nachádza auditor a spôsobu zapojenia auditora a auditovaného. Prvá metóda spočíva v realizácii auditu **na mieste s interakciou** medzi auditorom a auditovaným. Spravidla sa jedná v priestoroch auditovanej organizácie. Pod interakciou je myslené uskutočňovanie rozhovorov medzi jedincami, kladenie otázok a vyplňovanie checklistu, prípadne dotazníka podľa zvoleného vzorkovania. Ďalej pri tejto metóde auditu je možné preskúmanie dokumentácie za účasti auditovaného. Pri **metóde na mieste a bez interakcie** auditor preskúmava dokumentáciu, pozoruje vykonávanie činností, prehliadky na mieste a z pozorovania vypĺňa checklist. Ďalšia metóda môže byť nie priamo na mieste, teda **vzdialene s interakciou** medzi auditorom a auditovaným. To znamená, že audit sa uskutočňuje kdekoľvek mimo priestorov auditovanej organizácie prostredníctvom interaktívnych komunikačných techník. V rámci tejto metódy sa vykonávajú rozhovory, pozorovanie úkonov pri vykonávaní práce so sprievodcom na vzdialenej lokalite, vypĺňanie checklistu prípadne dotazníkov a preskúmava sa dokumentácia spolu s auditovanou osobou. Poslednou metódou výkonu auditu je **vzdialene bez interakcie**. Auditor preskúmava dokumentáciu a pozoruje vykonávané práce, za pomoci dohľadových systémov (napr. kamerové systémy). [6] [7]

Pred samotným zahájením auditu osoba riadiaca program auditov určí vedúcu osobu za tím auditorov. **Vedúci tímu auditorov** je zodpovedný za uskutočnenie daného auditu. Ďalej je vytýčené zloženie tímu auditorov osobou riadiacou program auditov, pričom musí byť zvážený predmet auditu a podľa toho sú vybraní auditori, prípadne experti zo špecifických oblastí (napr. pokiaľ bude audit preverovať plnenie povinností z oblasti kybernetickej bezpečnosti, je vhodné zvážiť vybranie technického špecialistu na kybernetickú alebo informačnú bezpečnosť). Tak isto do tímu môže byť vybraný aj auditor vo výcviku pod vedením auditorov. V prípade menšieho rozsahu auditu, alebo menšej organizácie môže audit vykonávať len jeden auditor, ktorý, avšak má zodpovednosť aj za vedúceho tímu auditorov. [6] [7]

Príprava činností

Akonáhle auditovaná organizácia sprístupní relevantné dokumentácie obsahujúce informácie o systéme riadenia bezpečnosti informácií, tak sú tieto dokumenty zhromaždené a preskúmané pre pochopenie procesov v organizácii. Medzi poskytnutými

dokumentami by mali byť zahrnuté aj dokumenty a záznamy o systéme riadenia bezpečnosti informácií, ale aj správy z predošlých auditov. [6] [7]

Vedúci tímu auditorov navrhuje **plán auditu**, pričom je potrebné prispôsobiť rozsah a obsah. Ten sa môže líšiť podľa toho, či sa jedná o prvotný alebo následný audit. Plán auditu by mal zahŕňať ciele auditu, predmet auditu, konkretizovanie auditovanej organizácie vrátane ich funkcií či auditovaných procesov, kritériá, podľa ktorých bude audit vykonávaný, metódy auditu (vrátane vzorkovania). Ďalšou nie menej dôležitou súčasťou plánu auditu je určenie miesta, predpokladané intervaly jednotlivých činností auditu. Vytvorený návrh plánu auditu je následne prezentovaný auditovanému. Prípadné otázky alebo námietky sú zodpovedané, vyriešené vedúcim tímu auditorov. [6] [7]

Medzi povinnosti vedúceho tímu auditorov pri prípravných činnostiach patrí aj pridelenie práce pre tím auditorov, respektíve pridelí jednotlivým auditorom zodpovednosť za auditovanie konkrétnych činností, procesov alebo funkcií auditovanej organizácie. Pri prideľovaní práce auditorom musia byť brané na zreteľ kompetencie jednotlivcov. Po zvážení vedúceho tímu auditorov je možné upraviť, prerozdeliť pracovné úlohy aj počas auditu. [6] [7]

Jednotliví auditori si po pridelení pracovných úloh majú zhromaždiť a preskúmať relevantné zdroje informácií týkajúce sa ich úloh. Ďalej úlohou auditorov pred samotným uskutočnením auditu je príprava relevantných podkladov pre výkon auditu, spravidla sa jedná o vytvorenie zoznamu kontrolných otázok, ktoré budú kladené auditovanému. [6] [7]

Vykonávanie činností auditu

Po spomenutých prípravných činnostiach na audit prechádzame na praktický výkon auditnej činnosti, ktorý začína pri úvodnom jednaní. **Úvodné jednanie** spočíva z predstavenia tímu auditorov, finálneho odsúhlasenia plánu auditu tak ako zo strany auditovaného subjektu, tak aj od tímu auditorov. Ďalšou úlohou vedúceho tímu auditorov je viesť úvodné jednanie, ktoré je vhodné vykonávať za účasti managementu (vrcholové vedenie) auditovanej organizácie a zodpovedných osôb za auditované procesy, či funkcie. Za účasti spomenutých entít je zhrnutý plán priebehu auditu, metódy auditu, spôsob oznámení o zisteniach z vykonávaného auditu (súčasne s klasifikačnými kritériami zistení), spôsob riešenia možných zistení počas auditu, či podmienky, za akých je možné audit predčasne ukončiť. [6] [7]

Počas trvania auditu je neoddeliteľnou súčasťou výkonu tejto práce stretávanie sa auditorov pre výmenu zistených informácií a to najmä z dôvodu posúdenia nasledujúceho postupu auditu. V prípade, že dôjde k zisteniam, ktoré môžu znamenať

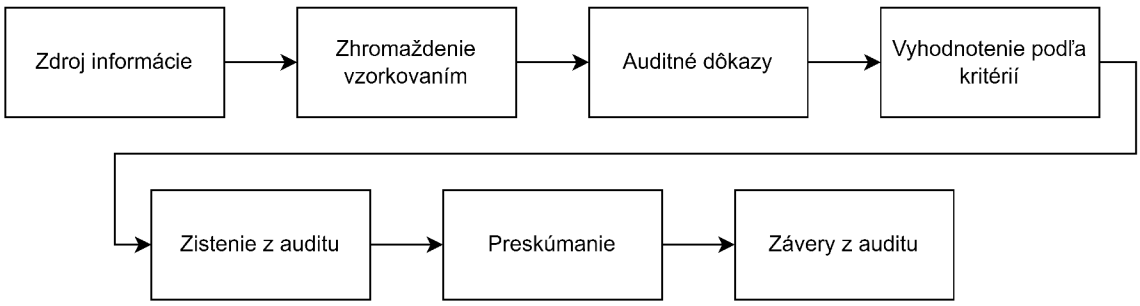
významné riziká, tak je táto skutočnosť vyrozumená auditovanej organizácii vedúcim tímu auditorov. [6] [7]

Pri výkone činnosti auditu sú **zhromaždené** relevantné **informácie** (vhodným vzorkovaním) z hľadiska spomínaných aspektov konkrétneho auditu. Tieto zistené informácie je potrebné vyhodnodiť a overiť ich pravdivosť. **Overenie informácií** spočíva v zvážení, či zistené informácie vypovedajú v dostatočnej miere o plnení požiadaviek auditovanej oblasti. Úvahy pri overovaní informácií majú zahŕňať kontrolu informácií z hľadiska úplnosti, správnosti (v súvislosti s inými zdrojmi ako napr. normy, predpisy), konzistencii (napr. v spojitosti so súvisiacimi dokumentami) a v poslednom rade či sú poskytnuté informácie aktuálne. Pokiaľ auditori obdržia informácie od osôb zodpovedných za inú oblasť, tak je nutné tieto informácie overiť z hľadiska integrity. Medzi metódy zhromažďovania informácií patria napríklad:

- **rozhovory** so zamestnancami a ďalšími relevantnými osobami k auditu,
- **preskúmavanie dokumentácií** vrátane počítačových logov a konfiguračných dát
- **pozorovanie procesov ISMS** a súvisiacich opatrení

[6] [7]

Postup procesov v rámci zhromažďovania a overovania informácií je graficky znázornený na 2.1



Obr. 2.1: Postup zhromažďovania a overovania informácií

Vzorkovanie zohráva dôležitú úlohu pri zhromažďovaní informácií najmä v kontexte veľkého množstva zaistených informácií, ktoré nie je možné preskúmať, alebo ich kompletné skúmanie je nákladovo neefektívne. Príkladom okrem veľkého množstva informácií môže byť geografická vzdialenosť častí auditovanej organizácie. Vzorkovanie teda predstavuje výber zo všetkých zaistených zdrojov dát, ktorý bude menší ako ich kompletné množstvo, pričom tento redukovaný výber vzorkovaním musí auditorovi poskytnúť ekvivalentné informácie pre naplnenie cieľov auditu. [6] [7]

Rozoznávame dva typy vzorkovania:

1. **Vzorkovanie založené na úsudku** je závislé na skúsenostiach a kompetencii auditorov.
2. **Štatistické vzorkovanie** využíva proces výberu vzorku na základe teórie pravdepodobnosti.

[6] [7]

Dôkazy zaistené počas auditnej činnosti, ktoré môžu viesť k zisteniu z auditu sú zaznamenávané. Pri vytváraní **zistení z auditu** môžu auditori zaznamenávať zhodu alebo nezhodu s kritériami auditu. Pri zaznamenávaní zhody má auditor popísať dôkazy z vykonávaného auditu reflektujúce daný fakt, ďalej odkázať na kritérium auditu, s ktorým je zhoda zistená. Ďalej môže auditor pri vytváraní zistení prieskumom zistiť nezhodu, kde je povinnosťou auditora poukázať na dôkazy z auditu, prípadné iné súvisiace zistenia z auditu a odkázať pritom na nesplnené auditné kritérium. [6] [7]

Po korektnom vykonaní auditu a s tým súvisiacimi procesmi sa vykonáva **záverečné jednanie**. Rovnako ako pri úvodnom, tak aj záverečné jednanie sa uskutočňuje za prítomnosti vrcholového vedenia, managementu, tímu auditorov, prípadne osoby zodpovedajúce za auditované funkcie. Záverečné jednanie vedie vedúci tímu auditorov, v rámci ktorého sú prezentované zistenia či záver auditu (prezentovanie nielen v čisto technickom ponímaní pre management), možné následky nedostatočného riešenia zistení z auditu, doporučenia pre možné zlepšenia a iné súvisiace činnosti po audite (napr. implementácia nápravných opatrení). [6] [7]

Správa z auditu

Po záverečnom jednaní je jednou z posledných úloh vedúceho tímu auditorov podanie správy z auditu. Správa z auditu má obsahovať úplný a presný záznam o vykonanom audite. Konkrétne by nemali byť opomenuté: ciele auditu, predmet auditu, údaje o klientovi, identifikácie tímu auditorov (prípadne iných účastníkov zo strany auditovaného), dôležité dátumy a miesta, kritériá auditu, zistenia z auditu a s nimi súvisiace dôkazy, záver auditu a fakt, že audit nemusí kompletne reflektovať aktuálny stav auditovanej organizácie v súvislosti s využitým vzorkovaním.

Vytvorená správa z auditu musí byť predložená v dohodnutej lehote auditovanej organizácii a osobe riadiacej program auditov. Pre distribúciu správy z auditu je vhodné, priam nevyhnutné, využiť spôsob, ktorý zaručí dôvernosť obsiahnutých informácií z dôvodu obsahu citlivých informácií pre auditovanú organizáciu. [6] [7]

Ukončenie auditu

Audit je ukončený po vykonaní všetkých naplánovaných činností, prípadne po odsúhlasení klienta auditu (napr. neočakávané situácie, ktoré zabraňujú korektnému dokončeniu výkonu auditnej činnosti). V súvislosti so zákonom alebo na základe dohody s klientom sú dokumentované informácie týkajúce sa auditu zlikvidované alebo uschované. Tím auditorov alebo osoba riadiaca program auditov je povinná dodržať mlčanlivosť ohľadom auditu v plnej miere. Výnimku môže predstavovať explicitný súhlas klienta, alebo prípad nutnosti vyplývajúcej z povahy zákona.

S výsledkom auditu môže byť oboznámený auditovaný klient s doporučeniami, príležitosťami k zlepšeniu alebo o potrebe nápravných opatrení. Po oboznámení má auditovaný prijať nápravné opatrenia v dohodnutom čase. Akonáhle auditovaný klient prijme stanovené nápravné opatrenia, mal by o tejto skutočnosti informovať osobu riadiacu program auditov, alebo tím auditorov. Následne sú nápravné opatrenia šetrené tímom auditorov s podaním správy osobe riadiacej program auditov a management auditovaného. Treba podotknúť, že toto overenie správnosti nápravných opatrení môže byť súčasťou nasledujúceho auditu. [6] [7]

3 Právna úprava kybernetickej bezpečnosti v Českej republike de lege lata

Kľúčovým prameňom pre právnu úpravu kybernetickej bezpečnosti v Českej republike (ČR) je zákon č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (skr. ZKB), ktorý nadobudol účinnosť ku dňu 1.1.2015. ZKB upravuje práva a povinnosti osôb a právomoci orgánov verejnej moci v oblasti kybernetickej bezpečnosti, zároveň zavádza príslušné predpisy Európskej únie (Smernica Európskeho parlamentu a Rady (EU) 2016/1148, známa tiež ako NIS). [12]

Dôležité je podotknúť, že ZKB sa nevzťahuje na informačné a komunikačné systémy pracujúce s utajovanými informáciami (definícia pojmu v znení zákona č. 412/2005 Sb., zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti). [12]

Nielen vyššie spomenuté právne pramene upravujú kybernetickú bezpečnosť v rámci Českej republiky. S vyššie uvedenými s právnymi úpravami sú úzko späté aj:

- Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat,
- Nariadenie vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury,
- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích,
- Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby,
- Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci,
- Vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu. [13]

3.1 Zákon o kybernetické bezpečnosti

Cieľom zákona je bezpochyby zvýšenie bezpečnosti v oblasti kybernetického priestoru, pričom mieri v nemalej časti na úpravu práv a povinností kritickej informačnej infraštruktúry, významným informačným systémom, základným službám, správcom zákonom vytýčených systémov, ale aj v neposlednom rade ústrednému správnemu úradu pre oblasť kybernetickej bezpečnosti - Národní úřad pro kybernetickou a informační bezpečnost (skr. NÚKIB). [12] [13]

Ustanovenie ZKB v § 3 vymedzuje rozsah zákona pre osem povinných subjektov, konkrétne sa jedná o:

- poskytovateľov služby elektronických komunikácií a subjekt zaisťujúci sieť elektronických komunikácií,
- orgány alebo osoby zaisťujúce významnú sieť,
- správcov a prevádzkovateľov informačného systému kritickej informačnej infraštruktúry,
- správcov a prevádzkovateľov komunikačného systému kritickej informačnej infraštruktúry,
- správcov a prevádzkovateľov významného informačného systému,
- správcov a prevádzkovateľov informačného systému základnej služby,
- prevádzkovateľov základnej služby,
- poskytovateľov digitálnej služby.

Okrem exaktne vymenovaných subjektov ZKB v oblasti kybernetickej bezpečnosti určuje práva a povinnosti Národnímu úřadu pro kybernetickou a informační bezpečnost, vládnemu CERTu a prevádzkovateľovi národného CERTu. [12]

3.1.1 Poskytovateľ služby elektronických komunikácií a subjekt zaisťujúci sieť elektronických komunikácií

V ZKB § 3 písm. a) je definovaný povinný subjekt, ktorého význam nie je v rámci daného zákona vymedzený. Využitá terminológia pochádza zo zákona č. 127/2005 Sb., Zákon o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). [12]

V zákone o elektronických komunikacích sa rozumie pod pojmami:

- ***Služba elektronických komunikácií*** (§ 2 ods. 3 písm. a)) ako služba poskytovaná za úplatu prostredníctvom sietí elektronických komunikácií. Zahrnuté sú druhy služieb: služba prístupu k internetu, interpersonálna komunikačná služba a služby pozostávajúce úplne alebo prevažne v prenose signálov.
  Taktiež sú definované výnimky, ktoré nespadajú pod služby elektronických komunikácií a to nasledovné: služby poskytujúce obsah prenášaný prostredníctvom sietí a služieb elektronických komunikácií alebo vykonávajúcich redakčný dohľad. [14]
- ***Sieť elektronických komunikácií*** (§ 2 ods. 2 písm. b)) ako prenosové systémy. Nie je brané na zreteľ či sú založené na trvalej infraštruktúre alebo sú centralizovane kapacitne riadené alebo nie sú. Ďalej spadajú pod daný pojem spojovacie alebo smerovacie zariadenia (aj neaktívne sieťové prvky umožňujúce prenos signálu rôznymi spôsobmi), družicové siete, okruhovo ale aj paketovo komutované siete vrátane internetu, mobilné siete, siete pre rozvod elektrickej

energie (len v rozsahu používanom pre prenos signálu bez rozlišovania typu informácie) [14]

Poskytovateľ služby elektronických komunikácií a subjekt zaisťujúci sieť elektronických komunikácií má **ohlasovaciu povinnosť týkajúcu sa kontaktných údajov** a ich prípadných zmien prevádzkovateľovi národného CERTu.

