Zdravotně sociální fakulta
Faculty of Health and Social Sciences

Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice

Současnost a budoucnost kybernetické bezpečnosti vybraného územního samosprávného celku

DIPLOMOVÁ PRÁCE

Studijní program:
Ochrana obyvatelstva

Autor: Bc. Pragerová Tereza

Vedoucí práce: Ing. Kudlák Aleš, Ph.D.

České Budějovice 2021

Prohlášení

Prohlašuji, že svoji diplomovou práci s názvem ***„Současnost a budoucnost kybernetické bezpečnosti vybraného územního samosprávného celku“*** jsem vypracovala samostatně pouze s použitím pramenů v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své diplomové práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby diplomové práce. Rovněž souhlasím s porovnáním textu mé diplomové práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne 02.08.2021 ……

Bc. Tereza Pragerová

Poděkování

Mnohokrát děkuji panu Ing. Aleši Kudlákovi, Ph.D. za cenné rady, odborné vedení mé diplomové práce, vynaložený čas a trpělivost. Dále bych chtěla poděkovat všem odborníkům, kteří mi poskytli cenné informace ke zpracování této práce. Rovněž děkuji všem svým kolegyním a prim. MUDr. Jakubovi Rytířovi, že mi bylo umožněno studium při práci. V neposlední řadě celé své rodině, která mě celou dobu plně podporovala.

Současnost a budoucnost kybernetické bezpečnosti vybraného územního samosprávného celku

Abstrakt

Téma diplomová práce pojednává o současnosti a budoucnosti kybernetické bezpečnosti ve vybraných územně samosprávních celcích. Tuto problematiku lze vzhledem k rychlosti nárůstu hrozeb považovat za velmi aktuální. Dopady kybernetických útoků, které umí zasáhnout najednou i miliony lidí, jsou odstrašující a této tématice by měla být věnována zvýšená pozornost. Komplexní zpracování tohoto problému by mohlo být základem pro později úspěšný boj proti kyberterorismu.

Cílem diplomové práce bylo zjištění a porovnání současného stavu kybernetické bezpečnosti ve vybraných územně samosprávných celcích. Vybrán byl Kraj Vysočina a Jihočeský kraj. Informace a data byla pořízena pomocí studia příslušné legislativy, odborných dokumentů, článků, rozhovoru a dotazníkového šetření, které se zaměřovalo na odborníky pracující s kybernetickou bezpečností příslušné obce s rozšířenou působností. Aby byla diplomová práce kvalitně a originálně zpracována a vzhledem k protiepidemickým opatřením, která byla zavedena kvůli pandemii Covid-19, byla využita smíšená metoda výzkumu, která obsahuje jak kvalitativní indukci, tak kvantitativní výzkum.

Data byla získána pomocí rozhovoru, následně zaznamenána formou dotazníku. Prošla porovnáním, analyzováním, případně tabulkovým a grafickým znázorněním. Součástí výzkumu jsou i prognostické metody. Analýza trendů, megatrendů a kolo budoucnosti, které umožňuje přehledný, ale zároveň celistvý pohled na danou problematiku. Zjištěno bylo mnoho zajímavých poznatků. Odborníci na kybernetickou bezpečnost se pravidelně vzdělávají v daném oboru. Připravenost, koordinace a řešení při nastalém kybernetickém incidentu by v některých obcích proběhly bez většího problému. Tématu kybernetické bezpečnosti, by měla být věnována velká pozornost do budoucna. Tato diplomová práce by mohla sloužit jako uvedení do dané problematiky pro laickou i odbornou veřejnost.

Klíčová slova

Kybernetická bezpečnost, obec s rozšířenou působností, bezpečnostní incident, kyberterorismus.

The present and the future of cyber security of the selected territorial self-governing unit

Abstract

The topic of the thesis discuss about the present and future of the cyber security in the selected self-governing units. This problematics can be, due to the rate of the increase in threats, considered as very current. Impacts of the cyber attacks, which can hit millions of people at once, are deterrent and people shoul pay an increased attention to this theme. Complex elaborationof this problém could later serve as a basis for a successful fight against cyberterorrism.

The aim of the thesis was the finding and then the comparison of the current status of the cyber security in a selected territorial self-governing units. Selected were the Vysocina region and the South Bohemia region. The information and data were taken by studying the relevant legislation, vocational documents, articles, intervies and the questionnaire survey, which focused on the experts working with cyber security of the relevant municipality with extended powers. In order to process the thesis well and original and having regard to the anti-pandemic measures introduced the following covid-19 pandemic, it was used the mixed research method, which contains both qualitative induction and quantitative research.

Data were obtained through an interview, then recorded in the form of a questionnaire. They went through comparison, analyzing, or eventuel tabular and graphical representation. The prognostic methods are part of the research as well. Analysis of trends, megatrends and the wheel of the future, which allows a clear but at the same time holistic view of the issue. Many interesting findings were identified. Cyber security experts educate themselves in the field regularly. In the case of the cyber incident, the preparedness, coordination and the resolution would take place without major problems in some municipalities. It should be paid close attentio to the theme of the cyber security in the future. This diploma thesis could serve as an introduction to the issue for the lay and professional public as well.

Key words

Cyber security, municipality with extended powers, security incident, cyberterrorism.

Obsah

Úvod

Kybernetická bezpečnost patří bezesporu k aktuálním tématům poslední doby. Jedná se o velmi mladý obor, který se velice rychle vyvíjí. Zabývání se připraveností na kybernetické útoky, řešení těchto incidentů, plánování a nácvik, patří bezpochyby k neodmyslitelným úkolům 21. století. Kybernetické útoky se postupem času velice zdokonalují, jejich tempo vzrůstá a dochází k větším hrozbám než kdy dříve. Stoupající počet obyvatel na planetě, modernizace společnosti a vysoká úroveň technologií, vede zároveň k vzrůstajícímu nebezpečí. Je důležité se pravidelně vzdělávat, zpracovávat postupy k řešení vzniklé krizové situace, vyhledávat aktivně hrozby a rizika, postupně je definovat a odstranit.

Diplomová práce se zaměřuje na současnost a budoucnost kybernetické bezpečnosti územně samosprávných celků. Zhodnocení současného stavu a vyvození možných prognóz do budoucna je velmi důležité. Pro tuto práci byly vybrány obce s rozšířenou působností a jejich městské úřady. Obce s rozšířenou působností mají své odborníky na informační technologie/kybernetickou bezpečnost a jejich cílem je danou obec na krizovou situaci týkající se kybernetických útoků dobře připravit. Pokud by došlo k útoku, je nejdůležitější okamžitě jednat. Mít obecně nacvičený postup, aby se zamezilo co nejrychleji úniku dat, nabourání systémů, omezení provozu, aj.

Cílem této práce je analyzovat nejzávažnější kybernetické útoky za posledních 10 let ve vybraných územně samosprávných celcích a provést prognózu možného vývoje kybernetického terorismu dle zjištěné analýzy.

1 Současný stav

1.1 Kyberprostor (Cyberspace)

Pojem kyberprostor, neboli ono pomyslné „hrací pole“, kde dochází k „útokům a obraně“, lze popsat různě. Jako první použil pojem kyberprostor v roce 1982 William Gibson v povídce „Jak vypálit chrom“. O dva roky později v knize Neuromancer již začíná být jasné, že kyberprostor lze obecně nazvat jako „*nedomyslitelná komplexnost*“. Okamžikem obecného povědomí o kyberprostoru se však stává chvíle, kdy vychází deklarace Johna Barlowa: „A Declaration of the Independence of Cyberspace“ (Kolouch et al., 2019).

Definovat kyberprostor lze i pomocí slovníků. Například Oxford dictionary uvádí, že se jedná o komunikaci přes počítačovou síť, kdy vše probíhá ve fiktivním prostředí (Definition of cybersecurity…, 2018).

Pokus o definování kyberprostoru uvádí i Výkladový slovník kybernetické bezpečnosti, kde se nedefinuje kyberprostor jako takový, ale pouze ten, který spadá pod jurisdikci České republiky, tzv. „Český kyberprostor“ (Jirásek et al., 2015).

O legální, avšak obecnou definici se zasloužil § 2 písm. zákona č. 181/2004 Sb., o kybernetické bezpečnosti znění: *„kybernetickým prostorem je digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací“*.

1.1.1 Vrstvení kyberprostoru

Kyberprostor tvoří komunikační a informační technologie, které za pomoci primárního přenosového protokolu/protokolu síťové vrstvy (dále jen protokol TCP/IP) vytváří celosvětovou síť, do které jsou ještě připojeny interagující jednotlivé počítačové systémy. Opomenout samozřejmě nelze jednotlivé uživatele, protože bez nich by vlastní interakce systémů nebyla možná. Takto je vytvořen dynamický, avšak neustále se vyvíjející a měnící systém, který je navázán na hardware. Tato skutečnost dokazuje, že kyberprostor lze jen těžko přesněji definovat. Je takřka neomezený (Zákon č.181/2014 Sb.).

Nemít konec ani začátek je jedno z prvenství kyberprostoru, který je tzv. virtuální realitou. Zajímavostí zůstává fakt, že virtuální realita je plně závislá na podstatě materiální, tudíž technologických vymoženostech, které jsou součástí reálného světa.

K poškození či dokonce zániku kyberprostoru by mohlo dojít v situaci, kdy zkolabuje materiální médium. Vzniká paradox, kdy nehmotné medium (kyberprostor) je schopné existovat díky hmotnému médiu (např. jednotlivé počítačové systémy), protože dochází k jeho distribuovanosti. A to dále navazuje na schopnost adaptace a změny v momentě poškození média materiálního. Pokud dojde k úplnému kolapsu média materiálního, nastává poškození, či zánik kyberprostoru. Mnohé státy dnes považují kyberprostor za pátou sféru, hned po vzduchu, zemi, ohni a také vodě. Tato sféra není vnímána jen jako válečná zóna, je o ní čím dál tím větší zájem celkově, a to nejen z řad státních organizací (Reed, 2004).

Do znaků kyberprostoru lze zařadit:

- globálnost,
- bohaté zdroje informací,
- decentralizovanost,
- ovlivňování veřejného mínění,
- interaktivnost.

Primární rolí se v kyberprostoru stala návaznost technologií na služby. To v posledních letech dokazuje velký vliv virtuálního světa na svět reálný (Reed, 2004).

Podle Cyberspace Operations: Concept Capability Plan 2016-2028 je kyberprostor složen ze tří vrstev: fyzické, sociální a logické. Ty jsou složeny z pěti komponentů. Ve fyzické vrstvě se nalézají dva komponenty. Jedním je „geographic component“, pro který není v českém jazyce přesný ekvivalent a druhým jsou fyzické síťové komponenty. Ve fyzickém světě je pojmem „geographic component“ myšleno přesné uložení síťových prvků. Fyzické síťové komponenty pak zahrnují infrastrukturu řídících prvků sítě (router, switch), kabely a ostatní zařízení. Rozložení fyzické vrstvy je naprosto logické, protože překročení geopolitických hranic různých států není v kyberprostoru žádným problémem. Ale v reálném světě nadále existují omezení a pravidla, která vyplývají z fungování fyzického světa. Logická vrstva se skládá z logicky propojených síťových uzlů, které se obecně nazývají logické síťové komponenty. Vrstva sociální v sobě ukrývá komponenty nazývané osobnost, což je skutečná osoba připojena k síti, a pak také „kyberosobnost“, která identifikuje osobu na síti. Příkladem je e-mailová adresa nebo číslo telefonu. Jedna osobnost v reálném světě, může mít v kyberprostoru více „kyberosobností“ (Concept Capability Plan..., 2010).

Pokud by se kyberprostor dělil podle dohledatelnosti a dostupnosti dat pro běžného uživatele, pak by bylo možné použít podrobnější rozdělení na:

- data, která jsou dostupná pomocí internetu a na to navazující služby,
- data a služby dostupné v konkrétních sítích a zařízeních,
- data a služby, které jsou záměrně skryté a k jejich dostupnosti je zapotřebí použití speciálních nástrojů (Fleischmanová, 2015).

Pokud jsou utvořeny tyto 3 kategorie, pak se používají tyto názvy:

1) Dark Web,
2) Surface Web a
3) Deep Web (Bartlett, 2016).

Dark a Deep Weby mohou být souhrnně označeny jako D4rkN3ts, tj. Darknets. Skutečný kyberprostor poté tvoří společně všechny tyto součásti. Pro laickou veřejnost se bohužel do mysli zaryla jednoduchá rovnice: WEB = INTERNET = KYBERPROSTOR. Kyberprostor se netýká pouze webových stránek, nýbrž všech počítačových systémů, uživatelů, služeb a dat, pohybujících se v tomto prostoru (Bartlett, 2016).

1.2 Kybernetická bezpečnost (cyber security)

Premisa, že se kybernetická bezpečnost týká pouze specialistů na informační technologie, je velice mylná. Každý, kdo využívá jakkoliv prvky informačních technologií v každodenním životě si musí uvědomit, že je klíčovým a v některých případech i stěžejním subjektem kybernetické bezpečnosti (Jirásek et al., 2015).

Oxfordský slovník definuje kybernetickou bezpečnost jako stav ochrany před neautorizovaným či kriminálním užitím elektronických dat (Definition of cybersecurity…, 2018).

Dle Jiráska et al. (2015) je kybernetická bezpečnost: souhrn organizačních, právních, vzdělávacích a technických prostředků, které slouží k zajištění obrany kybernetického prostoru.

Security neboli bezpečnost se dá vysvětlit jako obecná ochrana před poškozením, zcizením nebo třeba zničením. Přívlastek kyber (cyber) se používá v souvislosti s počítačovými systémy a počítači obecně. Kybernetická bezpečnost by tedy šla také definovat jako ochrana počítačových sítí a počítačů před kybernetickými útoky, které jsou

vedeny z kyberprostoru. Pokud dojde k tzv. kybernetickému útoku (cyber attack), nejedná se o zcizení, poškození či zničení, protože by se hovořilo o hmotných aktivech. V našem případě se tedy jedná o napadení základních bezpečnostních atributů. Konktrétně se to poté týká: availability (dostupnosti), integrity (integrity) a confidentiality (důvěrnosti) (Šulc, 2018).

V ideálním případě by se cílem měl stát stav „absolutního bezpečí". O tom by se však dalo spíše mluvit jako o utopii, protože stavu absolutního bezpečí nelze reálně dosáhnout. I když je vytvořený koncept bezpečnosti, existují vždy rizika či hrozby, které nejsou do tohoto dokumentu zapsány. Buď nejsou do dokumentu zahrnuty, nebo jejich riziko bylo opomenuto (Waisová, 2005).

1.2.1 Kybernetická bezpečnost a její principy

Pokud hovoříme o kybernetické bezpečnosti, nastává implementace principů, které jsou nazývány jako triády. V této problematice jsou dále vymezeny tři triády:

1) Prvky kybernetické bezpečnosti (Procesy, Lidé, Technologie);
2) KB a její životní cyklus (Reakce, Prevence, Detekce;
3) CIA, kde písmeno C = Confidentiality, písmeno I = Integrity a písmeno A = Availability (Smejkal et al., 2019).

Nejpoužívanejší a zároveň nejznámější triádou je CIA. Tato triáda základních principů bez implementací by byla v současné době nedostačující. Odborná literatura poukazuje na použití Parkerian hexad, neboli rozšířenou verzi CIA triády o tři další prvky: A = Authenticity, P/C = Possession/Control a U = Utility (Hsu et al., 2013; Smejkal et al., 2019).

Triádu CIA je důležité aplikovat i na další prvky kybernetické bezpečnosti jako jsou počítačové systémy, data aj. (Andress, 2014).

1.2.2 Confidentiality, Integrity, Availability

Confidentiality (důvěrnost) je pojem, který definuje fakt, že jen oprávněné osoby (subjekty) mají přístup k datům, informacím aj. Jsou aplikovány tzv. Bezpečnostní standardy ISO/IEC 27000, ve kterých je například definováno, jakým způsobem by měly být klasifikovány informace, zacházení s nimi, jaká jsou pravidla pro jejich manipulaci, ukládání apod (Kolouch et al., 2019).

Příklady klasifikačních schémat:

1) Klasifikace dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů:

- *přísně tajné* (top secret), tj. únik informací a nevhodné nakládání s nimi by mohlo způsobit mimořádně vážné problémy České republice;
- *tajné* (secret), tj. únik informací a nevhodné nakládání s nimi by mohlo způsobit vážné problémy České republice;
- *důvěrné* (confidential), tj. únik informací a nevhodné nakládání s nimi by mohlo způsobit prosté komplikace České republice;
- *vyhrazené* (restricted), tj. únik informací a špatné nakládání s nimi by mohlo být nevhodné pro zájmy České republiky (Zákon č. 412/2005 Sb.).

2) Klasifikace využívaná ve sféře komerční:

- *chráněné*, tj. zneužití informací by mohlo způsobit zničení či závažné poškození organizace;
- *interní*, tj. zneužití informací by mohlo způsobit poškození organizace,
- *citlivé*, tj. zneužití informací by mohlo mít negativní dopady na organizaci;
- *veřejné*, tj. zde by jakékoliv použití informací nemělo mít negativní dopady na společnost (Šulc, 2018).

3) Traffic Light Protocol – v roce 2000 byl v National Infrastructure Security Coordination Centre vytvořen protokol TLP, který má za úkol usnadnit, zrychlit a zabezpečit přenos informací mezi subjekty kybernetické komunity (Traffic Light Protocol, 2015).

Integrity (Integrita) je definována jako vlastnost úplnosti a přesnosti dle výkladového slovníku (Jirásek et al., 2015). Integrita dat je vlastně jakási záruka, že daná data nejsou jakýmkoliv způsobem změněna nebo upravena. Integrita je vlastnost systému, který vykonává svou funkci nenarušeným způsobem. Integrita se tedy stává ochráncem dat a informací, kdy je představitelem nemožnosti zásahu jiným uživatelem. Také by se dalo říct, že je jakousi zárukou neporušenosti systému (Šulc, 2018).

Integritu lze rozdělit do čtyř kategorií:

- *nízká*, kdy pro aktivum není vyžádána ochrana;

- *střední*, kdy aktivum z hlediska integrity může vyžadovat ochranu;
- *vysoká*, kdy z hlediska integrity aktivum potřebuje ochranu (využitím speciálních prostředků lze pro ochranu integrity zaznamenat identitu osoby, která provádí změny a jsou prováděny i změny v systému; kryptografické prostředky slouží jako ochrana informací, které jsou přenášeny komunikačními sítěmi);
- *kritická*, kdy z hlediska integrity aktivum vyžaduje ochranu (zde jsou využívány speciální technologie k identifikaci osoby, která provádí změnu – např: technologie digitálního podpisu (Jirásek, 2015).

Availability (dostupnost) je definována jako použitelnost a přístupnost k informacím a datům na žádost entity, která je k tomuto počinu oprávněna. Dalo by se také říci, že je to garantovaný přístup k informacím v okamžiku potřeby. Pokud dojde ke zničení určitých informací, tak v kybernetické bezpečnosti mluvíme o tzv. narušení jejich dostupnosti (Kolouch et al., 2019).

Dostupnost je podle vyhlášky o kybernetické bezpečnosti rozřazena dle stupnice do čtyř kategorií:

- *nízká* – narušení aktiva není důležité a k obnovení by měl stačit týden, ochrana probíhá pravidelným zálohováním dat;
- *střední* – narušení aktiva by mělo být opět funkční do jednoho dne, ochrana probíhá metodami obnovy a zálohování;
- *vysoká* – dostupnost aktiva nemá překročit několik hodin, pro tento případ jsou používány záložní systémy;
- *kritická* – nedostupnost a výpadek aktiva není tolerován ani v řádu desítek minut, pro obnovu dostupnosti jsou používány záložní zdroje (Šulc, 2018).

1.2.3 Kybernetická bezpečnost a její prvky

Vzájemná interakce tří prvků, kterými jsou technologie, procesy a lidé by měla nastolit či vytvořit do jisté míry kybernetickou bezpečnost. Pokud by byl sestrojen izolovaný počítačový systém, který by byl uzavřen např. ve Faradayově kleci, kde by byli přesně definováni lidé, kteří by k němu měli přístup a nebylo by možné vynášet ani vnášet žádné médium, poté by se dalo hovořit o bezpečném systému. Zůstává zde však otázka, jak by vlastně takový systém vůbec mohl fungovat. Technologie slouží jako prostředek umožňující se připojit k internetu, aplikacím či sociálním sítím. Je to nástroj, který

využívá různé kancelářské balíčky, mezi které patří zasílání e-mailů, sledování videí atd. Pokud se jedná o organizace, zde technologie plní funkce určené jednak *pro uživatele* (mobilní zařízení), dále pro *infrastrukturu sítě* (LAN – Local Area Network, Wi-Fi prvky, aktivní prvky), pro prvky *zasluhující se o zabezpečení* již na perimetru (honeypot, firewall, IDS - Intrusion Detection System/IPS -Intrusion Prevention System aj.) a v neposlední řadě pro *ostatní infrastruktury* (monitoring, analýza atd.) (Kolouch et al., 2019).

Aby technologie a s nimi propojené služby bylo možné využívat lidmi, je třeba zapojit procesy, které svou činností přesně toto umožňují. Do procesů je možné zařadit například analýzu nápravných opatření, autentizace a autorizace, opatření nápravných realizací, cvičení a školení, detekce kybernetických útoků či anomálií nebo třeba řízení rizik a aktiv. Výčet jednotlivých procesů není úplný, záleží zde na jejich využití a konečném produktu. Každý určitý systémový proces je realizován v celoživotním cyklu ICT (informační a komunikační technologie), dat a informací a také vždy závisí na vztahu k uživateli. Nejnáročnější práci z hlediska budování kybernetické bezpečnosti zaručeně tvoří vlastní nastavení procesů, jejich modifikace či neustálá údržba. Zároveň klade nejpřísnější nároky na správce (Schneier, 2003).

Pokud je to v organizaci možné, je velice výhodné provádět zde simulace obvyklých kybernetických útoků, mezi které se nyní řadí nejvíce business e-mail compromise nebo třeba phishing. Pokud jsou již nastavené procesy v provozu, lze v nich díky penetračnímu testování nalézt chyby. Při nastavování pravidel a tvorbě kybernetické bezpečnosti by měla být organizace především zaměřena na oblast lidských zdrojů a náležitou edukaci (Šulc, 2018).

Lidé v této interakci hrají roli tzv. tvůrců dané bezpečnosti. Schneier však zmiňuje, že právě nejslabší článek v systému jako takovém představují právě lidé samotní. Tento názor mohou doplňovat 3 základní důvody tohoto tvrzení. Prvním je relativně krátká doba, kdy lidstvo jako takové využívá ony počítačové systémy, druhým je dynamika vývoje hardwaru i softwaru a třetím je neodmyslitelná součást lidských životů, kdy se z osob díky informačním technologiím často stávají zcela odlišní lidé (Schneier, 2003).

Pokud se na roli lidí v systému kybernetické bezpečnosti nahlíží v souvislosti se zákonem o kybernetické bezpečnosti zákon č.181/2014 Sb. o kybernetické bezpečnosti, je nutné si uvědomit potřebu vytvoření následujících pozic, tj. uživatel, administrátor, provozovatel,

technický správce, věcný správce, garant (primárních aktiv a podpůrných aktiv), tým kybernetické bezpečnosti, auditor kybernetické bezpečnosti, architekt kybernetické bezpečnosti, manager kybernetické bezpečnosti a výbor kybernetické bezpečnosti . Pro uživatele je proto nezbytné při využívaní ICT znát alespoň základní pravidla kybernetické bezpečnosti, porozumět počítačovým funkcím a vzdělávat se (Gála et al., 2015).

1.2.4 Kybernetická bezpečnost a její životní cyklus

K realizaci kybernetické bezpečnosti je zapotřebí uplatňovat, případně modifikovat triádu CIA a poté dílčí prvky kybernetické bezpečnosti po celou dobu jejich životního cyklu. Mezi dílčí prvky se řadí prevence, detekce a v neposlední řadě reakce na útok. Udržování i budování kybernetické budoucnosti lze přirovnat k nekončící analýze rizik, kterou je třeba doplňovat o podpůrné procesy. Ty by měly sloužit ke zvýšení kybernetické bezpečnosti (Kolouch et al., 2019).

1.2.5 Informace a typy dat

Všechny organizace, bez ohledu na své odvětví a velikost, zpracovávají informace a data. Identifikace informací a dat, která se většinou opakují a jsou tedy i pro útočníka mnohdy cílem, je důležité umět rozeznat. Informace i data se v organizaci mohou nacházet v podobách, jako je např. papírová forma nebo elektronická forma. Jsou uloženy na nejrůznějších nosičích. Základními nosiči jsou např.: SSD disky počítačů, HDD, SAN/NAS případně i v cloudu, vyjímatelná či přenosová média, mezi která patří optické disky (DVD, CD, BR), USB flash disk, micro SD a SD karty apod. (Požár, 2005).

Na každém nosiči se pak nacházejí informace a data, která jsou vytvářená, zpracovávaná a uložená pomocí programu, aplikace či systému. Nejčastěji se zde nacházejí v podobě souborů v databázi či adresářové struktury. Nehledě na použitý formát dat, způsob uložení a použité kódování se nejčastěji jedná o informace týkající se jedné z těchto oblastí:

- *finanční řízení* – výkazy, účetní doklady;
- *ICT* – databáze, aplikace, systémy, zdrojové kódy, síťová infrastruktura;
- *management* – taktické plány, strategické plány, projektová dokumentace, pracovní postupy, operativní plány, směrnice a standardy, bezpečnostní politika;
- *marketing* – informace o dodavatelích a klientech, analýzy, průzkum trhu, informace o produktech a službách, připravované marketingové kampaně, detaily

o stávajících, proběhlých a budoucích obchodech, facility – umístění čidel, kamer, spínačů, ostraha a její úkoly, plány budov;

- *řízení lidských zdrojů* – pracovní pozice, jejich obsazenost a popis, osobní údaje zaměstnanců (kontaktní informace, osobní číslo, výsledky hodnocení, pracovní zařazení, výše mzdy), motivační systém (zaměstnanecké výhody, bonusy, systém hodnocení) (Singer et al., 2013).

Vypsaný výčet není samozřejmě kompletní – je na něm však jasné, jak jsou informace zajímavé a velmi snadno zneužitelné (Singer et al., 2013).

1.2.6 Informace a její životní cyklus

Celý životní cyklus informace musí být chráněný (information life cycle). Patří do něj uložiště (data at rest), přenos (data in motion) a samotné používání (data in use). Stačilo by, aby jeden z těchto úseků cyklu byl nedostatečně chráněn a mohlo by dojít k narušení dostupnosti, důvěrnosti a integrity (Amoroso, 2006).

Způsob, jakým je informace chráněna, se odvíjí od její citlivosti a kritičnosti. Z tohoto důvodu by každá informace měla mít svého vlastníka, který za ni zodpovídá a prováděl její klasifikaci. Ta spočívá v rozhodnutí o tom, kdo k informaci bude mít přístup a jaký (Šulc, 2018).

Data at rest je klíčový přístup k datům v uložišti. Zde by měl být vytvořen vždy řízený přístup, který by zabezpečoval, aby se k daným datům dostala pouze pověřená osoba a nakládala s nimi jen podle její úrovně prověření. Jelikož může dojít k fyzické krádeži uložiště, měla by být data vždy dostatečně šifrována. Na druhé straně se může útočník pokoušet pouze o zničení odcizených dat. Z tohoto důvodu by měla být vždy adekvátně zálohovaná. Archivace by pak nadále měla probíhat v lokalitě geograficky vzdálené. Narušení integrity je možné zabránit například tzv. vytvářením kontrolních součtů dat nebo podepisováním. Důležitá součást je i bezpečná likvidace dat, která zabraňuje snadnému obnovení již zničených dat (Šulc, 2018).

Data in motion pokud dochází k přenosu dat do/z uložiště, je důležité tato data dostatečně šifrovat. Pokud by data nebyla dostatečně šifrována, mohlo by dojít k odposlechnutí, zahození či změně ze strany útočníka (obzvlášť je kladen důraz na přenos dat přes veřejnou síť příkladem je internet). Vhodné je číslování zpráv, protože je jasné při příjmu zpráv do uložiště, zda došla ve správném pořadí nebo zda nedošlo k tzv. replay attack.

Možností je také podepisování zpráv, kdy je snadné pak pozměněnou nebo podvrženou zprávu odhalit (Šulc, 2018).

Data in use největšímu riziku jsou data vystavena ze strany uživatele, ten data pořizuje a nejčastěji k nim má přístup pomocí operačního systému, aplikace či databáze. Takový uživatel potřebuje k práci s daty oprávnění. V některých případech však nemusí mít ani přístupové právo, neboť jeho přístup k datům je skrz aplikace. Proto je vhodné, aby systém byl často auditován, jelikož by mohl uživatel svého legitimního přístupu zneužít. Je důležité dodržet veškerá opatření k pozitivním výsledkům (Šulc, 2018).

1.2.7 Aktivum, riziko, zranitelnost

Aktivem se rozumí cokoliv, co má hodnotu pro organizaci, osobu či stát. Z pohledu občanského práva lze aktivum rozdělit na věc hmotnou (sítě, energie, zboží, budova) nebo nehmotnou (data, znalosti, informace). Dále může být aktivem i vlastnost (funkčnost a dostupnost dat), reputace či dobré jméno a lidé (administrátoři aj.) (Jirásek et al., 2015).

Dle výkladového slovníku kybernetické bezpečnosti lze definovat **riziko** jako: možnost ztráty, škody a nezdaru při vzniklém nebezpečí (Jirásek et al., 2015).

Pravděpodobnost, s jakou nastává nechtěná událost, se nazývá riziko. Pomocí analýzy rizik lze poté vyjádřit míru pravděpodobnosti této události (Jirásek et al., 2015).

Valášek et al. (2008), upozorňují na tři základní otázky, které se využívají ke stanovení rizika. Příkladem může být otázka: „Co může selhat?“. Pokud se určuje charakteristika rizika podrobně, využívají se tzv. doplňující otázky.

Při určování každého rizika se dále počítá i stupeň rizika a jeho význam (Kolouch et al., 2019).

Lze vyjádřit takto:

$$R \times D = V \qquad (1)$$

přičemž:
R je pravděpodobnost výskytu rizika,
D je rizika a jeho dopady,
V je významnost rizika.

Následky neboli dopady rizika lze hodnotit v pětibodové stupnici. Pro určení

pravděpodobnosti vzniku rizika slouží opět pětibodová stupnice. Po výpočtu stupně významnosti nám výsledek vychází buď nízký, střední nebo vysoký (Kolouch et al., 2019).

Vulnerability neboli **zranitelnost** označuje slabé místo softwaru, aktiva, zabezpečení, které je využito hrozbami. Celou řadou faktorů může být způsobena jak hrozba, tak i zranitelnost, ať už se jedná o technickou závadu, jednání člověka atd. Zranitelnost se může v kybernetické bezpečnosti dělit na:

- zranitelnost známou (opravené, neopravené) a
- zranitelnost neznámou (skrytá, neobjevená).

Ve zranitelnosti neznámé hraje hlavní roli fakt, kdo tuto skutečnost objevil (Jirásek et al., 2015).

1.3 Česká republika a kybernetická bezpečnost

V dnešní době je lidstvo velice závislé na komunikačních a informačních technologiích, což vede k využívání kybernetického prostoru. Tuto skutečnost si uvědomují hlavně jednotlivé zájmové skupiny, u kterých hrozí potencionální zneužití informací a dat, které později i mnohdy nastává. A to je jeden ze základních důvodů nastavení kybernetických pravidel, která by byla uplatnitelná v kyberprostoru. Tato pravidla vznikají jako tzv. regulace, které mají za úkol ochránit především poskytovatele infrastrukturních služeb a kritickou informační infrastrukturu. Kritickou informační infrastrukturu (dále jen KII) vymezuje zákon č. 240/2000 Sb., o krizovém řízení a změně některých zákonů (krizový zákon), ve znění pozdějších předpisů. V tomto zákoně se jasně vymezuje komplex informačních systémů. V případě jejich nefunkčnosti by to mělo velký dopad na ekonomiku státu, její bezpečnost, základní životní potřeby obyvatelstva a veřejnou správu (Doucek et al., 2019).

Mezi hlavní důvody vytvoření regulace kybernetické bezpečnosti patří: rychlý vývoj technologií, vzrůstající počty kybernetických útoků, narůstající riziko a dopady těchto rizik ve spojitosti s využíváním komunikačních a informačních technologií, každodenní využívání komunikačních a informačních technologií a jednoznačná lidská závislost na nich, požadavek na koordinaci ze strany státu, předcházející kybernetickým bezpečnostním incidentům, požadavky ze stran NATO, OSN a v neposlední řadě i evropské unie. Důležitý je i fakt, že kybernetický prostor nezná hranice států, proto je

nutné vytvořit pro všechny „hráče“ stejná globální pravidla. Z těchto a dalších důvodů již jasně vyplývá nutnost zavedení regulací. V České republice se setkáváme s Národním úřadem pro kybernetickou bezpečnost (dále jen NÚKIB), který je gestorem kybernetického zákona (Doucek et al.,2019).

