Kriminalita jako jedna z významných bezpečnostních hrozeb

Aleš Králík

Bakalářská práce

2023

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva

Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Aleš Králík**
Osobní číslo:	**L20080**
Studijní program:	**B1032A020002 Ochrana obyvatelstva**
Forma studia:	**Kombinovaná**
Téma práce:	**Kriminalita jako jedna z významných bezpečnostních hrozeb**

Zásady pro vypracování

1. Zpracujte rešerši s důrazem na monografie, stati, studie a články, jakož i koncepčně analytické dokumenty orgánů státní správy.
2. Charakterizujte bezpečnostní hrozby v České republice.
3. Pojednejte o bezpečnostních hrozbách v kyberprostoru a porovnejte s obdobím před pandemií a v průběhu pandemie Covid-19.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. EICHLER, Jan. *Evropská bezpečnost 30 let po skončení studené války*. Praha:Oeconomica, nakladatelství VŠE, 2019, 269 s. ISBN 9788024522968.
2. JUŘÍČEK, Ludvík a Petr ROŽŇÁK. *Bezpečnost, hrozby a rizika v 21. století*. Ostrava: Key Publishing, 2014, 323 s. Monografie. ISBN 9788074182013.
3. SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, 934 s. ISBN 9788073807207.

Další odborná literatura podle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **doc. RSDr. Václav Lošek, CSc.**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **1. prosince 2022**
Termín odevzdání bakalářské práce: **5. května 2023**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2022

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 5.5.2023

Jméno a příjmení studenta: Aleš Králík

.....
podpis studenta

ABSTRAKT

Bakalářská práce je zaměřena na charakteristiku bezpečnostních hrozeb, kterým je na základě analýz věnována pozornost ve strategických a koncepčních dokumentech České republiky, a následuje část věnovaná kybernetické kriminalitě.

V teoretické části jsou definovány základní pojmy bezpečnosti, charakterizovány bezpečnostní hrozby a druhy kriminality na základě analýz. Praktická část je zaměřena na statistickou analýzu kybernetické kriminality páchané za období let 2019-2022. Na základě vlastních poznatků, odborné literatury a statistik za užití SWOT analýza a případové studie jsou zpracovány doporučení na zlepšení ochrany a zajištění bezpečnostního prostředí proti kriminalitě páchané v kybernetickém prostoru.

Klíčová slova: bezpečnost, hrozba, kriminalita, kybernetická kriminalita, riziko, bezpečnostní strategie, bezpečnostní hrozby

ABSTRACT

The bachelor thesis focuses on the characteristics of security threats, which, on the basis of analyses, are given attention in strategic and conceptual documents of the Czech Republic, followed by a section devoted to cybercrime.

The theoretical part defines the basic concepts of security, characterizes security threats and types of crime based on analyses. The practical part is focused on statistical analysis of cybercrime committed in the period 2019-2022. Based on own knowledge, literature and statistics using SWOT analysis and case studies, recommendations are developed to improve the protection and security environment against cybercrime.

Keywords: security, threat, crime, cybercrime, risk, security strategy, security threats

Velmi rád bych poděkoval vedoucímu bakalářské práce doc. RSDr. Václavu Loškovi CSc., za velmi vstřícný přístup, odborné vedení a věnovaný čas při zpracování mé bakalářské práce.

Velké díky bych chtěl také vyjádřit mé rodině, a to zejména manželce a mým dětem, kteří mě podporovali po celou dobu mého studia.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

„Vzdělání je pasem do budoucnosti, protože zítřek patří těm, kteří se na něj dnes připravují.“

Malcolm X.