Kontaktnými údajmi sa rozumie podľa ZKB § 16 ods. 1 pre:

- **právnické osoby:** obchodná firma alebo názov, adresa sídla, identifikačné číslo osoby alebo zahraničný ekvivalent,
- **podnikajúce fyzické osoby:** obchodná firma alebo meno vrátane odlišujúceho dodatku, adresa sídla a identifikačné číslo osoby,
- **orgány verejnej moci:** názov, adresa sídla, identifikačné číslo osoby (pokiaľ bolo pridelené) a identifikátor orgánu verejnej moci (v prípade nepridelenia identifikačného čísla osoby). [12]

Pre všetky vytýčené entity **je nutné doplnenie údajov o fyzickej osobe**, ktorá je za povinný subjekt oprávnená jednať. Jedná sa o meno, priezvisko, telefónne číslo a e-mailovú adresa. [12]

V súčasnej dobe napĺňa rolu národného CERTu tím CSIRT.CZ. Nahlásenie kontaktných údajov sa uskutočňuje prostredníctvom formulára na webových stránkach CSIRT tímu.[15] Toto ohlásenie je nutné uskutočniť najpozdejšie do 30 dní odo dňa nadobudnutia účinnosti tohto zákona. V prípade, že sa stane povinným subjektom po dátume účinnosti ZKB, ohlási kontaktné údaje bezodkladne. [12]

Pri ohlasovaní kontaktných údajov prostredníctvom vyššie uvedeného webového formulára je potrebné nad rámec zákonom uvedených kontaktných údajov vyplniť v *časti B* aj základný popis systému (popis charakteru služieb, ktoré sú povinným subjektom poskytované). V prípade poskytovateľa internetového pripojenia (skr. ISP) je doporučené v popise obsiahnuť: poskytovateľov konektivity, čísla autonómnych systémov (skr. AS), región alebo lokalitu poskytovania služieb a pri poskytovaní neštandardných služieb uviesť ich bližší popis. [15]

Pokiaľ neoznámi poskytovateľ služby elektronických komunikácií a subjekt zaisťujúci sieť elektronických komunikácií kontaktné údaje alebo ich zmenu, tak sa dopustí priestupku podľa § 25 ods. 1 písm c). [12]

Ďalšia povinnosť vyplývajúca zo zákona o kybernetickej bezpečnosti podľa § 11 ods. 3 písm. a) je **vykonávanie reaktívnych opatrení** v prípade stavu kybernetického nebezpečia alebo počas núdzového stavu. Po splnení reaktívneho opatrenia bez zbytočného odkladu oznámi výsledok vykonania podľa § 13 ods. 4. Formulár oznámenia o vykonaní reaktívneho opatrenia (aj návod k vyplneniu formulára) sa nachádza na webových stránkach NÚKIBu. Vyplnený formulár je potrebné zaslať do dátovej schránky NÚKIBu elektronicky podpísaný oprávnenou osobou. [16] V prípade neohlásenia výsledku reaktívneho opatrenia sa povinný subjekt dopustí priestupku podľa

§ 25 ods. 1 písm. b). [12]

Stav kybernetického nebezpečia je podľa § 21 ods. 1 vysvetlený ako stav, počas ktorého je vo veľkom rozsahu ohrozená bezpečnosť informácií v informačných systémoch alebo bezpečnosť služieb elektronických komunikácií, prípadne bezpečnosť a integrita sietí elektronických komunikácií, v dôsledku čoho by mohlo dôjsť k porušeniu alebo by došlo k ohrozeniu záujmu Českej republiky (podľa zákona o ochrane utajovaných informácií). [12]

Núdzový stav nie je v zákone o kybernetickej bezpečnosti vymedzený, ale odkazuje sa na ústavní zákon č. 110/1998 Sb., Ústavní zákon o bezpečnosti České republiky. V článku 5 je núdzový stav definovaný ako stav v prípade živelných pohrom, ekologických alebo priemyselných havárií, nehôd alebo iného nebezpečia, ktoré v značnom rozsahu ohrozuje životy, zdravie alebo majetkové hodnoty, prípadne majetkové hodnoty a bezpečnosť. [17]

Povinný subjekt podľa § 3 písm. a) je povinný **splniť rozhodnutie NÚKIBu alebo opatrenie obecnej povahy** počas núdzového stavu alebo stavu kybernetického nebezpečia podľa § 13 ods. 1. Môže sa jednať o reaktívne opatrenie k riešeniu kybernetického bezpečnostného incidentu alebo o zabezpečenie informačných systémov alebo sietí a služieb elektronických komunikácií pred kybernetickým bezpečnostným incidentom. Nesplnenie takéhoto rozhodnutia od NÚKIBu je chápaná ako priestupok podľa § 25 písm. a). [12]

Poslednou povinnosťou povinného subjektu podľa § 3 písm. a) je vykonať potrebné úkony k splneniu **nápravného opatrenia** podľa § 24 v časovom horizonte určenom Národním úřadem pro kybernetickou a informační bezpečnost, tým pádom je povinný plniť bezpečnostné opatrenia podľa § 4 ods. 1. V opačnom prípade sa dopustí priestupku podľa § 25 písm. d). [12]

Nápravné opatrenie môže byť uložené od Národního úřadu pro kybernetickou a informační bezpečnost po vykonaní kontroly.

Kontrola je uskutočňovaná zamestnancami NÚKIBu podľa § 23 za účelom zistenia ako povinné subjekty podľa § 23 ods. 1 plnia im stanovené povinnosti. [12]

3.1.2 Orgán alebo osoba zaisťujúca významnú sieť

Významná sieť je v znení zákona o kybernetickej bezpečnosti vysvetlená (§ 2 písm. h)) ako sieť elektronických komunikácií, ktorá zaisťuje priame hraničné prepojenie do verejných komunikačných sietí ale má zaisťovať priame prepojenie ku kritickej informačnej infraštruktúre. Avšak pojem významná sieť sa tiež spája so sieťou elektronických komunikácií, teda z tejto strany sa tiež riadi podľa § 2 ods. 3 písm. a) zákona o elektronických komunikácií (viď kapitola 3.1.1). [12] [14]

Orgán alebo osoba zaisťujúca významnú sieť je povinným subjektom podľa ZKB § 3 písm. b). Na tento povinný subjekt sa vzťahujú taktiež zákonom vymedzené povinnosti. Medzi ne patrí: plnenie bezpečnostných opatrení, ohlasovanie kontaktných údajov a ich prípadných zmien, detekovanie kybernetických udalostí a incidentov, hlásenie detekovaných kybernetických incidentov a ďalšie. Príležiace povinnosti entity zaisťujúcej významnú sieť budú v nasledujúcej časti priblížené.

Povinná osoba podľa ZKB §3 písm. b) je povinná **hlásiť kontaktné údaje**. Rovnako ako povinný subjekt podľa ZKB §3 písm. a) musí hlásiť kontaktné udaje a ich zmeny národnému CERT týmu (CSIRT.cz). Čo všetko hlásenie kontaktných údajov a ich prípadných zmien zahŕňa bolo vysvetlené v kapitole 3.1.1. [12]

Kybernetická bezpečnostná udalosť (§ 7 ods. 1 ZKB) je definovaná ako udalosť, ktorá môže spôsobiť narušenie bezpečnosti informácií (platí pre informačné systémy) alebo narušiť bezpečnosť služieb, alebo bezpečnosť a integritu sietí elektronických komunikácií. Je to udalosť, ktorá mohla spôsobiť uvedené dôsledky, ale nedošlo k nim.

Orgán alebo osoba zaisťujúca významnú sieť je povinná **detekovať kybernetické bezpečnostné udalosti** (skr. KBU) vyskytujúce sa v rámci jej významnej siete podľa § 7 ods. 3. V prípade nedodržania povinnosti sa dopustí priestupku podľa § 25 ods. 2 písm. a). [12]

Kybernetický bezpečnostný incident (§ 7 ods. 2 ZKB) zákon o kybernetickej bezpečnosti vysvetľuje ako narušenie bezpečnosti informácií v informačných systémoch, alebo narušenie bezpečnosti služieb, prípadne narušenie bezpečnosti a integrity sietí elektronických komunikácií. Na rozdiel od kybernetickej bezpečnostnej udalosti exaktne už došlo k spomenutým nežiadanúcim stavom. [12]

Nasledujúcou povinnosťou je podľa ZKB § 8 ods. 1 **hlásenie kybernetického bezpečnostného incidentu** (skr. KBI) v subjektom zaisťujúcej významnej sieti. Toto hlásenie je povinný hlásiť bezodkladne po detekcii KBI národnému CERT tímu (§ 8 ods. 3). Lehota na implementáciu detekcie KBI je zo ZKB stanovená na 1 rok od nadobudnutia účinnosti zákona o kybernetické bezpečnosti. Pokiaľ by sa nový subjekt stal povinný podľa ZKB § 3 písm. b) už počas účinnosti zákona, tak nie je stanovená časová lehota dokedy má povinný subjekt implementovať detekciu KBI a následne ich hlásiť národnému CERT tímu. [12] Môžeme len predpokladať, že lehota je rovnaká ako pri začiatku účinnosti zákona. Hlásenie o kybernetických bezpečnostných incidentoch sa uskutočňuje **prostredníctvom webového formulára** stránok národného CERT týmu (CSIRT.CZ). Do webového formulára je potrebné vyplniť o aký orgán alebo osobu podľa ZKB sa jedná, kontaktnú e-mailovú adresu, telefónne číslo, detaily incidentu (napr. popis incidentu, dátum a čas zistenia, kategorizáciu incidentu, súčasný stav zvládania KBI, odhad počtu dotknutých užívateľov) a systémové detaily (napr. hostiteľ, IP adresa, funkcia hostiteľa). [18]

Ekvivalentným spôsobom hlásenia kybernetického bezpečnostného incidentu je **oznámenie cez e-mailovú správu** na adresu CSIRT.CZ. Do predmetu mailu je vhodné zahrnúť IP adresu a typ incidentu, zvyšné atribúty korešpondujú do značnej miery s vyššie spomínaným webovým formulárom. Komplexné informácie vrátane PGP kľúča pre zaistenie dôvernosti a integrity zasielaných informácií sú zverejnené na webových stránkach CSIRT.CZ. [19]

Pokiaľ nebude orgán alebo osoba zaisťujúca významnú sieť podľa určených podmienok ohlasovať kybernetické bezpečnostné incidenty, sa dopustí priestupku podľa ZKB § 25 ods. 2 písm. b). [12]

Počas stavu kybernetického nebezpečia alebo núdzového stavu je orgán alebo osoba povinná **vykonávať reaktívne opatrenia** podľa zákona § 11 ods. 3 písm. a). Po splnení týchto opatrení je nutné o tomto fakte NÚKIB informovať spolu s jeho výsledkom (ZKB § 13 ods. 4). Oznámenie sa vykonáva prostredníctvom formulára o vykonaní reaktívneho opatrenia. Vyplnenie formulára bolo vysvetlené v kapitole 3.1.1. Neoznámenie o vykonaní reaktívneho opatrenia predstavuje pre povinný subjekt dopustenie sa priestupku podľa § 25 ods. 2 písm. d). [12]

Ako všetky z povinných subjektov podľa ZKB, tak aj orgán alebo osoba podľa § 3 písm. b) je povinná **strpieť kontrolu** podľa § 23 (viď 3.1.1). Akonáhle zamestnanci NÚKIB poverení kontrolnou činnosťou zistia nedostatky pri plnení zákonom vymedzených povinností určených pre orgán alebo osobu zaisťujúcu významnú sieť, uložia povinnosť na odstránenie týchto nedostatkov. Nesplnenie určených povinností uložených **nápravným opatrením** predstavuje dopustenie sa priestupku podľa § 25 ods.2 písm. f). [12]

Poslednou povinnosťou povinného subjektu je plnenie rozhodnutia alebo opatrenia všeobecnej povahy podľa § 13 v čase vyhláseného stavu kybernetického nebezpečia alebo núdzovom stave. Nesplnením sa povinný subjekt dopustí priestupku podľa § 25 ods. 2 písm. c). [12]

3.1.3 Správca a prevádzkovateľ informačného alebo komunikačného systému kritickej informačnej infraštruktúry

V rámci vymedzenia pojmov podľa ZKB sa definícia systému kritickej informačnej infraštruktúry odkazuje na zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (**krizový zákon**). V znení krízového zákona je **kritickou infraštruktúrou** chápaný prvok kritickej infraštruktúry alebo systém viacerých prvkov kritickej infraštruktúry, ktorých narušenie funkcie môže mať závažný dopad na bezpečnosť štátu, prípadne na zdravie osôb, ekonomiku štátu a podobne. [35] Pri pospájaní si významu definovaného krízovým zákonom a ZKB, je kritická informačná

infraštruktúra prvok alebo systém prvkov kritickej informačnej infraštruktúry v oblasti kybernetickej bezpečnosti informačných a komunikačných systémov, ktorých narušenie chodu môže mať závažný dopad na bezpečnosť štátu a i. Jedná sa o informačné alebo komunikačné systémy, ktoré spadajú pod kritériá pre určenie prvku kritickej informačnej infraštruktúry v oblasti kybernetickej bezpečnosti. Určenie tohto prvku prebieha po konzultáciách medzi pracovníkmi NÚKIBu a možnými zákonom regulovanými subjektami. Presne popísaný **proces určovania** prvku kritickej informačnej infraštruktúry je možné nájsť na webových stránkach NÚKIBu. [21]

Správcom informačného alebo komunikačného systému sa rozumie orgán, prípadne osoba určujúca účel komunikačného systému, či účel spracovania informácií a podmienky prevádzky informačného alebo komunikačného systému.

Prevádzkovateľ informačného alebo komunikačného systému je orgán alebo osoba, ktorá zabezpečuje funkčnosť hardvérových a softvérových prostriedkov spolu predstavujúcich informačný alebo komunikačný systém. Túto osobu určuje a neodkladne oboznamuje o tejto skutočnosti správca informačného alebo komunikačného systému preukázateľným spôsobom.

Prvou povinnosťou regulovaného subjektu podľa § 16 ods. 2 písm. b) ZKB je **hlásenie kontaktných údajov**, avšak tentokrát iným spôsobom ako pri vyššie uvedených subjektoch. V tomto prípade sa jedná o nahlásenie kontaktných údajov **vládnemu CERTu** prostredníctvom formulára dostupného na ich webových stránkach.[22] Vyplnený formulár je potrebné zaslať e-mailovou komunikáciou alebo dátovou schránkou najneskôr do 30 dní odo dňa, kedy bol určený ich informačný alebo komunikačný systém kritickej informačnej infraštruktúry. [12]

Správcovia a prevádzkovatelia majú ďalšiu povinnosť, ktorou je **hlásiť KBI** zaznamenané v ich informačnom alebo komunikačnom systéme kritickej informačnej infraštruktúry. Toto hlásenie má byť adresované **vládnemu CERTu**, ktorý zabezpečuje NÚKIB. Hlásenie prebieha vyplnením elektronického formulára (je potrebné vyplniť obdobné náležitosti ako aj pri hlásení KBI národnému CERTu) a zaslaním na príslušnú dátovú schránku, e-mailovou komunikáciou. Vo vážnych prípadoch je možné kontaktovať pracovníkov vládneho CERTu priamo telefonicky aj mimo pracovnú dobu. [23]

Ďalej je povinný subjekt podľa ZKB § 3 písm. c) a d) zaviesť a vykonávať **bezpečnostné opatrenia** tak, aby bolo možné zaistiť kybernetickú bezpečnosť informačného alebo komunikačného systému v dostačujúcom rozsahu a viesť o nich bezpečnostnú dokumentáciu (ZKB § 4 odst. 2). Čo presne obnáša bezpečnostná dokumentácia je vysvetlené v rámci vykonávacieho právneho predpisu VKB. [12]

Nasledujúca povinnosť sa vzťahuje na **výber dodávateľa** pre informačný alebo komunikačný systém KII, kedy je potrebné zaviesť zohľadnené požiadavky bezpečnostných opatrení, ktoré sú definované vo VKB § 8 Riadenie dodávateľov (bližšie

informácie viď podkapitola 3.2). [29]

Zvyšné povinnosti tohoto zákonom regulovaného subjektu sú zhrnuté vymenovaním (z dôvodu vyššie uvedeného bližšieho popisu):

- vykonávanie detekcie KBU,
- vykonávanie reaktívnych opatrení,
- informovanie vládneho CERTu o vykonanom reaktívnom opatrení a o jeho výsledku,
- vykonávanie ochranných opatrení,
- strpenie kontroly zo strany NÚKIB,
- splnenie povinností uložených nápravným opatrením.

3.1.4 Správca a prevádzkovateľ významného informačného systému

Povinné osoby podľa ZKB § 3 písm. e) sa rozumejú ako osoby alebo orgány spravujúce či prevádzkujúce významný informačný systém. Tento systém je v zákone ponímaný ako **informačný systém pod správou orgánu verejnej moci**, ktorého narušenie bezpečnosti informácií môže mať dopad na regulérny výkon pôsobnosti orgánu verejnej moci. V praxi sa môže jednať o informačné systémy elektronickej pošty, spisovej služby, medzinárodné spolupráce a iné. [12]

Identifikácia významného systému sa vykonáva tzv. **samourčením**. Akonáhle orgán verejnej moci spravujúci informačný systém, ktorý objektívne napĺňa zákonnú definíciu má dôjsť k riadnej identifikácii významného informačného systému. Orgán verejnej moci pre riadnu identifikáciu má vychádzať nielen zo ZKB, ale aj z vyhlášky č. 317/2014 Sb., Vyhláška o významních informačních systémech a jejich určující kritériích. Bližší popis identifikácie je uvedený na webových stránkach NÚKIBu. [24]

Povinnosti, ktoré povinná osoba podľa § 3 písm. e) má plniť, sú:

- hlásenie kontaktných údajov vládnemu CERTu,
- hlásenie kybernetických bezpečnostných incidentov vládnemu CERTu,
- vykonávanie detekcie KBU,
- zavedenie a vykonávanie bezpečnostných opatrení s vedením dokumentácie,
- vykonávanie reaktívnych opatrení,
- informovanie vládneho CERTu o vykonanom reaktívnom opatrení a o jeho výsledku,
- vykonávanie ochranných opatrení,
- stanovenie požiadaviek na dodávateľa a ich zohľadnenie pri jeho výbere,
- strpenie kontroly zo strany NÚKIB,
- splnenie povinností uložených nápravným opatrením.

3.1.5 Správca a prevádzkovateľ informačného systému základnej služby

Informačný systém základnej služby je podľa ZKB **informačný systém slúžiaci na zabezpečenie fungovania základnej služby**. Definícia základnej služby je vysvetlená pri nasledujúcej zákonom vytýčenej povinnej osobe. [12]

Povinnosti vyplývajúce zo zákona pre správcu a prevádzkovateľa informačného systému základnej služby sú:

- hlásenie kontaktných údajov vládnemu CERTu,
- hlásenie kybernetických bezpečnostných incidentov vládnemu CERTu,
- vykonávanie detekcie KBU,
- zavedenie a vykonávanie bezpečnostných opatrení s vedením dokumentácie,
- vykonávanie reaktívnych opatrení,
- informovanie vládneho CERTu o vykonanom reaktívnom opatrení a o jeho výsledku,
- vykonávanie ochranných opatrení,
- stanovenie požiadaviek na dodávateľa a ich zohľadnenie pri jeho výbere,
- strpenie kontroly zo strany NÚKIB,
- splnenie povinností uložených nápravným opatrením.

3.1.6 Prevádzkovateľ základnej služby

Základnou službou podľa zákona § 2 písm. i) je chápaná služba, ktorej poskytovanie priamo závisí na informačných systémoch, prípadne sieťach elektronických komunikácií. Jej narušenie môže mať závažný dopad na kybernetickú bezpečnosť spoločenských alebo ekonomických činností v určitých oblastiach ako napríklad energetika, zdravotníctvo či chemický priemysel. [12]

Zákonné povinnosti prevádzkovateľa základnej služby sú:

- informovanie správcu a prevádzkovateľa informačného systému základnej služby o nadobudnutí povinností plynúcich zo ZKB,
- hlásenie kontaktných údajov vládnemu CERTu,
- hlásenie kybernetických bezpečnostných incidentov vládnemu CERTu za okolností,
- strpenie kontroly zo strany NÚKIB,
- splnenie povinností uložených nápravným opatrením.

3.1.7 Poskytovateľ digitálnej služby

V zákone o kybernetickej bezpečnosti je pojem digitálnej služby vychádzajúci zo zákona č. 480/2004, **Zákon o některých službách informační společnosti**, kde digitálna služba môže byť služba poskytovaná elektronickými prostriedkami a zároveň spĺňa náležitosti:

- bola žiadaná individuálne prostredníctvom elektronických prostriedkov,
- bola poskytnutá za úplatu, a
- bola poskytnutá prostredníctvom elektronických prostriedkov. [30]

V ZKB je definovaná ako služba poskytujúca on-line trhovisko, internetový vyhľadávač či cloud computing.

Spôsob identifikácie možného poskytovateľa je k dispozícii na webových stránkach NÚKIBu. [25]

Prevádzkovateľ digitálnej služby má zákonom vytýčené nasledovné povinnosti:

- hlásenie kontaktných údajov vládnemu CERTu,
- hlásenie kybernetických bezpečnostných incidentov národnému CERTu,
- zavedenie a vykonávanie bezpečnostných opatrení s vedením dokumentácie,
- strpenie kontroly zo strany NÚKIB za okolností podozrenia nespĺňania zákonných povinností,
- splnenie povinností uložených nápravným opatrením. [12]

3.2 Vyhláška o kybernetické bezpečnosti

Vyhláška č. 82/2018 Sb. nadobudla účinnosť ku dňu 21. mája 2018 a stanovuje dôležité míľniky pre oblasť kybernetickej bezpečnosti, nielen pre zákonom regulované subjekty ako sú obsah a štrukturovanie bezpečnostnej dokumentácie, obsah a rozsah bezpečnostných opatrení, rozdelenie a hodnotenie závažnosti kybernetických bezpečnostných incidentov, náležitosti oznámení kontaktných údajov, vykonania reaktívneho opatrenia a iné. [29]

V tejto vyhláške sú zapracované niektoré povinnosti zo smernice Európskeho parlamentu a Rady (EU) 2016/1148 o opatreniach k zaisteniu vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (**Smernica NIS**) zo dňa 6. júla 2016. [26]

Ako hlavnú časť možno považovať bezpečnostné opatrenia, ktoré sú rozdelené do troch hláv:

- **Hlava I** - organizačné opatrenia (§ 3 - § 16),
- **Hlava II** - technické opatrenia (§ 17 - § 29),
- **Hlava III** - bezpečnostná politika a bezpečnostné dokumentácie (§ 30).