Vznik Národního úřadu pro kybernetickou bezpečnost podpořila i strategie Evropské unie a její direktiva, tj. Směrnice NIS (EU, 2016a). Velmi podobný přístup České republiky ke kybernetické bezpečnosti má například Estonsko, to je považováno za velmoc e-Governmentu. Odlišný přístup k regulacím má například USA nebo Velká Británie, kde kybernetickou bezpečnost má na starosti poměrně rozsáhlá struktura státních institucí, na rozdíl od České republiky a Estonska, kde za kybernetickou bezpečnost odpovídá plně pouze jedna státní instituce (Riigi Teataja, 2010).

1.3.1 Regulační rámec kybernetické bezpečnosti a Směrnice NIS

Směrnice NIS – „*Směrnice Evropského parlamentu a rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (EU, 2016a).*“ (Směrnice Evropského parlamentu a Rady, 2016).

Členské státy Evropské unie musí směrnici přijmout a dále ji zapracovat do národní legislativy. V Evropské unii však existovaly státy, pro které v oblasti ICT bezpečnosti, nebyly regulace žádnou novinkou. Jednou z takových zemí byla i Česká republika, která měla účinnost prvotní verze zákonu o kybernetické bezpečnosti již v lednu 2015 (Doucek et al., 2019).

Podle Směrnice NIS povinné subjekty rozdělujeme na 2 základní skupiny. Jako první jsou provozovatelé základních služeb (PZS), kteří jsou alternativou kritické informační infrastruktury. Druhou skupinou jsou poskytovatelé digitálních služeb (dále jen PDS). Provozovatelé základních služeb (dále jen PZS) jsou veřejné nebo soukromé subjekty z určitého odvětví. To spadá do poskytování základních služeb z hlediska zachování ekonomické nebo společenské činnosti, přičemž poskytovaná služba je závislá na komunikačních a informačních technologiích, a pokud by došlo ke kybernetickému útoku, mohlo by se významně narušit poskytování této služby. Příkladem mohou být dodavatelé pitné vody a její distributoři (Doucek et al., 2019).

Pro PDS Směrnice NIS stanovuje, že tímto statutem je definována právnická osoba. Tato

osoba musí poskytovat některou ze tří uvedených služeb (EU, 2016a) – internetový vyhledávač, on-line tržiště nebo službu cloud computingu (Doucek et al., 2019).

Bezpečnostní požadavky jsou kladeny na oba typy povinných subjektů. Vše je řízeno Směrnicí NIS (EU, 2016a). Mezinárodně uznávané normy nebo standardy týkající se ICT bezpečnosti samozřejmě Evropská unie podporuje, ale zároveň se snaží o zachování technologické neutrality (Směrnice Evropského parlamentu a Rady, 2016).

Povinnosti pro PZS – nahlášení kybernetického incidentu (týmu CERT/CSIRT), řízení rizik, postupy vedoucí k předcházení incidentu a popřípadě minimalizace jeho dopadu, určení míry rizika k vyhotovení bezpečnostních opatření (Doucek et al., 2019).

Povinnosti pro PDS – nahlášení kybernetického incidentu (týmu CERT/CSIRT), řízení rizik, postupy vedoucí k předcházení incidentu a popřípadě minimalizace jeho dopadu, určení míry rizika se zohledněním na – řízení kontinuity provozu, audity a testování, monitoring, soulad s mezinárodními normami, bezpečnost systémů a zařízení (Doucek et al., 2019).

Subjekty spadající pod regulaci eIDAS (Electronic Identification and Services) – (EU, 2014) a také subjekty, které patří pod regulaci zákona o elektronických komunikacích, jsou výjimkami, a tudíž se na ně nevztahuje požadavek o nahlašování incidentů ani jiné bezpečnostní požadavky. Pouze v případě, že by tento subjekt patřil zároveň do kategorie kritické informační infrastruktury dle kybernetického zákona, pak by tato výjimka neplatila (Doucek et al., 2019).

1.3.2 Computer Security Incident Response Team a Computer Emergency Response Team

CSIRT (Computer Security Incident Response Team) nebo CERT (Computer Emergency Response Team) je tým odborníků, který se zabývá informační bezpečností. Jejich úkolem je řešit bezpečnostní incidenty a znovu obnovit napadené systémy. CSIRT/CERT poskytuje svým zákazníkům také vzdělávací a preventivní služby (Jirásek et al., 2015).

CSIRT/CERT odpovídá za agendu, která souvisí s bezpečnostními incidenty v rámci státu, komunity, odvětví, sítě či organizace. Pokud se jedná o poskytovatele digitálních služeb, využívá se metoda maximální harmonizace. Tato metoda spočívá v naplnění dané direktivy členského státu a neměla by být mírnější či přísnější než je nastavena. Po

poskytovateli základních služeb však Česká republika může vymáhat přísnější bezpečnostní požadavky, než je uvedeno ve Směrnici NIS (Jirásek et al., 2015).

1.3.3 Agentura European Union Network and Information Security Agency

Evropská unie zaštítila v roce 2004 vznik agentury ENISA (European Union Network and Information Security Agency), která se zaměřuje na kybernetickou bezpečnost. Původním cílem této agentury byla podpora činností souvisejících se Směrnicí NIS. Do činnosti se řadí tvorba Směrnice NIS a její prosazování. Agentrua ENISA má také jako další úkol podporu dalších regulací Evropské unie jako je např.: GDPR (General Data Protection Regulation), eIDAS (eID And Signature EU, 2014). Spolupráci navazuje agentura hlavně s členskými státy EU a se soukromým sektorem (ENISA, 2021).

Obecné činnosti agentury ENISA rozdělené do 3 základních skupin:

- Subvence při tvorbě národní politiky a její další implementace.
- Udělení doporučení.
- Praktická interakce napříč EU, např.: koordinace vzdělávání (Doucek et al., 2019).

1.3.4 Kyber balíček

Význam agentury ENISA vzrostl v okamžiku, kdy Evropská unie vydala legislativní návrhy a soubor koncepčních dokumentů, kterému začala říkat „kyber balíček“. Vznikl za účelem obranyschopnosti Evropské unie, velkou výhodou je i zvýšení bezpečnosti spotřebitelů a posílení funkce digitálního trhu. „Kyber balíček“ je založen na 4 pilířích: krizové plány vytvořené k rozsáhlým kybernetickým útokům, posílení role ENISA, uznávání národních certifikačních rámců, harmonizace opatření, které byly přijaty v rámci Směrnice NIS (Doucek et al., 2019).

1.4 Česká republika a vznik kybernetického zákona

Začátek je evidován v roce 2011. V tomto roce Česká republika nejdříve schválila svým usnesením Strategii pro oblast kybernetické bezpečnosti České republiky. Tato strategie byla vyhotovena na období 2011 až 2015. K této strategii vyhotovila a zpracovala ještě Akční plán pro období 2011 až 2015. Hlavním úkolem akčního plánu a strategie bylo vytvoření zákonodárného rámce. Touto dobou však v České republice nabyla žádná instituce, která by se problematikou kybernetické bezpečnosti zabývala a byla za ni plně odpovědná. Vláda České republiky dne 19. října 2011 svým usnesením rozhodla, že

gestorem této problematiky se stane nově vzniklý Národní bezpečnostní úřad (NBÚ). Ten měl jako první úkol aktualizovat akční plán a strategii. Stejným usnesením, kterým vznikl Národní bezpečnostní úřad, vláda zřídila Radu pro kybernetickou bezpečnost. Spolu s NBÚ vzniká ještě tzv. Národní centrum kybernetické bezpečnosti. To slouží jako organizační celek a je součástí NBÚ. V tuto chvíli NBÚ, působil jako gestor dané problematiky a oblast kybernetické bezpečnosti představovala velkou výzvu (Doucek et al., 2019).

1.4.1 Strategie kybernetické bezpečnosti České republiky v období 2012–2015

V období 2012–2015 byly stanoveny Národním bezpečnostním úřadem prioritní cíle Strategie pro oblast kybernetické bezpečnosti České republiky následovně: zvyšování znalostí a povědomí a kybernetické bezpečnosti, vybudování legislativního rámce pro oblast kybernetické bezpečnosti, mezinárodní podpora a spolupráce v oblasti kybernetické bezpečnosti, národní spolupráce (spolupráce soukromé, veřejné a akademické sféry), řízení a koordinace rizik kybernetické bezpečnosti (Doucek et al., 2019).

Ze Strategie dále vychází Akční plán opatření ke Strategii. V něm jsou zapracované jednotlivé strategické úkoly do činností a projektů a ty jsou přiřazeny jednotlivým orgánům veřejné správy. Kromě NBÚ byly problémy některých bodů řešeny Ministerstvem obrany České republiky, Ministerstvo vnitra České republiky, Ministerstvo průmyslu a obchodu, Český telekomunikační úřad, Ministerstvo zahraničních věcí, zpravodajské služby a další organizace (Doucek et al., 2019).

To, jak byl rok úspěšný z hlediska kybernetické bezpečnosti, plnění akčního plánu a strategie, se vyhodnocuje na konci každého roku. Hlášení o stavu se zpravidla píše do tzv. Zprávy o stavu kybernetické bezpečnosti České republiky (Doucek et al., 2019).

1.4.2 Rada pro kybernetickou bezpečnost

Rada pro kybernetickou bezpečnost (dále jen RKB) je poradním a koordinačním orgánem předsedy vlády. Slouží pro oblast kybernetické bezpečnosti. Vzniká 19. října 2011. Cílem rady je podpora výkonu koordinační a gesční role gestora pro kybernetickou bezpečnost, která vyžaduje součinnost subjektů kritické infrastruktury a státních institucí. Tato rada se skládá z předsedy, tím je současně předseda vlády, výkonného místopředsedy tuto pozici zastává ředitel NBÚ (poté NÚKIB), členů a tajemníka, kterým je pracovník NBÚ

(následně NÚKIB), jmenován je předsedou rady. Mezi členy rady jsou nejčastěji delegováni zástupci ze státních institucí, nejčastěji ze zpravodajských služeb, zástupci ministerstev a zástupci dalších ústředních správních úřadů. Rada zasedá minimálně jednou za rok. Pokud by byla potřeba můžou k radě přisednout představitele kritické infrastruktury nebo externí odborníci. Rada pro kybernetickou bezpečnost má 8 základních bodů, které plní. Mezi ně patří například: analýzy a shromažďování údajů o vývoji současné situace týkající se kybernetické bezpečnosti, vytváření podmínek pro snadné fungování členů rady mezi sebou, kladení a následné řešení otázek týkajících se kybernetické bezpečnosti, předkládání návrhů vládě aj. (Doucek et al., 2019).

1.4.3 Zákon o kybernetické bezpečnosti

Na základě dílčích činností v souvislosti s akčním plánem a již dříve uvedené strategie byl přijat v České republice kybernetický zákon v prvotní verzi. V tomto případě byl uplatněn zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. Jedná se o kybernetický zákon. Této zákon měl účinnost od 1. ledna 2015. Zákon č. 181/2014 Sb. o kybernetické bezpečnosti, prošel v roce 2017 dvěma obsahově významnými novelami (Šulc, 2018).

Prostřednictvím osob soukromého práva, které nespadaly pod specifické regulace, se řešila ochrana kybernetického prostoru před vznikem kybernetického zákona. Největší podporu při vzniku kybernetického zákona tvořily požadavky mezinárodních společenství a dále pak závazky České republiky vůči Evropské unii a NATO (Šulc, 2018).

Vznik kybernetického zákona byl důležitý také kvůli narůstajícím počtům DDoS (Distributed Denial of Service) útokům. Jedná se o zvláštní techniky útoků na internetové služby. Pokud dojde k takovému útoku, vznikne přehlcení požadavky a nefunkčnost nebo pád služeb pro ostatní uživatele. Pokud se jedná o útok tohoto typu, je využíván princip tzv. velkého množství rozptýlených počítačů, který je cílený na bankovní servery, finanční instituce, kam spadá např. i Česká národní banka, zpravodajské servery, internetové stránky mobilních operátorů a Pražské burzy cenných papírů. Tento typ útoků byl hodně populární v České republice hlavně začátkem roku 2013 (Maisner, 2015).

Kybernetický zákon má za cíl vytvoření zákonného postavení státní instituce, kdy tato

instituce bude oprávněná k regulaci základních subjektů a bude mít zodpovědnost za kybernetickou bezpečnost státu. V České republice lze státní moc uplatňovat pouze v mezích zákona. Povinnosti osobám soukromoprávním lze ukládat pouze zákonem (Doucek et al., 2019).

Za dobu své účinnosti prošel zákon o kybernetické bezpečnosti několika drobnými legislativními změnami. Zásadní však byly dvě významné novelizace v období roku 2017, a to mezi měsícem červenec a srpen. Poslední novela se podílí na vzniku Národního úřadu pro kybernetickou bezpečnost. Další novelizace se týkala transpozic Směrnice NIS Evropské unie. Většina změn se týkala zkušeností od NÚKIB. Cílem bylo zaměření na zvýšenou kybernetickou bezpečnost. Po novelizaci, zákon dopadá hlavně na provozovatele a správce důležitých systémů (Doucek et al., 2019).

1.4.4 Související legislativa

Mezi související právní předpisy patří např.:

- zákon č. 240/2000 Sb., o krizovém řízení a změně některých zákonů;
- zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti;
- zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce;
- zákon č. 250/2017 Sb., o elektronické identifikaci;
- zákon č. 110/2019 Sb., o zpracování osobních údajů;
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy;
- zákon č. 413/2005 Sb., o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti;
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy;
- zákon č. 181/2014 Sb., o kybernetické bezpečnosti;
- vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích;
- vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti;
- vyhláška č. 437/2017 Sb., o kritériích o určení provozovatele základní služby;
- Směrnice Evropského parlamentu a Rady (EU) 2016/1148, provádějící nařízení ke směrnici NIS aj.

1.4.5 Národní strategie kybernetické bezpečnosti České republiky 2015–2020

Usnesení Vláda České republiky dne 16. února 2015 svým usnesením schválila Národní strategii kybernetické bezpečnosti na období 2015-2020. Tento dokument navazuje na předešlou strategii a akční plán. Národní strategie pro kybernetickou bezpečnost za období 2015-2020 představuje zásadní změnu pro vnímání kybernetické bezpečnosti. Věnuje se hlubšímu a pokročilému zajišťování kybernetické bezpečnosti. Prioritní cíle strategie jsou rozděleny do 8 oblastí:

- Ochrana významných informačních systémů a národní kritické informační infrastruktury.
- Mezinárodní aktivní spolupráce.
- Posilování všech struktur, spoluprací a procesů, které zefektivní zajištění kybernetické bezpečnosti.
- Soukromý sektor a spolupráce s ním.
- Spotřebitelská důvěra nebo vývoj/výzkum.
- Kybernetická bezpečnost a práce na právní úpravě vycházející z Evropských a mezinárodních pravidel.
- Postihování kyberkriminality a posílení rozvoje a schopností Policie ČR v tomto směru.
- Osvěta, vzdělávání a rozvoj informační společnosti (Doucek et al., 2019).

Na národní strategii je navázán akční plán. Ten rozpracovává strategické úkoly do činností a projektů (Doucek et al., 2019).

1.4.6 Národní strategie kybernetické bezpečnosti České republiky 2021-2025

Národní strategie pro nynější období poukazuje hlavně na fakt, že zajištění kybernetické bezpečnosti v dnešní době výrazně přesahuje technologickou rovinu a tím pádem i vyžaduje ucelený přístup (NÚKIB, 2020).

Vize se rozděluje na 3 základní pilíře, ve kterých jsou dále strategické cíle.

1. Sebevědomě v kyberprostoru: posílení odolnosti a zabezpečení infrastruktury, účinná strategická komunikace, potírání a prevence kyberkriminality aj.

2. Silná a spolehlivá spojenectví: podpora bezpečného a otevřeného chování v kyberprostoru, prosazení zájmů ČR v zahraničí, tvorba spojenců, mezinárodní efektivní spolupráce aj.
3. Odolná společnost 4.0: činnost osvěty, zajištění bezpečnosti eGovernmentu a digitalizace státní správy, kvalitní systém vzdělávání, spolupráce soukromé sféry, státu a občanů aj. (NÚKIB, 2020).

1.4.7 Česká republika a dílčí cíle v oblasti regulace Kybernetické bezpečnosti

Tabulka 1 – Dílčí cíle v oblasti KB

Určité období	Dílčí cíle
7/2011	Národní strategie kybernetické bezpečnosti České republiky a akční plán 2011-2015
10/2011	Národní bezpečnostní úřad se stává gestorem problematiky pro kybernetickou bezpečnost
10/2011	Vzniká - Rada pro kybernetickou bezpečnost
7/2014	Vznik Národního centra pro kybernetickou bezpečnost
12/2014	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
12/2014	Vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti
2/2015	Vyhláška č. 317/2014 o VIS a jejich určujících kritériích
6/2016	Národní strategie kybernetické bezpečnosti České republiky a akční plán 2015-2020
7/2016	Vyhláška č. 317/2014 Sb., o významných informačních syst. a jejich určujících kritériích – aktualizace
7/2016	Regulační rámec – Směrnice NIS
7/2016	Novela – zákona o kybernetické bezpečnosti
7/2017	Vznik Národního úřadu pro kybernetickou a informační bezpečnost
12/2017	Vyhláška č. 437/2017 o kritériích pro určení provozovatele základní služby
5/2018	Vznik nové vyhlášky č. 82/2018 o kybernetické bezpečnosti

Určité období	Dílčí cíle
6/2019	První ročník mezinárodní expertní konference Prague 5G Security Conference
12/2020	Národní strategie kybernetické bezpečnosti České republiky a akční plán 2021-2025

Zdroj: vlastní zpracování

1.5 Kybernetické útoky

Mezi nejzávažnější bezpečnostní rizika se v dnešní době řadí do předních příček kybernetické útoky. Nebezpečí se v případě kybernetických útoků nachází především v asymetrii. Náklady na realizaci kybernetického útoku jsou zanedbatelné oproti škodě, která jejich působením vzniká. Dopady kybernetických útoků již mohou přesahovat i klasické teroristické útoky nebo například následky přírodních katastrof. Dochází při nich totiž k selhání až rozpadu kritické infrastruktury, na které je společnost zcela závislá (Doucek, 2011).

V průběhu posledních let vzrůstá počet věcí a zařízení připojených do internetu, počet útočníků, počty potencionálních obětí a v neposlední řadě samotné útoky. Kybernetické útoky se stávají čím dál více výnosných byznysem, který současně ohrožuje miliony lidí (Fischer, 2009).

Při pohledu pár desítek let zpět nebylo tyto útoky možné provést, přitom dnes jsou zcela běžné. Málokdo měl v této době připojení k internetu, přes telefonní linky se nedalo stahovat velké množství dat, klíčové systémy navíc vůbec nebyly k internetu vůbec připojeny. Připojení tedy fungovalo přes vytáčenou pevnou linku, kdy počet přenesených dat byl velmi omezen. Průnik do systému spočíval pouze ve využití technik zvaných sociální inženýrství. Tyto techniky jsou využívány dodnes, ale explozivní nárůst zaznamenaly hlavně kybernetické útoky. Jejich tempo neustále vzrůstá díky nižšímu riziku odhalení a nízkým nákladům. Novým trendem dnešní doby se stává propojení pracovního a soukromého života. Firmy a organizace se snaží zaměstnancům zpřístupnit informační systém firmy odkudkoli, kdykoli a z čehokoli. Zaměstnanci tudíž využívají čím dál více připojení ze svých soukromých zařízení a tím podstatně zvyšují riziko kybernetických útoků. Počet elektrických zařízení v domácnostech se v průběhu let zvyšuje. Jedná se např. o televize, herní konzole, domácí spotřebiče apod. Všechna tato

zařízení jsou schopna připojení do sítě. Všechny tyto přístroje obsahují aplikace a různé operační systémy, které jsou v průběhu let stále složitější, ale současně se v nich vyskytuje velké množství chyb. Systémy jsou tvořeny lidmi, a pokud se změní velikost systému z pár KB (kilobyte je jednotka množství informace, která se využívá v informatice) na GB (gigabyte je jednotka množství informace, která se využívá v informatice), je jasné, že budou obsahovat i více chyb. Postupem času také vzrůstá objem přenášených dat, rychlost přenosu, různorodost i počet připojených systémů k internetu. Jediné, co nemá vzrůstovou tendenci, je povědomí o bezpečnosti. Uživatelé a jejich bezpečnostní návyky jsou prakticky nulové, je to věc, která je spíše obtěžuje. Příkladem může být prostý požadavek na vytvoření hesla. Uživatelé jsou systémem naváděni na vytvoření silného hesla, ale tuto nápovědu záměrně obcházejí, stále raději volí hesla typu 1234. Není tomu jinak ani u zámku obrazovky na jejich mobilních telefonech. Vytváří jednoduchá gesta k odemykání svých telefonů. Uživatelé dnes rovněž nemají problém se sdílením informací na sociálních sítích a internetu (Jirovský, 2007).

Díky výše uvedeným návykům přibývá útočníků, jelikož návratnost investice je mnohonásobně vyšší než vklad. Web 2.0 nyní nahrává lidstvu ke sdílení dříve těžko přístupných informací. Pokud jsou do vyhledávače zadána správná klíčová slova, lze dnes na internetu najít např. nástroj, který napomůže k vytvoření vlastního virusu. O něco jednodušší variantou je pořízení již hotového virusu za, který se dá objednat za pár dolarů. V tu chvíli se jedná o službu, zahrnující v sobě i podporu tzv. CaaS (Crym as a Service), tím pádem služba „se vším všudy“. Pomocí této služby je jednoduché rozeslat např. phishing emaily, na druhé straně zeměkoule shodit server nebo nahrát podvodnou aplikaci na Google Play (Lidinský et al., 2008).

Pomalu přichází generace Z (je nástupcem Generace Y a patří do ní lidé narozeni po roce 1997) a tím se prodlužuje i vzdálenost mezi obětí a útočníkem. Tato generace je otevřenější, bude se snažit činnosti více automatizovat a je příčinou prosazování průmyslu 4.0. Výpočetní technika a její systémy se dnes již propojují napříč zeměmi i světadíly, a proto se hroutí a selhávají klasické bezpečnostní řešení. Vzrůst kybernetických útoků na společnosti, ať už malé, střední či velké, neustále přibývá. Každá z těchto společností by si měla vzít za vlastní bezpečnostní opatření technické i organizační povahy, protože jejich náklady jsou v porovnání s dopady kybernetických útoků minimální. Mylná představa většiny organizací a firem spočívá v domněnce jejich nedostatečné atraktivity pro útočníka i složitosti provedení takového útoku. Útočník však

prochází celý internet a hledá jakoukoli slabinu využitelnou na webu, takže mu stačí např. rozeslat velké množství podvodných emailů a pak už pouze čekat, kdo přílohu/odkaz rozklikne (Yannakogeorgos et al., 2013).

Odborná veřejnost stále diskutuje nad zveřejňováním zranitelných informací. Jedni tvrdí, že tyto informace útočníkům nepomáhají, druzí zastávají názor, že zveřejňování zranitelných informací útočníkům pomáhá. Skutečnost ukazuje, že pokud se objeví nové zranitelné informace, tak chvilku na to unikají exploity a na to vázané zdrojové kódy, začínají se objevovat nové malware varianty a začíná dramaticky vzrůstat zranitelnost dané informace (Šulc, 2018).

1.5.1 Sociální inženýrství

Technika nazývaná sociální inženýrství spočívá v tzv. přesvědčování, ovlivňování a manipulaci s lidmi. Člověku, který disponuje těmito vlastnostmi, se říká sociotechnik. Sociotechnik se snaží oběť přesvědčit, aby mu poskytla požadované informace nebo se chovala, tak jak se hodí jemu. Hlavním úkolem je získat informace, aniž by si toho oběť byla vědoma. Vystupování takové osoby je autoritativní, vzbuzuje pocit časové tísně, působí dojmem vyššího postavení v sociální hierarchii, tudíž je pro oběť přirozené se podvolit takové dominantní osobě (Shackelford et al., 2016).

Ke komunikaci může sociotechnik zvolit kterékoliv médium. Oslovit oběť může, jak přes podvodný e-mail, SMS, či telefonicky, ale nebojí se ani osobního setkání. Pokud zaměstnanci přijde podvodný e-mail, může po jeho otevření dojít k spuštění souboru, který se na první pohled „tváří“ jako obyčejný dokument, ale může obsahovat nebezpečné makry, ty se spustí a tento útok se pak nazývá spear phishing. Může být však využita i technika nazývající se watering hole. Tato technika se dostane do systému daného počítače, tím že oběť navštěvuje web, ze kterého se samovolně škodlivý kód stáhne do počítače, aniž by oběť musela na něco kliknout (Reveron, 2012).

1.5.2 Plošné a cílené útoky

Většina útočníků hledá nejjednodušší, nejlacinější a nejrychlejší způsob, jak proniknout do systému. Chtějí ho nejdříve kompromitovat a potom využít. Útoky většinou nejsou cílené, útočníci používají tzv. low hanging fruit. Pokud útok nevyjde podle plánu útočníka, nezdržuje se ničím a pokračuje v hledání oběti. Je si vědom faktu, že brzy najde firmu, která nedbá na bezpečnostní opatření (Kolouch et al., 2019).

Část útočníků je odrazena ve chvíli, kdy zjistí, že firma nebo organizace má alespoň základní sadu opatření, která vedou k jejímu zabezpečení. Většina útočníků nejsou žádní experti na informační systémy a jejich zabezpečení, umí pouze využívat sestavené exploity a nástroje od schopnějších (Doucek et al., 2019).

Informace o zranitelnostech firmy, které se dají pod zárukou exkluzivity koupit i za několik tisíc dolarů se využívají už k cíleným útokům. Subjekt má za cíl tuto investici mnohonásobně zvýšit, a proto se na takový útok může připravovat i několik měsíců (Shackelford et al., 2016).

Plošné útoky (bulk/mass attack) jsou velmi časté oproti cíleným útokům. Týkají se v podstatě všech málo zabezpečených subjektů, ale dá se proti nim snadno bránit. V případě plošného útoku je oběť zcela náhodná. Strategie těchto útoků často mývá podobný scénář. Útočník se zmocní díky plošnému útoku snadno některé ze svých obětí. Počítače firmy se v tu chvíli stávají součástí botnetu a přes ně je nadále už veden útok do jiných organizací (Shackelford et al., 2016).

Cílené útoky (targeted attack) jsou méně časté, zároveň jsou ekonomicky více náročné a obrana proti nim je složitá. Útočník v tomto případě veškerou svou pozornost upíná pouze k jednomu vytipovanému subjektu (Shackelford et al., 2016).

Šulc (2018) uvádí příklad z praxe, kdy vlastníci firem a vysoce postavení manažeři se domnívají, že jejich organizace nebo firma není pro útočníka atraktivní. Pokud se však do jejich zařízení dostane nějaký malware (malicious software), neboli škodlivý software, mohou nastat v zásadě čtyři základní situace:

- přímá finanční ztráta firmy;
- napadené počítače se stávají součástí botnetu a jsou pomocí nich vedené útoky na jiné ekonomické subjekty;
- odcizení dat a jejich prodej na černém trhu nebo konkurenci;
- zašifrování dat na disku a tím znemožnění fungování firmy.

Následky, které nastávají po útoku škodlivým softwarem:

Odcizení přihlašovacích údajů týkající se různých služeb, např.: e-shopy, sociální sítě, Paypal a další platební portály, obchodní systémy, aukční portály, internetové bankovnictví, e-mail, VoIP/Skype, FTP servery, on-line muzika, hry a filmy.

- Napadení nainstalovaného SW a jeho sériových čísel.
- Krádež telefonních čísel, kontaktů, e-mailových adres, dat.
- Narušení duševního vlastnictví – to se obzvlášť týká v případě APT (Šulc, 2018).

Napadané zařízení začleněné do botnetu s účelem poškození způsobuje např.: rozesílaní e-mailů typu phishing, SCAM, SPAM a ransomware. Útoky realizované pomocí DDoS na aplikační vrstvě nebo na síťové vrstvě fungující jako C&C server, DNS server nebo proxy server. Uložení malware, ukradených dat (to může fungovat jako tzv. drop-zóna), podvodných webů nebo warezu (obrázky, audio, video). Klikání na podvodné reklamy tipu click fraud. Luštění CAPTCHA (Šulc, 2018).

Odčerpávání prostředků, především finančních. Dochází k tomu podvodnou transakcí v internetovém bankovnictví, nabídkou falešných antivirů, které nechrání nebo zasílání SMS na zpoplatněné číslo. Sledování uživatelů, jejich trasování, jaké otevírají stránky (spyware). Zobrazování nechtěných reklam na stránkách, které byly navštíveny (adware). Přesměrovávání na jiné weby, kde dochází ke samovolnému stažení dalších malware aj. (browser hijacker). Smazání dat na napadeném počítači pomocí malwaru (Šulc, 2018).

Tato ukázka následků může mít fatální dopady na fungování firmy či organizace. Dojde k vyšetřování orgány činnými v trestním řízení. Média označují tuto firmu za napadenou. Důvěra klientů v zabezpečení firmy prudce klesá, a tudíž dochází i k snížení zisku (Singer et al., 2013).

1.5.3 Malware

Malware (malicious software) neboli škodlivý software má za cíl v podstatě cokoliv a jeho projevy na zařízení mohou být různé. Malwary většinou mají za cíl zůstat v zařízení skryti a snažit se přizpůsobit tak, aby přežili např. restart počítače (persistence). Na koncové zařízení může být malware doručen různými vektory útoku, což jsou způsoby napadení zařízení oběti. Může se jednat například o tzv.:

Phishing, tj. že malware je doručen jako příloha v e-mailu.

Drive-by download malware, tj. pouhá návštěva napadené webové stránky zapříčiní stažení malware.

Trojanizovaná aplikace se může nacházet buď na oficiálním nebo neoficiálním marketu, na přenosném médiu i na uložišti (Šulc, 2018).

Podle toho, jak se malware šíří ho můžeme rozdělit na několik typů:

- Trojský kůň (Trojan horse) se z počátku tváří jako aktualizace nebo užitečná aplikace, kterou si pak oběť většinou sama do zařízení stáhne, ale v pozadí provádí škodlivou činnost. Mohou to být např.: screengrabbery (záznam dění na obrazovce), dialery (zasílání zpoplatněných SMS nebo premium volání), minery (špatné nakládání s kryptoměnou) a keyloggery (slouží k odchytávání hesel).
- Červ (worm) jedná se o program, který se šíří po síti zcela sám, dokáže se i rozesílat sám mezi e-maily. Využívá slabých hesel, neaktualizovaného SW, sdílených adresářů a sám sebe tímto způsobem se kopíruje. Nebezpečí spočívá v tom, že se červ dokáže vydávat za někoho, koho oběť dobře zná. Tudíž oběť nepojme ze začátku žádné podezření.
- Virus pokud se spustí infikovaný soubor, dochází k zapsaní dat do spustitelného souborupřípadně do disků či boot sektoru disket. Taková operace je v dnešní době dobře detekovatelná pomocí antivirusu, tudíž nepředstavuje takovou hrozbu.
- Macrovirus tento virus má kód napsaný v jazyce VBA a ten pak sám sebe kopíruje do souborů MS Office. Detekce však není složitá, proto se tolik nevyskytuje. Slouží spíše jako tzv. dropper, který se používá ke stažení dalšího malware (Shoemaker et al., 2011).

Podle toho, jak se malware projevuje, ho můžeme rozdělit na:

- Rootkit jeho funkcí je ovládání na velkou vzdálenost, je součástí systému a snaží se skrývat před odhalením.
- Logická bomba (Logical bomb) jedná se o aplikaci, která se spustí po splnění určitých podmínek. Většinou je nainstalována do systému nespokojeným zaměstnancem.
- Bankovní malware (Banking malware) tento specifický druh malware krade údaje, pomocí kterých se uživatel přihlašuje do internetového bankovnictví. Vyjmečný je i tím, že si dokáže poradit s autorizací transakce i dvoufaktorovou autentizací.
- Spyware je jeden ze špionážních softwarů. Přes internet odesílá informace o uživateli. Nejčastěji spolu s trojským koněm se dostává do počítače. Často se vyskytují i takové případy, kdy při instalaci aplikace jsou citlivé údaje uživatele zmíněny již v licenčních podmínkách, které téměř nikdo při instalaci nečte. Mezi

spyware patří i například keyloggery. Ty mají za úkol snímat otisky kláves, a to využít pří krádeži hesla.