Spojitosť medzi VKB a radou noriem ISO/IEC 27000 je nepopierateľná, nakoľko ich obsah a štrukturovanie sa do veľkej miery prekrýva. Príkladom môžu byť začlenené v oboch dokumentoch riadenie aktív, kryptografické prostriedky či fyzická bezpečnosť. [27]

Nasledujúce popisy jednotlivých paragrafov VKB budú zamerané na najsignifikantnejšie povinnosti, ktorými sa vyznačujú (všetky povinnosti sú obsiahnuté v rámci platného znenia vyhlášky).

3.2.1 Organizačné opatrenia

§ 3 - Systém riadenia bezpečnosti informácií

S pojmom systém riadenia bezpečnosti informácií bol v rámci tohoto dokumentu spomínaný v podkapitole 2.1 v súvislosti s rodinou noriem ISO/IEC 27000. Najdôležitejšie informácie vyplývajúce z § 3 VKB je **stanovenie systému riadenia bezpečnosti informácií** (ISMS) a jeho ciele, pretože od toho sa odvíjajú ďalšie požiadavky plynúce z VKB ako sú riadenie aktív, riadenie rizík alebo iné naviazané bezpečnostné opatrenia. ISMS predstavuje časť systému riadenia organizácie, ktorá berie v úvahu riziká informačného alebo komunikačného systému. Vzhľadom k nim je nutný monitoring, pravidelný prieskum a zlepšovanie bezpečnosti informácií či dát prostredníctvom bezpečnostných opatrení. [29]

Ďalšou neodmysliteľnou súčasťou je nutnosť pravidelného **vyhodnocovania účinnosti ISMS** a jeho **aktualizovanie**. Tento prístup je obdobný ako v prípade normy ČSN ISO/IEC 27001 (kap. 2.1) pracujúci v duchu spomínaného PDCA cyklu. Vyhodnocovanie je potrebné z dôvodu existencie viacerých vstupov, ktoré je nutné zohľadniť a aktualizovať. Vstupy môžu predstavovať vykonané audity a prípadné zistenia nedostatkov, rovnako ako aj penetračné testovanie, významné zmeny alebo vyskytnuté KBI.

§ 4 - Riadenie aktív

Aktíva sú podľa vyhlášky členené na primárne a podporné. Pričom **primárnym aktívom** môžu byť poskytované služby alebo informácie, s ktorými kooperuje informačný alebo komunikačný systém. Pod pojmom **podporné aktíva** sú vyhláškou chápané technické aktíva (napr. servery, počítače, sieťové prvky), zamestnanci prípadne dodávatelia dôležití pre správny chod informačného či komunikačného systému. Vo všeobecnosti ale platí, že aktíva predstavujú všetko čo má hodnotu v oblasti bezpečnosti informácií a dát pre danú organizáciu. **Medzi primárnymi a podpornými aktívami** je potrebné zvážiť **väzby či závislosti medzi nimi**. Z praxe je časté preberanie hodnoty primárneho aktíva aj na podporné. Dôvodom

môže byť napríklad technický výpadok podporného aktíva a v dôsledku toho dôjde k nedostupnosti aj primárneho aktíva. [29]

V rámci riadenia aktív je potrebné vytvorenie vhodného postupu pre identifikovanie aktív a ich následné hodnotenie. Pri hodnotení aktív je **vhodné zakomponovať prílohu č. 1 VKB**. Spomenutá príloha predstavuje vzorové požiadavky pri vytváraní stupníc pre hodnotenie dôvernosti, integrity a dostupnosti informácií, ktoré je vhodné prispôsobiť podľa potrieb jednotlivých organizácií. Pre podrobnejšie objasnenie problematiky je vydaný podporný materiál na webových stránkach NÚKIBu. [28]

§ 5 - Riadenie rizík

Aj pri tomto paragrafe vyhlášky je postup systematický, kedy sa začína stanovením metodiky pre hodnotenie rizík a zostavením kritérií pre akceptovateľnosť rizík. **Hodnotenie rizík** prebieha priradením hodnoty rizika spôsobom **zohľadnenia potenciálnych hrozieb a zraniteľností a následný dopad** pre organizáciou vytýčené aktíva. [28]

Hodnotenie rizík je vhodné vykonávať v pravidelných intervaloch. VKB stanovuje pre povinné subjekty s kritickou informačnou infraštruktúrou a informačným systémom základnej služby **hodnotenie rizík na báze ročného cyklu**. Pri povinnom subjekte s významným informačným systémom VKB ukladá povinnosť hodnotenia rizík aspoň **raz za 3 roky**.

Ďalej je potrebné spracovanie **výstupnej správy o hodnotení rizík** s následným prehlásením o aplikovateľnosti s obsiahnutými bezpečnostnými opatreniami a ich spôsobom realizácie.

Neodmysliteľnou súčasťou riadenia rizík je vytvorenie **plánu zvládania rizík**, v ktorom je potreba obsiahnuť napríklad spojitosti medzi rizikami a prináležiacimi bezpečnostnými opatreniami, finančné či ľudské zdroje. [29]

§ 6 - Organizačná bezpečnosť

Paragraf pojednávajúci o organizačnej bezpečnosti je cielený najmä na manažment, prípadne vrcholové vedenie zákonom regulovaných subjektov, v rámci ktorého sa kladie dôraz na už vyššie uvedené povinnosti súvisiace s ISMS.

Ďalej je povinným subjektom uložená povinnosť **určiť bezpečnostné role** (bude priblížené v rámci VKB § 7) a **zriadenie výboru** pre riadenie kybernetickej bezpečnosti, ktorý primárne zodpovedá za riadenie a rozvoj kybernetickej bezpečnosti v rámci organizácie.

Výborom pre riadenie kybernetickej bezpečnosti sa rozumie skupina, ktorej náplň je kontrola aktuálneho stavu, koordinovanie a plánovanie či schvaľovanie

zmien v oblasti kybernetickej bezpečnosti. Členmi takéhoto výboru sú osoby s právomocami a odbornými znalosťami v oblasti kybernetickej bezpečnosti, zástupca vrcholového vedenia a manažér kybernetickej bezpečnosti. [29]

§ 7 - Bezpečnostné role

VKB v poradí siedmom paragrafe, s názvom bezpečnostné role, definuje 4 bezpečnostné role.

Prvou z nich je **manažér kybernetickej bezpečnosti** zodpovedajúci za systém riadenia bezpečnosti informácií, informovanie vrcholového vedenia o vykonávaných činnostiach v oblasti ISMS a celkovom stave ISMS. Nasledujúca rola, **architekt kybernetickej bezpečnosti**, má na starosti navrhovanie a implementovanie bezpečnostných opatrení v rámci informačného alebo komunikačného systému. V poradí tretia bezpečnostná rola nesie názov **garant aktív** zodpovedá za bezpečnosť aktíva, jeho používanie a prípadný rozvoj. Poslednou bezpečnostnou rolou je **auditor kybernetickej bezpečnosti**, ktorý je zodpovedajúci za výkon auditu kybernetickej bezpečnosti bez zainteresovanosti, teda nestranne. [29]

Pri výbere bezpečnostných rolí je vhodné brať do úvahy **prílohu č. 6 VKB** definujúcu ďalšie doporučené požiadavky, ktoré by mali spĺňať jednotlivé bezpečnostné role.

§ 8 - Riadenie dodávateľov

Významným dodávateľom je podľa vyhlášky prevádzkovateľ informačného alebo komunikačného systému a iné orgány alebo osoby vstupujúce do právneho vzťahu, pričom sú z hľadiska kybernetickej bezpečnosti takýchto systémov významní. [29]

Pri riadení dodávateľov majú povinné osoby určené povinnosti pri ich výbere. V prvom rade je potrebné **nastavenie pravidiel pre dodávateľov** vychádzajúcich zo zavedeného systému riadenia bezpečnosti informácií, s ktorými ich pri výbere oboznámi. Ďalej všetkých svojich **významných dodávateľov eviduje**. Pred výberom dodávateľa k určitému informačnému alebo komunikačnému systému musí **riadiť riziká spojené s dodávateľom** a predmetom výberového konania, ktoré budú obsiahnuté v spomínanej správe o hodnotení rizík. [31] **Zmluvy** uzatvárané medzi významným dodávateľom a zákonom regulovaným subjektom musia obsahovať aspoň minimálne požiadavky, ktoré sú uvedené **v prílohe č. 7 VKB** (napr. ustanovenie o bezpečnosti informácií, autorstve programového kódu a iné). Po výbere dodávateľa má povinný subjekt povinnosť pravidelne preskúmávať hodnotenie rizík a kontrolovať plnenie určených bezpečnostných opatrení (v prípade zistených rizík alebo zistených nedostatkov zaistiť ich riešenie). [29]

§ 9 - Bezpečnosť ľudských zdrojov

Nie menej dôležitým prvkom je aj bezpečnosť ľudských zdrojov, nakoľko môže mať organizácia zavedené sebe lepšie technické zabezpečenie, ale zlyhanie ľudského faktora vie napomôcť útočníkovi k prevedeniu kybernetických bezpečnostných udalostí alebo incidentov. Toto je jeden z dôvodov, prečo je deviaty paragraf zahrnutý v rámci VKB. Najdôležitejšou časťou z bezpečnosti ľudských zdrojov je **stanovenie plánu bezpečnostného povedomia**, ktorého úlohou má byť zaistenie vzdelania a ďalšieho zlepšovania bezpečnostného povedomia v oblasti kybernetickej bezpečnosti. V pláne nesmú chýbať popisy spôsobov poučení (forma, obsah, rozsah) administrátorov, osôb zastávajúcich bezpečnostné role, dodávateľov ale aj prostých užívateľov o ich povinnostiach. Plán má určovať spôsob akým budú spomenuté osoby preškolené (napr. sa môže jednať o prezentácie, školenia v informačnom systéme), oblasti zahrnuté v pláne vzdelávania (napr. politika tvorby bezpečného hesla, rozpoznanie phishingu), pravidelnosť školení, rozsah líšiaci sa pre jednotlivé typy užívateľov a spôsoby riešenia prípadov porušenia určených bezpečnostných pravidiel. [29]

§ 10 - Riadenie prevádzky a komunikácií

V rámci riadenia prevádzky a komunikácií je zdôrazňovaná dôležitosť na **zaistenie bezpečného chodu informačného a komunikačného systému**, ku ktorému majú byť zavedené prevádzkové postupy, pravidlá alebo návody týkajúce sa napríklad inštalácií technických aktív, ochrany pred škodlivým kódom alebo obnovenia chodu systému po zlyhaní či kybernetickom bezpečnostnom incidente. V praxi je často zaužívané a odporúčané mať stanovené prevádzkové postupy a pravidlá (vyplývajúce z VKB § 10) v offline forme, ktorá je dostupná aj pri rozsiahlejšom výpadku systému. [29]

§ 11 - Riadenie zmien

Prvou povinnosťou zákonom regulovaných subjektov v rámci riadenia zmien v informačnom a komunikačnom systéme je **definovanie pojmu významnej zmeny**, ktorá môže mať alebo má presah do kybernetickej bezpečnosti a predstavuje vysoké bezpečnostné riziko pre danú organizáciu.

Po definovaní významných zmien a ich určení je potrebná **dokumentácia**, do ktorej musí byť **zahrnutá analýza rizík**. V prípade zistených rizík je potrebné prijať opatrenia pre docielenie eliminácie takýchto rizík týkajúcich sa významných zmien. Po technickej stránke je potrebné uskutočniť testovanie významných zmien takým spôsobom, aby bolo možné navrátenie do pôvodného stavu (napr. využívanie sandboxing, oddelenie testovacej podsiete, využitie záloh). [29]

§ 12 - Riadenie prístupu

V rámci riadenia prístupu k informačnému a komunikačnému systému ukladá VKB podľa § 12 niekoľko povinností pre zákonom regulovaný subjekt ako sú **riadenie prístupu** na základe skupín a rolí, čo predstavuje rozdelenie užívateľov do jednotlivých skupín, podľa ktorých ich bude možné jednotne modifikovať (skupiny môžu byť napríklad administrátori, dodávatelia, bežní užívatelia). Ďalej má povinná osoba **využívať bezpečnostné opatrenia** pre bezpečné riadenie mobilných, prípadne iných technických zariadení (môže sa jednať o technologické riešenie spadajúce pod skratku MDM - Mobile Device Management), prideliť jednotlivým užívateľským účtom prístupové oprávnenia len do takej miery aká vyžaduje ich náplň práce. [29]

Prideľovanie a odoberanie prístupových opatrení má pritom vychádzať z vytvorenej **politiky riadenia prístupu**. **Kontrola** nastavených **prístupových oprávnení** sa má pritom vykonávať v nastavenej pravidelnej báze, okrem iného aj pri zmene pracovnej pozície zamestnanca alebo ukončení zmluvného vzťahu medzi entitami. Úkony prideľovania a odoberania prístupových oprávnení musí povinná osoba dokumentovať pre možnú spätnú dohľadateľnosť. [29]

§ 13 - Akvizícia, vývoj a údržba

Pri akvizícii (napr. spojení dvoch aktív do jedného), vývoji či údržbe informačného systému majú podľa VKB § 13 povinné subjekty riadiť riziká a významné zmeny, ktoré by mohli nastať pri týchto úkonoch. Dôležitou časťou je **stanovenie bezpečnostných požiadaviek**, ktoré je potrebné zahrnúť do projektu akvizície, vývoja a údržby.

Pred zavedením významných zmien je potrebné vykonať **bezpečnostné testovanie** vo vývojovom, alebo testovacom prostredí (oddelenom od produkčného prostredia). [29]

§ 14 - Zvládanie kybernetických bezpečnostných udalostí a incidentov

Pojmy kybernetický bezpečnostný incident a udalosť boli vysvetlené v rámci predchádzajúcich kapitol (viď 3.1.2).

Povinnosťou zákonom regulovaného subjektu je pre zvládanie KBU a KBI zaviesť procesy pre **včasnú detekciu KBU a zvládanie KBI**. Ďalej musia byť určené **zodpovedné osoby za vyhodnocovanie** KBU a koordináciu pri zvládaní KBI podľa predom stanovených postupov. Detekcia KBU nemusí byť docielená len spôsobom podporných technických aktív, ale aj prijímaním hlásení od zamestnancov alebo dodávateľov o neobvyklom chovaní informačného alebo komunikačného systému (napr. prostredníctvom service desku, telefonicky, e-mailovou komunikáciou).

Pri vzniknutých KBI je nutné viesť **záznamy** o ich zvládaní, nájsť príčiny ich vzniku a po ich vyriešení vyhodnotiť vykonané procesy (v prípade potreby zvážiť aktualizovanie súčasných bezpečnostných opatrení pre zamedzenie ich vzniku do budúcna). [29]

§ 15 - Riadenie kontinuity činností

Povinnej osobe je uložená povinnosť posúdenia možných rizík dopadajúcich na kontinuitu činností pomocou hodnotenia rizík, analýzy dopadov a zdokumentovaných dopadov KBI. Vychádzajúc z hodnotenia rizík a analýzy dopadov je potrebné **stanovenie cieľov riadenia kontinuity činností**, ktoré sú definované vyhláškou:

- minimálna úroveň poskytovaných služieb - taká úroveň, ktorá je akceptovateľná pre dočasnú prevádzku a správu informačného alebo komunikačného systému,
- doba obnovenia chodu - doba nutná pre obnovenie minimálnej úrovne poskytovaných služieb informačného alebo komunikačného systému po vzniknutom KBI,
- bod obnovenia dát - časový horizont, počas ktorého budú dáta obnovené po vzniknutom KBI či zlyhaní informačného alebo komunikačného systému. [29]

Poslednou povinnosťou v rámci tohoto paragrafu je **vypracovanie a pravidelné testovanie** plánu kontinuity činností spolu s havarijnými plánmi týkajúcich sa informačných a komunikačných systémov, prípadne služieb. Aj v tomto prípade je vhodné mať havarijné plány k dispozícii v offline (napr. papierovej) podobe, alebo na inej lokalite z dôvodu zabezpečenia ich dostupnosti pri rozsiahlom výpadku systémov. [29]

§ 16 - Audit kybernetickej bezpečnosti

Posledný paragraf VKB týkajúci sa organizačných opatrení nesie názov audit kybernetickej bezpečnosti. Ukladá povinnosť zákonne povinným subjektom vykonávanie auditu a následné **dokumentovanie dodržiavania určených bezpečnostných politík**. Výsledné **zistenia** auditu je potrebné zakomponovať do plánu rozvoja bezpečnostného povedomia a plánu zvládania rizík. Okrem definovaných bezpečnostných politík majú byť kontrolované bezpečnostné opatrenia podľa najlepšej praxe, právnych ale aj interných predpisov, záväzkov vyplývajúcich zo zmlúv týkajúcich sa informačného alebo komunikačného systému. Výkon auditu uskutočňuje auditor kybernetickej bezpečnosti, ktorého bezpečnostná rola bola vyššie priblížená.

Pre vykonávanie auditov je definovaná minimálna **pravidelnosť** pre zákonom regulované subjekty na raz za dva roky (v prípade významných informačných systémov postačuje raz za tri roky) a pri významných zmenách. [29]

3.2.2 Technické opatrenia

§ 17 - Fyzická bezpečnosť

Prvý paragraf technických opatrení VKB pojednáva o fyzickej bezpečnosti, teda o zabezpečení priestorov, v rámci ktorých sa nachádza informačná a komunikačná technika alebo iné aktíva. Stanovuje povinnosť **predchádzať poškodeniam**, ukradnutiu alebo iného zneužitia aktív, prípadne znedostupneniu poskytovaných služieb. **Stanovenie fyzického bezpečnostného perimetru** je dôležitou súčasťou fyzickej bezpečnosti, kedy sa určí oblasť, v ktorej je potrebné zabezpečenie informácií a iných aktív za použitia prostriedkov fyzickej bezpečnosti pre zaistenie ochrany na úrovni objektov ale aj v rámci nich. [29] Týmito prostriedkami sa rozumejú napríklad mechanické zábranné prostriedky (napr. brány, turnikety, oplotenie), systém elektronickej kontroly vstupu tzv. EKV, elektronický zabezpečovací systém (skr. EZS), systémy obmedzujúce pôsobenie živelných udalostí (napr. požiarny zabezpečovací systém, záplavové detektory) alebo kamerové systémy (skr. CCTV).

Prerušením poskytovania služieb poskytovaných povinnou osobou sa môže predchádzať napríklad použitím neprerušiteľných napájacích zdrojov (skr. UPS) spolu s elektrocentrálami vytvárajúcimi elektrický prúd. [32]

§ 18 - Bezpečnosť komunikačnej siete

Súvisiacimi povinnosťami pre zákonom regulované subjekty pri zabezpečení komunikačnej siete je zaistenie segmentácie komunikačnej siete. **Segmentovanie siete** na podsiete sa využíva pre zvýšenie efektivity a zamedzenie prípadného výskytu škodlivého softvéru či iných hrozieb na menšiu časť siete, ktorá bude izolovaná od ostatných častí. [33]

Pri vzdialenom prístupe je ďalšou povinnosťou **zaistenie dôvernosti a integrity dát**, ktoré môže byť napríklad docielené využívaním technológií a protokolov, ktoré neprenášajú dátový tok formou nešifrovaného plaintextu (napr. Telnet) ale naopak prenášané informácie sú šifrované (napr. VPN). [29]

Napokon povinný subjekt je povinný **aktívne blokovať nežiadúcu komunikáciu**. [29] Aktívne blokovanie môže byť vykonávané firewallami, ochrannými systémami pred DDoS útokmi alebo prostredníctvom systémov prevencie prieniku tzv. IPS. [34]

§ 19 - Správa a overovanie identít

Paragraf 19 stanovuje povinnosť **používania nástroja** určeného pre správu a overovanie identít užívateľov a aplikácií informačného a komunikačného systému. Tento n**ástroj by mal disponovať** napríklad:

- overovaním identity pred záhájením aktitít - predstavuje napr. prihlásenie sa do systému,
- riadením počtu neúspešných pokusov príhlásenia - ochrana pred prípadným útokom hrubou silou,
- ukladaním autentizačných údajov takým spôsobom aby boli odolné proti off-line útokom,
- centralizovanou správou identít. [29]

Principiálne sa môže jednať o Active Directory (platforma Microsoft) alebo iné technológie riešiace správu identít (často označované skratkami IdM, PIM, PAM). [36]

Forma autentizácie je stanovená tromi rôznymi spôsobmi. Pričom prvý spôsob je **formou viacfaktorovej autentizácie** s minimálne dvomi rôznymi typmi faktorov (napr. zadanie PIN, zadanie hesla, autentizácia pomocou biometrických údajov - odtlačok prsta, sietnica, krvné riečisko).

Pokiaľ nie je možné splniť využívanie viacfaktorovej autentizácie (napr. nedisponovanie potrebných prostriedkov a technológií) je potrebné **autentizovanie pomocou kryptografických kľúčov**.

V poslednom rade pre ostatné prípady je možné využitie **autentizácie** len za pomoci využitia jedinečného **identifikátora užívateľa a hesla**. Pri tomto spôsobe autentizácie musia byť vynucované špecifické požiadavky pri tvorbe hesla podľa § 19 VKB (napr. dĺžka hesla, rôznorodosť znakov). Dôležité je podotknúť, že tento posledný a najmenej sofistikovaný spôsob ochrany je možné používať len do doby, kým nebude možné využívať viacfaktorovú autentízáciu, alebo autentizáciu pomocou kryptografických kľúčov. [29]

§ 20 - Riadenie prístupových oprávnení

V ďalšom poradí paragraf pod číslom 20 popisuje riadenie prístupových oprávnení, ktorý v skratke stanovuje povinnosť pre **využívanie centralizovaného nástroja** pri správe prístupových oprávnení. Tento nástroj musí disponovať možnosťou úpravy prístupových oprávnení k stanoveným aktívam informačného a komunikačného systému spolu s možnosťou úprav pre čítanie, zapisovanie dát (často pod skratkami RWX - Read Write eXecute) a zmenu oprávnení. [29]

§ 21 - Ochrana pred škodlivým kódom

Pre zákonom regulované subjekty s informačným systémom základnej služby alebo systémom spadajúcim pod kritickú informačnú infraštruktúru povinnosti pre zaistenie ochrany pred škodlivým kódom. V preklade ochranu pred škodlivým kódom môžeme rozumieť antivírusovú ochranu [38] alebo technológie pod skratkou EDR (Endpoint Detection and Response)[37], pričom tieto technologické prostriedky je

povinný subjekt pravidelne **aktualizovať**. Aktualizácie sú dôležité pre včasné pridanie potenciálnych hrozieb do databáz týchto systémov, čo môže pomôcť pre včasnú detekciu novými neznámymi škodlivými kódmi. [29]

Pre ochranu pred škodlivým kódom je nutné využívanie nástrojov **automatickej detekcie** takého kódu s ohľadom na dôležitosť aktív (napr. koncové stanice, servery, mobilné zariadenia alebo prvky komunikačnej siete). Ďalej tieto nástroje majú monitorovať používanie dátových nosičov a riadiť oprávnenia pre spustiteľnosť kódu (často spolupráca s Mobile Device Management - skr. MDM).

Vyššie spomenuté povinnosti sú platné aj pre povinné subjekty s významným informačným systémom, avšak pri ich aplikácii majú postupovať primerane (podľa právneho prekladu do maximálnej možnej miery). [29]

§ 22 - Zaznamenávanie udalostí informačného a komunikačného systému, jeho užívateľov a administrátorov

Ďalšou stanovenou povinnosťou je zaznamenávanie dôležitých udalostí v rámci informačných a komunikačných systémov. V preklade tohto dlhšieho názvu paragrafu sa jedná o **zaznamenávanie logov**, často označované aj ako logovanie. V rámci nich je potrebné obsiahnuť jedinečný sieťový identifikátor, ktorým môže byť napríklad logická IP adresa, fyzická MAC adresa prípadne vystavený certifikát certifikačnou autoritou. Nasledujúce stanovené atribúty logov sú: časová značka, typ činnosti, identifikátor účtu a stav úspešnosti vykonávanej činnosti pričom všetky zaznamenané údaje musia byť chránené pred čítaním a prípadným pokusom o ich pozmenenie. Dodržanie syntaxe logov, teda ich normalizovanie je dôležité pre nasledovné s nimi späté činnosti (bude vysvetlené v rámci nasledujúcich paragrafov VKB). [29]

Vyhláška podľa § 22 stanovuje zaznamenávanie viacerých dôležitých činností, ktorými sú napríklad prihlasovanie a odhlasovanie k účtom, administrátorské činnosti, prístup a snaha o manipuláciu zaznamenaných udalostí a iné.

Pri logovaní je nutné **dodržanie synchronizácie času** u technických aktív aspoň raz za 24h. Na časovú synchronizáciu je možné využiť NTP protokol spolu s NTP serverom (NTP - Network Time Protocol). [39]

Pre povinné osoby disponujúce informačným systémom základnej služby a systémom KII je stanovené **uchovávanie zaznamenávaných udalostí** po dobu 18 mesiacov a pre VIS po dobu 12 mesiacov. Pri tejto povinnosti je dôležité korektné nastavenie kapacity úložných prostriedkov pre dodržanie určeného časové horizontu. [29]

§ 23 - Detekcia kybernetických bezpečnostných udalostí

Zákonom regulovanému subjektu je stanovená povinnosť **detekcie KBU** v rámci komunikačnej siete **za pomoci nástroja**, ktorý dokáže overiť a kontrolovať dáta prenášané v rámci komunikačnej siete a na jej perimetre. V prípade nutnosti by nástroj mal byť schopný o **zablokovanie nežiadúcej komunikácie**. [29] Takýto nástroj môže predstavovať systém prevencie prieniku pracujúci v rámci komunikačnej siete (NIPS - Network based Intrusion Prevention System). [34]

Povinnosť detekcie KBU na určených typoch aktív je len pre subjekty s informačným systémom základnej služby a systémom kritickej informačnej infraštruktúry. Spomenutými aktívami sú napríklad koncové stanice, mobilné zariadenia, servery a iné. [29] Pre takúto detekciu sú vhodné napríklad systém prevencie prieniku pracujúci na konkrétnom technickom prostriedku (HIPS - Host based IPS). [34]

§ 24 - Zber a vyhodnocovanie kybernetických bezpečnostných udalostí

V predchádzajúcich dvoch paragrafoch boli zaznamenané udalosti normalizované a zdetekované KBU. Ďalšími súvisiacimi povinnosťami pre zákonom regulované subjekty s informačným systémom základnej služby alebo systémom KII je využívanie nástroja, ktorý dokáže **zozbierať a centralizovať zaznamenané kybernetické bezpečnostné udalosti** na jedno miesto (inými slovami sa jedná o agregáciu logov z rôznych podporných aktív), následne ich vyhodnocovať a identifikovať kybernetické bezpečnostné incidenty. Pri vyhodnotení je potrebné **vyhľadávanie súvislostí** medzi viacerými logmi z rôznych aktív, kedy hovoríme o korelácií logov. Poslednými atribútmi, alebo funkciami, ktoré by mal takýto nástroj spĺňať je včasné **informovanie bezpečnostných rolí o vyhodnotení KBI** a možnosť **aktualizácie** vyhodnocovacích pravidiel pre zamedzenie nesprávneho vyhodnotenia KBI. [29] Tento obecný popis nástroja a jeho funkcionalít napovedá, že riešením spĺňajúcim tieto požiadavky sú napr. zariadenia s technológiou SIEM (angl. Security Information and Event Management). [40]

Okrem využívania spomínaného nástroja, je ďalšia povinnosť pracovanie s jeho výstupnými informáciami a využívať ich pre optimalizáciu jeho funkcionality, ako napr. zamedzenie false postive identifikácie KBI. [29]

§ 25 - Aplikačná bezpečnosť

V súvislosti s aplikačnou bezpečnosťou sú určené povinnosti pre **vykonávanie penetračných testov** u dôležitých aktív pri príležitosti ich zavádzania do prevádzky ale aj pri významnej zmene (popísané v kapitole § 11). Penetračné testy môžu napomôcť pre overenie odolnosti zabezpečenia pred kybernetickými hrozbami alebo

pre odhalenie zraniteľností a následne ošetriť zistené nedostatky napríklad vydanou bezpečnostnou aktualizáciou či dodatočnou konfiguráciou. Ďalej pri aplikačnej bezpečnosti je potrebné trvalé zaistenie aplikácií, informácií či transakcií pred neoprávnenou činnosťou, ktorou môže byť škodlivá činnosť zneužitím zraniteľností. [29]

§ 26 - Kryptografické prostriedky

Povinné osoby majú určenú povinnosť pri využívaní kryptografických prostriedkov určených pre ochranu aktív informačného a komunikačného systému **používať aktuálne odolné kryptografické algoritmy** a aj **dĺžky kryptografických kľúčov**. Pri ich výbere je potrebné brať do úvahy doporučenia Národního úřadu pro kybernetickou a informační bezpečnost.[29] Veľmi známou inštitúciou, ktorá vydáva doporučenia v oblasti kybernetickej bezpečnosti obsahujúce aj doporučené dĺžky kľúčov spolu s aktuálne bezpečnými kryptografickými algoritmami je NIST.

Ďalej pri správe kľúčov a certifikátov sú zákonom regulované subjekty povinné spĺňať požiadavky na systém, ktorý dokáže zaistiť generovanie, distribúciu, expiráciu ich platnosti, zneplatnenie či likvidáciu. V praxi sa jedná o systémy často uvádzané pod skratkou PKI (angl. Public Key Infrastructure). [41]

§ 27 - Zaisťovanie úrovne dostupnosti informácií

Povinné subjekty pri zavádzaní technických opatrení pre zaistenie úrovne dostupnosti je povinná zaistiť dostupnosť informačného prípadne komunikačného systému podľa, VKB § 15, riadenia kontinuity činností ale aj odolnosť takého systému voči KBI, ktoré by mohli znížiť jeho dostupnosť. [29] KBI incidenty obmedzujúce dostupnosť sú kybernetickými útokmi typu DoS (angl. Denial of Service) alebo DDoS (angl. Distrubuted DoS). Tým pádom môžeme konštatovať, že zákonom regulované subjekty majú zaviesť také technické opatrenia, ktoré sú cielené na spomínané typy útokov. [34]

Súvisiacou povinnosťou je zavedenie opatrení pre zaistenie dostupnosti dôležitých technických aktív ako takých. Pod takéto opatrenia môžu byť zahrnuté napríklad aj vyššie spomínané opatrenia v rámci fyzickej bezpečnosti, technológie UPS, alebo záložné elektrocentrály. [29]

§ 28 - Priemyslové, riadiace a obdobné špecifické systémy

Tento paragraf vychádzajúc z názvu pojednáva o priemyselných, riadiacich a iných špecifických systémoch, pri ktorých sú povinné subjekty povinné **pristupovať špecificky pri zavádzaní technických opatrení**. V praxi sa jedná napríklad o riadiace systémy elektrární, vodární alebo inej infraštruktúry, ktorej životnosť je vyššia

oproti bežným technickým aktívam, rádovo v desiatkach rokov. Nakoľko takéto zariadenia môžu využívať systémy a protokoly staršieho dáta bez technickej podpory a bezpečnostných aktualizácií, tak sú povinné subjekty povinné zavádzať vyčlenenie komunikačnej siete týchto systémov so samostatných segmentov siete mimo ostatnú infraštruktúru.[42] Teda z toho dôvodu je ďalšou povinnosťou zavádzať technické opatrenia pre obmedzenie fyzického prístupu k takýmto zariadeniam a ich infraštruktúre. [29]

Ako vyplýva z vyššie popísaného, takéto systémy sú náchylnejšie na rôzne hrozby z dôvodu možnej expirovanej technickej podpory (často označované pod skratkami EOL /End Of Life/ alebo EOSL /End Of Support Life/). Z uvedeného dôvodu musia povinné subjekty zaistiť obnovenie chodu týchto systémov po prípadnom kybernetickom bezpečnostnom incidente podľa vypracovaných bezpečnostných dokumentácií obnove po havárií (skr. DRP /Disaster Recovery Plan/).[29]

§ 29 - Digitálne služby

Vyhláška o kybernetickej bezpečnosti určuje povinnosť pre poskytovateľov digitálnej služby zavádzať **bezpečnostné opatrenia plynúce z vykonávajúceho nariadenia Komisie (EU) 2018/151**.[29] Týmto vykonávacím nariadením sú stanovené pravidlá plynúce zo smernice NIS I. Toto **nariadenie umožňuje** poskytovateľom digitálnych služieb **zavádzať organizačné a technické opatrenia**, pokiaľ ich považujú za vhodné podľa riadenia bezpečnostných rizík. [43]

Okrem už spomínaného vyhláška ukladá povinnosť hlásenia kontaktných údajov na národný CERT tím a hlásenie kybernetických bezpečnostných incidentov (spôsoby hlásení boli vyššie popísané).[29] Naviac okrem ostatných zákonom vytýčených subjektov, musí poskytovateľ digitálnej služby zohľadňovať pri posudzovaní možného významného dopadu incidentu (podľa nariadenia Komisie (EU) 2018/151 článku 3) napríklad množstvo fyzických a právnických osôb dotknutých takýmto incidentom, dĺžku trvania incidentu či zemepisný rozsah oblasti dotknutej incidentom (či sa incident týka aj iných členských štátov európskej únie z hľadiska poskytovania jeho služieb).

Naplnenie významu slovného spojenia významný dopad incidentu sa nariadením podľa článku 4 rozumie splnenie aspoň jednej situácie z nasledujúceho výpisu:

- nedostupnosť poskytovanej služby na dobu väčšiu ako 5 000 000 užívateľských hodín,
- incident viedol k strate integrity, autenticity či dôvernosti dát alebo súvisiacich služieb a bolo ovplyvnených viac ako 100 000 užívateľov naprieč európskou úniou,

- incidentom bolo vytvorené riziko pre verejnú bezpečnosť a ochranu, či stratu života,
- incidentom spôsobená škoda prekračujúca finančnú čiastku 1 000 000 EUR. [43]

3.3 Bezpečnostné politiky a bezpečnostné dokumentácie

V rámci VKB sú stanovené aj povinnosti pre oblasť stanovenia bezpečnostných politík a dokumentácií, konkrétne v **§ 30**. Spomenuté politiky a dokumentácie majú byť **pravidelne preskúmavané, upravované a aktualizované** podľa aktuálnej situácie. V skratke majú zahŕňať spôsoby, postupy a súčasný stav plnenia jednotlivých bezpečnostných opatrení, či už organizačné alebo technické opatrenia. [29] Všetky obsiahnuté oblasti bezpečnostných politík a dokumentácií podľa **VKB prílohy č. 5** sú zahrnuté v rámci prílohy B tejto diplomovej práce, z dôvodu ich rozsiahlosti.

Opodstatnenie nutnosti ich začlenenia do diplomovej práce súvisí s praktickou časťou a navrhovaným nástrojom pre podporu auditu kybernetickej bezpečnosti (jeho súčasťou je aj nahrávanie jednotlivých bezpečnostných politík a dokumentácií ako súčasť plnenia zákonných požiadaviek vychádzajúcich zo ZKB a VKB).

4 Právna úprava kybernetickej bezpečnosti v Českej republike de lege ferenda

V tejto, v poradí štvrtej kapitole diplomovej práce bude pojednávané o možných zmenách v oblasti právnej úpravy kybernetickej bezpečnosti, ktoré so sebou prináša smernica NIS2. Táto smernica má platnosť naprieč Európskou úniou a teda aj Česká republika podlieha povinnosti transponovania tejto smernice do národných právnych úprav.

Zmeny, ktoré prináša táto smernica sú značné a pri transpozícií smernice pristúpil Národní úřad pro kybernetickou a informační bezpečnost (ako ústredný správny orgán, v ktorého gescii je táto problematika) k prepracovaniu a vydaniu nového zákona o kybernetickej bezpečnosti spolu s vyhláškami. Aktuálne zamýšľaná podoba právnej úpravy kybernetickej bezpečnosti reflektujúca požiadavky NIS2 bola na začiatku tohto roku zverejnená pre odbornú verejnosť, ktorá mohla pripomienkovať aktuálne znenie, tzn. že môže dôjsť ešte k zmenám po zapracovaní doručených podnetov, taktiež aj v ďalšom kroku medzirezortného pripomienkovania.[44] Práve z tohoto dôvodu je názov kapitoly s dodatkom *de lege ferenda*, teda sa jedná o úvahy, ktoré sa môžu premietnuť do budúcej národnej legislatívy.

Súčasťou zadania diplomovej práce v rámci vytvoreného nástroja, ako pomôcky pre audity KB, je požiadavka na možnosť editácie priechodu súčasných zákonných povinností. Táto požiadavka bola splnená (viď kapitola 5.2.3) a tým je nástroj pripravený aj na legislatívne zmeny súvisiace práve so smernicou NIS2.