- Backdoor neboli zadní vrátka. Díky backdooru se útočník dokáže dostat do aplikace či systému. Způsobené to je neautorizovaným přístupem. Jsou to malwary ponechány v systému či aplikaci pro pozdější přístup. Buď je tam zanechán útočníkem, poté co daný systém, či aplikaci kompromitoval nebo to bylo vlaženo přímo autorem za účelem podpory a testování.
- Adware jedná se o software způsobující zobrazení nežádoucí reklamy. Většinou se jedná o legitimní způsob, jak autor aplikace získává alespoň některé finanční prostředky zpět, po vytvoření aplikace.
- Ransomware jedná se o vyděračský software. Jeho úkolem je zašifrování dat na disku. Dokáže zablokovat koncové zařízení. Poté co uživatel pachateli zaplatí výkupné (ransom), je mu zasláno nové heslo.
- Scareware jedná se o tzv. fake antivir neboli falešný antivir. Pokud uživatel navštíví infikované webové stránky, zobrazí se mu nabídka na stažení a instalaci tohoto falešného antiviru (Jirovský, 2007).

1.5.4 Malvertising

V dnešní době i naprosto důvěryhodné webové stránky mohou být napadené. Rok od roku roste počet webů, které jsou nakažené. Od desítek partnerů se pak na těchto webech zobrazuje obsah, dále jsou na nich widgety, reklamy třetí strany a aplikace a ty tvoří samotný web.

Zpravidla právě ve widgetách, aplikacích a reklamách třetí strany se pak nachází škodlivý kód, který se po rozkliknutí webu spouští bez jakékoliv spolupráce s uživatelem. V tu chvíli se tedy jedná o tzv. drive-by download malware. Útočníci jsou dnes velmi vynalézaví. Hodně navštěvované weby jsou dnes zabezpečené, a proto volí následující postup pro splnění jejich cíle. Stačí jim ukrýt malware (škodlivý kód) do zcela na první pohled neškodné reklamy, která se většinou týká nějaké hry nebo flashové animace. Ty jsou málokdy testovány a jejich analýza může být nezajímavá. Pokud jsou splněny útočníkem předem nastavené požadavky, spouští se škodlivý kód v zařízení uživatele. Útočník se vydává buď za reklamní agenturu (advertising agencies) nebo zadavatele reklamy (advertisers). Proto se tato činnost vykonávající útočníkem nazývá malvertising a škodlivému kódu se říká malvertisement (malicious advertisement) (Kolouch et al.,

2019).

Uživateli se po navštívení napadeného webu spouští reklamy, pokud je nemá předem zablokované. A pak už záleží na škodlivém kódu, zda dokáže zneužít zranitelnost dané aplikace nebo systému ve svůj prospěch. Je velmi obtížné se bránit malware, který se stahuje již při zobrazení webu. O to víc by měli uživatelé udržovat svoje aplikace a operační systém aktuální (McQuade, 2009).

I na webech, co které mají EV (Extended Validation) certifikát (zabezpečení adresního řádku na vysoké úrovni) zabezpečení se může nacházet malvertisement. Pro útočníka je takový web velmi zajímavý a snaží se na něj umístit škodlivý kód. Přenos mezi klientem a serverem je šifrován, a proto útočník využívá jinou cestu průniku. Škodlivý kód prochází přes zařízení, které zajišťuje ochranu na perimetru a dostává se až do koncového zařízení uživatele (McQuade, 2009).

Jakýkoliv zprostředkovatel i poskytovatel reklamního obsahu může být obětí útoku, který spočívá ve vložení či modifikaci škodlivého kódu např. Google (Baggili, 2011).

1.5.5 Watering holes

Pokud je proveden tzv. watering holes attack má útočník za cíl konkrétní osobu nebo organizaci. Tato technika je často využívaná ve spojitosti s průmyslovou špionáží. Cílem jsou hlavně citlivé informace. Může se jednat třeba o vyřazení některého důležitého zařízení (např. elektrárna) nebo výsledky některých výzkumů. Útočník si nejdříve vytipuje oblasti zájmu a navštěvované webové stránky skupiny osob či určité osoby, na kterou chce zaútočit. Vybranou webovou stránku, která je špatně zabezpečena kompromituje a vloží na ní kód, který poslouží jako přesměrování na stránku, která bude obsahovat nějaký exploit. Ve chvíli, kdy jí oběť navštíví, dochází ke zranitelnosti v některé aplikaci či systému, který je zrovna použit uživatelem. K exploitaci dochází pouze u konkrétních osob nebo předem určených skupin (McQuade, 2009).

1.5.6 Botnet

Botnety jsou tzv. armáda zombií a jsou rozmístěny po celém světě. V nabídce jsou za určitou cenu a dají se využít k nejrůznějším typům kybernetických útoků. Botnet může čítat několik stovek nebo také několik milionů zařízení, které jsou kompromitovány. Zneužití může být využito k: rozesílání nevyžádané pošty, lámání hesel, DDoS útokům,

luštění CAPTCHA, těžení bitcoinů apod. Napadený počítač není vůbec jednoduché poznat. Velkou roli zde hrají IP adresy. Každý server má přidělené na internetu jméno (hostname) a IP adresu. Jedno hostname má většinou jednu IP adresu. Ale bývají i vyjimky, kdy jich obsahuje více, např.: nouzové řešení při přírodních katastrofách, nouzové řešení při odpojení serveru od sítě atd. Pokud je vytvořeno pro jedno hostname víc IP adres, nemusí být hned zadány do DNS. Až v okamžiku potřeby se může DNS záznam aktualizovat. Této skutečnosti využívají útočníci k nelegálnímu businessu. Organizované skupiny díky botnetu dokáží přesunout nelegální aktivitu snadno na druhou stranu zeměkoule během pár sekund. Dochází sice ke změně IP adresy, ale hostname zůstává stejné. Data jsou samozřejmě šifrována, a tak i komunikace například za pomoci např. freewarového nástroje TrueCrypt, používaný symetrickou šifrou AES. Pokud je disk zabavený, nejdou z něj žádná data rozluštit (Wall, 2007; Kopecký et al., 2010; Mc Quade, 2009).

1.5.7 Distributed Denial of Service

Jedná se o útoky, které odepřou uživateli služby. Jak už napovídá zkratka DDoS (Distributed Denial of Service). Útoky probíhají formou množstvím požadavků, které systém dokáží zahltit. Rozlišují se dva typy DDoS útoků, a to aplikační a volumetrické. K útoku může dojít ve všech vrstvách ISO/OSI (International standard organization je organizace na mezinárodní úrovni, která slouží pro normalizaci/Open system interconnection je referenční model sloužící k propojení otevřených systémů) (Kolouch et al., 2019).

DDoS útok je od samého začátku přesně cílený. Útočník z botnetu otevírá dotazy na web nebo server a hromadícím se počtem požadavků se cílový systém zhroutí nebo velmi zpomalí. Realizace takového útoku je jednoduchá, stačí si pronajmout velký botnet. Pronájem botnetu, který je rozesetý po celém světě obsahující 1 000 až 10 000 zombií stojí 500 až 5 000 Kč. Pokud by zájemce stál o botnet nacházející se pouze v Evropě, zaplatí asi jednou tolik. Součástí botnetů v tomto případě jsou i například zařízení s Andridem, Linuxem a dalšími systémy, které nebyly aktualizované (Kolouch, 2016).

1.5.8 Advanced Persistent Threat

Advanced Persistent Threat (dále jen APT), neboli přetrvávající pokročilé hrozby, které

jsou vedeny na přesné cíle, ať už proti konkrétní organizaci či osobě. Takový útočník je vysoce motivován, má schopnosti útok realizovat a disponuje potřebnými zdroji. APT může být buď trvalý nebo pokročilý (Baggili, 2011).

APT pokročilé hrozby, útočník je díky pokročilým technikám schopen proniknout do systému. Je připraven nad útokem strávit hodně času a dostat se až do jádra organizace. A poté pomocí sociálního inženýrství přesvědčit danou osobu ke spuštění malware (Baggili, 2011).

APT trvalé hrozby cílem útočníka je zajištění trvalého přístupu do systému organizace. Primárním cílem je vždy získání informací, které jsou klíčové pro danou organizaci. Jelikož jsou cílem jen informace, snaží se je útočník zanechat na svém původním místě a nenápadně se zde udržet delší dobu bez povšimnutí. Tím si dokáže zajistit trvalý přístup do prostředí organizace a kompromitovat i další systémy (Baggili, 2011).

APT útoky jsou prováděny ve 4 základních fázích.

1. Příprava,
2. průnik,
3. kompromitace,
4. dokončení (Amoroso, 2006).

1.5.9 Bezpečnostní politika, příručky a standardy

Bezpečnostní zásady potřebují být sepsané tak, aby bylo jednoduché jim porozumět a dodržovat je. Zaměstnavatel vyžaduje po zaměstnanci seznámení s bezpečnostními opatřeními. Bezpečnostní zásady bývají popisovány ve standardech, bezpečnostní politice a příručkách. Mezi těmito dokumenty jsou značné rozdíly, ale v praxi bývají často zaměněny. Tyto dokumenty jsou určitým předpokladem pro dosažení určité úrovně bezpečnosti. Důležité je v nich myslet na srozumitelnost a formulovatelnost, která je snadno pochopitelná a bude proto pro zaměstnance o to lepší doporučené opatření dodržovat (Kný et al., 2010).

Ve většině společností či organizací se zaměstnanec seznamuje v bezpečnostními opatřeními při nástupu do nového zaměstnání. To, zda porozuměl a se vším se seznámil, stvrzuje nejčastěji svým podpisem. Bohužel se ve většině případů jedná pouze o formalitu, a proto zůstává bezpečnostní povědomí zaměstnanců na velmi nízké úrovni.

Na bezpečnostní politiku se dá zeptat otázkou PROČ? Na standardy se dá využít otázka CO? Na příručky by mohla být využita otázka JAK? (Yannakogeorgos, 2013).

Jednotlivé dokumenty se dají rozdělit do 3 základních kategorií:

Bezpečnostní politika (policy) jedná se o strategický dokument, který by měl být pro všechny zaměstnance dostupný například na intranetu. Každý zaměstnanec by ho měl znát a dodržovat ho. V tomto dokumentu je definován cíl, účel, záměr vedení společnosti a vůle v oblasti bezpečnosti. Management se tímto dokumentem snaží dát najevo, že společnost či organizace musí čelit určitým rizikům a je si tím vědoma. Měly by zde být použity jasné formulace, aby nedocházelo k mylným domněnkám.

Standard (standard) jedná se taktický dokument. Ten detailněji popisuje obecné požadavky, které jsou uvedeny v bezpečnostní politice. Standardy by měly poskytnout popis, co se má udělat.

Příručka (procedure) jedná se o provozní dokument, ten popisuje krok za krokem určitou činnost nebo konkrétní opatření. Jeho zavedení má za cíl minimalizovat riziko chyb. Nejčastěji zde bývají popsány detailní postupy. Popisuje, jak splnit standardy a jejich požadavky (Yannakogeorgos, 2013).

1.6 Typy bezpečnostních opatření

Opatření (security measures), mají za cíl snížit riziko na úroveň, která je nějakým způsobem akceptovatelná. Dle způsobu provedení se dají opatření rozdělit na tyto typy:

- Organizační (administrativní) patří zde standardy, postupy, policy, závazná pravidla atd.
- Technická (logická či fyzická) zde se nachází kontrola osob v prostorech, které jsou střeženy, logické a fyzické řízení přístupu pomocí autentizace, identifikace a autorizace (Požár, 2005).

Technická opatření se dají dále rozdělit na:

- Systémová (systém) patření, které je velmi specifické na úrovni operačního systému.
- Databázovaná (database) opatření, které je velmi specifické na úrovni databáze.
- Aplikační (application) opatření, které je velmi specifické na úrovni aplikace.

- Kryptografická (cryptography) opatření týkající se symetrické a nesymetrické kryptografie.
- Komunikační (communication) jedná se o specifické nastavení týkající se aktivních siťových prvků.
- Organizační (administrativní) patří zde standardy, postupy, policy, závazná pravidla atd. (Požár, 2005).

Další způsob dělení:

- Detekční (detection) používá se k odhalení nežádoucích aktivit pomocí analýz z kamerových záznamů a sensorem.
- Preventivní (prevention) měly by zabraňovat realizaci útoků, které by mohly vézt k nežádoucím aktivitám.
- Reaktivní (reaction) po odhalení nežádoucí aktivity je třeba na ni adekvátně zareagovat, a to buď defenzivně nebo ofenzivně.
- Zdržující (delay) aby byla aktivita útočníka včasně detekována, musí být jeho postup co nejvíce zpomalen.
- Odstrašující (detergent) opatření by měla být viditelná, pro dostatečné zastrašení útočníka.
- Obnova (recovery) pomocí tohoto opatření dochází k obnově funkčnosti systému.
- Direktivní (directive) musí docházet ke kontrole postupů a jejich obnovování.
- Kompenzační (compensation) opatření mohou nahradit běžně zavedená opatření.
- Nápravná (corrective) opatření má za cíl zabránit opakování daného procesu (Singer, 2013).

1.7 Příklady kybernetických útoků

Kybernetické útoky jsou nedílnou součástí každodenního života mnoha lidí. V posledních letech byly pozorovány některé větší kybernetické útoky (Šulc, 2018).

1.7.1 Kybernetický útok na Olomoucký magistrát

V dubnu roku 2021 pronikli hackeři do sítě magistrátu města Olomouc pomocí technické chyby v systému. Útočníci využili jednoho veřejně dostupného prvku, skrze něj a spolu s dalšími útoky se jim podařilo dostat do interní sítě magistrátu. Prolomili hesla (kdy jedno z nich bylo administrátorské) a zašifrovali data. Útočníci vyhrožovali zveřejněním

uniklých informací a dalšími útoky, pokud nebude nezaplaceno výkupné. Magistrát Olomouc však na výhružky nepřistoupil a peníze nezaplatil. Poté se hackeři rozhodli postupně zveřejnit získané informace. Zatím byly zveřejněny např.: kontaktní údaje některých pracovníků magistrátu nebo informace týkající se plateb komunálního odpadu. Použitý vir ransomware, který byl ke zmíněnému útoku požit se jmenuje Avaddon a dá se koupit na dark webu. Technici začali obnovovat systém úřadu a do toho museli odrážet další útoky, jako: zasílání zavirovaných e-mailů a zahlcení webových stránek. Cílem je lepší zabezpečení sítě, které by příště odolalo kybernetickému útoku. Zabezpečení systému a následná celková obnova bude stát téměř jeden milion korun (iRozhlas Olomoucký magistrát…, 2021).

1.7.2 Kybernetický útok na největšího amerického provozovatele ropných potrubí

Společnost Colonial Pipeline je největším firmou v USA, která se zabývá přepravou ropných produktů. K tomu jí slouží potrubní síť. V květnu 2021 byla tato společnost napadena hackery. Celé Mexické pobřeží bylo náhle nuceno si začít objednávat tankery, aby mělo kde uschovat ropné produkty. Colonial Pipeline se stala objetí vyděračského programu ransomware, který zablokoval systém a za odblokování pak útočníci požadovali výkupné. Společnost Marathon Oil byla schopna začít plnit závazky vzniklé k odběratelům, ve chvíli kdyby se nepodařilo delší dobu obnovit potrubní síť Colonial Pipeline. Touto mimořádnou událostí se začal zabývat i Bílý Dům. Byl vyhlášen stav nouze a začala obnova činnosti společnosti. Tato událost měla vliv i na cenu ropy na světových trzích. Společnost Colonial Pipeline dokáže denně přepravit až 2,5 milionů barelů nafty, ropy, leteckého paliva a dalších obdobných komodit (iRozhlas ropné potrubí…, 2021).

1.7.3 Kybernetický útok na Nemocnici Rudolfa a Stefanie Benešov

V roce 2019 se odehrál kybernetický útok na Nemocnici Rudolfa a Stefanie v Benešově. Z dostupných informací se mělo jednat o počítačový vir ransomware, který napadl nemocnici. Podle Policie ČR neunikly žádné informace a data o pacientech. Největší omezení a ztrátu financí nemocnice zaznamenala kvůli omezení lékařských výkonů. Nemocnice tudíž nedostala zaplaceno za zákroky, operace a plánované vyšetřen od pojišťovny. Nové zabezpečovací zařízení, obnova a zlepšení zabezpečení softwarů, proškolení personálu a již zmíněné neproplacené výkony nakonec vyšly nemocnici na 59 milionů korun českých (Centrum kybernetické bezpeč…, 2019).

2 Cíl práce a hypotézy

2.1 Cíl práce

Analyzovat nejzávažnější kybernetické útoky za posledních 10 let ve vybraném územním samosprávném celku a provést prognózu možného vývoje kybernetického terorismu dle zjištěné analýzy.

2.2 Hypotézy

1. Vybraný územní samosprávný celek má dostatečně zpracované dokumenty, řešení a koordinaci kybernetických bezpečnostních incidentů.

2. Pravidelně se vzdělává a cvičí proti kybernetickému terorismu.

3 Metodika práce

K vypracování diplomové práce byla v první řadě pečlivě prostudována dokumentace týkající se kybernetické bezpečnosti z platné legislativy, odborné literatury, metodik, směrnic, postupů zkoumaných ORP, internetových pramenů a článků. Následovalo rozplánování postupu zpracování diplomové práce.

Teoretickou část diplomové práce tvoří kapitola 1. Tato část byla zpracována pomocí metody obsahové analýzy, rešerše a deskripce. Teorie je sepsána tak, aby vedla k přehlednému uvedení do problematiky kybernetické bezpečnosti. Témata uvedená v této části jsou zásadní pro pochopení praktické části.

V praktické části diplomové práce se projevuje využití metody analyticko-syntetické. Aplikace analýzy je vhodná v případě, kdy jednotlivé kroky postupu v daném systému je nutné pochopit. Takovým systémem je i kybernetická bezpečnost. Syntézou lze zkoumané prvky spojit a vytvořit velmi zajímavé výsledky. K prohloubení a dosažení zajímavých výsledků, byl zvolen smíšený výzkum. Creswell a Plano Clark (2007) popisují využití smíšeného výzkumu ke zpracování závěrečné práce, jako výzkum kde musí být alespoň jeden kvalitativní aspekt v kombinaci s alespoň jedním aspektem (přístupem) kvantitativním, analýzou dat nebo sběrem dat. Základním předpokladem pro využití smíšeného výzkumu, kde se propojuje kvantitativní a kvalitativní přístup, je lepší pochopení a zpracování výzkumného problému, než kdyby se k tomuto tématu přistupovalo pouze jedním z nich. Kvalitativní indukce sloužila ke kvalitnímu zpracování jak teoretické práce, tak k vedení strukturovaných rozhovorů. Strukturované rozhovory byly vedené s odborníky na kybernetickou bezpečnost z vybraných územně samosprávných celků. Vybrané otázky byly kategorizovány a přepsány pro lepší přehlednost do tabulek. Ke kvantitativnímu přístupu byl zvolen polostrukturovaný dotazník, který byl odborníkům dodatečně zasílán po rozhovoru. Otázky připravené k rozhovoru a otázky, ze kterých byl dotazník, byly stejné. Otevřené otázky se řešily již zmíněným rozhovorem a uzavřené otázky poté odborníci v zaslaném dotazníku zodpovídali. Všechny otázky byly kombinovány tak, aby došlo k tematickému navázání v dotazníku. Tato metoda se velmi osvědčila především v době pandemie způsobené virem Covid-19. Poskytuje nevšední náhled na zkoumaný problém a bylo díky ní možné při tomto zkoumání dodržovat protiepidemiologické požadavky. Odpovědi z rozhovoru a dotazníku byly propojeny a sepsány pro větší přehlednost. Pro dosažení cíle bylo nutné

použít metodu indukce. Získaná data byla sepsána a zpracována (pro větší přehlednost byly nejzajímavější a nejpodnětnější odpovědi vybrány a zaznamenány do přehledných tabulek a obrázků). Výsledky byly mezi sebou porovnávány, hledaly se podobnosti a odlišnosti pro správné vyvození cíle práce a daných hypotéz (Gavora, 2010).

Výzkum se zaměřoval na obce s rozšířenou působností (dále jen ORP) nacházející se v Jihočeském kraji a Kraji Vysočina. Osloveno bylo celkem 17 ORP z Jihočeského kraje a 15 ORP z Kraje Vysočina. Vzorek respondentů tvořili odborníci na kybernetickou bezpečnost, kteří zastupovali vybrané obce s rozšířenou působností a byli osloveni pomocí osobních e-mailů. E-mailová adresa byla vždy získána na oficiálních webových stránkách ORP. Po potvrzení spolupráce byla navázána telefonická komunikace a proběhl rozhovor na téma kybernetické bezpečnosti s předem připravenými otázkami, které jsou sepsány v polostrukturovaném dotazníku, s daným odborníkem, který ji má v obci s rozšířenou působností v kompetenci. Vzhledem k omezením, která vznikla v souvislosti s pandemií Covid-19, byli odborníci požádáni o dodatečné doplnění polostrukturovaného dotazníku s převážnou částí otevřených odpovědí, kam předešlý rozhovor zaznamenali a zbylé otázky zodpověděli. Dále byla s odborníky vedena komunikace pomocí e-mailu a mobilního telefonu pro doplnění veškerých informací. Vždy byl především kladen důraz na dodržování vládních nařízení s ohledem na bezpečí zúčastněných osob. Vlastní polostrukturovaný dotazník byl sestaven po prostudování odborné literatury a souběžných konzultacích s vedoucím práce. Tímto způsobem byla získána data, která jsou dále využita při dalším zpracování. Dotazník se skládá ze tří částí. Část první: Identifikační část pracovníka MÚ zodpovídajícího za kybernetickou bezpečnost. Část druhá: Obec s rozšířenou působností a její krizové řízení týkající se kybernetické bezpečnosti. Část třetí: Osvěta a prevence týkající se kybernetické bezpečnosti. Data byla získávána od února do června 2021. Predikce byla založena na využití tří prognostických metod. Jako první byla použita analýza trendů k identifikaci dat souvisejících s časem, která slouží jako nástroj pro modelaci budoucího chování. Získaný vzorek dat byl převeden pro větší přehlednost do grafického soupisu a porovnán s odbornou publikací. Druhá metoda, analýza megatrendů porovnává rozsáhlé vývojové tendence. Jako třetí byla využita metoda kola budoucnosti, která je velmi netradiční, nenákladnou, podnětnou, avšak přehlednou metodou k určení důsledku událostí a jejich dalším vývojem do budoucnosti.

4 Výsledky

Odpovědi na předem připravené otázky posloužily ke zpracování diplomové práce. Na získání odpovědí se podílelo celkem 14 ORP z Jihočeského kraje a Kraje Vysočina. Odborníci na kybernetickou bezpečnost byli osloveni a následně požádáni o spolupráci na tvorbě této diplomové práce. Byly s nimi vedeny rozhovory přes mobilní telefon, protože, opatření proti pandemii Covid-19 neumožnovala bezpečné osobní setkání.

S odborníky na kybernetickou bezpečnost příslušného ORP, byl veden již zmíněný rozhovor a poté byli požádáni o vyplnění dotazníku s velkým počtem otevřených otázek (celé znění dotazníku viz příloha A), kam měli zanést odpovědi z předešlého rozhovoru. Po celou dobu byla s odborníky vedena komunikace telefonická a e-mailová. Struktura dotazníku byla psána v dokumentu WORD. Využití jiných veřejných portálů, které by sloužily jako zaznamenání on-line odpovědí, bylo vzhledem k tématu práce zamítnuto. Právě takové portály se totiž po vyplnění odpovědí stávají majiteli psaného obsahu.

V této kapitole jsou odpovědi pomocí přepisu uvedeny do souhrnného, logicky členěného textu. Celý souhrnný text je psán v oznamovacích větách. Pro zlepšení čitelnosti textu mají odpovědi občas změněné pořadí, oproti zmíněnému dotazníku.

Po předchozí žádosti oslovených odborníků a po domluvě s vedoucím práce zůstanou odpovídající i jejich přesné zařazení do ORP anonymní.

4.1 Kraj Vysočina

4.1.1 Obec s rozšířenou působností č. 1

Odborník městského úřadu (dále jen MÚ) na kybernetickou bezpečnost pracuje na své pozici 10-20 let. Zároveň nepůsobí v jiných oblastech krizového řízení. Na tvorbě a udržení kybernetické bezpečnosti zde působí 1-2 pracovníci. ORP č. 1 nemá zřízené samostatné oddělení zabývající se pouze informačními technologiemi a kybernetickou bezpečností. Odborník na kybernetickou bezpečnost bohužel není seznámen s informacemi, zda bude samostatné oddělení v budoucnu vytvořeno. Vzdělání má středoškolské. Dále se vzdělává ve svém zaměstnání, a to jednou za půl roku. Zároveň je kontaktní osobou pro komunikaci s vládním CERT týmem.

V ORP č. 1 má městský úřad zřízené krizové řízení, a to je zároveň součástí kanceláře tajemníka. Krizový plán v ORP č. 1 neobsahuje opatření týkající se kybernetické bezpečnosti/kritické informační infrastruktury. Odborník na danou problematiku se nepodílí na tvorbě předpisů, směrnic, metodických pokynů aj. Za posledních 10 let proti ORP č. 1 nebyl veden žádný kybernetický útok. Tento MÚ má vedenou statistiku kybernetických útoků v průběhu let a také má vytvořenou analýzu týkající se kybernetické bezpečnosti. Dle odborníka se trend kybernetických útoků vyznačuje nejvíce rychlým vývojem a silou daných útoků. MÚ nejvíc ohrožuje kombinace útoků: DoS/DDoS, sociálním inženýrství, škodlivým malware a kinetický zásah. Jako hlavní motivaci ke kybernetickým útokům považuje odborník hacktivismus, vnitřní hrozbu, konflikt se státním či nestátním aktérem a špionáž. MÚ má zřízen svůj intranet a zároveň mají zaměstnanci možnost se přihlásit z pracovních elektronických zařízení na veřejnou síť například Google či Seznam. Odborník se domnívá, že potencionálním útočníkům by nešlo o získání citlivých dat a informací, ale o přerušení provozu celého MÚ.

Odborník MÚ nesleduje vývoj kybernetických útoků, ale v poslední době zaregistroval kybernetický útok ve veřejné správě České republiky na magistrát města Olomouc. Neumí přesně odpovědět na otázky, jak by poznal, že na MÚ právě probíhá nebo proběhl kybernetický útok. Neví, jak přesně postupovat, při probíhajícím kybernetickém útoku. Nezná rozdíl mezi vládním CERT (GovCERT.cz) týmem a národním CERT (CSIRT.cz) týmem. Nesleduje nejnovější inovace a trendy v oboru kybernetické bezpečnosti. Věděl by kam kybernetický útok nahlásit. Z „hlavy“ nezná číslo vyhlášky, podle které se

incident kybernetické povahy nahlašuje. Dle odborníka může kybernetický útok mít fatální dopady na MÚ. Vynaložené finance pro obor kybernetické bezpečnosti nepovažuje za dostatečné. Nezná číslo vyhlášky podle, které se incident kybernetické povahy nahlašuje. Digitalizace veřejné správy je dle jeho slov pomalá a dochází k její malé propagaci, proto není ze stran občanů příliš velká důvěra pro nově vzniklé inovace. Jako podařený informační systém, který vznikl digitalizaci veřejné správy, považuje „portál občana“. Myslí si, že nedochází k dostatečné osvětě, co se týče kybernetické bezpečnosti ve veřejné správě, týkající se obyvatel České republiky. Za nedostatečné považuje i proškolení personálu MÚ, ke kterému dochází nepravidelně, a to pomocí e-learningu. MÚ neprovádí zkušební nácviky kybernetického bezpečnostního incidentu. S Národní strategií kybernetické bezpečnosti ČR 2021-2025 není odborník detailně seznámen.

4.1.2 Obec s rozšířenou působností č. 2

Odborník pracuje na MÚ 20 a více let, jako odborník na kybernetickou bezpečnost působí na úřadě 5-10 let. Zároveň nepůsobí v jiných oblastech krizového řízení. Na tvorbě a udržení kybernetické bezpečnosti zde působí 1-2 pracovníci. ORP č. 2 nemá zřízené samostatné oddělení zabývající se pouze informačními technologiemi a kybernetickou bezpečností. V blízké době se MÚ nechystá zřídit samostatné oddělení informačních technologií. Vzdělání má středoškolské. Dále se vzdělává samostatně pomocí odborných článků, knih, aj., jednou za půl roku a jezdí na odborné semináře pořádané kvalifikovanými subjekty. Zároveň není kontaktní osobou pro komunikaci s vládním CERT týmem.

V ORP č. 2 má městský úřad zřízené krizové řízení, a to je zároveň součástí odboru správního a školského. Krizový plán v ORP č. 2 neobsahuje opatření týkající se kybernetické bezpečnosti/kritické informační infrastruktury. Odborník na danou problematiku se nepodílí na tvorbě směrnic, předpisů, metodických pokynů aj. Odborník neví, s jakými prvky kritické infrastruktury nejvíce souvisí kritická informační infrastruktura. Za posledních 10 let proti ORP č. 2 nebyl veden žádný kybernetický útok. Tento MÚ si nevede statistiku kybernetických útoků v průběhu let a nemá vytvořenou analýzu týkající se kybernetické bezpečnosti. Respondent vidí vyvíjející se trend kybernetického nebezpečí, jako velmi vzrůstající. MÚ nejvíc ohrožuje škodlivý malware. Jako hlavní motivaci ke kybernetickým útokům považuje odborník vnitřní hrozbu

(selhání zaměstnance) a materiální obohacení. MÚ nemá zřízen svůj intranet. Zaměstnanci MÚ mají možnost se přihlásit z pracovních elektronických zařízení na veřejnou síť př.: Seznam či Google. Odborník se domnívá, že potencionálním útočníkům by šlo nejvíce o získání osobních dat a bankovních údajů.

Odborník MÚ nesleduje vývoj kybernetických útoků. V poslední době zaregistroval kybernetický útok ve veřejné správě České republiky na magistrát města Olomouc. Právě probíhající kybernetický útok by poznal např.: nedostupností služeb, nestandardním chováním PC, serverů, sítě, aj. Útok, který již proběhl, by poznal př.: zašifrováním a nedostupností některých souborů. Pokud by to bylo možné, tak by na právě probíhající útok reagoval detekováním útočníka a jeho postupným zablokování (např. na firewallu nebo na úrovni poskytovatele konektivity). V postiženém segmentu dále LAN a vše odstavit a až do odstranění problému nic nezapínat. Po proběhlém kybernetickém útoku by mohla bezprostředně poté nastat nedostupnost elektronických služeb a dat pro veřejnost i vnitřní chod úřadu. V případě kybernetického útoku by vše hlásil na Polici České republiky a na vládní CERT. Vládní CERT (GovCERT.cz) tým, se zaměřuje na řešení problémů ve státní správě a KII a národní CERT (CSIRT.cz) tým řeší ostatní incidenty v rámci celé České republiky. Incident kybernetické povahy by nahlašoval podle vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti. Vynaložené finance pro obor kybernetické bezpečnosti považuje za dostatečné. Sleduje nejnovější trendy a inovace v oboru kybernetické bezpečnosti. Inovace a trendy se snaží postupně zařadit např.: modernizace firewallů, upgrade a update OS server, aj. Digitalizaci považuje za pomalou a špatně koordinovanou. Systémy jsou vytvářeny a dodávány různými dodavateli a dochází k jejich špatnému propojení. Jako podařený informační systém, který vznikl digitalizací veřejné správy, považuje CzechPOINT, který je úřadem i veřejností velmi využívaný a funguje bez problému a ISZR (Informační systém základních registrů), který slouží k velkému usnadnění při ověřování osobních údajů. Veřejnost neumí využívat nové informační systémy, u některých je potřeba e-identita nebo datová schránka, což zatím mnozí nemají nebo ani nechtějí používat. Myslí si, že dochází k dostatečné osvětě, co se týče kybernetické bezpečnosti ve veřejné správě, týkající se obyvatel České republiky. Za dostatečné považuje i proškolení personálu MÚ, ke kterému dochází pravidelně, a to za pomoci on-line školení a seminářů od odborných vzdělávacích firem. Vzdělávání poskytují i samotní odborníci z městského úřadu. MÚ neprovádí zkušební nácviky kybernetického bezpečnostního incidentu. V Národní strategii kybernetické

bezpečnosti ČR 2021-2025 jsou přehledně definované obecné principy kybernetické bezpečnosti, kterým porozumí i široká veřejnost, až po složitější část určenou spíše odborníkům.