4.1 Smernica NIS2

Nová smernica NIS2, celým názvom Smernica Európskeho parlamentu a Rady (EU) 2022/2555, o opatreniach k zaisteniu vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii (nástupca vyššie spomínanej Smernice Európskeho parlamentu a Rady (EU) 2016/1148 (NIS)) bola publikovaná dňa 27. decembra 2022 v Úradnom vestníku Európskej únie a ku dňu 16. januára 2023 sa stala smernica platnou. Aktuálne povinnosti plynú len pre členské štáty pre prevedenie (transpozíciu) NIS2 do národného práva. Určený časový rámec na **transponovanie** európskej smernice **do národnej legislatívy** je stanovený na 21 mesiacov od začiatku jej platnosti, t.j. **do 16. októbra 2024**. [45]

Za najzásadnejšiu časť smernice NIS2 je možné považovať článok 21, ktorý bude mať najväčší dopad na zákonom regulované subjekty. Tieto subjekty budú musieť prijať rôzne opatrenia k riadeniu bezpečnostných rizík, ktorým sú vystavené ich siete a informačné systémy s poskytovanými službami. Vďaka opatreniam budú

tieto subjekty predchádzať, prípadne minimalizovať dopady bezpečnostných rizík na spotrebiteľov. Dôležité je podotknúť, že článok 21 (aj celkovo smernica NIS2) **stanovuje požadovaný štandard** týkajúcich sa opatrení a právna úprava na úrovni štátov môže byť prísnejšia, avšak v rámci jednotného medzinárodného prístupu nie je žiadúce aby národná legislatíva bola z podstaty veci prísnejšia, než požiadavka smernice. [45]

Smernica rozoznáva dva druhy regulovaných subjektov (podľa článku 3), konkrétne základné (essential) subjekty a dôležité (important) subjekty. Pod **základné subjekty** môžu spadať typicky odvetvia energetiky (napr. elektrina, zemný plyn), dopravy (napr. letecká, železničná), bankovníctva, odpadových vôd, verejnej správy, prevádzkovatelia DNS, kritické subjekty a iné (uvedené v prílohe I k NIS2). Tieto subjekty zo spomenutých odvetví musia spĺňať definíciu veľkých podnikov, ktorá je stanovená v rámci doporučenia Komisie (EU) 2003/361/EC (tieto budú vždy regulované podľa režimu essential).[45] Dôležité je zdôrazniť, že v súčasnej dobe spadá pod ZKB niekoľko stoviek regulovaných subjektov a po novelizácii legislatívy bude spadať rádovo niekoľko tisíc regulovaných subjektov, teda je **očakávaný výrazný nárast počtu povinných subjektov** spadajúcich pod ZKB. [44]

Za **dôležité subjekty** môžu byť potom typicky považované subjekty odvetví z prílohy I, ktoré na rozdiel od základných subjektov sú strednými podnikmi. Ďalej podľa prílohy II môžu spadať (veľké aj stredné podniky podľa spomínaného doporučenia) do dôležitých subjektov napríklad odvetvia poštových služieb, chemického priemyslu, potravinárstva či výskumu. V krátkosti na vysvetlenie - dôležitými subjektmi budú podniky poskytujúce aspoň jednu službu z príloh smernice (prílohy I a II) a zároveň budú stredne veľkým alebo veľkým podnikom (50 a viac zamestnancov, prípadne ich ročný finančný obrat je aspoň 10 miliónov EUR). [45]

Oblasť oznamovacích povinností pokryla NIS2 článkom 23, v ktorom je stanovená rovnaká povinnosť pre základné aj dôležité subjekty **hlásiť zaznamenané významné incidenty**. Takýmto incidentom sa rozumie podľa čl. 23 odst. 3 incident, ktorý mohol spôsobiť alebo spôsobil finančnú ujmu či narušenie prevádzkovaných služieb závažným spôsobom a ďalej mohol spôsobiť alebo spôsobil hmotnú či nehmotnú ujmu na strane fyzických, prípadne právnických osôb. [45]

Smernica NIS2 apeluje na súčasnú dobu a potrebu automatizácie v oblasti hlásenia kontaktných údajov (podľa čl. 27) a hlásenia incidentov (podľa čl. 23). Pre tieto oznamovacie povinnosti smernica doporučuje zriadenie **jednotného kontaktného miesta**. [45]

Oblasť dohľadu týkajúcu sa základných a dôležitých subjektov upravuje smernica v článkoch 32 a 33. Tento dohľad spočíva najmä v kontrole plnenia opatrení k riadeniu kybernetických bezpečnostných rizík (čl. 21) a oznamovacích povinností (čl. 23) a to ako *ex ante* proaktívna kontrola (vyšší režim), tak aj ex post reaktívna

kontrola (nižší režim) za rôznych okolností ako napríklad pravidelné bezpečnostné audity, auditom *ad hoc*, pričom môžu byť vykonávané rozličnými spôsobmi napríklad aj externistami. Túto problematiku približuje recitál 122 smernice NIS2. Zaujímavou novinkou je individuálna zodpovednosť jednotlivcov jednajúcich za regulované subjekty v prípade nedodržania ich povinností. V prípade základných subjektov je možnosť **odobratia certifikácie** alebo licencie udelenej danej organizácii až **uloženie dočasného zákazu výkonu riadiacich funkcií** ako donucovací prostriedok. [45]

Vychádzajúc z názvu smernice NIS2 je ďalším nespochybniteľným cieľom **zlepšenie zdieľania informácií** o kybernetickej bezpečnosti či už medzi štátmi naprieč Európskou úniou alebo aj v rámci štátov. Práve tejto problematike je venovaný článok 29, ktorý hovorí o vytvorení platformy na dobrovoľné zdieľanie informácií o KB, kybernetických hrozbách či pracovných postupov na mitigovanie zaznamenaných hrozieb a pod. [45]

4.2 Návrh právnej úpravy

V rámci predchádzajúcej kapitoly boli predstavené niektoré z požiadaviek smernice NIS2, ktoré musia byť premietnuté (spolu s ďalšími požiadavkami) do právnej úpravy na úrovni štátu.

V súčasnom znení ZKB sú povinné osoby rozdelené do niekoľkých podkategórií, avšak po zohľadnení smernice NIS2 sú tieto povinné osoby centralizované do jedného typu povinnej osoby, nesúcej názov poskytovateľ regulovanej služby.

Povinné osoby, po novom poskytovatelia regulovaných služieb budú podľa návrhu rozdelení do dvoch kategórií povinností: vyšších a nižších povinností. Ako vychádza z pomenovania, na organizáciu spadajúcu pod vyššie povinnosti (podľa NIS2 základné subjekty) sú kladené vyššie požiadavky a zase naopak na organizáciu spadajúcu pod nižšie povinnosti (podľa NIS2 dôležité subjekty) sú kladené nižšie požiadavky. Na rozdiel od súčasného znenia zákona môže jeden subjekt alebo organizácia aplikovať len jeden druh povinností. Pre prípady súčasného naplnenia režimov vyšších aj nižších povinností budú aplikované len vyššie povinnosti naprieč všetkými regulovanými službami vyskytujúcimi sa v organizácii. [44]

Opatrenia k riadeniu kybernetických bezpečnostných rizík (NIS2 čl. 21) sú premietnuté do dvoch znení VKB. Prvou je vyhláška o bezpečnostných opatreniach poskytovateľov regulovanej služby v režime vyšších povinností, ktorá do veľkej miery obsahuje ekvivalentné povinnosti ako VKB súčasného znenia. Novinkami sú napríklad: povinnosti vrcholového vedenia, dĺžky hesiel pre technické aktíva, vykonávanie skenu zraniteľností alebo konkrétnejšie spôsoby vykonávania penetračného testovania. Druhá vyhláška o bezpečnostných opatreniach poskytovateľa regulovanej služby

v režime nižších povinností ukladá povinnosti, ktoré sú jednoduchšie. Na prvý pohľad je zrejmé, že podoba s prvou spomínanou navrhovanou vyhláškou nie je veľká a v konečnom dôsledku sa pracuje s nižšími nárokmi na opatrenia. Ďalej na rozdiel od vyhlášky pre režim vyšších povinností je § 4 venovaný zaisťovaniu minimálnej úrovne kybernetickej bezpečnosti. [44]

Hlásenie incidentov od poskytovateľov regulovanej služby pre režim vyšších povinností sa vyznačuje povinnosťou hlásenia akéhokoľvek kybernetického bezpečnostného incidentu obratom po detekcii. Povinným subjektom s režimom nižších povinností je uložená povinnosť hlásenia len KBI, ktoré sú organizáciou považované za významné. Povinnosti týkajúce sa hlásenia incidentov sú premietnuté vo vyššie spomínaných navrhovaných vyhláškach. [44]

NIS2 operovala s nástrojom na hlásenie kontaktných údajov a incidentov, ktorý Národní úřad pro kybernetickou a informační bezpečnost zapracoval do platformy Portál NÚKIB. Bližšie podrobnosti a špecifikácie sú spracované v rámci návrhu úplne novej vyhlášky o Portálu NÚKIB. [44]

Spôsob kontrol plnenia povinností podľa navrhovanej právnej úpravy bude rôzny pre subjekty s vyššími povinnosťami, alebo nižšími povinnosťami. U poskytovateľov regulovaných služieb s režimom vyšších povinností nedochádza takmer k žiadnym zmenám a teda kontroly budú vykonávané v proaktívnom režime pracovníkmi NÚKIB z oddelenia kontroly. Poskytovatelia regulovaných služieb s nižším režimom povinností majú podliehať kontrolám vykonávaných pracovníkmi NÚKIBu, avšak tieto kontroly nebudú vykonávané v takej miere rozsahu (ako v prípade poskytovateľov regulovaných služieb v režime vyšších povinností) a až keď vyhodnotí NÚKIB potrebu zahájenia kontroly za určitých dôvodov (napr. na základe obdržania podnetu alebo pri opakovaní výskytu významných kybernetických bezpečnostných incidentov). Spomenuté návrhy zakomponovania do národnej legislatívy nie sú charakterom interné informácie Národního úřadu pro kybernetickú a informační bezpečnost, ale informácie, ktoré sú komunikované úradom voči partnerom a odbornej verejnosti.

Opäť je však nutné dodať a zdôrazniť, že akékoľvek zo spomenutých navrhovaných riešení zapracovania smernice do nových zákonov a spomenutých vyhlášok môžu podliehať zmenám, pričom musia byť dodržané minimálne požiadavky stanovené smernicou NIS2.

5 Nástroj pre podporu auditu kybernetickej bezpečnosti

V rámci praktickej časti diplomovej práce bol navrhnutý nástroj, ktorý má pomôcť povinným subjektom vytýčených zákonom pre lepšie zorientovanie v spleti povinností vymedzených legislatívou ale aj auditorom pred zahájením auditu pre ucelenejší pohľad na plnenie povinností zo strany auditovaného subjektu. Nástroj vychádza najmä z pomôcky k auditu bezpečnostných opatrení podľa zákona o kybernetickej bezpečnosti, ktorý bol zverejnený ako podporný materiál na webových stránkach NÚKIBu. Vyvíjaný nástroj prevedie užívateľov radom otázok týkajúcich sa bezpečnostných opatrení, prípadne iných zákonom stanovených povinností, ktoré vyplývajú z Vyhlášky o kybernetickej bezpečnosti či Zákona o kybernetickej bezpečnosti. Pri každom jednotlivom opatrení je užívateľ vyzvaný pre zadanie súčasného plnenia daného opatrenia s pridaním relevantnej dokumentácie. Vďaka programu užívatelia nemusia zložito hľadať povinnosti vo VKB pre ich konkrétny typ systému. Výstupom tohto nástroja je sumarizácia plnenia bezpečnostných opatrení spolu s vloženými dokumentáciami v rámci jedného celistvého dokumentu.

5.1 Motivácia

Motivácia pre vytvorenie nástroja vychádza z faktu, že v blízkej dobe bude vydaný nový Zákon o kybernetickej bezpečnosti spolu s vykonávacím právnym predpisom, Vyhláškou o kybernetickej bezpečnosti, ktoré budú zohľadňovať požiadavky smernice Európskeho parlamentu a Rady Európskej únie o opatreniach k zaisteniu vysokej spoločnej úrovne kybernetickej bezpečnosti v Európskej únii, v skrátenom názve tzv. smernica NIS2. Práve v súvislosti s NIS2 je očakávaný nárast zákonom regulovaných subjektov približne 15 násobný (cca. 6000 subjektov), ale nie všetky z nich budú podliehať legislatívnym auditom a kontrolám kybernetickej bezpečnosti. [44]

Je nutné podotknúť, že práve na tieto zmeny v právnej úprave KB je vytvorený nástroj taktiež pripravený. Bližšie vlastnosti tohto nástroja budú priblížené v rámci nasledujúcich podkapitol.

5.1.1 Ekvivalentné nástroje na trhu

Pred samotným návrhom funkcionality tohto nástroja bol preskúmaný trh v oblasti pomôcok alebo iných ekvivalentných nástrojov pri auditoch kybernetickej bezpečnosti. Dohľadávanie nebolo náročné, nakoľko sa podarilo nájsť iba dva druhy pomôcok s obdobným zameraním.

Prvou z nich je tzv. VKB checklist existujúci vo forme tabuľky v MS Excel dostupný na stránkach NÚKIBu (tabuľka využitá ako základný podklad pre konvertovanie povinností do súboru *questions.json* v rámci diplomovej práce). Prakticky sa jedná o prepis povinností vyplývajúcich zo ZKB a VKB, ku ktorým si môže užívateľ vložiť poznámky. Žiadnou inou funkcionalitou nedisponuje. [46]

Druhým a posledným nájdeným nástrojom je v tomto prípade praktická časť diplomovej práce študenta (forma webovej stránky), ktorá je primárne zameraná na hodnotenie aktív, správu hrozieb, zraniteľností. Teda táto pomôcka môže slúžiť najmä povinným subjektom, ktoré sa stali v nedávnej dobe povinnými zaviesť legislatívne povinnosti a bezpečnostné opatrenia. [47]

Najbližšou nájdenou pomôckou je práve prvá nájdená. Praktická časť tejto diplomovej práce na rozdiel od nej navyše pridáva možnosť priloženia relevantných súborov, centralizovanie plnených povinností spolu s priloženými súbormi, do jedného uceleného celku, do jedného reprezentatívneho, intuitívne a prehľadne členeného súboru vo formáte PDF. Vytvorený nástroj je k dispozícií vo forme programu s grafickým užívateľským rozhraním s vypĺňaním jednotlivých otázok a zákonných povinností v prehľadnejšej forme ako v spomínanom prípade. Nespornou výhodou vytvoreného nástroja je možnosť adaptácie nielen pre zákonom vytýčené osoby, ale aj pre iné organizácie, ktoré majú potrebu výkonu interných auditov, prípadne iných auditov (napr. ISO normy).

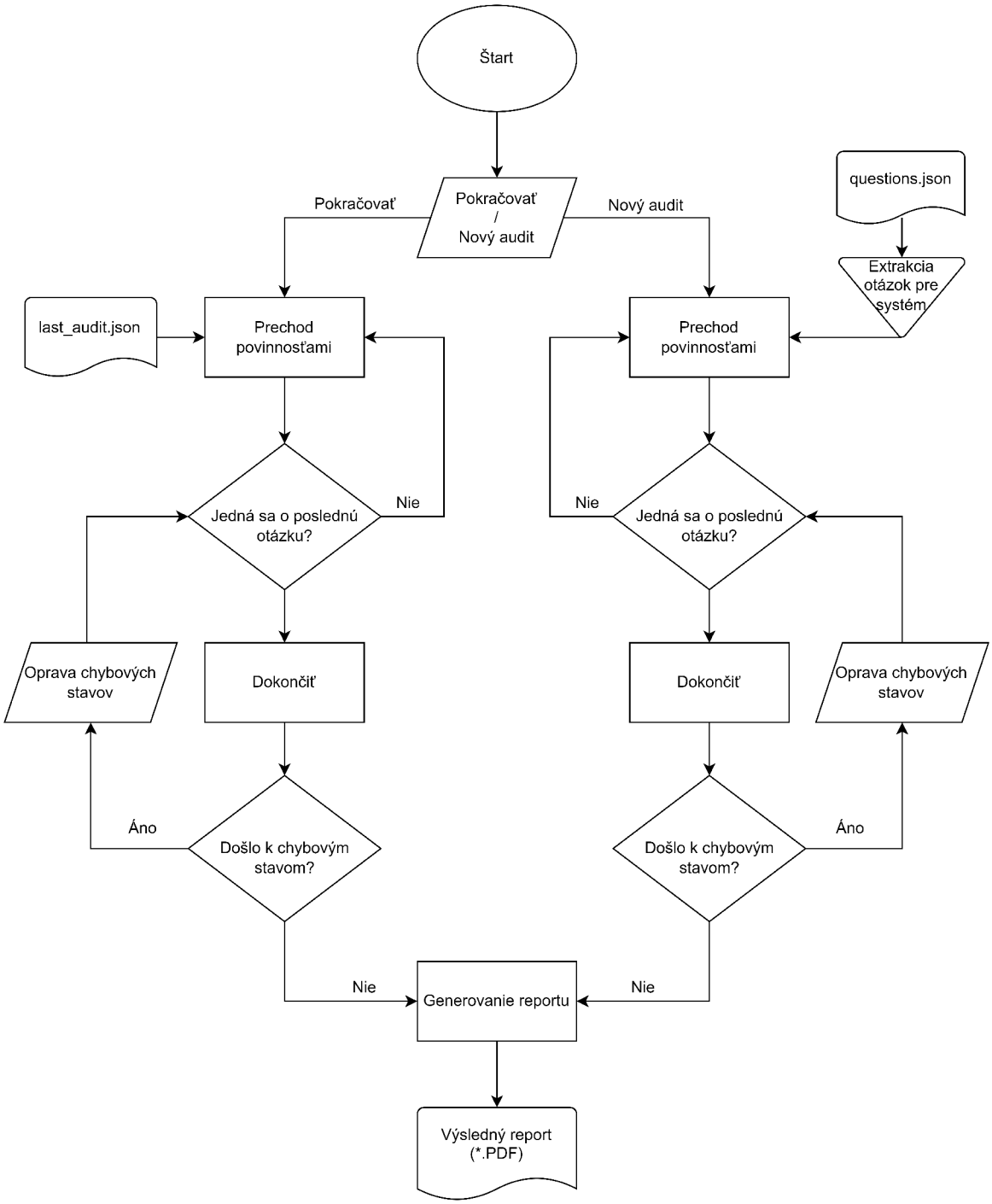
5.2 Programové riešenie

Nástroj bol vytvorený v programovacom jazyku Python s grafickým užívateľským rozhraním (skr. GUI), ktorý je spustiteľný na operačných systémoch platformy Microsoft Windows. Nástroj sa skladá z niekoľkých súborov, ktoré spolu tvoria funkčný celok:

- *main.py*,
- *menu.py*,
- *question.py*,
- *settings.py*,
- *listbox.py*,
- *pdf.py*,
- *questions.json*,
- *default_questions.json*,
- *internal_questions.json*.

Pre vytvorenie grafického užívateľského rozhrania (skr. GUI) bola použitá knižnica Tkinter. GUI je členené do troch častí: hlavné menu, nastavenia a prechod povinnosťami.[48]

Hlavná funkcionalita tohto nástroja je vyobrazená na vývojovom diagrame (obr. 5.1)



Obr. 5.1: Vývojový diagram hlavnej funkcionality nástroja

5.2.1 Popis jednotlivých súborov

Táto podkapitola v stručnosti popisuje programové riešenie jednotlivých častí programu.

Súbor main.py

- Implementácia triedy AuditApp ako spustiteľnej časti,
- definovanie parametrov hlavného okna,
- definovanie metódy switch_frame, ktorá otvára ďalšie okná (PageQuestion - prechod otázok, PageSettings - nastavenia).

Súbor menu.py

- Implementácia triedy PageMenu - hlavné menu,
- rozloženie tlačidiel Pokračovat, Nový audit . . . (podľa vytvorených kategórií v časti Nastavenia) , Nový interní audit, Nastavení (viď obr. 5.2,
- načítavanie otázok zo súborov questions.json, internal_questions.json, lastaudit.json (dešifrovanie súboru pomocou knižnice Fernet). [50]

Súbor question.py

- Implementácia triedy PageQuestion - prechod otázok,
- rozloženie tlačidiel, labelov, progress baru, comboboxu (viď obr. 5.5 a priradenie funkcionality pre jednotlivé prvky okna,
- metóda save_progress pre uloženie aktuálne vyplnených otázok a ich zápis do súboru last_audit.json,
- metódy next_category a prev_category slúžiace na rýchlejší prechod otázok (preskakovanie na ďalší alebo predchádzajúci paragraf),
- metóda finish_question slúžiaca pre kontrolu chybových stavov (nezadaný názov systému, rozpracovaná otázka bez vloženého popisu, neexistujúca cesta pridaného súboru), volanie metódy na generovanie výstupnej správy, zadanie umiestnenia generovanej výstupnej správy a následný prechod do okna hlavného menu.

Súbor settings.py

- Implementácia triedy PageSettings - nastavenia,
- rozloženie tlačidiel možných nastavení (viď obr. 5.3),
- metóda checkResetQuestion s pop-up message boxom pre overenie, či sa jedná o vedomé obnovenie pôvodných otázok (prepísanie súboru questions.json súborom default_questions.json).

Súbor listbox.py

- Implementácia triedy MultipleScrollingListbox - okná úpravy otázok a kategórií,
- rozloženie tlačidiel a stĺpcov s parametrami, kategóriami a textom otázok (viď. obr. 5.4),
- metódy delete_question, delete_all a add_question pre úpravu otázok,
- metóda close pre kontrolu vyplnenia otázok a ich uloženie do súboru questions.json (pri úprave otázok pre interné potreby uloženie do súboru internal_questions.json).

Súbor pdf.py (metóda generateReport)

- Nastavenie osí x a y pre rozloženie textu na stranách,
- generovanie titulnej strany s názvom a typom auditovaného systému,
- generovanie obsahu vyplnených otázok s klikateľnými odkazmi,
- generovanie stavu jednotlivých vyplnených otázok (v prípade priloženého súboru aj s klikateľným odkazom),
- generovanie zoznamu priložených súborov,
- zlúčenie všetkých generovaných strán.

Súbory json

- questions.json - súbor s aktuálnymi povinnosťami plynúcimi zo zákona,
- default_questions.json - súbor s pôvodnými povinnosťami plynúcimi zo zákona,
- internal_question.json - súbor s povinnosťami pre interný audit.

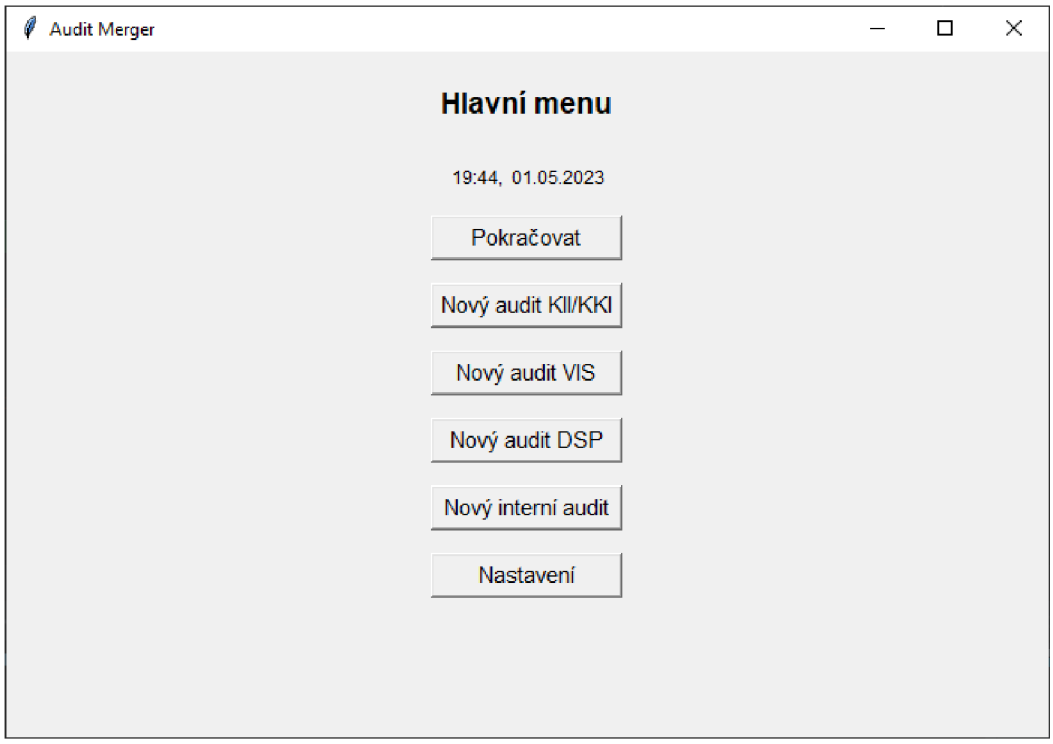
5.2.2 Hlavné menu

Po spustení programu sa otvorí úvodné okno s hlavným menu, kde sa užívateľovi zobrazí niekoľko ikon, resp. možností pre prácu s nástrojom (viď 5.2).

Tlačidlo nový audit

Voľba **Nový audit** predstavuje spustenie hlavnej časti programu, ktorý prevedie užívateľa (auditovaného alebo auditora) setom zákonných povinností, a bezpečnostných opatrení vyplývajúcich z VKB (bude nižšie popísané). Tlačidiel nový audit je hneď niekoľko z dôvodu rôznych povinností pre **rozdielne typy** zákonom regulovaných **subjektov a** ich typy **systémov**. Konkrétne sa (momentálne) jedná o (viď obr. 5.2):

- **KII/KKI** - systém kritickej informačnej alebo komunikačnej infraštruktúry,



Obr. 5.2: Hlavné menu

- **VIS** - významný informačný systém,
- **DSP** - poskytovateľ digitálnej služby.

Po kliknutí na nový audit sú načítané vyselektované povinnosti subjektu pre daný typ systému zo súboru *questions.json*, následne je spustená hlavná časť programu, v ktorej užívateľ prechádza priradenými povinnosťami. Týmto spôsobom je identifikovaný auditovaný systém povinného subjektu, čím je ovplyvnený výber priradených povinností, ktoré boli podrobne rozobraté v kapitole 3.

Tlačidlo **nový interný audit** je oproti trom predchádzajúcim špecifický. Prvotná myšlienka určenia tohto nástroja bola len pre uľahčenie auditovania, prípadne kontroly plnenia zákonných povinností z oblasti kybernetickej bezpečnosti. Avšak pri tvorbe bola zahrnutá možnosť využitia tohto nástroja pre rôzne typy auditov. Ako vychádza z nápisu tlačidla, tak sa môže jednať napríklad o audit podľa interných pravidiel organizácie, o audity požiadaviek na ISMS podľa spomínanej normy ČSN ISO/IEC 27001, o audity opatrení informačnej a kybernetickej bezpečnosti podľa novo vydanej normy ČSN ISO/IEC 27002, alebo o audity kybernetickej bezpečnosti podľa pripravovanej normy ČSN ISO/IEC TS 27100 (v súčasnosti sa jedná o predbežnú normu, ktorá zahŕňa len prehľad a pojmy v oblasti KB) . Možnosť pridania otázok pre interný audit je v rámci nastavení.

Tlačidlo pokračovať

Berúc na vedomie početnosť zákonných povinností bola do nástroja naimplementovaná možnosť uloženia súčasného stavu, čím je užívateľovi umožnené pokračovať v zadávaní plnenia povinností a teda nie je nutné vyplniť všetky povinnosti v rámci jedného spustenia nástroja.

Po zvolení tlačidla **pokračovať** je spustená hlavná časť programu s uloženými stavmi z predchádzajúcej spustenej relácie (nad tlačidlom je vyobrazený dátum a čas posledného uloženia). Informácie z posledného uloženého auditu sa nachádzajú v súbore *last_audit.json*. Obsiahnuté informácie v rámci súboru *last_audit.json* sú otázky spolu so zadaným stavom, vyplneným popisom, cesta k priloženému súboru a zadaný názov systému.

Vzhľadom na citlivý charakter otázok je súbor *last_audit.json* šifrovaný prostredníctvom knižnice Fernet. Fernet využíva symetrické šifrovanie, konkrétne algoritmus AES v CBC móde s dĺžkou kľúča 128 bitov.[50] Nakoľko nástroj predstavuje aplikáciu na lokálnom počítači, tak dôležitým aspektom zabezpečenia vkladaných údajov je bezpečnosť samotného počítača (napr. šifrovanie pevného disku BitLocker).

5.2.3 Nastavenia

Do časti nastavení sa užívateľ dostane prostredníctvom tlačidla v hlavnom menu (viď. obr. 5.2)

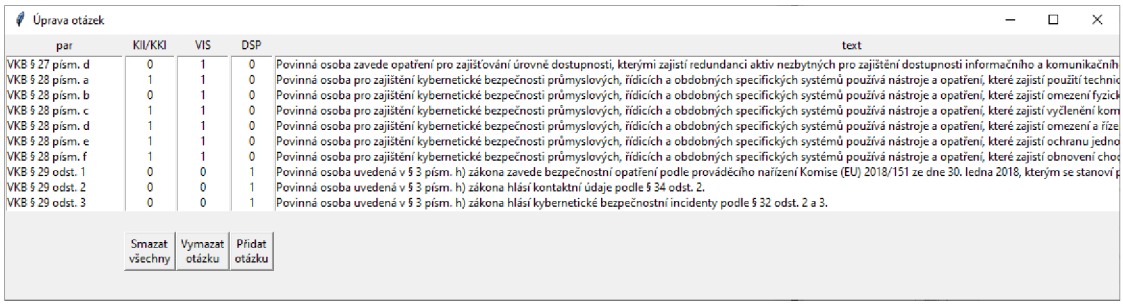
Obr. 5.3: Nastavenia nástroja

V rámci nastavení nástroja má užívateľ niekoľko možností modifikácie, resp. prispôsobenia.

Úprava otázok vyplývajúcich zo zákona

Po kliknutí na prvé tlačidlo (obr. 5.3) je otvorené okno so všetkými zákonnými povinnosťami. Ako bolo vyššie spomenuté, tak tieto povinnosti vychádzajú z tzv. *VKB checklistu*.[46] V prvom rade bolo potrebné tieto povinnosti preformátovať do podoby akceptovateľnej programom. V tejto súvislosti bol vytvorený script, ktorý prekonvertoval súbor formátu *xslx* (formát Microsoft Excel) do formátu *json*.

V okne vyobrazenom na obr. 5.4 môže užívateľ modifikovať, pridať, odobrať a vymazať všetky otázky. **Modifikovanie existujúcej otázky** je možné pomocou dvojkliku na ňu, zapísaním zmien a následným potvrdením tlačidlom Enter. **Pridanie otázky** sa vykonáva pomocou tlačidla Pridať otázku. Pridanie otázky bez predchádzajúceho označenia akejkoľvek otázky pridá nevyplnený riadok na koniec zoznamu, ktorý užívateľ modifikuje pomocou dvojkliku a potvrdením klávesou Enter. Pridanie otázky medzi existujúce je možné jej označením a zakliknutím tlačidla pridať, čo pridá otázku pod užívateľom zvolený riadok. **Vymazávanie jednotlivých otázok** je umožnené po voľbe otázky a kliknutím na tlačidlo vymazať. Pre prípad rozsiahlych legislatívnych zmien bolo pridané tlačidlo, ktorým je možné **vymazať všetky otázky**. Po tejto voľbe je nutné potvrdiť vo vyskakovacom pop-up okne túto voľbu, aby nedošlo k nechcenému vymazaniu všetkých otázok.



Obr. 5.4: Modifikovanie zákonných povinností

Pri pridávaní alebo modifikácii otázky musí užívateľ vyplniť všetky atribúty otázok, ktorými sú paragraf (prípadne iný parameter), relevantnosť pre systém (vyplnenie stĺpcov KII/KKI, VIS, DSP číslicou 0 a 1) a textové znenie povinnosti. O prípadnom nevyplnení všetkých atribútov otázky bude užívateľ oboznámený vyskakovacím oknom (pri prázdnom atribúte nie je umožnené užívateľovi zavrieť okno).

Úprava kategórií

V okne s úpravami kategórií je užívateľovi umožnené pridávať a odoberať kategórie pre zákonné povinnosti. V defaultnom nastavení sú tri: KII/KKI, VIS a DSP.

Pridávanie a odoberanie kategórií má logiku ovládania rovnakú ako v rámci okna určeného na úpravu otázok vyplývajúcich zo zákona.

Od počtu kategórií sa odvíjajú ikony Nový audit v hlavnom menu. V tomto prípade určujú kategórie typ regulovaného systému.

Úprava otázok pre interné potreby

Ďalšou možnosťou týkajúcou sa nastavení je úprava otázok pre interné potreby. V princípe sa jedná o novo otvorené okno, v rámci ktorého má užívateľ možnosť pridávať otázky podľa individuálnych potrieb obdobným spôsobom ako pri otázkach vyplývajúcich zo zákona. Spôsob pridávania a odoberania otázok je totožný s otázkami vychádzajúcimi z legislatívy.

Na rozdiel od otázok vyplývajúcich zo zákona nie je v tomto prípade rozdelenie otázok do kategórií a nemusí užívateľ vyplniť stĺpec s parametrami otázky (resp. zákonom a paragrafom v prípade zákonných otázok). Tieto otázky sú uložené v separátnom súbore *internal_question.json*.

Obnovenie pôvodných nastavení

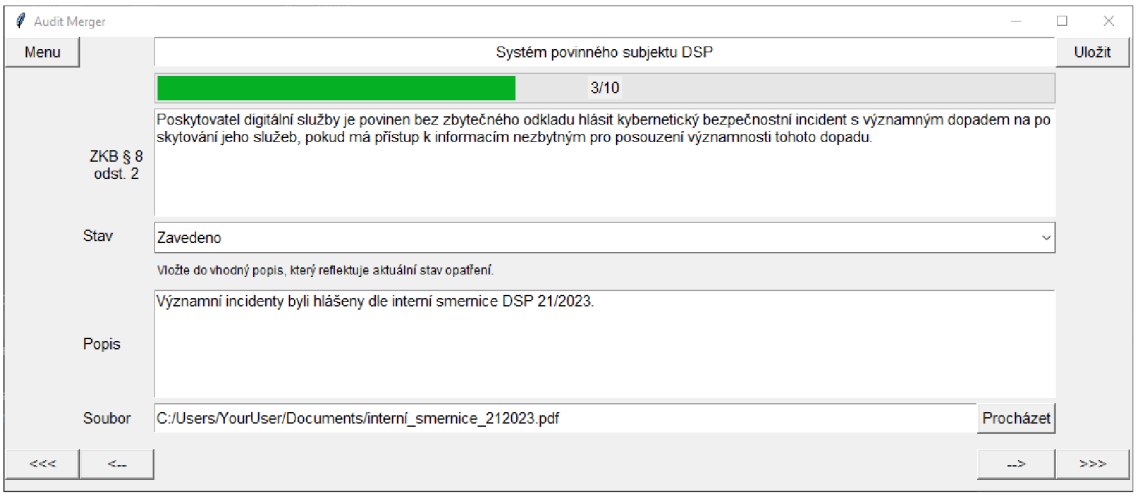
Poslednému tlačidlu v nastaveniach je priradená funkcionalita obnovy pôvodných nastavení pre otázky vyplývajúce zo zákona. Túto obnovu je potrebné potvrdiť v pop-up okne, kedy je následne prepísaný súbor *questions.json* zo súboru *default_question.json*. Výsledkom obnovy je nahranie pôvodných otázok s povinnosťami spolu s rozdelením do kategórií, pre prípady nechcenej zmeny, prípadne výmazu v okne otázok alebo kategórií.

5.2.4 Hlavná časť nástroja - prechod otázkami, resp. povinnosťami

Do hlavnej časti nástroja sa dostane užívateľ, ako bolo vyššie popísané, voľbou nový audit alebo pokračovať. Hlavná časť nástroja predstavuje prechod zákonom stanovených povinností, alebo bezpečnostných opatrení týkajúcich sa vybraného typu systému (KII/KKI, VIS, DSP alebo iné v prípade voľby interného auditu).

Vo vrchnej časti okna je možné vidieť pole pre uvedenie názvu auditovaného systému (obr. 5.5), ktoré defaultne obsahuje popis "Názov systému". Názov systému sa zadáva pomocou dvojkliku na pole s názvom systému a následné potvrdenie klávesou enter.

Pod názvom systému sa nachádza pole zobrazujúce pomer vyplnených povinností tzv. progress bar spolu s poradovým číslom aktuálnej otázky.



Obr. 5.5: Hlavná časť nástroja

Vo vyobrazenom okne je ďalej vypísaná **zákonná povinnosť** (alebo otázka - interný audit) spolu so zákonom a zodpovedajúcim paragrafom.

K danej povinnosti užívateľ zvolí stav aktuálneho plnenia prostredníctvom rolovacej ponuky - *Comboboxu*. Možné voľby stavu sú:

- nezavedené,
- zavedené,
- v procese zavádzania,
- neaplikovateľné.

Po zvolení stavu je interaktívne zobrazená **nápoveda**, ktorá navádza užívateľa akým spôsobom je potrebné vyplniť nasledujúci popis plnenia povinnosti.

Do časti **popis** užívateľ uvádza popis k súčasnému stavu plnenia povinnosti, ktorý bližšie popisuje aktuálne riešenie, spôsob zavedenia bezpečnostného opatrenia alebo popis aký súbor vložil do príloh.

Poslednou možnou funkciou je **vloženie súboru**. Vloženie súboru podporuje nahranie typy súboru striktne len vo formáte PDF. Nahraným relevantným dokumentom môže byť napríklad bezpečnostná dokumentácia, topológia siete, hodnotenie aktív, analýza rizík, konfiguračné súbory či výstupné reporty z penetračných testov. Vloženie súboru sa realizuje pomocou tlačidla **prehľadávať**.

Po vyplnení relevantných informácií k aktuálnemu plneniu povinnosti môže užívateľ prejsť na ďalšie (prípadne predchádzajúce) otázky alebo uložiť aktuálne vyplnenie otázok.

Prechod medzi jednotlivými otázkami sa vykonáva pomocou tlačidiel so symbolmi "− >" , "< −". Tieto tlačidlá disponujú aj kontextovou nápovedou, pre lepšie pochopenie funcionality. Ďalej bola implementovaná možnosť **prechodu medzi paragrafmi** pomocou tlačidiel so symbolmi ">>>" , "<<<"(taktiež s kon-

textovou nápovedou), pre rýchlejší prechod na povinnosti týkajúce sa konkrétnych paragrafov (využiteľné pri audite konkrétne vytýčených paragrafov).

Po prejdení na poslednú otázku sa zobrazí **tlačidlo dokončiť**, ktorým bude následne vygenerovaná súhrnná správa o aktuálnom plnení povinností subjektu (zákonných, interných alebo iného druhu v závislosti vyplnených otázok pre interné potreby), ktorá bude priblížená v nasledujúcej podkapitole. Pred samotným vygenerovaním reportu prebieha kontrola chybových stavov. Chybovými stavmi sa rozumie:

- **nezadaný popis** plnenia povinnosti - pokiaľ je zvolený stav a nezadaný popis, tak v pop-up okne je užívateľ upozornený o potrebnom dodatočnom vyplnení, zároveň je zobrazená daná neúplne vyplnená otázka,
- **neexistujúci súbor** - užívateľ je upozornený na neplatnú cestu k zvolenému súboru (pop-up okno), pri neexistujúcom súbore neprebehne vygenerovanie výstupného reportu,
- **nezadaný názov** auditovaného **systému** - užívateľ je upozornený pop-up oknom na potrebné vyplnenie názvu systému.

Po overení chybových stavov sa otvorí dialógové okno pre uloženie reportu, kde je potrebné zadať názov súboru a jeho umiestnenie.

5.2.5 Súhrn vyplnených povinností - report

Ako bolo uvedené v predchádzajúcej kapitole, výsledný súhrn vyplnených povinností je generovaný prostredníctvom tlačidla dokončiť po prejdení na poslednú otázku.

Generovanie reportu je vykonávané v python súbore *pdf.py* pomocou knižnice **ReportLab**.[49]

Samotné generovanie pozostáva z niekoľkých častí. Prvou časťou je vytvorenie titulnej strany, na ktorej sa nachádza názov zadaného systému, typ auditu (KII-/KKI, VIS, DSP alebo interný audit) a dátum vygenerovania súboru. Ďalšou časťou je obsah jednotlivých povinností spolu so stranou v dokumente vrátane klikateľných odkazov, ktoré presmerujú užívateľa priamo na konkrétnu povinnosť. Všetky vyplnené povinnosti sú rozdelené per strana, kde sa nachádza znenie povinností, užívateľom zadaný stav, popis jej plnenia a klikateľný odkaz na priložený súbor. Za všetkými otázkami sa nachádza strana oddeľujúca otázky a priložené súbory s nasledujúcim obsahom jednotlivých priložených súborov.

Výsledkom je prehľadný dokument obsahujúci súhrnnú správu plnených zákonných povinností legislatívou regulovaných subjektov. Dokument môže slúžiť ako pomôcka pre auditorov z Národního úřadu pro kybernetickou a informační bezpečnost, ktorý bude vytvorený subjektom, u ktorého bude vykonávaný audit alebo kontrola

v oblasti informačnej bezpečnosti. Za pomoci tohto dokumentu budú mať zosumarizované krátke popisy k plneniam spolu s relevantnou dokumentáciou. Ďalej môže tento dokument pomôcť pri rozhodovaní sa a výbere vhodného spôsobu vzorkovania ako bolo popísané v kapitole 2.1.1. Za značný prínos je možné pokladať priradenie relevantného dokumentu k určitej povinnosti, bez potreby zdĺhavého hľadania dokumentu v adresárovej štruktúre sprístupnenej zákonom regulovaným subjektom, ktorý je často neintuitívne (pre nezainteresované osoby) pomenovaný internými spôsobmi organizácie.