4.1.3 Obec s rozšířenou působností č. 3

Odborník městského úřadu na kybernetickou bezpečnost pracuje na své pozici 20 a více let. Zároveň nepůsobí v jiných oblastech krizového řízení. Na tvorbě a udržení kybernetické bezpečnosti zde působí 3-4 pracovníci. ORP č. 3 má zřízené samostatné oddělení zabývající se pouze informačními technologiemi a kybernetickou bezpečností. Vzdělání má vysokoškolské zakončené dosaženým titulem Mgr./Ing. Toto vzdělání se přímo netýkalo KB/IT. Dále se vzdělává ve svém zaměstnání pravidelně a průběžně, a to pomocí odborných knih, článků a časopisů. Účastní se také odborných seminářů, které jsou pořádané kvalifikovanými subjekty. Není kontaktní osobou pro komunikaci s vládním CERT týmem.

V ORP č. 3 má městský úřad zřízené krizové řízení, a to je zároveň součástí kanceláře starosty a tajemníka. Krizový plán v ORP č. 3 neobsahuje opatření týkající se kybernetické bezpečnosti/kritické informační infrastruktury. Odborník na danou problematiku se podílí na tvorbě předpisů, směrnic, metodických pokynů aj. Provádí se roční revize dokumentů a v případě potřeby se aktualizují. Tyto dokumenty schvaluje a zodpovídá za ně buď tajemník úřadu nebo starosta města. Kybernetických útoků bylo v posledních 10 letech proti ORP č. 3 vedeno 5 (dva v roce 2016, jeden v roce 2017, jeden v roce 2018 a jeden v roce 2019). Všechny tyto útoky byly vedeny pomocí ransomware. Tento MÚ nemá vedenou statistiku kybernetických útoků v průběhu let, ale má vytvořenou analýzu útoků týkající se kybernetické bezpečnosti. Dle odborníka trend kybernetických útoků průběžně roste. MÚ nejvíc ohrožuje kombinace útoků: DoS/DDoS a škodlivým malware. Jako hlavní motivaci ke kybernetickým útokům považuje odborník hacktivismus. Odborník se domnívá, že útoky vedené proti MÚ jsou buď to za materiálním obohacením anebo se pouze jedná o internetový exhibicionismus. MÚ má zřízen svůj intranet a zároveň mají zaměstnanci možnost se přihlásit z pracovních elektronických zařízení na veřejnou síť př.: Google či Seznam.

Odborník MÚ sleduje vývoj kybernetických útoků, v poslední době zaregistroval kybernetický útok na nemocnici Benešov a ve veřejné správě České republiky na magistrát města Olomouc. Právě probíhající útok by poznal podle nainstalovaných

obranných subjektů, dále by přestaly nějaké systémy fungovat, a to samé u kybernetického útoku, který již proběhl. Věděl by, jak přesně postupovat, při probíhajícím kybernetickém útoku. Nezná rozdíl mezi vládním CERT (GovCERT.cz) týmem a národním CERT (CSIRT.cz) týmem. Věděl by kam kybernetický útok nahlásit. ORP nepodléhá režimu zákona o kybernetické bezpečnosti. Dle odborníka může kybernetický útok způsobit nemožnost normální plnohodnotné provozní činnosti organizace. Vynaložené finance pro obor kybernetické bezpečnosti nepovažuje za dostatečné. Sleduje nejnovější inovace a trendy v oboru kybernetické bezpečnosti a podle možností úřadu se je snaží začlenit. Digitalizace veřejné správy je dle jeho slov pomalá, dochází k ní postupně. Úspěšně se realizovalo velké množství projektů např.: eGovernemt, bohužel jejich využívání občany je obecně nízké. Jako podařené informační systém, které vznikly digitalizací veřejné správy, považuje skoro všechny. Myslí si, že nedochází k dostatečné osvětě, co se týče kybernetické bezpečnosti ve veřejné správě, týkající se obyvatel České republiky. Lidé neumí efektivně využívat elektronické služby poskytované veřejnou správou a může za to malá informovanost. Za dostatečné považuje proškolení personálu MÚ, ke kterému dochází podle potřeby a za pomoci odborné externí firmy. MÚ neprovádí zkušební nácviky kybernetického bezpečnostního incidentu. S Národní strategií kybernetické bezpečnosti ČR 2021-2025 není odborník detailně seznámen.

4.1.4 Obec s rozšířenou působností č. 4

Odborník pracuje na MÚ 20 a více let, jako odborník na kybernetickou bezpečnost působí na úřadě 10-20 let. Zároveň působí i v jiných oblastech krizového řízení a to komunikaci. Na tvorbě a udržení kybernetické bezpečnosti zde působí 4 a více pracovníků. ORP č. 4 nemá zřízené samostatné oddělení zabývající se pouze informačními technologiemi a kybernetickou bezpečností. V blízké době se MÚ nechystá zřídit samostatné oddělení informačních technologií. Vzdělání má středoškolské. Dále se vzdělává nepravidelným školením v zaměstnání, a to jednou ročně. Zároveň není kontaktní osobou pro komunikaci s vládním CERT týmem.

V ORP č. 4 má městský úřad zřízené krizové řízení, a to je zároveň součástí správního odboru. Krizový plán v ORP č. 4 obsahuje opatření týkající se kybernetické bezpečnosti/kritické informační infrastruktury. Odborník na danou problematiku se podílí na tvorbě předpisů, směrnic, metodických pokynů aj. Tyto dokumenty je zapotřebí

aktualizovat jednou ročně. Zodpovídá za ně tajemník úřadu. Kybernetických útoků bylo vedeno v posledních 10 letech proti ORP č. 4: 0. Tento MÚ nemá vedenou statistiku kybernetických útoků v průběhu let, ale má vytvořenou analýzu týkající se kybernetické bezpečnosti. Dle odborníka se trend kybernetických útoků vyznačuje rostoucí tendencí. MÚ nejvíc ohrožuje kombinace útoků: DoS/DDoS, sociálním inženýrství, škodlivým malware a kinetický zásah. Jako hlavní motivaci ke kybernetickým útokům považuje odborník vnitřní hrozbu. MÚ má zřízen svůj intranet a zároveň mají zaměstnanci možnost se přihlásit z pracovních elektronických zařízení na veřejnou síť př.: Google či Seznam. Odborník se domnívá, že potencionálním útočníkům by nešlo o získání citlivých dat a informací.

Odborník MÚ nesleduje vývoj kybernetických útoků. V poslední době zaregistroval kybernetický útok na veřejnou správu. Právě probíhající útok by poznal podle zvýšené aktivity v síti a nefunkčnosti některých systémů. Věděl by, jak postupovat při probíhajícím kybernetickém útoku a následném nahlašování na patřičné orgány. Nezná rozdíl mezi vládním CERT (GovCERT.cz) týmem a národním CERT (CSIRT.cz) týmem. Dle odborníka může kybernetický útok způsobit nemožnost normální plnohodnotné provozní činnosti organizace. Vynaložené finance pro obor kybernetické bezpečnosti považuje za dostatečné. Nezná číslo vyhlášky podle, které se incident kybernetické povahy nahlašuje. Nesleduje nejnovější inovace a trendy v oboru kybernetické bezpečnosti. Digitalizace veřejné správy je dle jeho slov logická a postupná. Úspěšně se realizovalo velké množství projektů např.: ISZR. Lidé neumí efektivně využívat nové informační systémy veřejné správy. Myslí si, že nedochází k dostatečné osvětě, co se týče kybernetické bezpečnosti ve veřejné správě, týkající se obyvatel České republiky. Za nedostatečné považuje proškolení personálu MÚ, ke kterému dochází většinou jednou ročně a provádí si ho krajský úřad. MÚ neprovádí zkušební nácviky kybernetického bezpečnostního incidentu. S Národní strategií kybernetické bezpečnosti ČR 2021-2025 není odborník detailně seznámen.

4.1.5 Obec s rozšířenou působností č. 5

Odborník městského úřadu na kybernetickou bezpečnost pracuje na své pozici 10-20 let. Zároveň působí v oblasti krizového řízení. Na tvorbě a udržení kybernetické bezpečnosti zde působí 4 a více pracovníků. ORP č. 5 má zřízené samostatné oddělení zabývající se pouze informačními technologiemi a kybernetickou bezpečností. Vzdělání má

vysokoškolské zakončené dosaženým titulem Mgr./Ing. Toto vzdělání se přímo netýkalo KB/IT. Dále se vzdělává ve svém zaměstnání pravidelně a průběžně, a to pomocí odborných knih, článků a časopisů. Účastní se také odborných seminářů, které jsou pořádané kvalifikovanými subjekty. Není kontaktní osobou pro komunikaci s vládním CERT týmem.

V ORP č. 5 má městský úřad zřízené krizové řízení, a to je zároveň součástí odboru kanceláře vedení města. Krizový plán v ORP č. 5 obsahuje opatření týkající se kybernetické bezpečnosti/kritické informační infrastruktury. Odborník na danou problematiku se podílí na tvorbě směrnic, předpisů, metodických pokynů aj., průběžně dle aktuální situace. Nové dokumenty schvaluje tajemník úřadu a zodpovídá za ně vedoucí oddělení IT. Odborník neví, s jakými prvky kritické infrastruktury nejvíce souvisí kritická informační infrastruktura. Kybernetických útoků bylo vedeno v posledních 10 letech proti ORP č. 5: desítky tisíc týdně. Útoky probíhají neustále, zhruba stejnou silou, díky dostatečnému zabezpečení nikdy nedošlo k výpadku poskytovaných služeb. Tento MÚ si vede statistiku kybernetických útoků v průběhu let a má vytvořenou analýzu týkající se kybernetické bezpečnosti. Respondent vidí vyvíjející se trend kybernetického nebezpečí, jako velmi vzrůstající v čase. MÚ nejvíc ohrožuje kombinace útoků: DoS/DDoS, sociálním inženýrství, škodlivým malware a kinetický zásah. Jako hlavní motivaci ke kybernetickým útokům považuje odborník materiální obohacení. MÚ nemá zřízen svůj intranet. Zaměstnanci MÚ mají možnost se přihlásit z pracovních elektronických zařízení na veřejnou síť př.: Seznam či Google. Odborník se domnívá, že potencionálním útočníkům by šlo nejvíce o získání zpeněžitelných dat.

Odborník MÚ sleduje vývoj kybernetických útoků. V poslední době zaregistroval kybernetický útok ve veřejné správě. Právě probíhající kybernetický útok by poznal pomocí monitorovacího systému. Stejně i útok, který již proběhl. Je si vědom, jak postupovat při probíhajícím kybernetickém útoku. Bezprostředně po krizové situaci by mohlo dojít ochromení provozu MÚ. V případě kybernetického útoku by věděl, kam vše nahlásit a na koho se obrátit. Vládní CERT (GovCERT.cz) tým, se zaměřuje na řešení problémů ve státní správě a KII a národní CERT (CSIRT.cz) tým řeší ostatní incidenty v rámci celé České republiky. Incident kybernetické povahy by nahlašoval podle vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti. Vynaložené finance pro obor kybernetické bezpečnosti považuje za dostatečné. Sleduje nejnovější trendy a inovace v oboru kybernetické bezpečnosti. Inovace a trendy se snaží do MÚ zařadit

pořizováním nových technologií a aktualizací stávajících. S digitalizací veřejné správy je velmi spokojen. Jako podařený informační systém, který vznikl digitalizací veřejné správy, považuje CzechPOINT, Portál občana, aj. Veřejnost umí využívat nové informační systémy. Myslí si, že nedochází k dostatečné osvětě, co se týče kybernetické bezpečnosti ve veřejné správě, týkající se obyvatel České republiky. Za dostatečné považuje proškolení personálu MÚ, ke kterému dochází pravidelně jednou za rok, a to pomocí pracovníků IT oddělení. MÚ neprovádí zkušební nácviky kybernetického bezpečnostního incidentu. S Národní strategií kybernetické bezpečnosti ČR 2021-2025 není odborník detailně seznámen.

4.1.6 Obec s rozšířenou působností č. 6

Odborník městského úřadu na kybernetickou bezpečnost pracuje na své pozici 10-20 let. Zároveň nepůsobí v jiných oblastech krizového řízení. Na tvorbě a udržení kybernetické bezpečnosti zde působí 1-2 pracovníci. ORP č. 6 nemá zřízené samostatné oddělení zabývající se pouze informačními technologiemi a kybernetickou bezpečností. Odborník na kybernetickou bezpečnost bohužel není seznámen s informacemi, zda bude samostatné oddělení v budoucnu vytvořeno. Vzdělání má vysokoškolské zakončené dosaženým titulem Mgr./Ing. Toto vzdělání se přímo netýkalo KB/IT. Dále se vzdělává ve svém zaměstnání, a to jednou za půl roku, pomocí knih, odborných článků, časopisů a účastní se odborných seminářů, které pořádá kvalifikovaný subjekt. Zároveň není kontaktní osobou pro komunikaci s vládním CERT týmem.

V ORP č. 6 má městský úřad zřízené krizové řízení, a to je zároveň součástí odboru tajemníka. Krizový plán v ORP č. 6 neobsahuje opatření týkající se kybernetické bezpečnosti/kritické informační infrastruktury. Odborník na danou problematiku se nepodílí na tvorbě směrnic, předpisů, metodických pokynů aj., ale ví, že tyto nové dokumenty schvaluje tajemník MÚ, zodpovídá za ně a je potřeba je aktualizovat průběžně. Odborník si myslí, že prvky kritické infrastruktury nejvíce související s kritickou informační infrastrukturou jsou: emaily s přílohami, přístup k internetu, aj. Kybernetických útoků bylo vedeno v posledních 10 letech proti ORP č. 6 mnoho. Nejzásadnější se odehrál v roce 2015: ramsomware. Tento MÚ si nevede statistiku kybernetických útoků v průběhu let a nemá vytvořenou analýzu týkající se kybernetické bezpečnosti. Respondent vidí vyvíjející se trend kybernetického nebezpečí, jako stále vzrůstající. MÚ nejvíc ohrožuje kombinace útoků: sociálním inženýrství a škodlivým

malware. Jako hlavní motivaci ke kybernetickým útokům považuje odborník materiální obohacení. MÚ má zřízen svůj intranet. Zaměstnanci MÚ mají možnost se přihlásit z pracovních elektronických zařízení na veřejnou síť př.: Seznam či Google. Odborník se domnívá, že potencionálním útočníkům by šlo nejvíce o získání hesel a přístupových kódů.

Odborník MÚ nesleduje vývoj kybernetických útoků. V poslední době zaregistroval kybernetický útok na nemocnice. Právě probíhající kybernetický útok by poznal pomocí nestabilního internetového připojení a informačního systému. Kybernetický útok, který již proběhl, by rozeznal pomocí nefunkčnosti zařízení a informačního systému. Při probíhajícím kybernetickém útoku by odpojil internetu celého MÚ. Bezprostředně po krizové situaci by mohlo dojít k zhroucení systému (HW i SW). V případě kybernetického útoku by se obrátil na NÚKIB. Vládní CERT (GovCERT.cz) tým, se zaměřuje na řešení problémů ve státní správě a KII a národní CERT (CSIRT.cz) tým řeší ostatní incidenty v rámci celé České republiky. Incident kybernetické povahy by nahlašoval podle vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti. Vynaložené finance pro obor kybernetické bezpečnosti považuje za nedostatečné. Nesleduje nejnovější trendy a inovace v oboru kybernetické bezpečnosti. S digitalizací veřejné správy je spokojen, považuje to za zjednodušení práce. Jako podařený informační systém, který vznikl digitalizací veřejné správy považuje CzechPOINT a Portál občana. Veřejnost umí využívat nové informační systémy. Nemůže posoudit, zda dochází k efektivnímu využívání nových informačních systémů veřejné správy, ale jistě se stav zlepšuje. Myslí si, že nedochází k dostatečné osvětě, co se týče kybernetické bezpečnosti ve veřejné správě, týkající se obyvatel České republiky. Za dostatečné považuje proškolení personálu MÚ, ke kterému dochází pravidelně jednou za dva roky a provádí ho odborná firma. MÚ neprovádí zkušební nácviky kybernetického bezpečnostního incidentu. S Národní strategií kybernetické bezpečnosti ČR 2021-2025 není odborník detailně seznámen.

4.2 Jihočeský kraj

4.2.1 Obec s rozšířenou působností č. 7

Odborník městského úřadu na kybernetickou bezpečnost pracuje na své pozici 10-20 let. Zároveň nepůsobí v jiných oblastech krizového řízení. Na tvorbě a udržení kybernetické bezpečnosti zde působí 1-2 pracovníci. ORP č. 7 má zřízené samostatné oddělení zabývající se pouze informačními technologiemi a kybernetickou bezpečností. Vzdělání má středoškolské. Dále se vzdělává pravidelně, a to pomocí knih, odborných článků, časopisů. Účastní se odborných seminářů, které pořádá kvalifikovaný subjekt, probíhá zde i nepravidelné školení v zaměstnání a zároveň zde probíhá studium vysoké školy se zaměřením na krizové řízení/ochranu obyvatelstva/IT/KB. Není kontaktní osobou pro komunikaci s vládním CERT týmem.

V ORP č. 7 má městský úřad zřízené krizové řízení, a to je zároveň součástí kanceláře tajemníka. Krizový plán v ORP č. 7 neobsahuje opatření týkající se kybernetické bezpečnosti/kritické informační infrastruktury. Odborník na danou problematiku se podílí na tvorbě předpisů, směrnic, metodických pokynů aj. Provádí se revize dokumentů podle potřeby a popřípadě dochází k aktualizaci. Tyto dokumenty schvaluje a zodpovídá za ně tajemník úřadu města. Kybernetické útoky za posledních 10 let byly proti ORP č. 7 vedeny dva. Jednalo se v obou případech o šifrovací vir (Ransomware), který byl součástí aktivní přílohy emailu. K oběma incidentům kybernetické povahy došlo v roce 2015. Tento MÚ nemá vedenou statistiku kybernetických útoků v průběhu let, ale nemá vytvořenou analýzu útoků týkající se kybernetické bezpečnosti. Z dostupných informací vyplývá, že počty i sofistikovanost kybernetických útoků narůstá. MÚ nejvíc ohrožuje kombinace útoků: DoS/DDoS, sociální inženýrství, škodlivým malware a kinetický zásah. Jako hlavní motivaci ke kybernetickým útokům považuje odborník vnitřní hrozbu a špionáž. Odborník se domnívá, že útoky vedené proti MÚ se nejvíce týkají projektových a správních řízení. MÚ má zřízen svůj intranet a zároveň mají zaměstnanci možnost se přihlásit z pracovních elektronických zařízení na veřejnou síť př.: Google či Seznam.

Odborník MÚ sleduje vývoj kybernetických útoků. V poslední době zaregistroval kybernetický útok na Olomoucký magistrát. Právě probíhající kybernetický útok by poznal následovně: na vstupu do sítě MÚ je nasazen duální FortiGate vč. FortiAnalyzeru, nad sítí pak stojí HP IMC: obojí je online zobrazováno na monitoru v kanceláři IT oddělení. Na základě anomálií by se pravděpodobně dal odhalit probíhající útok. Do

budoucna je plánován v tomto směru rozvoj monitorovacích prostředků sítě ve formě síťové sondy. Již proběhlý kybernetický útok by měl odhalit FortiAnalyzer. Při probíhajícím kybernetickém útoku by odpojil síť MÚ od internetové konektivity a následovala by analýza dostupných dat. Bezprostředně po krizové situaci by mohlo dojít k úniku osobních údajů, znehodnocení dat a dočasné paralýze fungování úřadu. V případě kybernetického útoku by k nahlášení incidentu použil formulář „Hlášení incidentů“ na stránce NÚKIB (formulář viz příloha D), popřípadě CISRT. Vládní CERT (GovCERT.cz) tým, se zaměřuje na řešení problémů ve státní správě a KII a národní CERT (CSIRT.cz) tým řeší ostatní incidenty v rámci celé České republiky. Incident kybernetické povahy by nahlašoval podle vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti. Vynaložené finance pro obor kybernetické bezpečnosti považuje za nedostatečné. Sleduje nejnovější trendy a inovace v oboru kybernetické bezpečnosti. Inovace a trendy se snaží do MÚ zařadit pořizováním nových technologií a aktualizací stávajících, společně s odbornou externí firmou. S digitalizací veřejné správy je nyní spokojen. Jako podařený informační systém, který vznikl digitalizací veřejné správy považuje datovou schránku a portál občana. Veřejnost ještě neumí využívat nové informační systémy, ale věří, že postupem času se vše zlepší. Myslí si, že dochází k dostatečné osvětě, co se týče kybernetické bezpečnosti ve veřejné správě, týkající se obyvatel České republiky. Za nedostatečné považuje proškolení personálu MÚ, ke kterému dochází pravidelně jednou za rok, a to pomocí pracovníků IT oddělení. MÚ neprovádí zkušební nácviky kybernetického bezpečnostního incidentu. Národní strategie kybernetické bezpečnosti ČR 2021-2025 má teoretickou strategii zpracovanou kvalitně a v zásadě i přehledně. Otázkou zůstávají její reálné dopady.

4.2.2 Obec s rozšířenou působností č. 8

Odborník městského úřadu na kybernetickou bezpečnost pracuje na své pozici 20 a více let. Zároveň nepůsobí v jiných oblastech krizového řízení. Na tvorbě a udržení kybernetické bezpečnosti zde působí 1-2 pracovníci. ORP č. 8 nemá zřízené samostatné oddělení zabývající se pouze informačními technologiemi a kybernetickou bezpečností. Vzdělání má vysokoškolské zakončené dosaženým titulem Mgr./Ing. Toto vzdělání se přímo týkalo KB/IT. Dále se vzdělává ve svém zaměstnání pravidelně a průběžně, a to pomocí odborných knih, článků a časopisů. Studoval vysokou školu se zaměřením na IT. Není kontaktní osobou pro komunikaci s vládním CERT týmem.

V ORP č. 8 má městský úřad zřízené krizové řízení, a to je zároveň součástí odboru životního prostředí. Krizový plán v ORP č. 8 neobsahuje opatření týkající se kybernetické bezpečnosti/kritické informační infrastruktury. Odborník na danou problematiku se podílí na tvorbě směrnic, předpisů, metodických pokynů aj. Nové dokumenty jsou vytvořeny podle potřeby, schvaluje tajemník MÚ a zodpovídá za ně. Kybernetické útoky byly vedeny v posledních 10 letech proti ORP č. 8 dva. Oba se odehrály v roce 2017 pomocí ransomware. Tento MÚ si nevede statistiku kybernetických útoků v průběhu let a nemá vytvořenou analýzu týkající se kybernetické bezpečnosti. Respondent vidí vyvíjející se trend kybernetického nebezpečí, jako stále se zdokonalující a intenzivnější. MÚ nejvíc ohrožuje škodlivým malware. Jako hlavní motivaci ke kybernetickým útokům považuje odborník materiální obohacení. MÚ má zřízen svůj intranet. Zaměstnanci MÚ mají možnost se přihlásit z pracovních elektronických zařízení na veřejnou síť př.: Seznam či Google. Odborník se domnívá, že potencionálním útočníkům by šlo nejvíce o získání bankovních přístupů.

Odborník MÚ sleduje vývoj kybernetických útoků. V poslední době nezaregistroval kybernetický útok. Právě probíhající kybernetický útok by poznal a věděl by, jak se při něm zachovat. Kybernetický útok, který již proběhl, by rozeznal. Neví, k čemu by mohlo dojít bezprostředně po krizové situaci. V případě kybernetického útoku by věděl, jak incident nahlásit. Vládní CERT (GovCERT.cz) tým, se zaměřuje na řešení problémů ve státní správě a KII a národní CERT (CSIRT.cz) tým řeší ostatní incidenty v rámci celé České republiky. Incident kybernetické povahy by nahlašoval podle vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti. Vynaložené finance pro obor kybernetické bezpečnosti považuje za nedostatečné. Sleduje nejnovější trendy a inovace v oboru kybernetické bezpečnosti. S digitalizací veřejné správy je spokojen. Jako podařený informační systém, který vznikl digitalizací veřejné správy, považuje CzechPOINT a datové schránky. Neví, zda umí veřejnost využívat nové informační systémy. Nemůže posoudit, zda dochází k efektivnímu využívání nových informačních systémů veřejné správy. Myslí si, že nedochází k dostatečné osvětě, co se týče kybernetické bezpečnosti ve veřejné správě, týkající se obyvatel České republiky. Považuje proškolení personálu za dostatečné, provádí ho informatik jednou za rok. MÚ neprovádí zkušební nácviky kybernetického bezpečnostního incidentu. S Národní strategií kybernetické bezpečnosti ČR 2021-2025 není odborník detailně seznámen.

4.2.3 Obec s rozšířenou působností č. 9

Odborník městského úřadu na kybernetickou bezpečnost pracuje na své pozici 5-10 let. Zároveň nepůsobí v jiné oblasti krizového řízení. Na tvorbě a udržení kybernetické bezpečnosti zde pracují 3-4 pracovníků. ORP č. 9 má zřízené samostatné oddělení zabývající se pouze informačními technologiemi a kybernetickou bezpečností. Vzdělání má středoškolské. Dále se vzdělává ve svém zaměstnání pravidelně jednou za půl roku, a to pomocí odborných knih, článků a časopisů. Účastní se také odborných seminářů, které jsou pořádané kvalifikovanými subjekty. Není kontaktní osobou pro komunikaci s vládním CERT týmem.

V ORP č. 9 má městský úřad zřízené krizové řízení, a to je zároveň součástí oddělení informačních technologií. Krizový plán v ORP č. 9 obsahuje opatření týkající se kybernetické bezpečnosti/kritické informační infrastruktury. Odborník na danou problematiku se podílí na tvorbě předpisů, směrnic, metodických pokynů aj. Provádí se revize dokumentů jednou za čtyři roky. Tyto dokumenty schvaluje a zodpovídá za ně tajemník MÚ. Kybernetické útoky za posledních 10 let nebyly proti ORP č. 9 vedeny žádné. Kritická informační infrastruktura má stejné prvky s kritickou infrastrukturou v rozhraní vnitřní sítě a internetu, koncových PC a servrech. Tento MÚ nemá vedenou statistiku kybernetických útoků v průběhu let, nemá ani vytvořenou analýzu útoků týkající se kybernetické bezpečnosti. Z dostupných informací vyplývá, že počty kybernetických útoků narůstají a mohou zasáhnout kritická data. MÚ nejvíc ohrožuje sociální inženýrství. Jako hlavní motivaci ke kybernetickým útokům považuje odborník materiální obohacení. Odborník neví, čeho by se nejvíce týkaly útoky vedené proti MÚ. ORP č. 9 má zřízen svůj intranet a zároveň mají zaměstnanci možnost se přihlásit z pracovních elektronických zařízení na veřejnou síť př.: Google či Seznam.

Odborník MÚ nesleduje vývoj kybernetických útoků. V poslední době zaregistroval kybernetický útok na veřejnou správu. Právě probíhající útok by nepoznal. Kybernetický útok, který již proběhl, by nejspíše poznal ztrátou dat. Nevěděl by, jak postupovat při probíhajícím kybernetickém útoku a následném nahlašování na patřičné orgány. Nezná rozdíl mezi vládním CERT (GovCERT.cz) týmem a národním CERT (CSIRT.cz) týmem. Dle odborníka může kybernetický útok způsobit ztrátu dat organizace. Vynaložené finance pro obor kybernetické bezpečnosti považuje za dostatečné. Nezná číslo vyhlášky podle, které se incident kybernetické povahy nahlašuje. Nesleduje nejnovější inovace a

trendy v oboru kybernetické bezpečnosti. Digitalizace veřejné správy je úspěšná a nejvíce přínosná mu přijde e-identita. Myslí si, že dochází k dostatečné osvětě, co se týče kybernetické bezpečnosti ve veřejné správě, týkající se obyvatel České republiky. Lidé, co chtějí inovace používat, s nimi pracují. Za dostatečné považuje proškolení personálu MÚ, ke kterému dochází jednou ročně a provádí si ho oddělení informatiky. MÚ neprovádí zkušební nácviky kybernetického bezpečnostního incidentu. S Národní strategií kybernetické bezpečnosti ČR 2021-2025 není odborník detailně seznámen.

4.2.4 Obec s rozšířenou působností č. 10

Odborník městského úřadu na kybernetickou bezpečnost pracuje na své pozici 10-20 let. Zároveň nepůsobí v jiné oblasti krizového řízení. Na tvorbě a udržení kybernetické bezpečnosti zde pracují 3-4 pracovníků. ORP č. 10 má zřízené samostatné oddělení zabývající se pouze informačními technologiemi a kybernetickou bezpečností. Vzdělání má středoškolské. Dále se vzdělává ve svém zaměstnání pravidelně jednou za tři měsíce, a to pomocí odborných knih, článků, školení a časopisů. Účastní se také odborných seminářů, které jsou pořádané kvalifikovanými subjekty. Není kontaktní osobou pro komunikaci s vládním CERT týmem.

V ORP č. 10 má městský úřad zřízené krizové řízení, a to je zároveň součástí odboru kanceláře starosty. Krizový plán v ORP č. 10 neobsahuje opatření týkající se kybernetické bezpečnosti/kritické informační infrastruktury. Odborník na danou problematiku se podílí na tvorbě předpisů, směrnic, metodických pokynů aj. Provádí se revize dokumentů jednou za rok. Tyto dokumenty schvaluje a zodpovídá za ně tajemník MÚ. Kybernetické útoky za posledních 10 let proti ORP č. 10 jsou vedeny denně, nejčastější je ramsomware. V roce 2013 proběhl pokus o prolomení přístupu do vnitřní sítě MÚ. Průnik se nezdařil, došlo však k dočasné nefunkčnosti internetového připojení. Tento MÚ nemá vedenou statistiku kybernetických útoků v průběhu let, ale má vytvořenou analýzu útoků týkající se kybernetické bezpečnosti. Z dostupných informací vyplývá, že počty kybernetických útoků narůstají a mohou zasáhnout kritická data, kde nyní nejvíce využívají model zotročení. MÚ nejvíc ohrožuje sociální inženýrství. Jako hlavní motivaci ke kybernetickým útokům považuje odborník hacktivismus. Odborník se domnívá, že útočník by měl největší zájem o přístupové údaje. ORP č. 10 má zřízen svůj intranet a zároveň mají zaměstnanci možnost se přihlásit z pracovních elektronických zařízení na veřejnou síť př.: Google či Seznam.

Odborník MÚ nesleduje vývoj kybernetických útoků. V poslední době zaregistroval kybernetický útok na Olomoucký magistrát. Právě probíhající kybernetický útok by poznal zpomalením a částečnou či úplnou paralýzou některých systémů a věděl by, jak se zachovat. Kybernetický útok, který již proběhl, by rozeznal kontrolou logů síťových zařízení a sdělením externího subjektu. Bezprostředně po krizové situaci by mohlo dojít k úniku citlivých dat. V případě kybernetického útoku by se obrátil na vládní CERT. Vládní CERT (GovCERT.cz) tým, se zaměřuje na řešení problémů ve státní správě a KII a národní CERT (CSIRT.cz) tým řeší ostatní incidenty v rámci celé České republiky. Incident kybernetické povahy by nahlašoval podle vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti. Vynaložené finance pro obor kybernetické bezpečnosti považuje za nedostatečné. Sleduje nejnovější trendy a inovace v oboru kybernetické bezpečnosti a snaží se je po předchozí domluvě svedením města aplikovat do provozu. S digitalizací veřejné správy není spokojen, považuje to za pomalé a nekomplexní. Jako podařený informační systém, který vznikl digitalizací veřejné správy, považuje ISZR, Portál občana a datové schránky. Veřejnost neumí využívat nové informační systémy. Nedochází k efektivnímu využívání nových informačních systémů veřejné správy ze strany veřejnosti. Myslí si, že nedochází k dostatečné osvětě, co se týče kybernetické bezpečnosti ve veřejné správě, týkající se obyvatel České republiky. Za dostatečné považuje proškolení personálu MÚ, ke kterému dochází pravidelně jednou za ročně a při nástupu do zaměstnání a provádí ho oddělení IT. MÚ neprovádí zkušební nácviky kybernetického bezpečnostního incidentu. S Národní strategií kybernetické bezpečnosti ČR 2021-2025 není odborník detailně seznámen.

4.2.5 Obec s rozšířenou působností č. 11

Odborník městského úřadu na kybernetickou bezpečnost pracuje na své pozici 20 a více let. Zároveň nepůsobí v jiné oblasti krizového řízení. Na tvorbě a udržení kybernetické bezpečnosti zde pracují 4 a více pracovníků. ORP č. 11 má zřízené samostatné oddělení zabývající se pouze informačními technologiemi a kybernetickou bezpečností. Vzdělání má vysokoškolské zakončené dosaženým titulem Mgr./Ing. Toto vzdělání se přímo netýkalo KB/IT. Dále se vzdělává ve svém zaměstnání nepravidelně podle potřeby, a to pomocí odborných knih, článků, školení a časopisů. Účastní se také odborných seminářů, které jsou pořádané kvalifikovanými subjekty. Není kontaktní osobou pro komunikaci s vládním CERT týmem.

V ORP č. 11 má městský úřad zřízené krizové řízení, a to je zároveň součástí odboru kanceláře úřadu. Odborník na danou problematiku se podílí na tvorbě předpisů, směrnic, metodických pokynů aj. Provádí se revize dokumentů spolu s aktualizací a k tomu dochází v návaznosti na změnu vnějších podmínek. Tyto dokumenty schvaluje a zodpovídá za ně bud' tajemník MÚ, řídící výbor IT nebo rada města. Krizový plán v ORP č. 11 neobsahuje opatření týkající se kybernetické bezpečnosti/kritické informační infrastruktury. Prvky kritické infrastruktury jako je datová infrastruktura, síť elektronických komunikací a výroba elektřiny nejvíce podle respondenta souvisí s kritickou informační infrastrukturou. Kybernetické útoky za posledních 10 let proti ORP č. 11 jsou vedeny denně, nejčastěji ramsomware, kterých proběhlo cca 5 částečně úspěšných (z toho jeden v roce 2016, dva v roce 2018 a dva v roce 2019). Nejzávažnější vedl k zašifrování souborů ve složkách uživatele, který správně nerozpoznal nebezpečný email. Za posledních 7 dnů antivirový systém detekoval cca 500 vyřešených incidentů, jedna čtvrtina se pak týká e-mailů, další čtvrtina jsou nezabezpečené webové stránky a zbytek jsou pokusy o zneužití známých softwarových zranitelností. Tento MÚ nemá vedenou statistiku kybernetických útoků v průběhu let, ale má vytvořenou analýzu útoků týkající se kybernetické bezpečnosti. Z dostupných informací vyplývá, že dochází ke zvýšenému množství kybernetických útoků. MÚ nejvíc ohrožuje škodlivý kombinace útoků. Jako hlavní motivaci ke kybernetickým útokům považuje odborník materiální obohacení. Odborník se domnívá, že útočník by měl největší zájem o přístupové údaje. ORP č. 11 nemá zřízen svůj intranet a zároveň mají zaměstnanci možnost se přihlásit z pracovních elektronických zařízení na veřejnou síť př.: Google či Seznam.

Odborník MÚ sleduje vývoj kybernetických útoků. Ve vývoji ho nejvíce zaujalo množství softwarových zranitelností a množství pokusů o jejich zneužití v letošním roce. V poslední době zaregistroval kybernetický útok na veřejnou správu. Aby poznal právě probíhající útok, záleželo by na způsobu útoku. Detekce souvisí s nasazením obranných prostředků. Právě probíhající a již proběhlý kybernetický útok, by poznal pomocí zašifrovaných souborů. Při probíhajícím kybernetickém útoku by věděl, jak zareagovat. Bezprostředně po krizové situaci by mohlo dojít k omezení provozu organizace a ztráty nebo zveřejnění. Neví, jaký je rozdíl mezi vládním CERT (GovCERT.cz) týmem a CERT (CSIRT.cz) týmem. Nezná číslo vyhlášky podle, které by se incident kybernetické povahy nahlašoval. Vynaložené finance pro obor kybernetické bezpečnosti považuje za nedostatečné. Nesleduje nejnovější trendy a inovace v oboru kybernetické bezpečnosti.

Jako podařený informační systém, který vznikl digitalizací veřejné správy, považuje registr řidičů. Veřejnost umí využívat nové informační systémy. Myslí si, že dochází k dostatečné osvětě, co se týče kybernetické bezpečnosti ve veřejné správě, týkající se obyvatel České republiky. Za dostatečné považuje proškolení personálu MÚ, ke kterému dochází pravidelně jednou za několik let a probíhá pomocí on-line kurzů. MÚ neprovádí zkušební nácviky kybernetického bezpečnostního incidentu. S Národní strategií kybernetické bezpečnosti ČR 2021-2025 není odborník detailně seznámen.

4.2.6 Obec s rozšířenou působností č. 12

Odborník městského úřadu na kybernetickou bezpečnost pracuje na své pozici 5-10 let. Zároveň nepůsobí v jiné oblasti krizového řízení. Na tvorbě a udržení kybernetické bezpečnosti zde pracují 4 a více pracovníků. ORP č. 12 má zřízené samostatné oddělení zabývající se pouze informačními technologiemi a kybernetickou bezpečností. Vzdělání má vysokoškolské zakončené dosaženým titulem Mgr./Ing. Toto vzdělání se přímo netýkalo KB/IT. Dále se vzdělává ve svém zaměstnání nepravidelně podle potřeby, a to pomocí odborných knih, článků, školení a časopisů. Účastní se také odborných seminářů, které jsou pořádané kvalifikovanými subjekty. Není kontaktní osobou pro komunikaci s vládním CERT týmem.

V ORP č. 12 má městský úřad zřízené krizové řízení, a to je zároveň součástí kanceláře starosty. Pracovník neví, zda se nachází v plánu ORP č. 12 opatření týkající se kybernetické bezpečnosti. Odborník na danou problematiku se podílí na tvorbě předpisů, směrnic, metodických pokynů aj. Provádí se revize dokumentů spolu s aktualizací a k tomu dochází obvykle v intervalu 2-5 let. Tyto dokumenty schvaluje a zodpovídá za ně rada města a odbor ICT. Všechny prvky kritické infrastruktury souvisí s kritickou informační infrastrukturou. Kybernetické útoky za posledních 10 let proti ORP č. 12 jsou vedeny denně. Tento MÚ nemá vedenou statistiku kybernetických útoků v průběhu let, ale má vytvořenou analýzu útoků týkající se kybernetické bezpečnosti. Z dostupných informací vyplývá, že dochází ke zvýšenému množství kybernetických útoků, a to je málo radostná informace. MÚ nejvíc ohrožuje sociální inženýrství a kombinace DoS/DDoS a škodlivý malware. Jako hlavní motivaci ke kybernetickým útokům považuje odborník materiální obohacení a hacktivismus. Odborník neví, o jaké informace by měl útočník zájem. ORP č. 12 má zřízen svůj intranet a zároveň mají zaměstnanci možnost se přihlásit z pracovních elektronických zařízení na veřejnou síť př.: Google či Seznam.

Odborník MÚ nesleduje vývoj kybernetických útoků. V poslední době nezaregistroval žádný kybernetický útok na veřejnou správu. Právě probíhající a již proběhlý kybernetický útok byl poznán. Při probíhajícím kybernetickém útoku by věděl, jak postupovat. Není si jistý, k jakým krizovým situacím by mohlo dojít bezprostředně po incidentu. V případě kybernetického útoku by ho nikam nenahlásil. Neví, jaký je rozdíl mezi vládním CERT (GovCERT.cz) týmem a CERT (CSIRT.cz) týmem. Nezná číslo vyhlášky podle, které by se incident kybernetické povahy nahlašoval. Vynaložené finance pro obor kybernetické bezpečnosti považuje za dostatečné. Sleduje nejnovější trendy a inovace v oboru kybernetické bezpečnosti a poté se je snaží zařadit realizací pilotních projektů. Jako podařený informační systém, který vznikl digitalizací veřejné správy považuje portál občana, jinak není s digitalizací spokojen. Veřejnost neumí využívat nové informační systémy. Nedochází k efektivnímu využívání nových informačních systémů veřejné správy. Myslí si, že dochází k dostatečné osvětě, co se týče kybernetické bezpečnosti ve veřejné správě, týkající se obyvatel České republiky. Za dostatečné považuje proškolení personálu MÚ, ke kterému dochází jednou za dva roky a provádí ho externí firma. MÚ provádí zkušební nácviky kybernetického bezpečnostního incidentu, obvykle jednou za dva roky a výsledek je zapsán v závěrečné zprávě cvičení. S Národní strategií kybernetické bezpečnosti ČR 2021-2025 není odborník detailně seznámen.

4.2.7 Obec s rozšířenou působností č. 13

Odborník městského úřadu na kybernetickou bezpečnost pracuje na své pozici 10-20 let. Zároveň nepůsobí v jiné oblasti krizového řízení. Na tvorbě a udržení kybernetické bezpečnosti zde pracují 4 a více pracovníků. ORP č. 13 má zřízené samostatné oddělení zabývající se pouze informačními technologiemi a kybernetickou bezpečností. Vzdělání má středoškolské. Dále se vzdělává ve svém zaměstnání pravidelně, a to pomocí odborných knih, článků, školení a časopisů. Účastní se také odborných seminářů, které jsou pořádané kvalifikovanými subjekty. Není kontaktní osobou pro komunikaci s vládním CERT týmem.

V ORP č. 13 má městský úřad zřízené krizové řízení, a to je zároveň součástí kanceláře starosty a tajemníka. Odborník na danou problematiku se nepodílí na tvorbě předpisů, směrnic, metodických pokynů aj. Krizový plán ORP č. 13 neobsahuje opatření týkající se kybernetické bezpečnosti/kritické informační infrastruktury. Kybernetický útok za posledních 10 let proti ORP č. 13 byl veden jeden a odehrál se na podzim roku 2019

prolomením portů na FW. Tento MÚ nemá vedenou statistiku kybernetických útoků v průběhu let ani nemá vytvořenou analýzu útoků týkající se kybernetické bezpečnosti. Z dostupných informací vyplývá, že množství kybernetických útoků se neustále zvyšuje. MÚ nejvíc ohrožuje škodlivý malware. Jako hlavní motivaci ke kybernetickým útokům považuje odborník hacktivismus a vnitřní hrozbu. Odborník se domnívá, že útočník by měl největší zájem o osobní data. ORP č. 13 má zřízen svůj intranet a zároveň mají zaměstnanci možnost se přihlásit z pracovních elektronických zařízení na veřejnou síť př.: Google či Seznam.

Odborník MÚ nesleduje vývoj kybernetických útoků. V poslední době zaregistroval kybernetický útok na veřejnou správu. Síťová zařízení MÚ má na starosti odborná externí firma, která má pod dohledem potenciální probíhající i proběhlý kybernetický útok. Odborník zná postup při probíhajícím kybernetickém útoku a ví, kam daný incident nahlásit. Bezprostředně po krizové situaci budou odstaveny všechny informační systémy úřadu, takže nebude možné řešit požadavky občanů a řešit příslušnou agendu. Odborník nezná rozdíl mezi vládním CERT (GovCERT.cz) týmem a národní CERT (CSIRT.cz) týmem. Nezná číslo vyhlášky, podle níž by se incident kybernetické povahy nahlašoval. Vynaložené finance pro obor kybernetické bezpečnosti považuje za nedostatečné. Nesleduje nejnovější trendy a inovace v oboru kybernetické bezpečnosti. S digitalizací veřejné správy není spokojen, považuje to za složitý systém. Jako podařený informační systém neumí žádný označit. Veřejnost neumí využívat nové informační systémy. Nemůže posoudit, zda dochází k efektivnímu využívání nových informačních systémů veřejné správy. Myslí si, že dochází k dostatečné osvětě, co se týče kybernetické bezpečnosti ve veřejné správě, týkající se obyvatel České republiky. Za nedostatečné považuje proškolení personálu MÚ, který nemá zřízené pravidelné proškolení v dané kybernetické problematice. MÚ neprovádí zkušební nácviky kybernetického bezpečnostního incidentu. S Národní strategií kybernetické bezpečnosti ČR 2021-2025 není odborník detailně seznámen.

4.2.8 Obce s rozšířenou působností č. 14

Odborník městského úřadu na kybernetickou bezpečnost pracuje na své pozici 10-20 let. Zároveň nepůsobí v jiné oblasti krizového řízení. Na tvorbě a udržení kybernetické bezpečnosti zde pracuje 1-2 pracovníci. ORP č. 14 má zřízené samostatné oddělení zabývající se pouze informačními technologiemi a kybernetickou bezpečností. Vzdělání

má středoškolské. Dále se vzdělává ve svém zaměstnání pravidelně, a to pomocí odborných knih, článků, školení a časopisů. Účastní se také odborných seminářů, které jsou pořádané kvalifikovanými subjekty. Není kontaktní osobou pro komunikaci s vládním CERT týmem.

V ORP č. 14 má městský úřad zřízené krizové řízení, a to je zároveň součástí odboru životního prostředí. Krizový plán v ORP č. 14 neobsahuje opatření týkající se kybernetické bezpečnosti/kritické informační infrastruktury. Odborník na danou problematiku se nepodílí na tvorbě předpisů, směrnic, metodických pokynů aj. Za posledních 10 let proti ORP č. 14 nebyl veden žádný kybernetický útok. Tento MÚ má vedenou statistiku kybernetických útoků v průběhu let a má vytvořenou analýzu útoků týkající se kybernetické bezpečnosti. Dle odborníka trend kybernetických útoků průběžně roste. MÚ nejvíc ohrožuje škodlivým malware. Jako hlavní motivaci ke kybernetickým útokům považuje odborník vnitřní hrozbu. Odborník se domnívá, že útoky vedené proti MÚ jsou vedeny za materiálním obohacením. MÚ má zřízen svůj intranet a zároveň mají zaměstnanci možnost se přihlásit z pracovních elektronických zařízení na veřejnou síť př.: Google či Seznam.

Odborník MÚ sleduje vývoj kybernetických útoků. V poslední době zaregistroval kybernetický útok ve veřejné správě České republiky na magistrát města Olomouc. Právě probíhající kybernetický útok by poznal např.: nedostupností serverů, sítě, aj. Útok, který již proběhl, by poznal nedostupností některých souborů. Po proběhlém kybernetickém útoku by mohla bezprostředně poté nastat nedostupnost vnitřní sítě. V případě kybernetického útoku by vše hlásil na vládní CERT. Vládní CERT (GovCERT.cz) tým, se zaměřuje na řešení problémů ve státní správě a KII a národní CERT (CSIRT.cz) tým řeší ostatní incidenty v rámci celé České republiky. Incident kybernetické povahy by nahlašoval podle vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti. Vynaložené finance pro obor kybernetické bezpečnosti považuje za dostatečné. Sleduje nejnovější trendy a inovace v oboru kybernetické bezpečnosti a snaží se je postupně začlenit. Digitalizaci považuje za špatně koordinovanou. Jako podařený informační systém, který vznikl digitalizací veřejné správy, považuje ISZR. Veřejnost umí využívat nové informační systémy, u některých je potřeba e-identita nebo datová schránka, což zatím mnozí nemají nebo ani nechtějí používat. Myslí si, že dochází k dostatečné osvětě, co se týče kybernetické bezpečnosti ve veřejné správě, týkající se obyvatel České republiky. Za dostatečné považuje i proškolení personálu MÚ, ke kterému dochází pravidelně

jednou za rok. MÚ neprovádí zkušební nácviky kybernetického bezpečnostního incidentu. S Národní strategií kybernetické bezpečnosti ČR 2021-2025 není odborník detailně seznámen.

5 Zpracování dat

K rozhovoru a poté vyplnění dotazníku byly osloveny obce s rozšířenou působností v Jihočeském kraji a Kraji Vysočina. Celkem jich bylo 32. K výzkumu se připojilo 14 obcí s rozšířenou působností. Do tabulek 2 a 3 uvedených níže bylo zakresleno, které ORP se šetření účastnily. Jedna obec s rozšířenou působností z Kraje Vysočina chce zůstat v úplné anonymitě, avšak je zanesena do výzkumného šetření.

Tabulka 2 – Jihočeský kraj data

JIHOČESKÝ KRAJ	ANO	NE
Blatná	x	
České Budějovice	x	
Český Krumlov		x
Dačice	x	
Jindřichův Hradec	x	
Kaplice	x	
Milevsko		x
Písek	x	
Prachatice		x
Soběslav		x
Strakonice	x	
Tábor		x
Trhové Sviny		x
Třeboň		x
Týn nad Vltavou		x
Vimperk	x	
Vodňany		x

Zdroj: vlastní výzkum

Tabulka 3 – Kraj Vysočina data

KRAJ VYSOČINA	ANO	NE
Bystřice nad Pernštejnem		x
Havlíčkův Brod		x
Humpolec	x	
Chotěboř		x
Jihlava		x
Moravské Budějovice		x
Náměšť nad Oslavou	x	
Nové město na Moravě		x
Pacov	x	
Pelhřimov	x	
Světlá nad Sázavou		x
Telč		x
Třebíč	x	
Velké Meziříčí		x
Žďár nad Sázavou		x

Zdroj: vlastní výzkum

Předem vybraná data, která byla získána, jsou prezentována pomocí tabulek, grafů, metody trendů, megatrendů a kola budoucnosti. Všechny odpovědi jsou prezentovány v kapitole Výsledky, která je součástí této diplomové práce. Jako první byly vytvořené tabulky, kde jsou zpracovaný některé otevřené otázky, které vedly k zajímavým výsledkům. Tyto odpovědi jsou citovány. Jejich cílem je kvalitní přepis a kategorizace těchto dat. Dále byly vytvořeny grafy v podobě obrázků, které znázorňují odpovědi na otázky spíše uzavřeného charakteru. Pro lepší přehlednost obrázků je Jihočeský kraj znázorněn modrou barvou a Kraj Vysočina je znázorněn barvou žlutou. V diplomové práci se neporovnávají kraje navzájem, proto je v grafech použita ještě barva červená a slouží k celkovému součtu výsledků a je označena slovem Celkem a je pro výzkum zásadní.

5.1 Znázornění vybraných odpovědí za pomoci kategorizace v tabulkách

Vybrané odpovědi ze strukturovaného rozhovoru jsou rozřazeny do 4 kategorií. Jednotlivé kategorie jsou dále rozebrány a prezentovány pomocí tabulek. Součástí těchto tabulek jsou citace odpovědí participantů.

a) Kategorie 1 Informace, které chtějí útočníci nejvíce získat.
b) Kategorie 2 Kybernetické útoky na veřejnou správu v České republice.
c) Kategorie 3 Následky způsobené bezprostředně po kybernetickém útoku.
d) Kategorie 4 Národní strategie kybernetické bezpečnosti ČR 2021-2025.

5.1.1 Výsledky výzkumné šetření

a) Kategorie 1 Informace, které chtějí útočníci nejvíce získat.

Tabulka 4 – Informace, které chtějí útočníci nejvíce získat

Participanti	Informace, které chtějí útočníci získat
ORP č. 1	„Myslím si, že jim jde spíše o ohrožení chodu MÚ.“
ORP č. 2	„Nejvíce osobní nebo bankovní údaje.“
ORP č. 3	„Nevím. Může se jednat o materiální ohodnocení, pokud ne, domnívám se, že jde o internetový exhibicionismus.“
ORP č. 4	„Přihlašovací údaje.“
ORP č. 5	„Zpeněžitelná data.“
ORP č. 6	„Hesla.“
ORP č. 7	„Informace týkající se mimo jiné konkrétních správních, či projektových řízení.“
ORP č. 8	„Bankovní přístup.“
ORP č. 9	„Nevím.“
ORP č. 10	„Přístupové údaje, případně osobní údaje.“
ORP č. 11	„E-mailové zprávy včetně kontaktů a přihlašovacích údajů.“
ORP č. 12	„Osobní data, což jsou velice citlivá data.“
ORP č. 13	„Nevím.“
ORP č. 14	„Nevím.“

Zdroj: vlastní výzkum

Tabulka 4 prezentuje odpovědi na otázku č. 22 zaznamenanou v dotazníku. Z tabulky je patrné, že mezi informace, které by byly podle odborníků odcizeny, jednoznačně patří přihlašovací údaje, hesla, osobní údaje aj. Odpovědi se mohou lišit hlavně zkušenostmi v daném oboru a také rozlohou odpovídajících ORP.

b) Kategorie 2 Kybernetické útoky na veřejnou správu v České republice.

Tabulka 5 – Kybernetické útoky na veřejnou správu v České republice

Participanti	Zaregistrování kybernetických útoků v ČR
ORP č. 1	„Magistrát Olomouce.“
ORP č. 2	„Magistrát města Olomouce.“
ORP č. 3	„Magistrát Olomouce a útok na nemocnici Benešov.“
ORP č. 4	„Ano.“
ORP č. 5	„Ano, nemocniční zařízení.“
ORP č. 6	„Ano na nemocnice.“
ORP č. 7	„Olomoucký magistrát.“
ORP č. 8	„Ano.“
ORP č. 9	„Ano.“
ORP č. 10	„Březnový útok na MPSV či magistrát Olomouc.“
ORP č. 11	„Ano, dost jich bylo medializovaných.“
ORP č. 12	„Nesleduji to.“
ORP č. 13	„Magistrát města Prahy a Olomouc.“
ORP č. 14	„Ano.“

Zdroj: vlastní výzkum

Tabulka 5 prezentuje odpovědi na otázku č. 26 zaznamenanou v dotazníku. Odpověď na tuto otázku velmi ovlivnil útok na magistrát města Olomouce. Odborníci na kybernetickou bezpečnost registrují v průběhu poslední doby kybernetické útoky hlavně cílené na veřejnou správu.

c) Kategorie 3 Následky způsobené bezprostředně po kybernetickém útoku.

Tabulka 6 – Následky způsobené bezprostředně po kybernetickém útoku

Participanti	Bezprostřední následky po kybernetickém útoku
ORP č. 1	„Fatální důsledky pro městský úřad.“
ORP č. 2	„Dočasná nedostupnost dat nebo elektronických služeb pro veřejnost i vnitřní chod úřadu.“
ORP č. 3	„Nemožnost normální plnohodnotné provozní činnosti organizace.“
ORP č. 4	„Ztráta dat, nemožnost přístupu do sítě.“
ORP č. 5	„Ochromení provozu, neposkytování služeb.“
ORP č. 6	„Zhroucení celého systému HW i SW.“
ORP č. 7	„Únik osobních údajů, znehodnocení živých dat, následuje postupná rekonstrukce infrastruktury a obnovení provozu.“
ORP č. 8	„Nevím.“
ORP č. 9	„Ztráta dat.“
ORP č. 10	„Únik citlivých dat či informací.“
ORP č. 11	„Omezení provozu organizace, ztráta nebo zveřejnění dat.“
ORP č. 12	„Budou odstaveny všechny informační systémy úřadu, nebudeme schopni řešit požadavky občanů a vykonávat příslušné agendy.“
ORP č. 13	„Nevím.“
ORP č. 14	„Záleží na typu útoku, malé nebo velké.“

Zdroj: vlastní výzkum

Tabulka 6 prezentuje odpovědi na otázku č. 33 zaznamenanou v dotazníku. Odpovědi byly velmi rozmanité. Většina odpovědí však poukazuje na vyřazení městského úřadu z normálního provozu. Na tuto skutečnost dále navazuje mnoho činností, které ovlivňují nejen chod úřadu, ale také narušují poskytované služby pro občany.

d) Kategorie 4 Národní strategie kybernetické bezpečnosti ČR 2021-2025.

Tabulka 7 – Národní strategie kybernetické bezpečnosti ČR 2021-2025

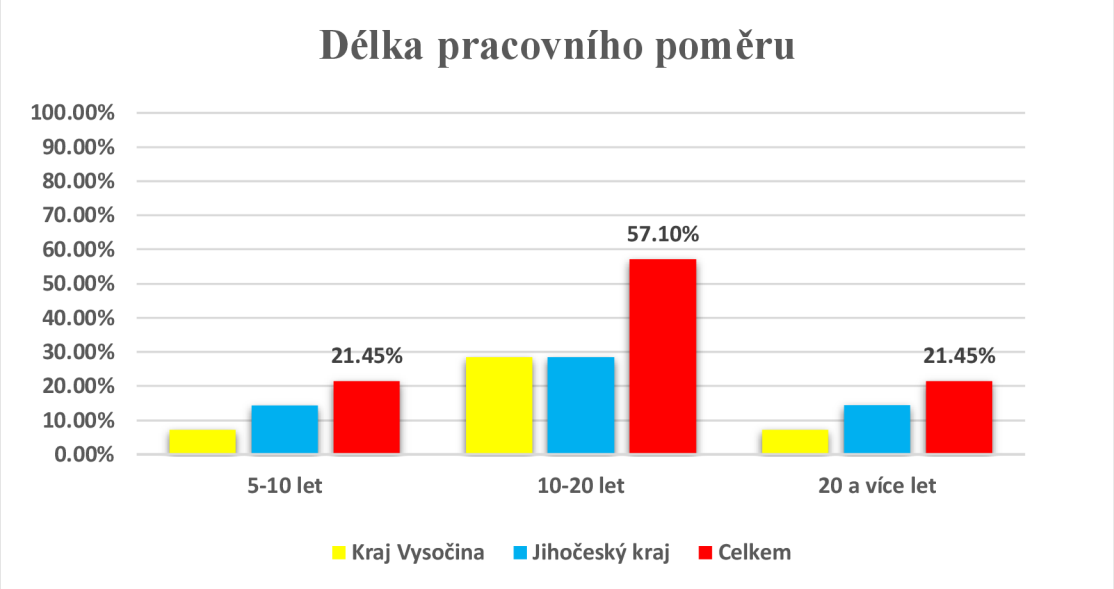
Participanti	Národní strategie kybernetické bezpečnosti ČR 2021-2025
ORP č. 1	„Nejsem s ní detailně seznámen.“
ORP č. 2	„Obecné principy, které jsou celkem přehledně definované od nejnižší úrovně až po návaznost na nadnárodní spojence.“
ORP č. 3	„Zatím jsem tento dokument neprostudoval.“
ORP č. 4	„Nevím.“
ORP č. 5	„Zatím nic.“
ORP č. 6	„Neumím posoudit.“
ORP č. 7	„Teoreticky je strategie zpracována kvalitně a v zásadě i přehledně. Otázkou zůstávají její reálné dopady.“
ORP č. 8	„Nevím.“
ORP č. 9	„Nevím.“
ORP č. 10	„Zběžně jsem tento dokument prošel, avšak nemám k tomu co říct.“
ORP č. 11	„Nevím.“
ORP č. 12	„Zatím jsem tuto strategii nečetl.“
ORP č. 13	„Nevím.“
ORP č. 14	„Nejsem s ní detailně seznámen.“

Zdroj: vlastní výzkum

Tabulka 7 prezentuje odpovědi na otázku č. 43 zaznamenanou v dotazníku. Zde bylo nemilým překvapením zjištění většinového nezájmu ze strany 11 odborníku na Národní strategii kybernetické bezpečnosti ČR 2021-2025. Tato strategie, kterou zpracovává Národní úřad pro kybernetickou bezpečnost, jistě patří mezi publikace, které by měly být důkladně prostudovány odborníky.

5.2 *Znázornění vybraných odpovědí za pomoci obrázků*

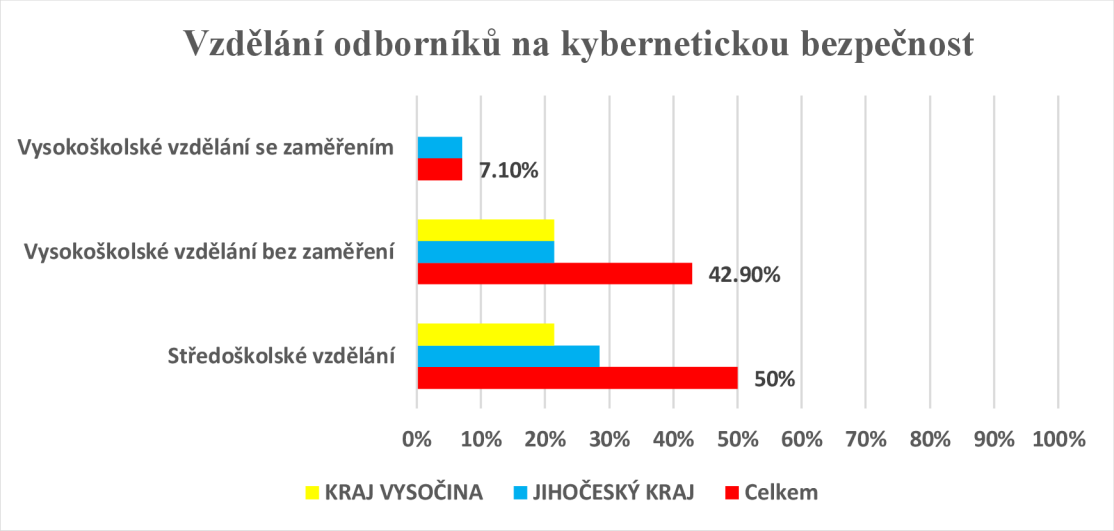
Z odpovědí vybraných otázek jsou sestaveny grafy, které jsou poté prezentovány ve formě obrázků. Grafické znázornění má za cíl přehledné prezentování podobností či rozdílů současné a budoucí kybernetické bezpečnosti v územně samosprávném celku v Jihočeském kraji a Kraji Vysočina. Do grafu je vždy zanesena ještě celková procentuální hodnota odpovědí na danou otázku. Jednotlivé odpovědi jsou zprůměrovány vždy tak, aby zanesená konečná hodnota odpovídala průměrně aktivním účastněným v obou zkoumaných krajích a jejich obcích s rozšířenou působností. Jelikož není ze zkoumaných krajů stejný počet odebraných dat a cílem práce není porovnání krajů mezi s sebou, je znázornění Kraje Vysočina a Jihočeského kraje zahrnuto spíše pro zajímavost a důležitá hodnota je vedena pod názvem Celkem.



Obrázek 1 Délka pracovního poměru na pozici zabývající se kybernetickou bezpečností

Zdroj: vlastní výzkum

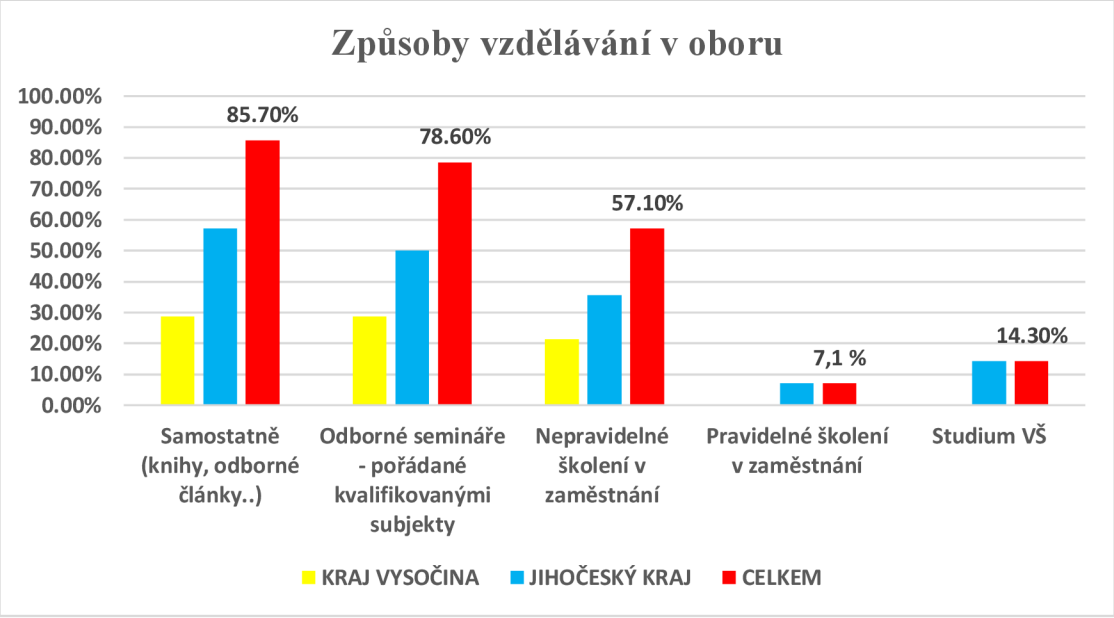
Obrázek „Délka pracovního poměru“ je zpracován z odpovědí na otázku č. 3 z dotazníku. Graf poukazuje na dlouhodobé působení odborníků na pracovní pozici zabývající se kybernetickou bezpečností u více než 78 % dotázaných. Pokud je hodnocena kybernetická bezpečnost zkoumána hlavně za posledních 10 let, jedná se o pozitivní zjištění.



Obrázek 2 Jaké má odborník na kybernetickou bezpečnost vzdělání

Zdroj: vlastní výzkum

Obrázek „Vzdělání odborníků na kybernetickou bezpečnost“ je zpracován z odpovědí na otázku č. 7 z dotazníku. Je zajímavé, že 50 % dotázaných odborníků má vysokoškolské vzdělání a přesně druhá polovina středoškolské vzdělání. Jeden z dotázaných odborníků má přímo vystudovánu vysokou školu se zaměřením na IT.