Záver

Diplomová práca sa zameriavala na priblíženie auditov v oblasti kybernetickej bezpečnosti. V teoretickej časti bol vysvetlený pojem kybernetickej bezpečnosti, kde boli vysvetlené dôležité pojmy spolu s najčastejšie aplikovaným princípom pre dosiahnutie kybernetickej či informačnej bezpečnosti. Ďalšou neoddeliteľnou súčasťou je práve audit v oblasti kybernetickej bezpečnosti. Pri tejto problematike bol priblížený audit KB podľa rodiny noriem ISO/IEC 27000 od začiatku auditu až po ukončenie auditu s vytýčenými povinnými úkonmi. Práve táto rodina noriem je významná najmä v súvislosti s právnou úpravou KB v Českej republike a to konkrétne s Vyhláškou o kybernetickej bezpečnosti. Spomenutá VKB na prvý pohľad vychádza práve zo skupiny noriem ISO/IEC 27000.

Ďalšia kapitola týkajúca sa teoretického zázemia tejto diplomovej práce sa venovala právnej úprave kybernetickej bezpečnosti v Českej republike. Jej súčasťou bolo vymedzenie najvýznamnejších právnych prameňov v tejto oblasti. V podkapitole Zákon o kybernetickej bezpečnosti boli ucelene priblížené povinnosti pre regulované subjekty vymedzené týmto zákonom. Ďalšou súčasťou teoretickej časti bol vykonávací predpis zákona, vyhláška o kybernetickej bezpečnosti, v ktorej boli rozobrané najsignifikantnejšie bezpečnostné opatrenia rozdelené do organizačných a technických opatrení. Posledná kapitola teoretickej časti bola venovaná predpokladaným legislatívnym zmenám súvisiacich s novou smernicou európskej únie o kybernetickej bezpečnosti, ktoré sa odzrkadlia v zákone a vyhláške o kybernetickej bezpečnosti.

V praktickej časti bol predstavený vytvorený nástroj pre podporu auditov kybernetickej bezpečnosti v programovacom jazyku Python, ktorý má primárne napomáhať zákonom vytýčeným subjektom pred auditom v oblasti kybernetickej bezpečnosti štrukturovaným prechodom zákonných povinností, s možnosťou popisu ich plnenia, prípadne priložením dokumentácie a spolu s výsledne generovanou súhrnnou správou reprezentujúcou aktuálny stav plnenia uložených povinností. Tak isto môže byť tento nástroj nápomocný pre auditorov vykonávajúcich audit, prípadne kontrolu plnenia zákonných povinností, ktorým výsledná súhrnná správa vytvorená spomínaným nástrojom poskytne prehľad o aktuálnom plnení povinností regulovaného subjektu spolu s vloženými súbormi v jednom ucelenom dokumente. Tým pádom sa nebudú musieť potýkať s problematickým zorientovaní sa v sprístupnenej dokumentácií, často s neodpovedajúcimi názvami súborov. Súčasne bola naimplementovaná možnosť využitia nástroja aj mimo audity a kontroly podľa zákona o kybernetickej bezpečnosti a možnosť modifikovania otázok na legislatívne zmeny, ktoré budú vydané v blízkej budúcnosti.

Literatúra

[1] *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020* [online] , 2021. 2021. Národní úřad pri kybernetickou a informační bezpečnost [cit. 2022-12-11]. Dostupné z: <https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020_verze_pro_tisk.pdf>

[2] *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019* [online] , 2020. 2020. Národní úřad pri kybernetickou a informační bezpečnost [cit. 2022-12-11]. Dostupné z: <https://www.nukib.cz/download/publikace/zpravy_o_stavu/NUKIB_ZSKB_2019_verze-pro-tisk.pdf>

[3] Kybernetická a informační bezpečnost. Legislativa, povinnosti a typy kybernetických útoků, 2021. *Magazín BezpečnostPráce.info, z.s.* [online]. **2021**(1), 12 [cit. 2022-12-11]. Dostupné z: <https://www.bezpecnostprace.info/kybernetika-informace/kyberneticka-bezpecnost-legislativa-povinnost/>

[4] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR, 2022. *Výkladový slovník kybernetické bezpečnosti: Páté doplněné a upravené vydání* [online]. 5. Praha: Centrum kybernetické bezpečnosti, z.ú. [cit. 2022-12-11]. ISBN ISBN 978-80-908388-4-0. Dostupné z: <https://www.nukib.cz/download/publikace/podpurne_materialy/Vkladov%20slovnk_5.ver.pdf>

[5] KOLOUCH, Jan a Pavel BAŠTA, 2019. *CyberSecurity* [online]. 1. Praha: CZ.NIC, z. s. p. o. [cit. 2022-12-11]. ISBN ISBN 978-80-88168-34-8. Dostupné z: <https://knihy.nic.cz/files/edice/cybersecurity.pdf

[6] ISO/IEC 27007, 2020. *Česká technická norma: Informační technologie, kybernetická bezpečnost a ochrana soukromí - Směrnice pro audit systémů řízerní bezpečnosti informací.* 3. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

[7] ČSN EN ISO 19011, 2019. *Česká technická norma: Směrnice pro auditování systémů managementu.* 3. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

[8] FAQ: Vyhláška o kybernetické bezpečnosti: Jak spolu souvisí vyhláška o kybernetické bezpečnosti a ISO normy?, 2018. *NÚKIB* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost [cit. 2022-12-11]. Dostupné z: <https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/faq/#otazka13

[9] ČSN EN ISO/IEC 27000, 2014. *Česká technická norma: Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovík.* 2. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

[10] ČSN ISO/IEC 27001, 2014. *Česká technická norma: Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky.* 2. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

[11] SEDLÁČEK, Miroslav, 2011. Demingův cyklus PDCA. *SystemOnLine: Časopis IT Systems* [online]. 11(12), 11 [cit. 2022-12-11]. Dostupné z: <`https://www.systemonline.cz/sprava-it/deminguv-cyklus-pdca.htm`

[12] ČESKÁ REPUBLIKA. Zákon č. 181/2014 Sb.: *Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).* In: Sbírka zákonů České republiky. 2014, částka 75. Dostupný tiež z: <`https://www.zakonyprolidi.cz/cs/2014-181/zneni-20220806`

[13] Legislativa KB, 2022. *NÚKIB* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost [cit. 2022-12-11]. Dostupné z: <`https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/`

[14] ČESKO. Zákon č. 127/2005 Sb.: *Zákon o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích).* In: Sbírka zákonů České republiky. 2005, částka 43. Dostupný tiež z: <`https://www.zakonyprolidi.cz/cs/2005-127/zneni-20220701`

[15] Formulář pro hlášení kontaktních údajů, 2015. *CSIRT* [online]. Praha: CZ.NIC, z. s. p. o. [cit. 2022-12-11]. Dostupné z: <`https://csirt.cz/cs/formulare/hlaseni-kontaktu-zkb/`

[16] Formuláre: Formulář oznámení o provedení reaktivního opatření, 2021. *NÚKIB* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost [cit. 2022-12-11]. Dostupné z: <`https://nukib.cz/cs/infoservis/dokumenty-a-publikace/formulare/`

[17] ČESKÁ REPUBLIKA. Ústavní zákon č. 110/1998 Sb.: *Ústavní zákon o bezpečnosti České republiky.* In: Sbírka zákonů České republiky. 1998, částka 39. Dostupný tiež z: <`https://www.zakonyprolidi.cz/cs/1998-110`

[18] Formulář hlášení kybernetického bezpečnostního incidentu podle Zákona o kybernetické bezpečnosti, 2015. *CSIRT* [online]. Praha: CZ.NIC, z. s. p. o. [cit. 2022-12-11]. Dostupné z: <https://www.csirt.cz/cs/formulare/hlaseni-incidentu-zkb/

[19] Hlášení incidentu - Jak má hlášení vypadat, 2015. *CSIRT* [online]. Praha: CZ.NIC, z. s. p. o. [cit. 2022-12-11]. Dostupné z: <https://csirt.cz/cs/hlaseni-incidentu/jak-ma-hlaseni-vypadat/

[20] NÚKIB představuje evropskou směrnici NIS2, 2022. *NÚKIB* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost [cit. 2022-12-11]. Dostupné z: <https://nukib.cz/cs/infoservis/aktuality/1874-nukib-predstavuje-evropskou-smernici-nis2/

[21] *Podpůrné materiály: Schéma KII* [online], 2020. Brno: Národní úřad pro kybernetickou a informační bezpečnost [cit. 2023-05-14]. Dostupné z: <https://nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/

[22] NCKB: Regulace a kontrola - formuláře, 2019. *Národní centrum kybernetické bezpečnosti* [online]. Brno: NCKB [cit. 2023-05-14]. Dostupné z: <https://www.govcert.cz/cs/regulace-a-kontrola/formulare/

[23] NCKB: Vládní CERT - hlášení incidentů, 2018. *Národní centrum kybernetické bezpečnosti* [online]. Brno: NCKB [cit. 2023-05-14]. Dostupné z: <https://www.govcert.cz/cs/vladni-cert/hlaseni-incidentu/

[24] Podpůrné materiály: Poskytovatelé digitálních služeb, 2018. *NÚKIB* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost [cit. 2023-05-14]. Dostupné z: <https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/#od-VIS

[25] Podpůrné materiály: Významné informační systémy, 2023. *NÚKIB* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost [cit. 2023-05-14]. Dostupné z: <https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/#od-DSP

[26] *Směrnice Evropského parlamentu a Rady (EU) 2016/1148: o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii*, 2016. In: . Štrasburk: Evropský parlament, Rada Evropské unie, ročník 2016, číslo 1148. Dostupné také z: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016L1148

[27] ISO 27001 a vyhláška upravující Zákon o kybernetické bezpečnosti uvádějí potřebu proškolit zaměstnance, 2020. *Next Generation Security Solutions* [online]. Praha: NGSS [cit. 2023-05-14]. Dostupné z: <https://www.ngss.cz/clanek/52-iso-27001-a-vyhlaska-upravujici-zakon-o-kyberneticke-bezpecnosti-uvadeji-potrebu-proskolit-zamestnance

[28] Průvodce řízením aktiv a rizik dle VKB, 2022. *NÚKIB* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost, 18.8.2022 [cit. 2023-05-15]. Dostupné z: <https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/#od-VKB

[29] ČESKÁ REPUBLIKA, 2018. Vyhláška č. 82/2018 Sb.: *Vyhláška o kybernetické bezpečnosti)*. In: Sbírka zákonů České republiky. 2018, částka 82. Dostupný tiež z: <https://www.zakonyprolidi.cz/cs/2018-82

[30] ČESKÁ REPUBLIKA, 2004. Zákon č. 480/2004 Sb.: *Zákon o některých službách informační společnosti.)*. In: Sbírka zákonů České republiky. 2004, částka 480. Dostupný tiež z: <https://www.zakonyprolidi.cz/cs/2004-480

[31] Zadávání veřejných zakázek v oblasti ICT a kybernetická bezpečnost, 2022. *NÚKIB* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost [cit. 2023-05-17]. Dostupné z: <https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/#od-obecne

[32] Fyzická bezpečnost (Physical Security), 2017. *Management Mania* [online]. Praha: ManagementMania [cit. 2023-05-17]. Dostupné z: <https://managementmania.com/cs/fyzicka-bezpecnost

[33] What is network segmentation?, 2022. *CISCO* [online]. USA: CISCO, 2022 [cit. 2023-05-17]. Dostupné z: <https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html

[34] AFOLABI, OLUWADEMILADE, 2022. Types of Active Attacks and How to Protect Against Them. *Make use of* [online]. Lagos State, Nigeria: Make use of [cit. 2023-05-17]. Dostupné z: <https://www.makeuseof.com/4-types-active-attacks-and-how-to-protect-against-them/

[35] ČESKÁ REPUBLIKA, 2000. Zákon č. 240/2000 Sb.: *Zákon o krizovém řízení a o změně některých zákonů.)*. In: Sbírka zákonů České republiky. 2000, částka 240. Dostupný tiež z: <https://www.zakonyprolidi.cz/cs/2000-240

[36] What is identity management?, 2022. *AMI* [online]. Praha: AMI, 15.03.2022 [cit. 2023-05-17]. Dostupné z: <https://ami.cz/en/news/what-is-identity-management-series-about-idm-part-1/

[37] What is endpoint detection and response (EDR)?, 2022. *Trellix* [online]. USA: Trellix [cit. 2023-05-17]. Dostupné z: <https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-detection-and-response.html

[38] What is endpoint antivirus?, 2022. *Trellix* [online]. USA: Trellix [cit. 2023-05-17]. Dostupné z: <https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-antivirus.html

[39] What is network time protocol (NTP)?, 2022. *TechTarget* [online]. USA: TechTarget [cit. 2023-05-17]. Dostupné z: <https://www.techtarget.com/searchnetworking/definition/Network-Time-Protocol

[40] What is Security Information and Event Management (SIEM)?, 2022. *IBM* [online]. USA: IBM [cit. 2023-05-17]. Dostupné z: <https://www.ibm.com/topics/siem

[41] What is public key infrastructure (PKI)?, 2022. *TechTarget* [online]. USA: TechTarget [cit. 2023-05-17]. Dostupné z: <https://www.techtarget.com/searchsecurity/definition/PKI

[42] What is a SCADA System and How Does It Work?, 2022. *ONLOGIC* [online]. USA: ONLOGIC [cit. 2023-05-17]. Dostupné z: <https://www.onlogic.com/company/io-hub/what-is-a-scada-system-and-how-does-it-work/

[43] *Prováděcí nařízení komise (EU) 2018/151, 2018.* In: Úřední věstník Evropské unie, ročník 2018, číslo 151. Dostupné také z: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32018R0151&from=ES

[44] Nová směrnice EU o kybernetické bezpečnosti „NIS2“ a návrh nového ZKB, 2022. *Osveta NÚKIB* [online]. Brno: NÚKIB [cit. 2023-05-17]. Dostupné z: <https://osveta.nukib.cz/course/view.php?id=145

[45] *Smernica Európskeho parlamentu a Rady (EU) 2022/2555, 2022.* In: Úřední věstník Evropské unie, ročník 2022, číslo 2555. Dostupné také z: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32022L2555&qid=1684329496720

[46] Podpůrné materiály: VKB checklist, 2020. *NÚKIB* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost [cit. 2023-05-17]. Dostupné z: <https://nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/

[47] JANŠA, Jakub, 2018. *Audit kybernetické bezpečnosti.* Praha. Diplomová práca. Vysoká škola ekonomická v Praze.

[48] Graphical User Interfaces with Tk, 2022. *Python Docs* [online]. USA: Python [cit. 2023-05-17]. Dostupné z: <https://docs.python.org/3/library/tk.html

[49] ReportLab - Documentation, 2023. *ReportLab Docs* [online]. USA: ReportLab [cit. 2023-05-17]. Dostupné z: <https://docs.reportlab.com/reportlab/userguide/ch1_intro/

[50] Fernet (symmetric encryption), 2021. *Cryptography* [online]. USA: Cryptography [cit. 2023-05-17]. Dostupné z: <https://cryptography.io/en/latest/fernet/

Zoznam symbolov a skratiek

AS	Autonómny systém
CERT	Computer Emergency Response Team - vládny bezpečnostný tím pre boj proti kyberkriminalite
CIA	Princíp pre dosiahnutie kybernetickej alebo informačnej bezpečnosti (vysvetlené v 1.1)
CSIRT	Computer Security Incident Response Team - národný bezpečnostný tím pre boj proti kyberkriminalite
GUI	Graphic User Interface - grafické užívateľské rozhranie
IEC	International Electrotechnical Commission - Medzinárodná elektrotechnická komisia
IP	Internet Protocol
ISMS	Systém riadenie bezpečnosti informácií
ISO	International Organization for Standardization - Medzinárodná organizácie pre normalizáciu
KB	Kybernetická bezpečnosť
KBI	Kybernetický bezpečnostný incident
KBU	Kybernetická bezpečnostná udalosť
KII	Kritická informačná infraštruktúra
NIS	Network and Information Systems
NÚKIB	Národní úřad pri kybernetickou a informační bezpečnost
PDCA	Demmingov cyklus tiež známy pod skratkou PDCA cyklus
PDF	Portable Document Format - formát súboru
PGP	Pretty Good Privacy - počítačový program umožňujúci podpisovanie a šifrovanie
VIS	Významný informačný systém
VKB	Vyhláška o kybernetickej bezpečnosti

ZKB Zákon o kybernetickej bezpečnosti

Zoznam príloh

A Opatrenia podľa ISO/IEC 27001 a ich ciele

V rámci tejto prílohy sú vymenované kategórie opatrení (a ich ciele) pre splnenie požiadaviek podľa ISO/IEC 27001. Vymenovanie kategórií opatrení má dať čitateľovi predstavu aké oblasti sú brané na zreteľ pri systéme riadenia bezpečnosti informácií.

Jednotlivé čiastkové opatrenia spadajúce pod kategórie sú uvedené v ISO/IEC 27001 v Prílohe A - Ciele opatrení a jednotlivé opatrenia (Tabulka A.1) [10]

A.1 Politiky bezpečnosti informácií

A.1.1 Smerovanie bezpečnosti informácií vedením organizácie

Cieľ: Určiť smer a vyjadriť podporu bezpečnosti informácií zo strany vedenia v súlade s požiadavkami týkajúcimi sa činnosti organizácie, príslušnými zákonmi a smernicami.

A.2 Organizácia bezpečnosti informácií

A.2.1 Interná organizácia

Cieľ: Zriadiť rámec riadenia pre zahájenie a riadenie implementácie a prevádzkovanie bezpečnosti informácií v organizácii.

A.2.2 Mobilné zariadenie a práca na diaľku

Cieľ: Zaistiť bezpečnosť pri použití mobilných zariadení a pre prácu na diaľku.

A.3 Bezpečnosť ľudských zdrojov

A.3.1 Pred vznikom pracovného vzťahu

Cieľ: Zaistiť, aby zamestnanci a zmluvné strany boli oboznámení so svojimi povinnosťami a aby pre jednotlivé role boli vybraní vhodní kandidáti.

A.3.2 V priebehu pracovného vzťahu

Cieľ: Zaistiť, aby si zamestnanci a zmluvné strany boli vedomí a plnili si svoje povinnosti v oblasti bezpečnosti informácií.

A.3.3 Ukončenie pracovného vzťahu

Cieľ: Chrániť záujmy organizácie v rámci procesu zmeny alebo ukončenia právneho vzťahu.

A.4 Riadenie aktív

A.4.1 Zodpovednosť za aktíva

Cieľ: Identifikovať aktíva organizácie a definovať povinnosti k ich primeranej ochrane.

A.4.2 Klasifikácia informácií

Cieľ: Zaistiť, aby informácie získali zodpovedajúcu úroveň ochrany v súlade s ich dôležitosťou pre organizáciu.

A.4.3 Manipulácia s médiami

Cieľ: Predchádzať neoprávnenému vyzradeniu, modifikácii, odstráneniu alebo zničeniu informácií uložených na médiách.

A.5 Riadenie prístupu

A.5.1 Požiadavky organizácie na riadeniu prístupu

Cieľ: Obmedziť prístup k informáciám a vybaveniu pre spracovanie informácií.

A.5.2 Riadenie prístupu užívateľov

Cieľ: Zaistiť oprávnený prístup užívateľov a predchádzať neoprávnenému prístupu k systému a službám.

A.5.3 Povinnosti užívateľov

Cieľ: Definovať zodpovednosť užívateľov za ochranu ich autentizačných informácií.

A.5.4 Riadenie prístupu k systémom a aplikáciám

Cieľ: Predchádzať neautorizovanému prístupu k systémom a aplikáciám.

A.6 Kryptografia

A.6.1 Kryptografické opatrenia

Cieľ: Zaistiť správne a efektívne používanie kryptografie k ochrane dôvernosti, autentickosti a integrity informácií.