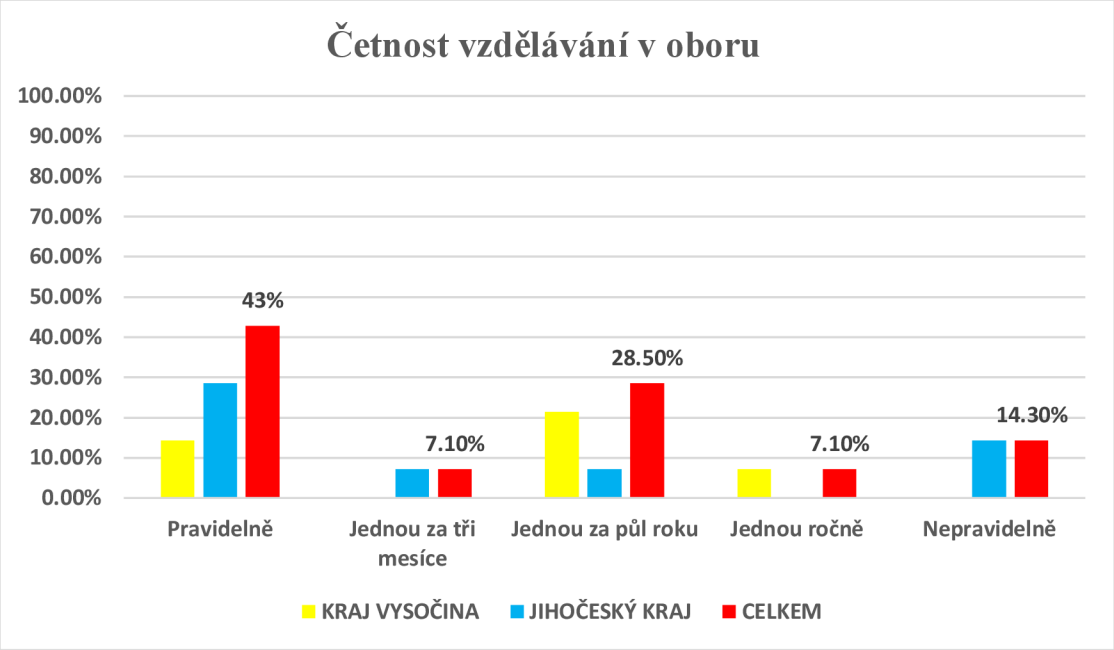


Obrázek 3 Způsoby, jakými se odborník vzdělává ve svém oboru

Zdroj: vlastní výzkum

Obrázek „Způsoby vzdělávání v oboru“ je zpracován z odpovědí na otázku č. 8 (bylo zde

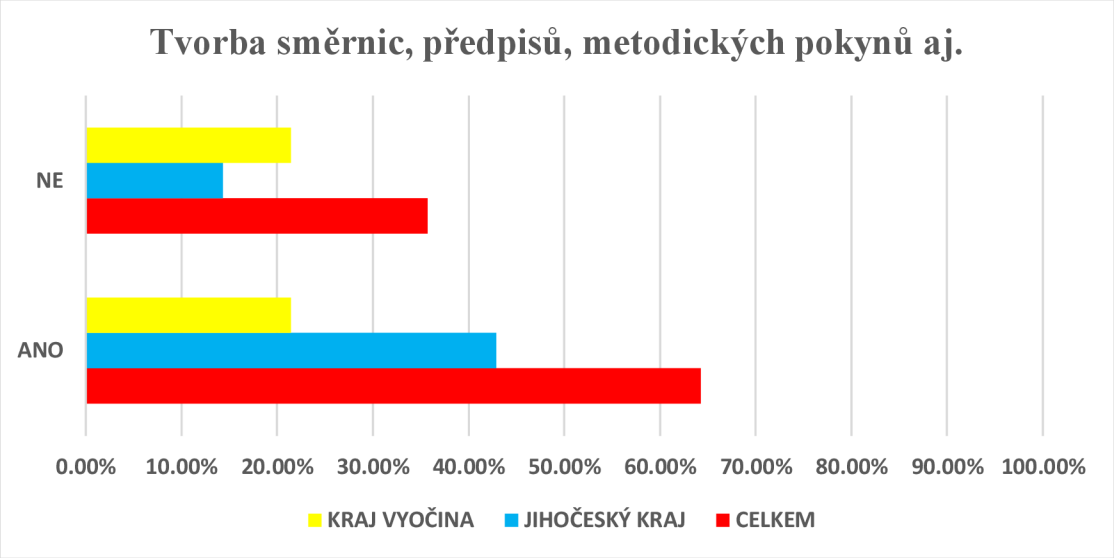
možné použít víc odpovědí) z dotazníku. Jako nejvíce používané (přes 85,7 %) se ukázalo samostatné vzdělávání pomocí odborných článků, knih, odborných časopisů aj. Mezi neméně používané patří odborné semináře, které jsou pořádány kvalifikovanými subjekty zaměřující se na IT. Jako skoro nevyužívané jsou pravidelné školení v zaměstnání.



Obrázek 4 Četnost vzdělávání v oboru

Zdroj: vlastní výzkum

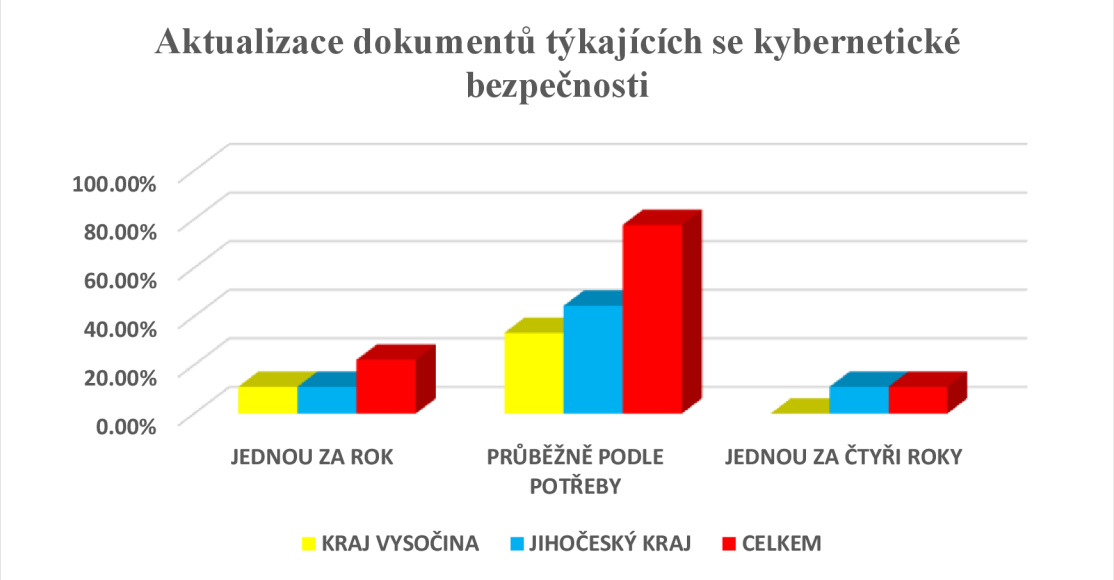
Obrázek „Četnost vzdělávání v oboru“ je zpracován z odpovědí na otázku č. 9 z dotazníku. Pravidelné vzdělávání v oboru je skoro u 43 % dotázaných zásadní. Přes 42,7 % odborníků zase preferuje, stejně se opakující interval vzdělávání.



Obrázek 5 Podílení na tvorbě směrnic, předpisů, metodických pokynů aj., které se týkají kybernetické bezpečnosti daného MÚ

Zdroj: vlastní výzkum

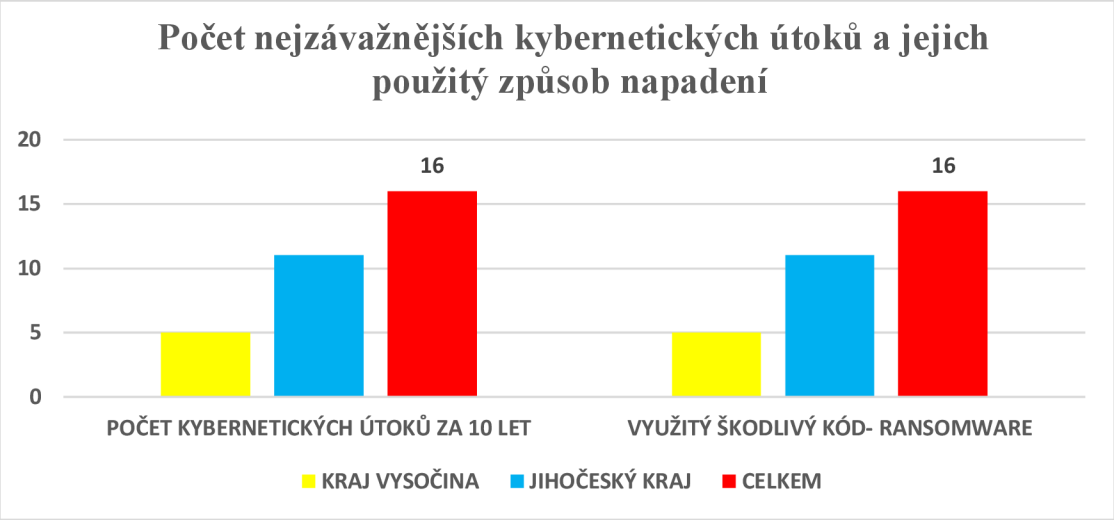
Obrázek „Tvorba směrnic, předpisů, metodických pokynů aj.“ je zpracována z odpovědí na otázku č. 13 z dotazníku. Je patrné, že přes 64 % dotázaných se podílí na tvorbě směrnic, předpisů, metodických pokynů aj.



Obrázek 6 Četnost potřeby aktualizace dokumentů MÚ, týkajících se kybernetické bezpečnosti

Zdroj: vlastní výzkum

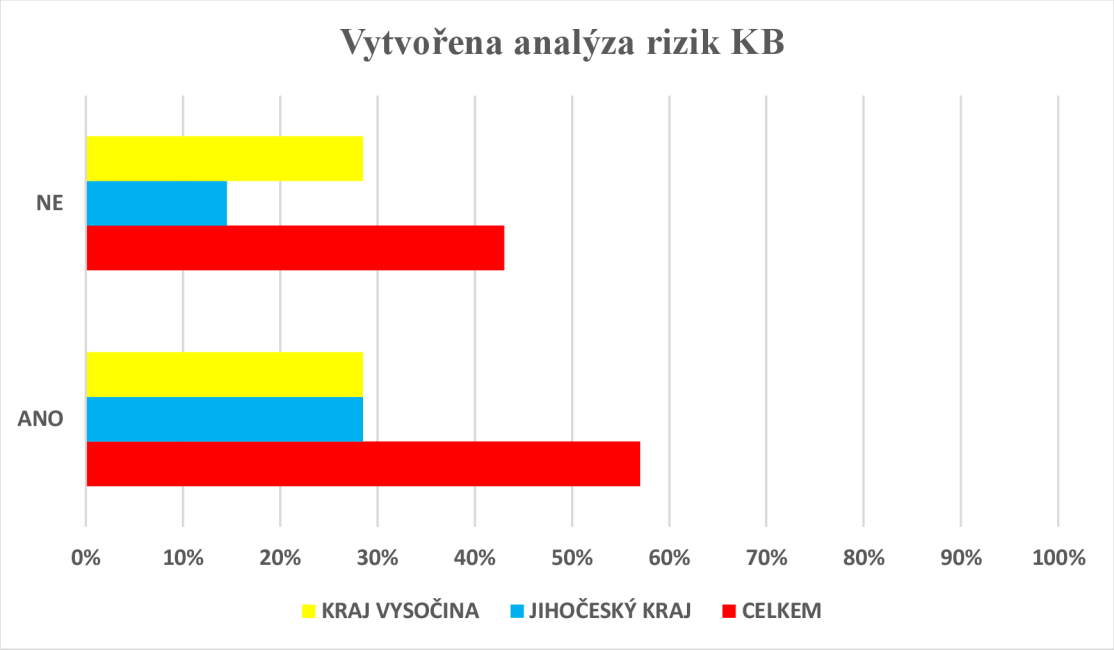
Obrázek „Aktualizace dokumentů týkajících se kybernetické bezpečnosti“ je zpracován z odpovědí na podotázku č. 13. a z dotazníku a poukazuje na aktualizování dokumentů, kdy přes 77 % dotázaných k této činnosti přistupuje průběžně dle potřeb MÚ.



Obrázek 7 Počet nejzávažnějších kybernetických útoků za posledních 10 let vedených proti zkoumaným obcím s rozšířenou působností a využitá forma napadení

Zdroj: vlastní výzkum

Obrázek „Počet nejzávažnějších kybernetických útoků a jejich použitý způsob napadení“ je zpracován z odpovědí na otázku č. 15, 16 z dotazníku. Z grafu je patrné, že za posledních 10 let ve vybraných územně samosprávných celcích proběhlo 16 nejzávažnějších útoků a ve 100 % případů šlo o napadení škodlivým kódem ransomware.



Obrázek 8 ORP a vytvořená analýza rizik týkající se kybernetických útoků

Zdroj: vlastní výzkum

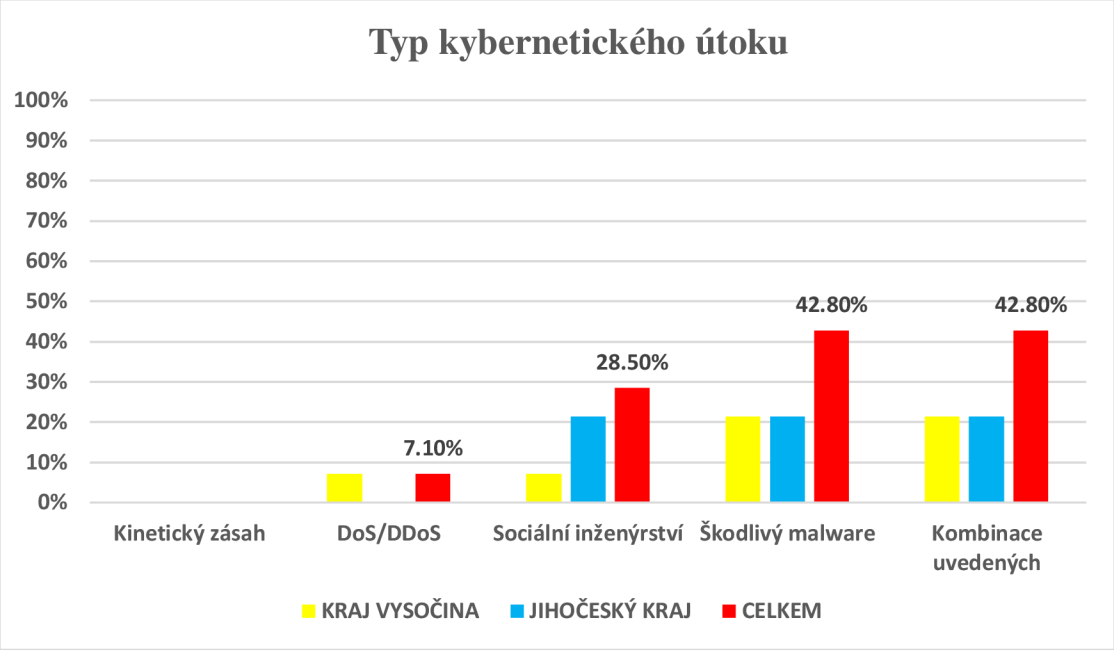
Obrázek „Vytvořena analýza rizik KB“ je zpracován z odpovědí na otázku č. 18 z dotazníku. Víc jak 57 % dotázaných odpověděla, že jejich příslušný MÚ má vytvořenou analýzu rizik týkající se kybernetické bezpečnosti.

Obrázek 9 Vývoj trendu kybernetických útoků

Zdroj: vlastní výzkum

Obrázek „Vývoj trendu kybernetických útoků“ je zpracován z odpovědí na otázku

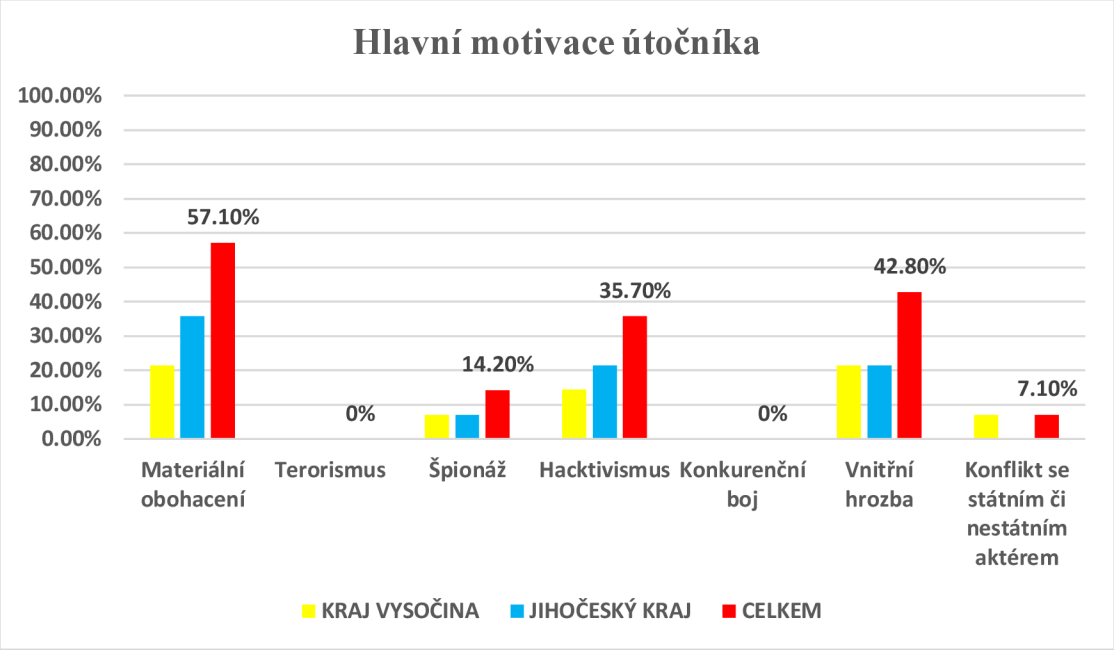
č. 19 z dotazníku. Přes 92 % dotázaných v oblasti trendů kybernetických útoků pozoruje zvýšený nárůst těchto útoků. Kvalita kybernetických útoků je spíše stejná.



Obrázek 10 Typ kybernetického útoku, kterým je MÚ nejvíce ohrožen

Zdroj: vlastní výzkum

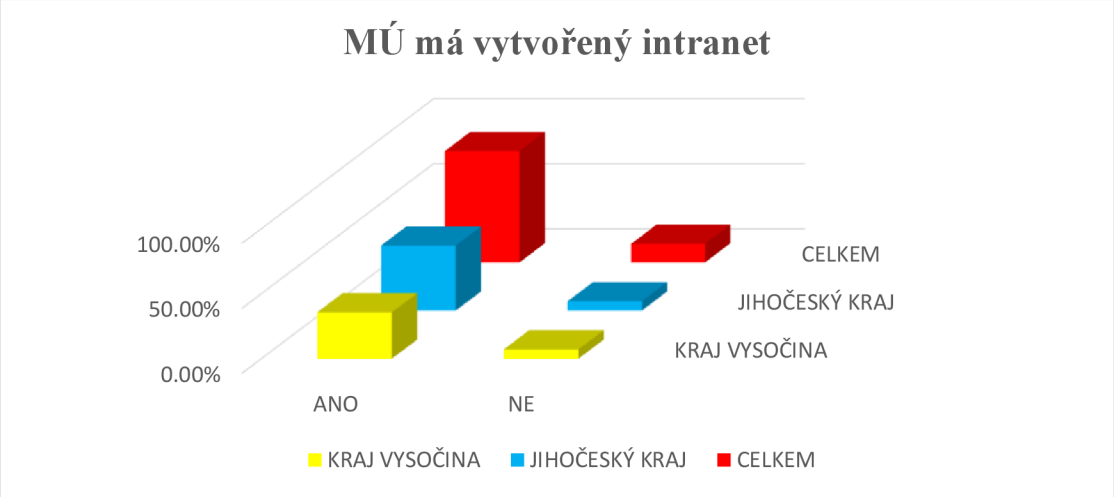
Obrázek „Typ kybernetického útoku“ je zpracován z odpovědí na otázku č. 20 (bylo zde možné použít víc odpovědí) z dotazníku. V otázce byly uvedeny 4 nejčastější typy útoků dle odborné literatury. Skoro 43 % odpovědí poukazovalo na škodlivý malware. Stejný počet odpovědí byl zodpovězen i u možnosti „kombinace uvedených útoků“.



Obrázek 11 Hlavní motivace útočníka při kybernetickém útoku

Zdroj: vlastní výzkum

Obrázek „Hlavní motivace útočníka“ je zpracován z odpovědí na otázku č. 21 (bylo zde možné použít víc odpovědí) z dotazníku. Odborníci na kybernetickou bezpečnost považují z 57 % za největší motivaci útočníka materiální obohacení a dále se bojí vnitřní hrozby – selhání zaměstnance. Jako jednou z obávaných motivací je také hacktivismus.

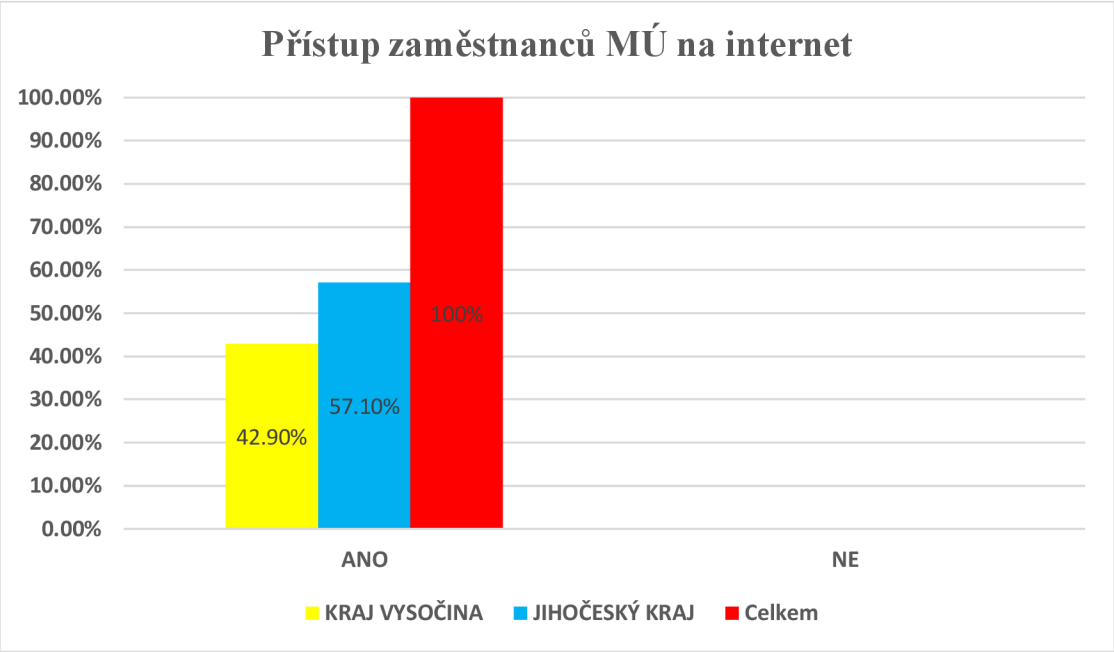


Obrázek 12 Městský úřad má zřízen a využívá svůj intranet

Zdroj: vlastní výzkum

Obrázek „MÚ má vytvořený intranet“ je zpracován z odpovědí na otázku č. 23

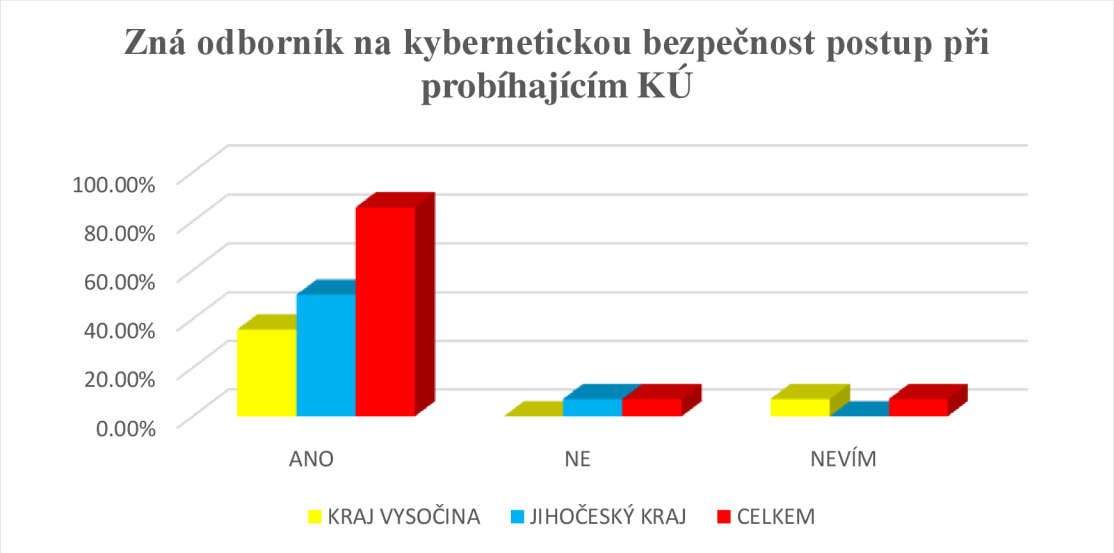
z dotazníku. Přes 85 % dotázaných MÚ má zřízený intranet, využívaný jako informační a komunikační portál.



Obrázek 13 Zaměstnanci mají možnost se přihlásit z pracovních elektronických zařízení na veřejnou síť

Zdroj: vlastní výzkum

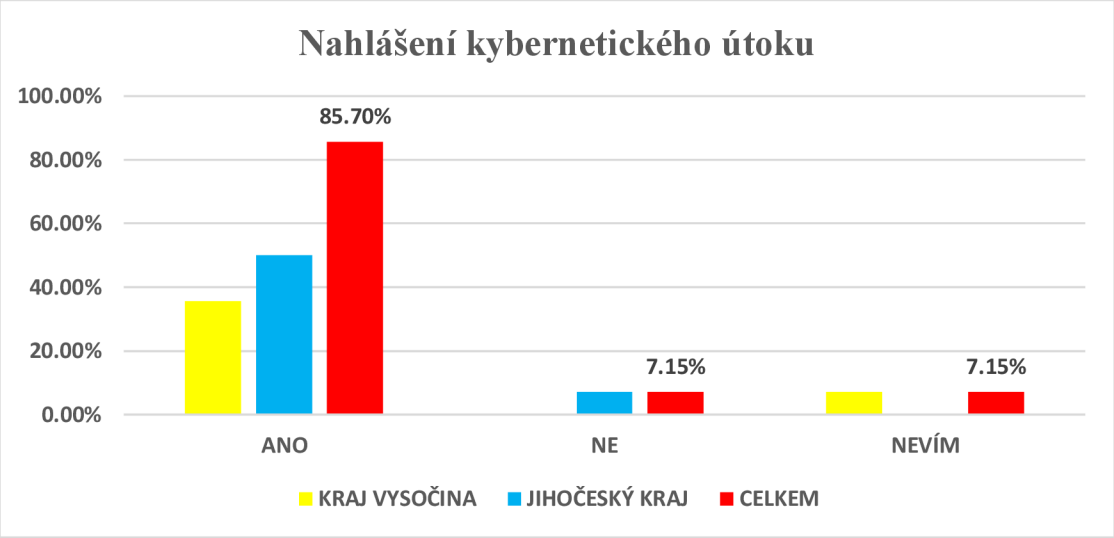
Obrázek „Přístup zaměstnanců MÚ na internet“ je zpracován z odpovědí na otázku č. 24 z dotazníku. Z grafu je patrné, že 100 % dotázaných ORP povolují svým zaměstnancům volný přístup na veřejnou síť (např.: Google, seznam) z pracovních zařízení.



Obrázek 14 Zná odborník na kybernetickou bezpečnost postup při probíhajícím kybernetickém útoku

Zdroj: vlastní výzkum

Obrázek „Zná odborník na kybernetickou bezpečnost postup při probíhajícím KÚ“ je zpracován z odpovědí na otázku č. 29 z dotazníku. Z grafu je možné vyvodit pozitivní zjištění, že přes 85 % dotazovaných odborníků ví, jak postupovat při probíhajícím útoku.

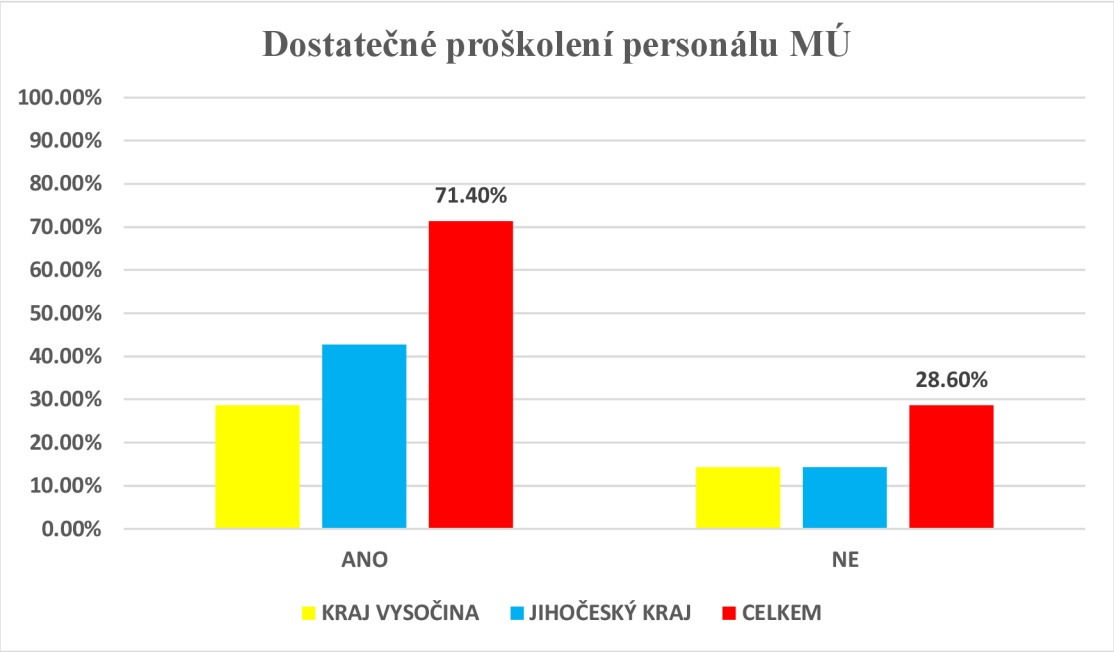


Obrázek 15 Ví odborník na kybernetickou bezpečnost, kam útok hlásit a na jaké pracovní orgány se obrátit

Zdroj: vlastní výzkum

Obrázek „Nahlášení kybernetického útoku“ je zpracován z odpovědí na otázku č. 30

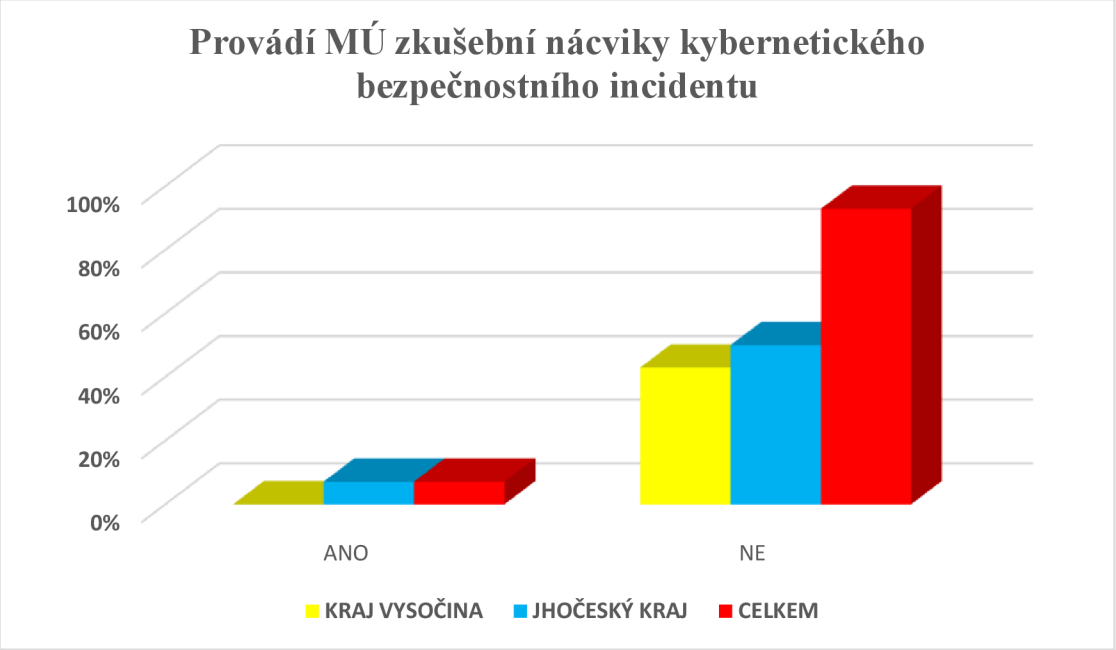
z dotazníku. Přes 85 % dotázaných odborníků zná postup nahlášení kybernetického útoku na příslušné orgány zabývající se kybernetickou bezpečností.



Obrázek 16 Dostatečné proškolení u personálu MÚ v oblasti kybernetických útoků

Zdroj: vlastní výzkum

Obrázek „Dostatečné proškolení personálu MÚ“ je zpracován z odpovědí na otázku č. 40 z dotazníku. K dostatečnému proškolení personálu MÚ dochází dle grafu u 71 % dotazovaných.



Obrázek 17 Dochází ke zkušebním nácvikům kybernetického bezpečnostního incidentu

Zdroj: vlastní výzkum

Obrázek „Provádí MÚ zkušební nácviky kybernetického bezpečnostního incidentu“ je zpracován z odpovědí na otázku č. 41 z dotazníku. Přes 92 % dotázaných neprovádí na svém MÚ zkušební nácviky kybernetického bezpečnostního incidentu.

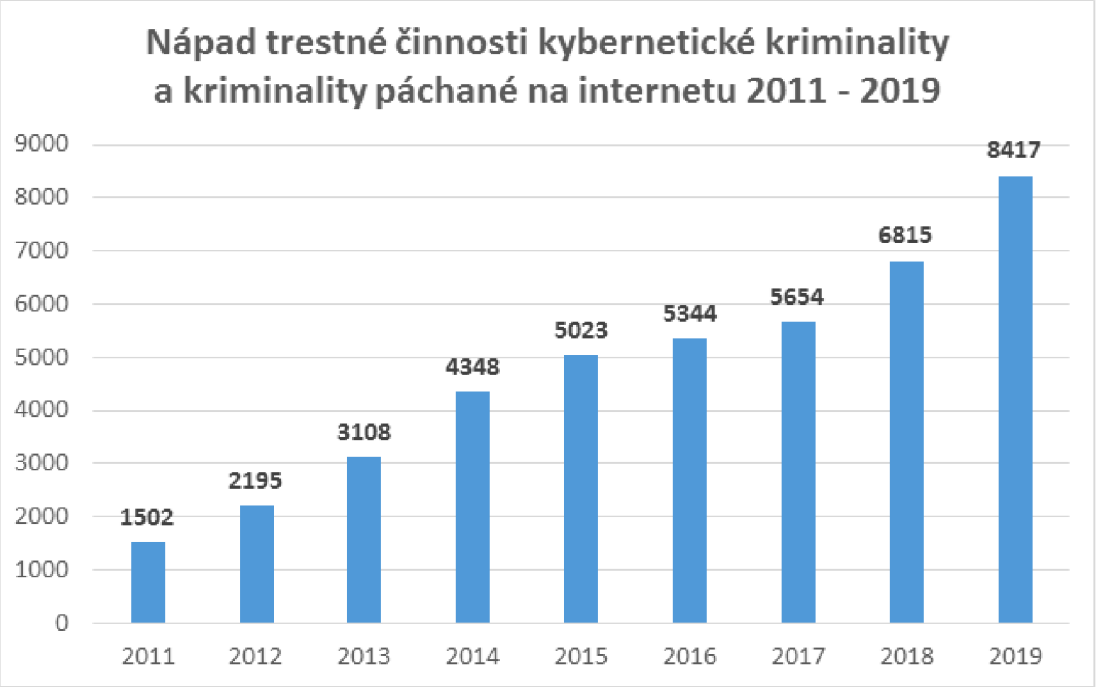
5.3 Analýzy trendů

Analýza trendů je metoda zabývající se vývojovou předpovědí v budoucnosti. Tento proces k charakteristice využívá matematické funkce. Ty se zahrnují do grafu, kde je viditelný vývoj trendu v minulosti a současnosti. Tímto způsobem lze předpovědět teoretický vývoj zkoumaného jevu v budoucnosti. Aby analýza správně fungovala v budoucnu, musí dojít k předpokladu, neměnnosti podmínek, které ovlivňují vývoj. Základem je určení dvou pramenů, které budou porovnány (Machula, 2016). V případě této práce se jedná o čas a počet útoků provedených v tomto čase.

Obrázek 18 Kybernetické útoky v průběhu let ve vybraných ORP

Zdroj: vlastní zpracování

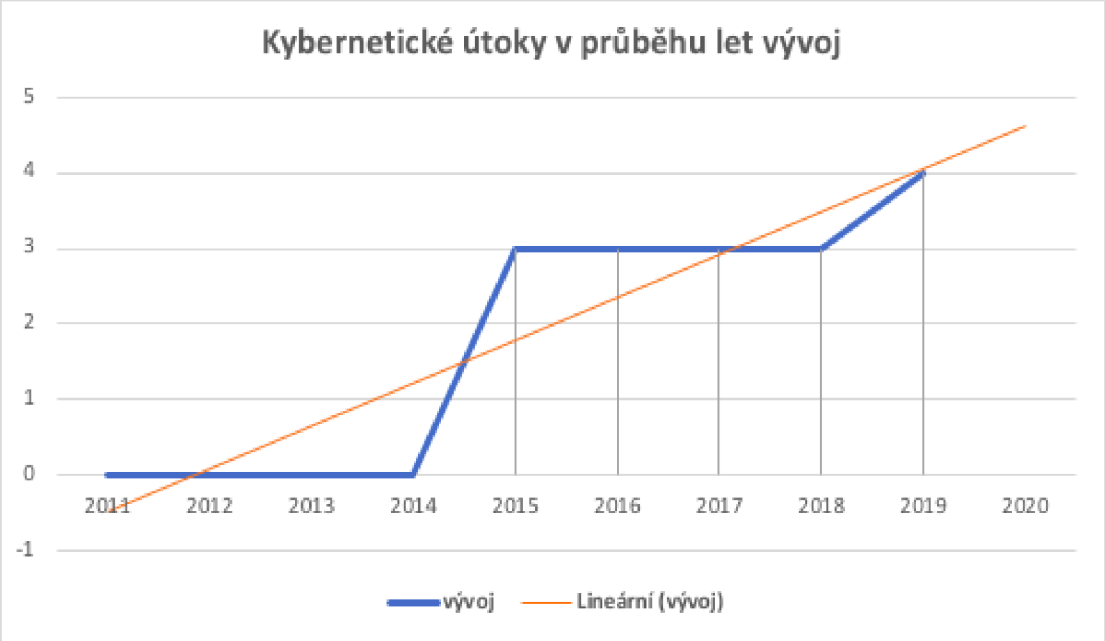
Na obrázku 18 je viditelný nárůst kybernetických útoků na vybrané ORP v průběhu let. Toto tvrzení potvrzují i odpovědi odborníků na kybernetickou bezpečnost, kteří se ve většině shodují v nárůstu kybernetických útoků a jejich postupnému zvyšování v průběhu let viz obrázek 9.



Obrázek 19 Nápad trestné činnosti kybernetické kriminality a kriminality páchané na internetu 2011–2019

Zdroj: Policie ČR

K porovnání s obrázkem 18 poslouží obrázek 19, který vypracovala Policie České republiky. Na obrázku 19 je zachycen ve sloupcovém grafu vývoj kybernetické kriminality v České republice mezi lety 2011-2019. Je zde vidět opět nárůst kybernetických incidentů v čase.



Obrázek 20 Kybernetické útoky v průběhu let vývoj

Zdroj: vlastní zpracování

Na obrázku 20 byla vytvořena matematická funkce pro znázornění prognostického tvrzení. K vývoji kybernetických útoků v průběhu let, byla vybrána funkce lineární (zaměřuje se na konstantní tempo nárůstu) označená oranžově. Vývoj poukazuje na možný nárůstu kybernetických útoků v budoucnosti.

5.4 Analýza megatrendů

Analýza megatrendů je metodou zabývající se vývojovou tendencí, která svým vlivem působení dokáže ovlivnit oblasti společnosti a zároveň tedy působí, jako „megatrend“. Na počátku zkoumání je důležité vymezit časové období a prostor, kterého se bude zkoumání týkat. Poté se určí seznam trendů. V tomto směru hraje největší roli představivost prognostika, který studiem odborných článků získává potřebné informace (Machula, 2016).

Zkoumanou oblastí jsou určené obce s rozšířenou působností a vliv na jejich MÚ. V tabulce jsou uvedeny odbory, kterých by se kybernetický incident mohl týkat a ovlivnit jejich další práci.

Tabulka 8 – Analýza megatrendů – dopady kybernetických útoků

ODBOR	KÚ má vliv na odbor	Popis pod číslem
Dopravy	ANO	1.
Finanční	ANO	2.
Interních auditů	ANO	3.
Kancelář starosty	ANO	4.
Rozvoje	ANO	5.
Sociálních věcí	ANO	6.
Správy majetku města	ANO	7.
Školství	ANO	8.
Vnitřní správy	ANO	9.
Výstavby a úz. plánov.	ANO	10.
Živnostenský a správní	ANO	11.
Životního prostředí	ANO	12.

Zdroj: vlastní zpracování

Popis tabulky:

1. Omezení provozu: oddělení registrace vozidel, evidence řidičů, silničního hospodářství; 2. omezení provozu: oddělení místních poplatků, účetnictví a rozpočtu; 3. omezení provozu: oddělení interních auditů aj. 4. omezení provozu: oddělení organizační, přestupků, obrany a krizového řízení, cestovního ruchu, právní; 5. omezení provozu: oddělení investic, regionálního rozvoje a památkové péče; 6. omezení provozu: oddělení sociálních služeb a sociálně-právní ochrany dětí; 7. omezení provozu: oddělení správy majetku; 8. omezení provozu: oddělení služeb pro školy a školství; 9. omezení provozu: oddělení provozní, personální, informatiky a výpočetní techniky; 10. omezení provozu: oddělení stavebního, územního řízení a územního plánování; 11. omezení provozu: oddělení matriky, živnostenské a správních činností (občasné průkazy aj.); 12. omezení

provozu: ochrany prostředí, vodního a lesního hospodářství... aj. (zařazení různých oddělení v úřadu se může lišit). Všechna vypsaná oddělení navazují na práci zaměstnanců MÚ. Práce zaměstnanců navazuje na širokou veřejnost. Tudíž dochází k vyvození velkého množství megatrendů, protože omezení provozu městského úřadu má obrovský vliv na širokou veřejnost.

5.5 Kolo budoucnosti

Prognostická metoda: kolo budoucnosti představuje podnětnou, levnou a jednoduchou metodu, která slouží k vyvození důsledků událostí a vývoje trendu v budoucnu. Schéma vzniká pomocí strukturovaného grafu. Jedná se o druh organizování myšlenek a důležité je pokládání otázek, které se zabývají budoucností. Kvůli těmto skutečnostem je kolo budoucnosti označováno jako jedna z metod Brainstormingu.

Jako první krok je důležité stanovit zkoumanou událost, která se zapíše do středu. Poté následuje pokládání otázek typu: „Jestliže se tato událost stane, co bude dále následovat?“ aj. Tyto důsledky jsou zapisovány postupně okolo a tvoří primární důsledky zkoumané události. Myšlenkové pochody se uzavírají do menších oválů a kruhů. Vztah vytvořený mezi příčinnou a následkem naznačují dále čáry, která spojují dva kruhy. Ve chvíli, kdy jsou určeny důsledky primárního charakteru, jsou použity původní otázky, zaměřující se nyní na vytvoření sekundárních důsledků (Machula, 2016).

Kolo budoucnosti 1, vyobrazené na obrázku 21 řeší důsledky nedostatečného zpracování dokumentů, řešení a koordinace KBI (viz příloha B).

Kolo budoucnosti 2, vyobrazené na obrázku 22 řeší následky kybernetických útoků při nepravidelném cvičení na bezpečnostní incident (viz příloha C).

Obě kola budoucnosti jsou sestaveny pomocí odpovědí od odborníků na kybernetickou bezpečnost a dále pak z odborné literatury a legislativy.

5.6 Statistické šetření

Pro vyhodnocení dat získaných při zkoumání bude sloužit aritmetický průměr. Stanovená hodnota pro potvrzení hypotézy je stanovena na 80 % kladných odpovědí. Pokud se jedná o kybernetickou bezpečnost, nesmí docházet k nepřipravenosti nebo chybám (Kladivo, 2013).

Oblast 1 vyhodnocení otázek č. 6, 12, 13, 18, 29, 30 a 35.

Oblast 2 vyhodnocení otázek č. 23, 40 a 41 .

Využit je vzorec pro určení aritmetického průměru, který lze vyjádřit například takto:

$$\frac{X}{Y} = Z \qquad (2)$$

přičemž:

X je počet odpovědí na určené otázky,

Y je počet otázek,

Z je výsledná aritmetická hodnota.

5.6.1 Statistické šetření oblast 1

Typ odpovědi „NE“: negativní participace odborníka.

Typ odpovědi „ANO“: pozitivní participace odborníka.

Typ odpovědi „NEVÍM“: nulová participace odborníka.

Aritmetický průměr „NE“:

$$\frac{ne5+ne10+ne5+ne6+ne1+ne1+ne7}{7} =$$

$$\frac{35,7\%+71,45\%+35,7\%+43\%+7,15\%+7,15\%+50\%}{7} = 36\ \%$$

Aritmetický průměr „ANO“:

$$\frac{ano\ 9+ano3+ano9+ano8+ano12+ano12+ne7}{7} =$$

$$\frac{64,3\%+21,4\%+64,3\%+57\%+85,7\%+85,7\%+50\%}{7} = 61\%$$

Aritmetický průměr „NEVÍM“ –

$$\frac{nevím1+nevím1+nevím1}{7} =$$

$$\frac{7,15\%+7,15\%+7,15\%}{7} = 3\ \%$$

Statistické šetření v oblasti jedna, charakterizuje připravenost, řešení a koordinaci na kybernetické útoky ve vybraných územně samosprávných celcích. Nejvíce označovaná byla odpověď „ANO“, procentuálně se jednalo o 61 %. Druhou nejvíce označovanou odpovědí bylo „NE“, procentuálně se jednalo o 36 %. Nezájem odborníků kybernetické bezpečnosti o tuto problematiku činil 3 %. Procentuální hodnocení odpovědi „ANO“ bylo přes polovinu, ale zároveň nesplnilo předem daný limit na potvrzení hypotézy, který byl určen 80 % hranicí pozitivních odpovědí.

5.6.2 Statistické šetření oblast 2

Typ odpovědi „NE“: negativní participace odborníka.

Typ odpovědi „ANO“: pozitivní participace odborníka.

Aritmetický průměr „NE“ –

$$\frac{ne2+ne4+ne13}{3} = \frac{14,3\%+28,6\%+92,9\%}{3} = 45\ \%$$

Aritmetický průměr „ANO“ –

$$\frac{ano\ 12+ano10+ano1}{3} = \frac{85,7\%+71,4\%+7,1\%}{3} = 55\ \%$$

Statistické šetření v oblasti dvě, charakterizuje pravidelné vzdělávání a cvičení vybraných územně samosprávných celků. Nejvíce označovaná byla odpověď „ANO“, procentuálně se jednalo o 55 %. Druhou označovanou odpovědí bylo „NE“, procentuálně se jednalo o 45 %. Procentuální hodnocení odpovědi „ANO“ bylo přes polovinu, ale zároveň nesplnilo předem daný limit na potvrzení hypotézy, který byl určen 80% hranicí pozitivních odpovědí.

6 Diskuze

Cílem diplomové práce bylo analyzovat nejzávažnější kybernetické útoky za posledních 10 let ve vybraných územně samosprávných celcích a provést prognózu možného vývoje kybernetického terorismu dle zjištěné analýzy. Ověřované hypotézy:

1. Vybraný územní samosprávný celek má dostatečně zpracované dokumenty, řešení a koordinaci kybernetických bezpečnostních incidentů.

2. Pravidelně se vzdělává a cvičí proti kybernetickému terorismu.

V diskuzi této diplomové práce jsou interpretovány zjištěné poznatky a skutečnosti, které se týkají kybernetické bezpečnosti vybraných ORP. Získaná data jsou shrnuta a dále porovnána, aby došlo k naplnění cíle a potvrzení či vyvrácení daných hypotéz.

Pomocí vedených rozhovorů s odborníky na kybernetickou bezpečnost a dále po doplnění odpovědí na předem vypracované otázky do polostrukturovaného dotazníku, byly získány informace a data, která jsou zde využita. K získání dat a informací bylo osloveno celkem 32 ORP z Jihočeského kraje a kraje Vysočina. V Jihočeském kraji nakonec rozhovor s dodatečným zápisem poskytlo 8 odborníků (viz tabulka 2). Návratnost v Jihočeském kraji byla tedy 47 %. V kraji Vysočina nakonec rozhovor s dodatečným zápisem poskytlo 6 odborníků (viz tabulka 3). Návratnost v kraji Vysočina byla tedy 40 %. Celkové získání dat z obou krajů tvořilo 44 %.

Cílem práce není porovnávání krajů navzájem. Je nutné podotknout, že složitost komunikace a rozsah 43 připravených otázek byla velmi náročná. Je pochopitelné, že neměli všichni odborníci na kybernetickou bezpečnost dostatek času, aby se výzkumu účastnili. S některými nešlo komunikaci vůbec navázat, jiní uvedli omluvu, do e-mailové konverzace. Nejčastěji uváděli nedostatek času, onemocnění v souvislosti s pandemií Covid-19 či nedostatečné působení na daném ORP v příslušné pozici. Vyhodnocení proběhlo porovnáním odpovědí na předem připravené otázky a dále statistickým šetřením, kde byla předem určena hodnota pro potvrzení hypotézy. Statistické šetření proběhlo pomocí aritmetického výpočtu.

První hypotéza se týká dostatečného zpracování dokumentů, řešení a koordinace kybernetických bezpečnostních incidentů. Na vyhodnocení této hypotézy se podílí nejvíce otázky č. 6, 12, 13, 15, 16, 18, 29, 30 a 35. U otázky č. 6 bylo překvapivé zjištění,

že přes 64 % dotázaných ORP, má vytvořené oddělení zabývající se pouze informačními technologiemi a kybernetickou bezpečností. Obce s rozšířenou působností, které nemají vytvořené oddělení zabývající se pouze kybernetickou bezpečností jsou ve většině rozlohou menší, ale do budoucna o vytvoření oddělení budou diskutovat. Zarážejícím zjištěním byla skutečnost (vyplývající z odpovědí na otázku č. 12), kdy 78,6 % dotázaných ORP nemá ve svém krizovém plánu zanesené krizové opatření týkající se kybernetické bezpečnosti/kritické informační infrastruktury. Myslím si, že toto zjištění je velmi znepokojující a do budoucna by bylo vhodné takové opatření začlenit do krizového plánu. Pouze 64,3 % odborníků se podílí na tvorbě směrnic, předpisů, metodických pokynů aj. (otázka č. 13 a 13a. – obrázek 5 a 6), které se týkají kybernetické bezpečnosti. Ministerstvo vnitra České republiky vydalo v roce 2018 metodické doporučení k činnosti územních samosprávných celků. Je zde zapsán proces tvorby a vydávání obecně závazných vyhlášek obcí. Tento dokument je velmi dobře zpracován a může fungovat jako návod při tvorbě těchto dokumentů a zodpovězení nejčastějších otázek týkající se této tématiky. Podlé mého názoru odborník, který se podílí na tvorbě těchto dokumentů je později i velmi dobře připraven na vzniklé komplikace tykající se kybernetické bezpečnosti a je schopen na ně adekvátně zareagovat. V obcích, které se účastnily výzkumu došlo celkově za posledních 10 let k 16 větším kybernetickým útokům (otázka č. 15, 16 – obrázek 7). Vždy byly tyto útoky zapříčiněny vyděračským softwarem ransomware, který kyberzločinci považují za velmi oblíbený. Tento software byl využit i při napadení největšího amerického provozovatele ropných potrubí od společnosti Colonial Pipeline (viz kapitola 1.7.2). Tento typ útoku tudíž dokáže zapříčinit velké ztráty a komplikace i v nadnárodních společnostech. Přes polovinu dotázaných odborníků uvedlo (otázka č. 18 – obrázek 8), že má jejich ORP zpracovanou analýzu rizik týkající se kybernetické bezpečnosti. Myslím si, že pokud chce obec s rozšířenou působností kvalitně a dostatečně bojovat proti kybernetické bezpečnosti, měla by být analýza rizik na toto téma zpracována. Analýza dokáže upozornit například na silné a slabé stránky, hrozby a příležitosti (Wikipedie, 2021). Velmi pozitivní zjištění vzniklo z odpovědí na otázky č. 29, 30 (obrázek 14 a 15). Přes tři čtvrtě dotázaných ví, jak postupovat při probíhajícím kybernetickém útoku a kam tento útok nahlásit. Podle NÚKIB je podstatnou a nedílnou součástí ICT prostředí, aby byl vytvořen dostatečný monitoring, který dokáže správně detekovat nadstandartní chování. Pokud dojde k potvrzení probíhajícího útoku, je důležité neprodleně kontaktovat bezpečnostní tým CERT a poskytovatele internetu. K nahlášení bezpečnostního incidentu slouží elektronický formulář (viz příloha B), vše

probíhá dle vyhlášky č. 82/2018 Sb. Nejnovější inovace a trendy v oboru kybernetické bezpečnosti (otázka č. 35) sleduje více jak polovina dotázaných odborníků. Z prostudované odborné literatury jasně vyplývá, že trendy a inovace v oboru KB se velice rychle vyvíjí. Je proto důležité, aby se odborníci o tuto část problematiky zajímali (NÚKIB, 2021; vyhláška č. 82/2018 Sb.; Ministerstvo vnitra, 2018; Kolouch et al., 2019; Wikipedie SWOT, 2021).

Výpočet pro potvrzení či vyvrácení hypotézy 1 je uveden v podkapitole 5.6.1 zapsané jako: statistické šetření v oblasti jedna a charakterizuje připravenost, řešení a koordinaci na kybernetické útoky ve vybraných územně samosprávných celcích. Nejvíce označovaná byla odpověď „ANO“, procentuálně se jednalo o 61 %. Druhou nejvíce označovanou odpovědí bylo „NE“, procentuálně se jednalo o 36 %. Nezájem odborníků kybernetické bezpečnosti o tuto problematiku činil 3 %. Hranice pro potvrzení hypotézy 1 byla předem určena na 80 % kladných odpovědí.

Z výše uvedené diskuze vyplývá, že hypotéza 1: Vybraný územní samosprávný celek má dostatečně zpracované dokumenty, řešení a koordinaci kybernetických bezpečnostních incidentů, bohužel není potvrzena. Pokud se jedná o kybernetickou bezpečnost, která dokáže ovlivnit mnoho aspektů života spousty lidí, mělo by být nasazení ze stran odborníků vždy 100 %. Je nutné zmínit, že některé ORP jsou dobře připravené na kybernetický útok, zdaleka se to však netýká všech. Jedná-li se o data a informace u kterých může dojít k odcizení a dále například prodeji těchto informací na „černém trhu“, musíme počítat s velkou zodpovědností a mělo by se tak k této problematice přistupovat. Na toto téma bylo vytvořeno kolo budoucnosti 1, kde jsou vidět některé z primárních a sekundárních následků KBI.

Druhá hypotéza se týká pravidelného vzdělávání a cvičení proti kybernetickému terorismu. Na vyhodnocení této hypotézy se nejvíce podílí otázky č. 7, 8, 9, 23, 24, 40 a 41. Vzdělání odborníků na kybernetickou bezpečnost (otázka č.7 – obrázek 2) je středoškolské nebo vysokoškolské. U dotázaných ORP přesně 50 % odborníků má vysokoškolské vzdělání z toho jeden přímo v oboru IT a zbylých 50 % má středoškolské vzdělání. Odpovědi na otázku č.8 a 9 (obrázek 3 a 4) dokazují, že vzdělávání preferují všichni odborníci pravidelné pomocí odborných knih, článků, časopisů, ale také odborných seminářů, které pořádají kvalifikované subjekty. Nepravidelné školení v zaměstnání patří také mezi velmi oblíbené, nejčastěji navazuje na vzniklé situace a

potřeby zaměstnanců a zaměstnavatele. Dle Národního úřadu pro kybernetickou bezpečnost (déle jen NÚKIB), by mělo docházet k pravidelnému školení vždy z kvalitních odborných zdrojů. Přímo NÚKIB nabízí kvalifikované kurzy, kterých mohou využívat i odborníci na kybernetickou bezpečnost (e-learningy pro úředníky veřejné správy). Otázka č. 23 (obrázek 12) mapovala zřízení a využívání intranetu ve zkoumaných obcích s rozšířenou působností. Přes tři čtvrtě dotázaných má zřízen intranet a plně ho využívá ke komunikaci, informovanosti, aj. Překvapivým zjištěním pro mě byly výsledky na otázku č. 24 (obrázek 13). Ve všech zkoumaných ORP mají zaměstnanci MÚ možnost se přihlásit z pracovních elektronických zařízení na veřejnou síť. Dle Doucka et al. je velmi nebezpečné již samotné „surfování" na internetu, které je zde podpořené ještě pracovními zařízeními, které jsou připojeny na interní síť MÚ. Z mého pohledu lze oprávnění v tomto směru udělit pouze zodpovědným osobám, které se prokáží jako dostatečně vzdělané v oblastmi kybernetické bezpečnosti. Pokud nejsou zaměstnanci v tomto ohledu dostatečně informování, mohlo by dojít k nežádoucím účinkům a v krajním případě i vzniku kybernetického bezpečnostního incidentu. Odborníci na kybernetickou bezpečnost se ze 71 % domnívají, že dochází k dostatečnému proškolení personálu MÚ v jejich příslušné ORP (otázka č. 40 – obrázek 16). Domnívám se, že toto tvrzení je povzbudivým výsledkem. Naopak velmi negativní zjištění nastává u otázky č. 41 (obrázek 17). Zde 92,9 % dotázaných odborníků odpovědělo, že neprovádí zkušební nácviky kybernetického bezpečnostního incidentu. Pokud dochází k nácviku jakékoliv činnosti, prohlubují se zkušenosti s možnými postupy, možnostmi, následky, aj. Je velmi důležité se alespoň pokusit předejít problémům vzniklých v souvislosti s kybernetickým bezpečnostním incidentem. Pouze vzdělávání v tomto oboru nestačí. Mělo by docházet i k praktickým nácvikům, které se pokouší postupně odstranit nedokonalosti při postupu řešení kybernetického útoku (NÚKIB, 2021; Doucek et al., 2019).

Výpočet pro potvrzení či vyvrácení hypotézy 2 je uveden v podkapitole 5.6.2, zapsané jako: statistické šetření v oblasti dvě a charakterizuje pravidelné vzdělávání a cvičení vybraných územně samosprávných celků. Nejvíce označovaná byla odpověď „ANO", procentuálně se jednalo o 55 %. Druhou označovanou odpovědí bylo „NE", procentuálně se jednalo o 45 %. Hranice pro potvrzení hypotézy 2 byla předem určena na hodnotu 80% kladných odpovědí.

Z výše uvedené diskuze vyplývá, že hypotéza 2: Pravidelně se vzdělává a cvičí proti kybernetickému terorismu, není potvrzena. Pokud se jedná pouze o pravidelné

vzdělávání, jsou obce s rozšířenou působností na velmi dobré cestě. Odborníci na kybernetickou bezpečnost se pravidelně vzdělávají a snaží se o to i u ostatních zaměstnanců MÚ. K tomu jsou jim nápomocné odborné semináře, knihy, časopisy, aj. Bohužel však převážná většina obcí s rozšířenou působností neprovozuje zkušební nácviky proti kybernetickému bezpečnostnímu incidentu. Domnívám se, že pokud nedochází k pravidelnému nácviku proti kybernetickému útoku, snižuje se šance na správný a pohotový potup při reálně probíhajícím kybernetickém bezpečnostním incidentu. Na téma nedostatečného nácviku proti kybernetickému terorismu je vytvořeno kolo budoucnosti 2, kde jsou vidět opět primární a sekundární následky.

Cílem diplomové práce bylo analyzovat nejzávažnější kybernetické útoky za posledních 10 let ve vybraných územně samosprávných celcích a provést prognózu možného vývoje kybernetického terorismu dle zjištěné analýzy. K zmapování kybernetických útoků byl vytvořen obrázek 7, 18 a 20. Na obrázku 7 jsou znázorněné počty závažných kybernetických útoků vedených proti vybraným ORP v průběhu 10 let. Na obrázku 18 jsou tyto útoky zaznamenány pomocí grafu do časové osy. Je na něm viditelný nárůst kybernetických útoků ve vybraných ORP v průběhu 10 let. Na obrázku 20 byla vytvořena matematická funkce pro znázornění prognostického tvrzení k vývoji kybernetických útoků. K matematickému znázornění byla vybrána funkce lineární, která se zaměřuje na konstantní tento nárůstu.

Na konec diskuze je vhodné zhodnocení faktu, že i když je vynaložena velká snaha k porozumění zadaného tématu a sestavení otázek, které jsou po zodpovězení zdrojem užitečných a jedinečných dat, nemůžeme předpokládat vývoj ostatních na to navazujících skutečností. V průběhu zpracovávání této diplomové práce došlo k nečekaným komplikacím a omezením ze strany vývoje pandemie Covid-19. Bylo nutné se vždy přizpůsobit dané situaci a vynaložit veškeré úsilí, aby zkoumané téma bylo kvalitně zpracováno. V praxi bylo viditelné, že pokud nejsou rozhovory vedeny osobně, je velmi náročné je provést a zaznamenat. I přes všechny komplikace, provedený výzkum v této diplomové práci nabízí velmi zajímavé poznatky.

7 Závěr

Diplomová práce se zaměřuje na koordinaci a řešení kybernetických útoků ve vybraných územně samosprávných celcích. K dosažení určeného cíle vedly rozhovory (na předem připravené otázky, následně zapsané do polostrukturovaného dotazníku) s odborníky na kybernetickou bezpečnost z vybraných obcí s rozšířenou působností a prostudování odborných materiálů.

První hypotéza: Vybraný územní samosprávný celek má dostatečně zpracované dokumenty, řešení a koordinaci kybernetických bezpečnostních incidentů. Odpověď: Hypotéza první nebyla potvrzena. K vyvrácení první hypotézy vedla data ze získaných odpovědí od vybraných odborníků na kybernetickou bezpečnost, výpočet aritmetického průměru s předem danou hodnotou úspěšného výsledku a porovnání s odbornými články a literaturou.

Druhá hypotéza: Pravidelně se vzdělává a cvičí proti kybernetickému terorismu. Odpověď: Hypotéza druhá nebyla potvrzena. K vyvrácení druhé hypotézy rovněž vedla data získaná z odpovědí od vybraných odborníků na kybernetickou bezpečnost, výpočet aritmetického průměru s předem danou hodnotou úspěšného výsledku a poté porovnání s odbornou literaturou a články.

Pomocí výše provedeného zkoumání došlo k analyzování nejzávažnějších kybernetických útoků za posledních 10 let ve vybraných územně samosprávných celcích a dále byla provedena prognóza možného vývoje kybernetického terorismu. Cíl práce byl tedy naplněn. Vybrané ORP z Jihočeského kraje a Kraje Vysočina se snaží postupně vzdělávat a zkoumat danou problematiku kybernetického terorismu.

Tato diplomová práce se snaží přinést zajímavý a originální pohled na problematiku kybernetických útoků, které jsou vedeny proti územně samosprávným celkům. Velká většina prací vytvořená na téma kybernetické bezpečnosti se spíše zabývá kybernetickou problematikou v celé Evropě. Práce může být dále například využita jako materiál k samostudiu pro obce s rozšířenou působností. Zpracovaná diplomová práce slouží pouze jako základní soupis kybernetického problému, který by měl být dále podrobněji prozkoumán.