A.7 Fyzická bezpečnosť a bezpečnosť prostredia

A.7.1 Bezpečné oblasti

Cieľ: Predchádzať neautorizovanému fyzickému prístupu, poškodeniu a zásahom do informácií a vybavenia pre spracovanie informácií organizácie.

A.7.2 Zariadenia

Cieľ: Predchádzať strate, poškodeniu, krádeži alebo kompromitácii aktív a prerušeniu činnosti organizácie.

A.8 Prevádzková bezpečnosť

A.8.1 Prevádzkové postupy a zodpovednosti

Cieľ: Zaistiť správnu a bezpečnú prevádzku vybavenia pre spracovanie informácií.

A.8.2 Ochrana proti malwaru

Cieľ: Zaistiť, aby informácie a vybavenie pre spracovanie informácií boli chránené proti malwaru.

A.8.3 Zálohovanie

Cieľ: Chrániť proti strate dát.

A.8.4 Zaznamenávanie formou logov a monitorovanie

Cieľ: Zaznamenávať udalosti a vytvárať o nich záznamy.

A.8.5 Správa prevádzkovaného softwaru

Cieľ: Zaistiť integritu prevádzkovaných systémov.

A.8.6 Riadenie technických zraniteľností

Cieľ: Zabrániť využívaniu technických zraniteľností.

A.8.7 Hľadiská auditu informačných systémov

Cieľ: Minimalizovať dopady auditných činností na prevádzkované systémy.

A.9 Bezpečnosť komunikácií

A.9.1 Správa bezpečnosti siete

Cieľ: Zaistiť ochranu informácií v sieťach a ich podporných prostrediach pre spracovanie informácií.

A.9.2 Prenos informácií

Cieľ: Zaistiť bezpečnosť informácií pri ich prenose v rámci organizácie a s externými subjektami.

A.10 Akvizícia, vývoj a údržba

A.10.1 Bezpečnostné požiadavky na informačné systémy

Cieľ: Zaistiť, aby sa bezpečnosť informácií stala neoddeliteľnou súčasťou informačných systémov v ich celom životnom cykle zahŕňajúc aj požiadavky na informačné systémy, ktoré poskytujú služby vo verejných sieťach.

A.10.2 Bezpečnosť v procesoch vývoja a podpory

Cieľ: Zaistiť, aby bezpečnosť informácií bola navrhovaná a implementovaná v životnom cykle vývoja informačných systémov.

A.10.3 Testovacie dáta

Cieľ: Zaistiť ochranu dát používaných pre testovacie účely.

A.11 Dodávateľské vzťahy

A.11.1 Bezpečnosť informácií v dodávateľských vzťahoch

Cieľ: Zaistiť ochranu aktív organizácie, ku ktorým majú dodávatelia prístup.

A.11.2 Riadenie dodávok služieb dodávateľov

Cieľ: Udržiavať dohodnutú úroveň bezpečnosti informácií a dodávky služieb v zhode s dodávateľskými dohodami.

A.12 Riadenie incidentov bezpečnosti informácií

A.12.1 Riadenie incidentov bezpečnosti informácií a zlepšovanie

Cieľ: Zaistiť odpovedajúci a efektívny prístup ku zvládaniu incidentov bezpečnosti informácií zahrňujúcim komunikáciu ohľadne bezpečnostných udalostí a slabých miest.

A.13 Aspekty riadenia kontinuity činností organizácie z hľadiska bezpečnosti informácií

A.13.1 Kontinuita bezpečnosti informácií

Cieľ: Kontinuita bezpečnosti informácií musí byť súčasťou systému riadenia kontinuity činnosti organizácie.

A.13.2 Redundancia

Cieľ: Zaistiť dostupnosť vybavenia pre spracovanie informácií.

A.14 Súlad s požiadavkami

A.14.1 Súlad s právnymi a zmluvnými požiadavkami

Cieľ: Vyvarovať sa porušeniu zákonných, predpisových alebo zmluvných povinností týkajúcich sa bezpečnosti informácií a akýchkoľvek bezpečnostných požiadaviek.

A.14.2 Preskúmanie bezpečnosti informácií

Cieľ: Zaistiť, že bezpečnosť informácií je implementovaná a prevádzkovaná v súlade s politikami a postupmi organizácie. [10]

B Bezpečnostné politiky a bezpečnostné dokumentácie

B.1 Bezpečnostná politika

B.1.1 Politika systému riadenia bezpečnosti informácií

1. Ciele, princípy a potreby riadenia bezpečnosti informácií.
2. Rozsah a hranice systému riadenia bezpečnosti informácií.
3. Pravidlá a postupy pre riadenie dokumentácie.
4. Pravidlá a postupy pre riadenie zdrojov a prevádzky systému riadenia bezpečnosti informácií.
5. Pravidlá a postupy pre vykonávanie auditov kybernetickej bezpečnosti.
6. Pravidlá a postupy pre preskúmavanie systému riadenia bezpečnosti informácií.
7. Pravidlá a postupy pre nápravné opatrenia a zlepšovanie systému riadenia bezpečnosti informácií.

B.1.2 Politika riadenia aktív

1. Identifikácia, hodnotenie a evidencia primárnych aktív.
   (a) určenie a evidencia jednotlivých primárnych aktív vrátane určenia ich garanta,
   (b) hodnotenie dôležitosti primárnych aktív z hľadiska dôvernosti, integrity a dostupnosti.
2. Identifikácia, hodnotenie a evidencia podporných aktív.
   (a) určenie a evidencia jednotlivých podporných aktív vrátane určenia ich garanta,
   (b) určenie väzieb medzi primárnymi a podpornými aktívami.
3. Pravidlá ochrany jednotlivých úrovní aktív
   (a) spôsoby rozlišovania jednotlivých úrovní aktív,
   (b) pravidlá pre manipuláciu a evidenciu aktív podľa úrovni aktív,
   (c) prípustné spôsoby používania aktív.
4. Spôsoby spoľahlivého mazania alebo ničenie technických nosičov dát, informácií, prevádzkových údajov a ich kópií.

B.1.3 Politika organizačnej bezpečnosti

1. Určenie bezpečnostných rolí a ich práv a povinností.

2. Požiadavky na oddelenie výkonu činnosti jednotlivých bezpečnostných rolí.
3. Požiadavky na oddelenie výkonu bezpečnostných a prevádzkových rolí.

B.1.4 Politika riadenia dodávateľov

1. Pravidlá a princípy pre výber dodávateľov.
2. Pravidlá pre hodnotenie rizík súvisiacich s dodávateľmi.
3. Náležitosti zmluvy o úrovni služieb a spôsobov a úrovní realizácie bezpečnostných opatrení a o určení vzájomnej zmluvnej zodpovednosti.
4. Pravidlá pre výkon kontroly zavedenia bezpečnostných opatrení.
5. Pravidlá pre hodnotenie dodávateľov.

B.1.5 Politika bezpečnosti ľudských zdrojov

1. Pravidlá rozvoja bezpečnostného povedomia a spôsoby jeho hodnotenia
   (a) spôsoby a formy poučenia užívateľov,
   (b) spôsoby a formy poučenia garantov aktív,
   (c) spôsoby a formy poučenia administrátorov,
   (d) spôsoby a formy poučenia osôb zastávajúcich bezpečnostné role.
2. Bezpečnostné školenia nových zamestnancov.
3. Pravidlá pre riešenie prípadov porušenia bezpečnostnej politiky systému riadenia bezpečnosti informácií.
4. Pravidlá pre ukončenie pracovného vzťahu alebo zmenu pracovnej pozície
   (a) vrátenie zverených aktív a odobranie práv pri ukončení pracovného vzťahu,
   (b) zmena prístupových oprávnení pri zmene pracovnej pozície.

B.1.6 Politika riadenie prevádzky a komunikácií

1. Právomoci a zodpovednosti spojené s bezpečnou prevádzkou.
2. Postupy bezpečnej prevádzky.
3. Požiadavky a štandardy bezpečnej prevádzky.
4. Pravidlá a obmedzenia pre vykonávanie auditov kybernetickej bezpečnosti a bezpečnostných testov.

B.1.7 Politika riadenia prístupu

1. Princíp minimálnych oprávnení alebo potreby poznať (need to know).
2. Požiadavky na riadenie prístupu.
3. Životný cyklus riadenia prístupu.
4. Riadenie privilegovaných oprávnení.

5. Riadenie prístupu pre mimoriadne situácie.
6. Pravidelné preskúmavanie prístupových oprávnení vrátane rozdelenia jednotlivých užívateľov v prístupových skupinách.

B.1.8 Politika bezpečného chovania užívateľov

1. Pravidlá pre bezpečné nakladanie s aktívami.
2. Bezpečné požitie prístupového hesla.
3. Bezpečné použitie elektronickej pošty a prístupu na internet.
4. Bezpečný vzdialený prístup.
5. Bezpečné chovanie na sociálnych sieťach.
6. Bezpečnosť vo vzťahu k mobilným zariadeniam.

B.1.9 Politika zálohovania a obnovy a dlhodobého ukladania

1. Požiadavky na zálohovanie a obnovu.
2. Pravidlá a postupy zálohovanie.
3. Pravidlá a postupy dlhodobého ukladanie.
4. Pravidlá bezpečného zálohovania a dlhodobého ukladanie informácií.
5. Pravidlá a postupy obnovy.
6. Pravidlá a postupy testovania zálohovania a obnovy.
7. Politika prístupu k zálohám, ukladaným informáciám.

B.1.10 Politika bezpečného odovzdávania a výmeny informácií

1. Pravidlá a postupy pre ochranu odovzdávaných informácií.
2. Spôsoby ochrany elektronickej výmeny informácií.
3. Pravidlá pre využívanie kryptografickej ochrany.

B.1.11 Politika riadenia technických zraniteľností

1. Pravidlá pre obmedzenie inštalácie programového vybavenia.
2. Pravidlá a postupy vyhľadávania opravných programových balíčkov.
3. Pravidlá a postupy testovania opráv programového vybavenia.
4. Pravidlá a postupy nasadenia opráv programového vybavenia.

B.1.12 Politika bezpečného používania mobilných zariadení

1. Pravidlá a postupy pre bezpečné používanie mobilných zariadení.
2. Pravidlá a postupy pre zaistenie bezpečnosti zariadení, ktoré povinná osoba nemá vo svojej správe.

B.1.13 Politika akvizície, vývoja a údržby

1. Bezpečnostné požiadavky pre akvizíciu, vývoj a údržbu.
2. Riadenie zraniteľností.
3. Politika poskytovania a nadobúdania licencií programového vybavenia a informácií
   (a) pravidlá a postupy nasadenia programového vybavenia a jeho evidencie,
   (b) pravidlá a postupy pre kontrolu dodržovania licenčných podmienok.

B.1.14 Politika ochrany osobných údajov

1. Charakteristika spracovávaných osobných údajov.
2. Popis prijatých a vykonaných organizačných opatrení pre ochranu osobných údajov.
3. Popis prijatých a vykonaných technických opatrení pre ochranu osobných údajov.

B.1.15 Politika fyzickej bezpečnosti

1. Pravidlá pre ochranu objektov.
2. Pravidlá pre kontrolu vstupu osôb.
3. Pravidlá pre ochranu zariadení.
4. Detekcia narušenia fyzickej bezpečnosti.

B.1.16 Politika bezpečnosti komunikačnej siete

1. Pravidlá a postupy pre zaistenie bezpečnosti siete.
2. Určenie práv a povinností za bezpečnú prevádzku siete.
3. Pravidlá a postupy pre riadenie prístupov v rámci siete.
4. Pravidlá a postupy pre ochranu vzdialeného prístupu k sieti.
5. Pravidlá a postupy pre monitorovanie a vyhodnocovanie prevádzkových záznamov.

B.1.17 Politika ochrany pred škodlivým kódom

1. Pravidlá a postupy pre ochranu sieťovej komunikácie.
2. Pravidlá a postupy pre ochranu serverov a zdieľaných dátových úložísk.
3. Pravidlá a postupy pre ochranu pracovných staníc.

B.1.18 Politika nasadenia a používania nástroja pre detekciu KBU

1. Pravidlá a postupy nasadenia nástroja pre detekciu KBU.
2. Prevádzkové postupy pre vyhodnocovanie a reagovanie na detekované KBU.
3. Pravidlá a postupy pre optimalizáciu nastavení nástroja pre detekciu KBU.

B.1.19 Politika využitia a údržby nástroja pre zber a vyhodnocovanie KBU

1. Pravidlá a postupy pre evidenciu a vyhodnocovanie KBU.
2. Pravidlá a postupy pravidelných aktualizácií pravidiel pre vyhodnocovanie KBU.
3. Pravidlá a postupy pre optimálne nastavenie bezpečnostných vlastností nástroja pre zber a vyhodnocovanie KBU.

B.1.20 Politika bezpečného používania kryptografickej ochrany

1. Úroveň ochrany s ohľadom na typ a silu kryptografického algoritmu.
2. Pravidlá kryptografickej ochrany informácií
   (a) pri prenose po komunikačných sieťach,
   (b) pri uložení na mobilné zariadenie alebo vymeniteľný nosič dát.
3. Systém správy kľúčov.

B.1.21 Politika riadenia zmien

1. Spôsob a princípy riadenia významných zmien v rámci povinnej osoby, ich procesov, informačných a komunikačných systémov.
2. Preskúmavanie dopadov významných zmien.
3. Spôsob vedenia evidencie a testovania významných zmien.

B.1.22 Politika zvládanie KBI

1. Definovanie kategórií KBI.
2. Pravidlá a postupy pre identifikáciu, evidenciu a zvládanie jednotlivých kategórií KBI.
3. Pravidlá a postupy testovania systému zvládania KBI.
4. Pravidlá a postupy pre vyhodnocovanie KBI a pre zlepšovanie kybernetickej bepečnosti.
5. Evidencia KBI.

B.1.23 Politika riadenia kontinuity činností

1. Práva a povinnosti zúčastnených osôb.
2. Ciele riadenia kontinuity činností
   (a) minimálna úroveň poskytovaných služieb,
   (b) doba obnovenia chodu,
   (c) bod obnovenia dát.
3. Politika riadenia kontinuity činností pre naplnenie cieľov kontinuity.
4. Spôsoby hodnotenia dopadov KBI na kontinuitu a posudzovanie súvisiacich rizík.
5. Určenie a obsah potrebných plánov kontinuity a havarijných plánov.
6. Postupy pre realizáciu opatrení vydaných NÚKIBom.

B.2 Obsah bezpečnostnej dokumentácie

B.2.1 Správa z auditu kybernetickej bezpečnosti

1. Ciele auditu kybernetickej bezpečnosti.
2. Predmet auditu kybernetickej bezpečnosti.
3. Kritériá auditu kybernetickej bezpečnosti.
4. Identifikovanie týmu auditorov a osôb, ktoré sa auditu kybernetickej bezpečnosti zúčastnili.
5. Dátum a miesto, kde boli vykonávané činnosti pri audite kybernetickej bezpečnosti.
6. Zistenie z auditu kybernetickej bezpečnosti.
7. Závery auditu kybernetickej bezpečnosti.

B.2.2 Správa a preskúmavanie systému riadenia bezpečnosti informácií

1. Vyhodnocovanie opatrení z predchádzajúceho preskúmavanie systému riadenia bezpečnosti informácií.
2. Identifikácie zmien a okolností, ktoré môžu mať vplyv na systém riadenia bezpečnosti informácií.
3. Spätná väzba o výkonnosti riadenia bezpečnosti informácií
   (a) nezhody a nápravné opatrenia,
   (b) výsledky monitorovania a merania,
   (c) výsledky auditu,
   (d) naplnenie cieľov systému riadenia bezpečnosti informácií.
4. Výsledky hodnotenia rizík a stav plánu zvládania rizík.

5. Identifikácie možností pre neustále zlepšovanie.
6. Doporučenie potrebných rozhodnutí, stanovení opatrení a osôb zaisťujúcich výkon jednotlivých činností.

B.2.3 Metodika pre identifikáciu a hodnotenie aktív a pre hodnotenie rizík

1. Určenie stupnice pre hodnotenie primárny aktív
   (a) určenie stupnice pre hodnotenie úrovni dôvernosti aktív,
   (b) určenie stupnice pre hodnotenie úrovni integrity aktív,
   (c) určenie stupnice pre hodnotenie úrovni dostupnosti aktív.
2. Určenie stupnice pre hodnotenie rizík
   (a) určenie stupnice pre hodnotenie úrovni dopadu,
   (b) určenie stupnice pre hodnotenie úrovni hrozby,
   (c) určenie stupnice pre hodnotenie úrovni zraniteľnosti,
   (d) určenie stupnice pre hodnotenie úrovni rizík.
3. Metódy a prístupy pre zvládanie rizík.
4. Spôsoby schvaľovania akceptovateľných rizík.

B.2.4 Správa a hodnotenie aktív a rizík

1. Prehľad primárnych aktív
   (a) identifikácia a popis primárnych aktív,
   (b) určenie garantov primárnych aktív,
   (c) hodnotenie primárnych aktív z hľadiska dôvernosti, integrity a dostupnosti.
2. Prehľad podporných aktív
   (a) identifikácia a popis podporných aktív,
   (b) určenie garantov podporných aktív,
   (c) určenie väzieb medzi primárnymi a podpornými aktívami.
3. Hodnotenie rizík
   (a) posúdenie možných dopadov na aktíva,
   (b) hodnotenie existujúcich hrozieb,
   (c) hodnotenie existujúcich zraniteľností, hodnotenie existujúcich opatrení,
   (d) stanovenie úrovne rizika, porovnávanie tejto úrovne s kritériami pre akceptovateľnosť rizík,
   (e) určenie a schvaľovanie akceptovateľnosti rizík.
4. Zvládanie rizík
   (a) návrh spôsobu zvládanie rizík,

(b) návrh opatrení a ich realizácie.

B.2.5 Prehlásenie o aplikovateľnosti

1. Prehľad vylúčených bezpečnostných opatrení požadovaných VKB vrátane odôvodnenia, prečo neboli aplikované.
2. Prehľad zavedených bezpečnostných opatrení vrátane spôsobu ich implementácie.

B.2.6 Plán zvládanie rizík

1. Obsah a ciele vybraných bezpečnostných opatrení pre zvládanie rizík vrátane väzby na konkrétne riziká.
2. Potrebné zdroje pre jednotlivé bezpečnostné opatrenia pre zvládanie rizík.
3. Osoby zaisťujúce jednotlivé bezpečnostné opatrenia pre zvládanie rizík.
4. Termíny zavedenia jednotlivých bezpečnostných opatrení pre zvládanie rizík.
5. Spôsob realizácie bezpečnostných opatrení.
6. Spôsoby hodnotenia úspešnosti zavedenie jednotlivých bezpečnostných opatrení pre zvládanie rizík.

B.2.7 Plán rozvoja bezpečnostného povedomia

1. Obsah a termíny poučenia užívateľov, administrátorov a osôb zastupujúcich bezpečnostné role.
2. Obsah a termíny poučení nových zamestnancov.
3. Prehľady, ktoré obsahujú predmet jednotlivých školení a zoznam osôb, ktoré školenie absolvovali.
4. Formy a spôsoby hodnotenia plánu.

B.2.8 Evidencia zmien

1. Evidencia životného cyklu významných zmien.
2. Záznamy o zmenách konfigurácie podporných aktív.

B.2.9 Hlásené kontaktné údaje

1. Prehľad hlásených kontaktných údajov.

B.2.10 Prehľad obecne záväzných právnych predpisov, vnútorných predpisov, iných predpisov a zmluvných záväzkov

1. Prehľad obecne záväzných právnych predpisov.
2. Prehľad vnútorných predpisov a iných predpisov.
3. Prehľad zmluvných záväzkov.

B.2.11 Doporučená dokumentácia

1. Topológia infraštruktúry.
2. Prehľad sieťových zariadení.