8 Seznam použité literatury

1. AMOROSO, E. *Cyber Security*. USA: Silicon Pr, 2006. ISBN: 0929306384.
2. ANDRESS, Jason. *The Basics of Information Security*. 2nd Edition. Syngress, 2014. ISBN: 9780128007440.
3. BARTLETT, Jamie. *The dark net: inside the digital underworld*. Brooklyn: Melville House, 2016. ISBN 978-1-61219-521-6.
4. BAGGILI, I. *Digital Forensics and Cyber Crime*. New York: Springer, 2011. ISBN 978-3-642-19513-6.
5. Definition of cybersecurity in English by Oxford Dictionaries. *Oxford Dictionaries* [online]. Oxford University Press, 2018 [cit. 25. 12. 2020]. Dostupné z: https://en.oxforddictionaries.com/definition/cybersecurity
6. DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 9788088260394.
7. DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.
8. ENISA, *European Union Agency for Cybersecurity*, © 2005-2021. [online], European Union [cit. 2020-06-02]. Dostupné z: https://www.enisa.europa.eu.
9. EU, 2016a. Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6.července 2016o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32016L1148.
10. FISCHER, E. A. *Creating a national Framework for cybersecurity: An analysis of issues and options*. New York: Nova Science Publishers, 2009. ISBN: 1604565594.
11. FLEISCHMANOVÁ, Veronika. *Kybernetická bezpečnost*. Praha, 2015. Diplomová práce. Vysoká škola ekonomická v Praze, Fakulta mezinárodních vztahů. Vedoucí práce Radka Havlová. Dostupné z: https://www.vse.cz/vskp/id/12
12. GÁLA, Libor, Zuzana ŠEDIVÁ, Jan POUR. Podniková informatika: Počítačové aplikace v podnikové a mezipodnikové praxi. 3. vydání. Praha: Grada, 2015. ISBN 978-80-247-9918-6.
13. GAVORA, Peter. *Úvod do pedagogického výzkumu*. 2., rozš. České vyd. Přeložil Vladimír JŮVA, přeložil Vendula HLAVATÁ. Brno: Paido, 2010. ISBN 978-80-7315-185-0.

14. HSU, D. Frank a D. MARINUCCI (eds.). *Advances in cyber security: technology, operations and experiences*. New York: Fordham University Press, 2013. ISBN 978-0-8232-4456-0.
15. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.
16. JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. ISBN 978-80-247-1561-2.
17. KLADIVO, Petr. *Základy statistiky*. Olomouc: Univerzita Palackého v Olomouci, 2013. ISBN 978-80-244-3841-2.
18. KNÝ, M.; J. POŽÁR. Aktuální pojetí a tendence bezpečnostního managementu a informační bezpečnosti. 1. vyd. Brno: Tribun EU, 2010. ISBN 978-8073399-067-1.
19. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 9788088168317.
20. KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.
21. KOPECKÝ, K.; V. KREJČÍ. *Rizika virtuální komunikace*. 1 vyd. Olomouc: NET University, 2010. ISBN: 978-80-254-7866.
22. Kyberkriminalita – Policie České republiky. *Úvodní strana – Policie České republiky* [online]. © 2021 Policie ČR, všechna práva vyhrazena [cit. 2021-06-06]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx.
23. Kyberútok na nemocnici v Benešově: nefungují žádné přístroje! – Centrum kybernetické bezpečnosti – Oficiální stránky Centra Kybernetické bezpečnosti v Praze [online], 2019. [cit. 2021-05-04]. Dostupné z: https://www.irozhlas.cz/zpravy-svet/colonial-pipeline-usa-hacker-preprava-ropa-benzin-kyberutok_2105081143_dok.
24. LIDINSKÝ, Vít; ŠVARCOVÁ, Ivana; BUDIŠ, Petr; LOEBL, Zbyněk; PROCHÁZKOVÁ, Barbora. *eGovernment bezpečně*. Praha: Grada Publishing, 2008, ISBN 978-80-247-2462-1.
25. MACHULA, Jan. Bezpečnostní vývoj států Evropské unie [online]. Zlín, 2016 [cit. 2020-06-09]. Diplomová práce. Univerzita Tomáše Bati ve Zlíně, fakulta aplikované informatiky. Vedoucí práce: Ing. Jan Valouch, Ph.D. Dostupné z:

https://digilib.k.utb.cz/bitstream/handle/10563/38295/machula_2016_dp.pdf?sequence=1.

26. MAISNER, Martin. *Zákon o kybernetické bezpečnosti: komentář*. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-817-8.
27. McQUADE, S. Encyclopedia of Cybercrime. Westport: Greenwood Press, 2009. ISBN: 978-0313-33974-5.
28. Ministerstvo vnitra České republiky. Metodické doporučení k činnosti územních samosprávných celků. Praha, 2018. ISBN 978-80-87544-86-0.
29. Národní úřad pro kybernetickou a informační bezpečnost – Hlášení incidentů. Národní úřad pro kybernetickou a informační bezpečnost – Úvodní stránka, © 2021. [online]. [cit. 2021-06-05] Dostupné z: https://www.nukib.cz/cs/kontakty/hlaseni-incidentu/.
30. Národní úřad pro kybernetickou a informační bezpečnost – Strategie / Akční plán. *Národní úřad pro kybernetickou a informační bezpečnost – Úvodní stránka*, © 2020. [online]. [cit. 2020-05-05] Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/.
31. Národní úřad pro kybernetickou a informační bezpečnost – Vzdělávání. *Národní úřad pro kybernetickou a informační bezpečnost – Úvodní stránka*, © 2021. [online]. [cit. 2021-05-06] Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/vzdělávání/.
32. Největšího provozovatele na přepravu ropných produktů v USA napadli hackeři. Přerušil činnost. iROZHLAS – spolehlivé zprávy. [online], 2021. [cit. 2021-05-03]. Dostupné z: https://www.irozhlas.cz/zpravy-svet/colonial-pipeline-usa-hacker-preprava-ropa-benzin-kyberutok_2105081143_dok.
33. Olomoucký magistrát čelí několik týdnů hackerským útokům. Odmítá zaplatit výkupné. iROZHLAS – spolehlivé zprávy [online], 2021. [cit. 2021-05-03]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/olomouc-magistrat-hackersky-utok-hackeri-ransomware-avaddon_2105221133_ako.
34. POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-86898-38-5.
35. REED, Chris. *EU internet law in the digital era*. 2004. Cham: Springer, [2020]. ISBN 978-3-030-25578-7.

36. REVERON, D. *Cyberspace and national security: Threats, opportunities and power in a virtual world.* Washington, DC: Georgetown University Press, 2012. ISBN: 9781589019188.
37. Riigi Teataja, © 2010. *Cybersecurity Act* [online]. Riigikantselei. [cit. 2020-07-01]. Dostupné z https://www.riigiteataja.ee/en/eli/523052018003/consolide.
38. SHACKELFORD, S. J.; S. RUSSEL; A. KUEHN. *Chicago Journal of International Law* Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors, 2016. ISSN: 1529-0816.
39. SHOEMAKER, D.; A. CONKLIN. *Cybersecurity: The Essential Body Of Knowledge.* USA: Cengage Learning, 2011. ISBN: 1435481690.
40. SCHNEIER, Bruce. *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*. New York: Copernicus, 2003. ISBN 978-0-387-02620-6.
41. SINGER, P. W. et Allan FRIEDMAN. *Cybersecurity: What everyone Needs to Know*. New York: Oxford University Press, 2013. ISBN 0199918112.
42. SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.
43. SWOT – Wikipedie. © 2021. *SWOT* [online]. [cit. 2021-03-05]. Dostupné z: https://cs.wikipedia.org/wiki/SWOT
44. ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.
45. The United States Army's 2010. *Cyberspace Operations: Concept Capability Plan 2016-2028* [online]. ARMY USA, s. 8-9 [cit. 2021-01-10]. Dostupné z: https://fas.org/irp/doddir/army/pam525-7-8.pdf.
46. VALÁŠEK, Jarmil a František KOVÁŘÍK. *Krizové řízení při nevojenských krizových situacích: účelová publikace pro krizové řízení*. Praha: Ministerstvo vnitra - generální ředitelství Hasičského záchranného sboru ČR, 2008. ISBN 978-80-86640-93-8.
47. *Traffic Light Protocol* (TLP) Definitions ana Usage. [online]. [cit. 25.4.2021]. Dostupné z: https://www.us-cert.gov/tlp.
48. WAISOVÁ, Šárka. *Bezpečnost: vývoj a proměny konceptu*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Politologické učebnice. ISBN 80-86898-2-10.
49. WALL, D. S. *Cybercrime: The transformation of crime in the information age*. Cambridge: Polity, 2007. ISBN: 978-0-745-62735-9.

50. YANNAKOGEORGOS, P.A. et Adam LOWTHER. *Conflict and cooperation in cyberspace the challenge to national security.* Boca Raton: Taylor Francis, 2013. ISBN: 9781466592025.
51. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), 2018. In: Sbírka zákonů Česká republiky, částka 43.
52. Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, 2014. In: Sbírka zákonů České republiky, částka 127.
53. Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby, 2017. In: Sbírka zákonů České republiky, částka 157.
54. Zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, 2020. In: Sbírka zákonů České republiky, částka 5.
55. Zákon č. 110/2019 Sb., o zpracování osobních údajů, 2019. In: Sbírka zákonů České republiky, částka 47.
56. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), 2014. In: *Sbírka zákonů České republiky,* částka 75.
57. Zákon č. 240 ze dne 28. června 2000 o krizovém řízení a o změně některých zákonů (krizový zákon), 2000. In: Sbírka zákonů České republiky, částka 73.
58. Zákon č. 250/2017 Sb., o elektronické identifikaci, 2017. In: Sbírka zákonů České republiky, částka 89.
59. Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, 2016. In: Sbírka zákonů České republiky, částka 115.
60. Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změněněkterých dalších zákonů, 2000. In: Sbírka zákonů České republiky, částka 99.
61. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, 2005. In: Sbírka zákonů České republiky, částka 143.
62. Zákon č. 413/2005 Sb., o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti, 2005. In: Sbírka zákonů České republiky, částka 143.

9 Seznam obrázků

10 Seznam tabulek

11 Seznam vzorců

12 Seznam příloh

Příloha A Polostrukturovaný dotazník

Příloha B Obrázek 21 Kolo budoucnosti 1 Nedostatečně zpracované dokumenty, řešení a koordinace KBI

Příloha C Obrázek 22 Následky kybernetických útoků (při nepravidelném cvičení na bezpečnostní incident)

Příloha D Formulář pro hlášení KBI

Příloha A: Polostrukturovaný dotazník

Vážený odborníku MÚ na kybernetickou bezpečnost,

jmenuji se Tereza Pragerová a jsem studentkou Jihočeské univerzity v Českých Budějovicích v navazujícím magisterském oboru Civilní nouzové připravenosti.

Obracím se na Vás s prosbou o vyplnění polostrukturovaného dotazníku, který poslouží pro zpracování mé diplomové práce na téma – Současnost a budoucnost kybernetické bezpečnosti vybraného územního samosprávného celku. Vše po předchozí domluvě. Cílem mé diplomové práce je zkoumání a zhodnocení kybernetické bezpečnosti obcí s rozšířenou působností. Svůj dotazník jsem rozdělila pro větší přehlednost do třech částí (identifikační část, krizové řízení obce s rozšířenou působností a osvětu/prevenci).

Pokud byste si našel/a alespoň chvilku Vašeho času na vyplnění mého dotazníku, byla bych Vám velmi vděčná. Dotazník je anonymní.

Poprosila bych Vás o zodpovězení níže uvedených otázek, doplněním do dokumentu word, který je součástí tohoto e-mailu. Odpovědi stačí zvýraznit například tučným písmem – **a) ANO**. V doplňovacích otázkách je předem určené místo na odpověď, kam ji napíšete. Je možné i daný dotazník z wordu vytisknout, ručně ho vyplnit a zpětně mi ho naskenovat do e-mailu nebo si ho mohu osobně vyzvednout.

Mnohokrát Vám děkuji za spolupráci a ochotu.

Část 1. Identifikační část pracovníka MÚ zodpovídajícího za kybernetickou bezpečnost.

1. **V jaké obci s rozšířenou působností pracujete?**
   ……..
2. **Jak dlouho pracujete na MÚ Vaší ORP?**
   a) Méně než 1 rok
   b) 1-3 roky
   c) 3-5 let
   d) 5-10 let
   e) 10–20 let
   f) 20 a více let
3. **Jak dlouho pracujete na pozici zabývající se kybernetickou bezpečností (popř. IT)?**

a) Méně než 1 rok
b) 1-3 roky
c) 3-5 let
d) 5-10 let
e) 10–20 let
f) 20 a více let

4. **Působíte současně i jako odborník v jiných oblastech krizového řízení Vašeho ORP? (Možno více odpovědí.)**
   - Krizové řízení
   - Ochrana obyvatelstva
   - Obranné plánování
   - Finance
   - Hospodářská opatření pro krizové stavy
   - Informace a jejich utajení
   - Služby
   - Bezpečnost práce
   - Válečné hrozby
   - Jiné ……..

5. **Kolik pracovníků se podílí na tvorbě a udržení kybernetické bezpečnosti ve Vaší ORP?**

a) 1-2
b) 3-4
c) 4 a více

6. **Máte vytvořené oddělení zabývající se pouze informačními technologiemi a kybernetickou bezpečností? (Pokud NE, odpovězte prosím na otázku 6a.)**

a) ANO
b) NE

6a. Pokud nemá Váš městský úřad vytvořené oddělení informačních technologií nebo kybernetické bezpečnosti, přemýšlí o jeho vytvoření?

a) ANO
b) NE
c) NEVÍM

7. **Jaké máte vzdělání?**
   - Středoškolské vzdělání
   - Vyšší odborné vzdělání (dosažení titul Dis.)
   - Vysokoškolské vzdělání (dosažený titul Bc.) – studium se přímo netýkalo KB/IT

- Vysokoškolské vzdělání (dosažený titul Bc.) – studium se přímo týkalo KB/IT
- Vysokoškolské vzdělání (dosažený titul Mgr/Ing.) – studium se přímo netýkalo KB/IT
- Vysokoškolské vzdělání (dosažený titul Mgr/Ing.) - studium se přímo týkalo KB/IT
- Vysokoškolské vzdělání (dosažený titul Ph.D.)

8. **Jakým způsobem se vzděláváte ve svém oboru? (možno více odpovědí)**
   - Samostatně (knihy, odborné články, odborné časopisy,…)
   - Odborné semináře pořádané kvalifikovanými subjekty.
   - Nepravidelné školení v zaměstnání.
   - Pravidelné školení v zaměstnání.
   - Studoval/a jsem/ Studuji vysokou školu se zaměřením na krizové řízení / ochranu obyvatelstva / IT / KB.
9. **Jak často se ve svém oboru vzděláváte?**
   - Pravidelně.
   - Jednou měsíčně.
   - Jednou za tři měsíce.
   - Jednou za půl roku.
   - Jednou ročně.
10. **Jste kontaktní osoba pro komunikaci s vládním CERT týmem?**
    a) ANO
    b) NE

Část 2. - Obec s rozšířenou působností a její krizové řízení týkající se kybernetické bezpečnosti.

11. **Má Váš městský úřad zřízené krizové řízení? (Pokud ANO, jakého odboru je součástí.)**
    a) ANO ……
    b) NE
12. **Obsahuje krizový plán Vaší ORP opatření týkající se kybernetické bezpečnosti/kritické informační infrastruktury?**
    a) ANO
    b) NE
13. **Podílíte se na tvorbě směrnic, předpisů, metodických pokynů aj. týkajících se kybernetické bezpečnosti ve Vaší ORP? (Pokud odpovíte ANO, odpovězte prosím na otázku 13a., 13b.)**
    a) ANO

b) NE

13a. Jak často je potřeba tyto dokumenty aktualizovat?

……

13b. Kdo tyto dokumenty schvaluje a zodpovídá za ně?

……

14. S jakými prvky kritické infrastruktury podle Vás nejvíce souvisí kritická informační infrastruktura ?

……

……

……

……

15. Kolik kybernetických útoků bylo vedeno v posledních 10 letech proti Vaší ORP/MÚ?

……..

16. Jaký z těchto útoků byl nejzávažnější a kdy se odehrál?

……

……

17. Vedete si statistiku kybernetických útoků v průběhu let?

a) ANO

b) NE

18. Máte jako MÚ vytvořenou analýzu rizik týkající se kybernetické bezpečnosti?

a) ANO

b) NE

19. Jak se vyvíjí trend kybernetických útoků podle Vás?

……

20. Jakým typem kybernetického útoku je nejvíce Váš městský úřad ohrožen? (Můžete vybrat více možností.)

- Kinetický zásah
- DoS/DDoS
- Sociální inženýrství
- Škodlivý malware
- Kombinace výše uvedených

21. Co si myslíte, že je hlavní motivací útočníka při kybernetickém útoku? (Můžete vybrat více možností.)

- Materiální obohacení
- Terorismus
- Špionáž
- Hacktivismus
- Konkurenční boj
- Vnitřní hrozba – selhání zaměstnance
- Konflikt se státním či nestátním aktérem

22. Jaký typ informací si myslíte, že chtějí útočníci nejvíce získat?

……

23. Máte jako MÚ svůj intranet?

a) ANO

b) NE

24. Mají zaměstnanci Vašeho MÚ možnost se přihlásit z pracovních elektronických zařízení na veřejnou síť (např. Google, Seznam, aj.)?

a) ANO

b) NE

Část 3. – Osvěta a prevence týkající se kybernetické bezpečnosti.

25. Sledujete, jak se vyvíjí kybernetické útoky? (Pokud odpovíte ANO, odpovězte prosím na otázku 25a.)

a) ANO

b) NE

25a. Mohl/a byste popsat, co Vás nejvíce zaujalo v tomto vývoji?

……..

……..

26. Zaregistroval/a jste v poslední době na území České republiky nějaký kybernetický útok na veřejnou správu?

……

……...

27. Jak byste poznal/a, že na Vašem MÚ probíhá kybernetický útok?

……

……

28. Jak byste poznal/a, že na Vašem MÚ proběhl kybernetický útok?

……

……

29. Víte, jak postupovat při probíhajícím kybernetickém útoku?

……

……

30. Víte, kam kybernetický útok hlásit / na jaké orgány se obrátit?

……

……

31. Víte, jaký je rozdíl mezi vládním CERT týmem (GovCERT.cz) a národním CERT týmem (CSIRT.CZ)?

……

……

32. Víte, podle jakého čísla vyhlášky se incident kybernetické povahy nahlašuje?

……

33. Jaké následky mohou podle Vás nastat bezprostředně po krizové situaci způsobené kybernetickým útokem?

……

……

34. Je podle Vás na obor kybernetické bezpečnosti vynaložen dostatek financí?

a) ANO

b) NE

35. Sledujete nejnovější inovace a trendy v oboru kybernetické bezpečnosti? (Pokud odpovíte Ano, odpovězte prosím na otázku 35a.)

a) ANO

b) NE

35a. Jak se tyto inovace a trendy snažíte zařadit do kybernetické bezpečnosti na Vašem MÚ?

……

……

……

36. Jak jste spokojen/a se současným digitalizováním veřejné správy?

……

37. Který z informačních systémů vzniklých díky digitalizaci veřejné správy plní svůj úkol nejlépe a proč?

……

……

38. **Myslíte si, že lidé umí efektivně využívat nové informační systémy veřejné správy, a proč?**
    a) ANO - ……
    b) NE - ……
39. **Myslíte si, že dochází k dostatečné osvětě, co se týče kybernetické bezpečnosti ve veřejné správě, týkající se obyvatel České republiky?**
    a) ANO
    b) NE
40. **Dochází podle Vás k dostatečnému proškolení u personálu MÚ v oblasti kybernetických útoků?**
    a) ANO
    b) NE
41. **Jak často k tomuto proškolení dochází a kdo ho provádí?**

……

……

……

42. **Provádíte zkušební nácviky kybernetického bezpečnostního incidentu? (Pokud odpovíte ANO, odpovězte prosím na otázku 42a., 42b.,42c.)**
    a) ANO
    b) NE

    42a. Jak často tyto nácviky provádíte?

    ……

    42b. Vyhodnocujete tyto nácviky? Popřípadě jakým způsobem?

    ……..

    ……..

    42c. Zapracováváte zjištěné poznatky do nových aktualizací dokumentů?

    a) ANO
    b) NE
43. **Co si myslíte o Národní strategii kybernetické bezpečnosti ČR 2021-2025?**

    ……

    ……

    ……

Mnohokrát děkuji za Váš čas a spolupráci.

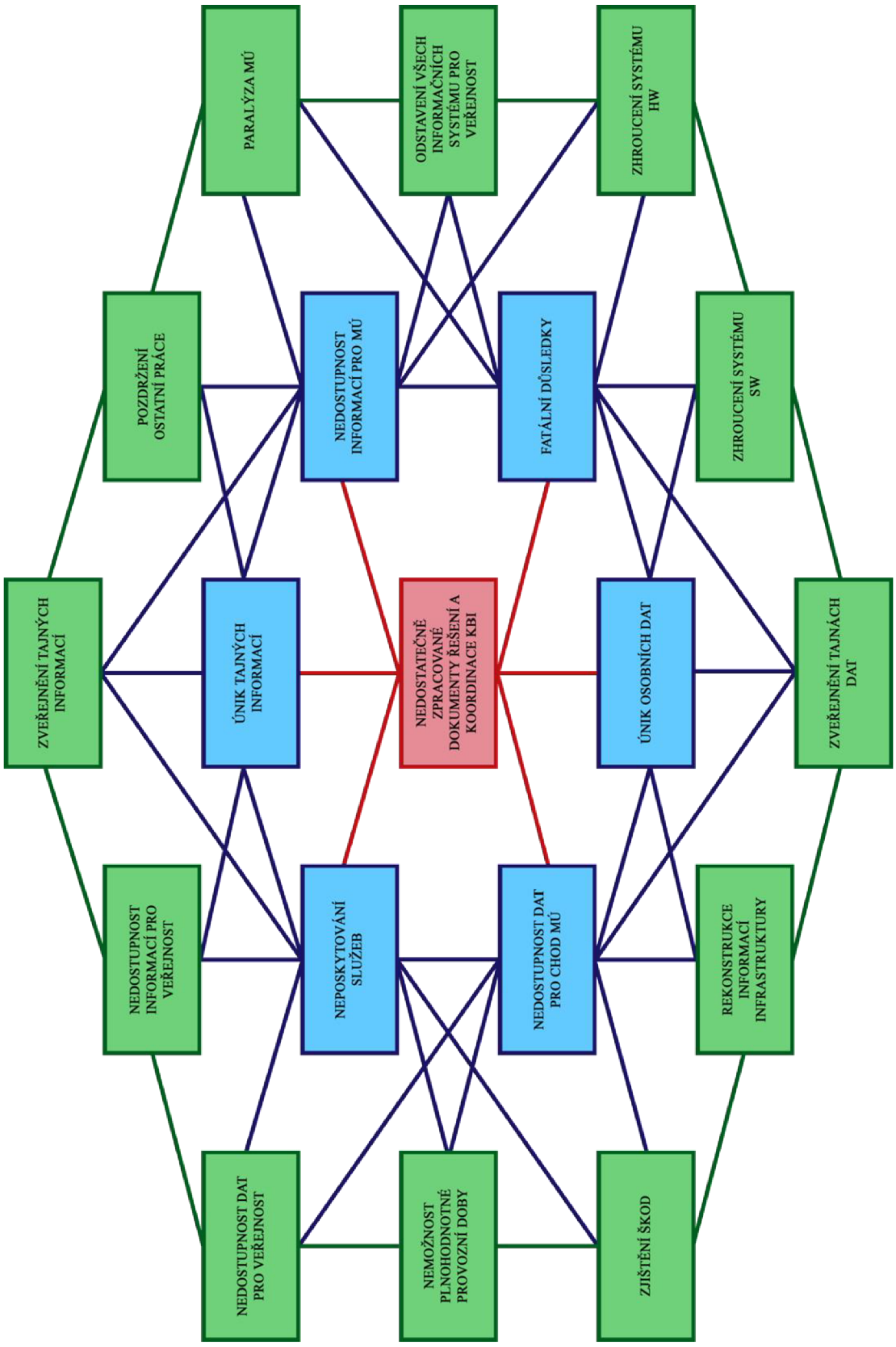
Použité zkratky:

MÚ – městský úřad

KB – kybernetická bezpečnost

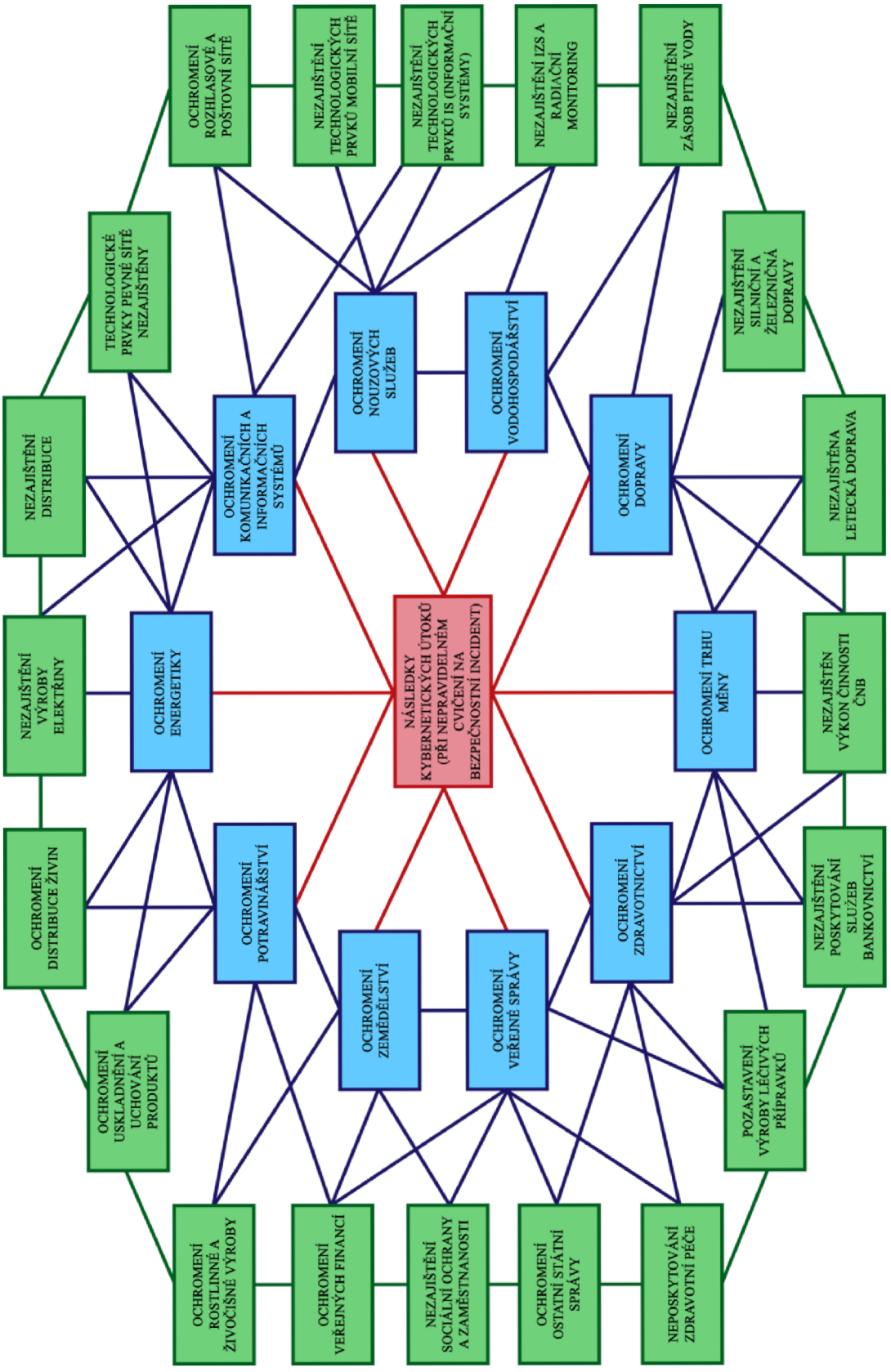
ČR – Česká republika

Příloha B: Obrázek 21 Kolo budoucnosti 1 Nedostatečně zpracované dokumenty, řešení a koordinace KBI



Zdroj: vlastní výzkum

Příloha C: Obrázek 22 Následky kybernetických útoků (při nepravidelném cvičení na bezpečnostní incident)



Zdroj: vlastní výzkum

Příloha D: Formulář pro hlášení KBI

Formulář hlášení kybernetického bezpečnostního incidentu

Míra ochrany informace *: Neomezeno (veřejné)

Kontaktní údaje

Orgán a osoba uvedená v § 3 písm. c) a e) zákona *:

Identifikátor ****:

E-mail *:

Telefon *:

Pokračování *: Iniciační oznámení CERT/CSIRT týmu **ID **:**

Detaily kybernetického bezpečnostního incidentu / kybernetické bezpečnostní události

Jedná se o hlášení: INCIDENTU

Datum a čas zjištění *: **YYYY MM DD hh : mm** **Časová zóna*:** **+- hh**

Datum a čas výskytu incidentu: **YYYY MM DD hh : mm** Časová zóna: **+- hh**

Kategorie incidentu *: Kategorie I – méně závažný kybernetický bezpečnostní incident

Typ incidentu *:

Kybernetický bezpečnostní incident způsobený kybernetickým útokem nebo jinou událostí vedoucí k p

Upřesnění podle standardu ENISA/eCSIRT.net - "Incident Classification" ***:

- Abusive Content (např. spam, kyberšikana, nevhodný obsah)
- Malicious Code (např. virus, červ, trojský kůň, dialer, spyware)
- Information Gathering (např. skenování, sniffing, sociální inženýrství)
- Intrusion Attempts (např. zneužití zranitelnosti, kompromitace aktiva, "0-day" útok)
- Intrusions (např. kompromitace aplikace nebo uživatelského účtu)
- Availability (např. narušení dostupnosti způsobené DoS/DDoS útokem nebo sabotáží)
- Information Security (např. neautorizovaný přístup nebo neautorizovaná změna informace, ...)
- Fraud (např. neoprávněné využití ICT - porušení licenčních práv, krádež identity aj.)
- ostatní

Současný stav zvládání kybernetického bezpečnostního incidentu *:

Probíhá analýza a šetření kybernetického incidentu

Počet zasažených systémů (odhad) *:

Odhad počtu dotčených uživatelů *:

1/2

Zdroj: NÚKIB

Popis incidentu *:

Rozsah škod:

Jaká opatření již byla přijata?:

Systémové detaily - cíl útoku (kompromitovaný systém)

Host nebo IP *:

Funkce hosta *:

Port:

Protokol:

OS / jiný systém + verze:

Umístění systému v architektuře:

Systémové detaily - zdroj útoku (je-li znám)

Host / IP nebo jiné (zařízení/uživatel):

Port:

Protokol:

** Povinné pole*
*** Povinné pole v případě, že je vybrána volba "Pokračování dříve oznámeného incidentu", jedná se o ID dříve oznámeného incidentu / události, na které chcete navázat nové hlášení*
**** zdroj: http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html*
***** Identifikátor zadávejte jen tehdy, pokud Vám byl sdělen ze strany GovCERTu (jde o jednoznačný identifikátor orgánu nebo osoby)*

UPOZORNĚNÍ:
Právo změny dokumentu vyhrazeno.
Orgány a osoby podle § 3 zákona o kybernetické bezpečnosti, písm. b) (orgány nebo osoby zajišťující významnou síť) hlásí kybernetické bezpečnostní incidenty národnímu CERT týmu (NIC.CZ) prostřednictvím formuláře, zveřejněného na: www.csirt.cz/stateincidentreport

2/2

Zdroj: NÚKIB

13 Seznam zkratek

AES – Advanced Encryption Standard

aj. – a jiné

APT – Advanced Persistent Threat

CAPTCHA – completely automated public Turing test to tell computers and hum. Apart

CaaS – Crym as a Service

CERT – Computer Emergency Response Team

CIA – Confidentiality, Intedrity, Availability

CSIRT –Computer Security Incident Response Team

ČR – Česká republika

DDoS – Distributed Denial of Service

DNS – Domain Name System

eIDAS – Electronic Identification and Services

ENISA – European Union Network and Information Security Agency

EU – Evropská unie

EV – Extended Validation

FTP – File Transfer Protol

GB – gigabyte

GDPR – General Data Protection Regulation

HDD – Hard Disk Drive

HW – hardware

IDS – Intrusion Detection Systém

IP – ingress protection

IT – informační technologie

kB – kilobyte

KB – kybernetická bezpečnost

KII – kybernetická informační infrastruktura

KÚ – kybernetický útok

LAN – Local Area Network

MÚ – městský úřad

Např. – například

NAS – Network Attached Storage

NATO – North Atlantic Treaty Organization

NBÚ – Národní bezpečnostní úřad

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

ORP – obec s rozšířenou působností

OSN – Organizace spojených národů

PDS – poskytovatele digitálních služeb

Př. – příklad

PZS – provozovatelé základních služeb

RKB – rada pro kybernetickou bezpečnost

SAN – Storage area network

SSD – Solid-state drive

SW – software

TCP – Transmission Control Protocol

TLP – Traffic Light Protocol

USA – United States of America

VBA – virtual private network

VoIP – Voice over Internet Protocol