OBSAH

ÚVOD

Bezpečnostní prostředí prochází v současné době dynamickými změnami a je ovlivňováno hrozbami, které se v závislosti na čase vyvíjí a mění nebo se objevují hrozby nové. Stát na tyto změny musí reagovat. Bezpečnostní prostředí je hlavním faktorem, které ovlivňuje bezpečnost. Hlavním úkolem státu je ochrana lidských životů, zdraví, majetku a životního prostředí. Bezpečnost se obecně odkazuje na stav, kdy je něco chráněno před nebezpečím, hrozbou nebo rizikem. To se může týkat jednotlivců, skupin, společnosti, ale i státu, a je zajišťována prostřednictvím bezpečnostních opatření nebo prostřednictvím bezpečnostní politiky. Hlavními dokumenty bezpečnostní politiky jsou Bezpečnostní strategie České republiky a další navazující strategické a koncepční dokumenty. Součástí těchto dokumentů jsou analýzy bezpečnostních hrozeb, které umožňují identifikovat rizika a přijímat opatření k minimalizaci jejich dopadů. Hrozby mohou být vnějšího či vnitřního charakteru, a mohou zahrnovat hrozby přírodního původu, hrozby vyvolané člověkem, ale také hrozby zahraničního, sociálního, ekonomického či politického původu. Bezpečnostní prostředí se může lišit podle geografického umístění nebo politického a sociálního kontextu, ve kterém se nachází. Například bezpečnostní prostředí v oblastech, kde dochází k ozbrojeným konfliktům, nebo kde je terorismus a kriminalita na vysoké úrovní, bude bezpečnostní prostředí více ohrožené, než v oblastech s nízkou kriminalitou a stabilní politickou situací. Vliv na bezpečnostní prostředí můžou mít i globální problémy, jakými jsou změny klimatu, pandemie nebo migrace, jež mají mezinárodní přesah. Je tedy důležité neustále monitorovat a analyzovat bezpečnostní prostředí a na základě identifikovaných hrozeb přijímat vhodná opatření k ochraně bezpečnosti osob, majetku a státu.

Bakalářská práce na téma Kriminalita jako jedna z bezpečnostních hrozeb na území České republiky je zaměřena na charakteristiku jednotlivých hrozeb podle strategických dokumentů a následuje část věnovaná kybernetické bezpečnosti a s ní spjatými hrozbami, jelikož v době trvající pandemie Covid-19 došlo k výraznému otevření se virtuálního světa veřejnosti, což mělo za následek značný nárůst kriminality páchané v kybernetickém prostoru. Vzhledem k dynamicky rostoucímu a měnícímu se prostředí kybernetické kriminality, která v sobě uchovává velké množství hrozeb, je potřeba se na problematiku zaměřit. V teoretické části jsou prezentovány základní legislativní a strategické dokumenty, na které navazuje vymezení pojmu bezpečnostního prostředí.

Praktická část bakalářské práce je věnována vyhodnocení statistických ukazatelů kybernetické kriminality v období let 2019-2022, kdy se jedná o období významně ovlivněné

pandemií Covid-19. Součástí praktické části je SWOT analýza kybernetické bezpečnosti vypracovaná na základě poznatků zjištěných při studiu materiálů dané problematiky.

V závěru praktické části je uvedena případová studie kybernetického útoku, který využil DDoS útok k napadení struktury informačního systému školského zařízení. Cílem práce je na základě aktuálních dokumentů, statistik a analýz vyhodnotit, jakým způsobem jsou hrozby páchané v kybernetické prostoru zásadní a pro obyvatelstvo, stát a jím chráněné zájmy nebezpečné. Ze zjištěných skutečností a jejich vyhodnocení bude závěr věnován případným návrhům opatření ke zlepšení bezpečnostní situace. Ke zpracování bakalářské práce byla užita statistická analýza na základě sběru dat a informací a metoda komparace, která byla využita při definování bezpečnostních hrozeb na základě strategických dokumentů.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ TERMINOLOGIE

Česká republika „*je svrchovaný, jednotný a demokratický právní stát založený na úctě k právům a svobodám člověka a občana.“* (Česko, 1993)

Bezpečnost vnímáme jako nejdůležitější hodnotu společnosti, přičemž je velmi složité ji popsat či měřit. Jedná se o pojem, který je skloňován téměř každý den, a vychází z celosvětového dění, které sebou přináší množství hrozících útoků či hrozeb naturogenního či antropogenního původu. Obecně znamená stav, kdy neexistují hrozby, které by byly rizikem pro referenční objekt, a tyto rizika jsou eliminována. (Lošek, 2013)

Bezpečnost je definována jako stav, *„kdy je systém schopen odolávat známým a předvídatelným vnějším i vnějším hrozbám, které mohou negativně působit proti jednotlivým prvkům, tak aby byla zachována jeho struktura, stabilita a spolehlivost.“* (Česko, 2016)

Hrozba je jev objektivního charakteru. Hrozbou může být projev, gesto nebo čin působící se záměrem někomu uškodit. Podle terminologického slovníku MV je hrozba definována jako *„přírodní nebo člověkem podmíněný proces představující potenciál, tj. schopnost zdroje hrozby být aktivován a způsobit škodu. Tento potenciál může být spuštěn záměrně nebo náhodně využit pro atakování specifických zranitelností aktiva. Hrozba bývá zdrojem rizika.“* (Česko, 2016)

Hrozby můžeme dělit a kategorizovat podle různých hledisek, a to hledisko geopolitické, časové, sektorové a hledisko podle původce hrozby. (Juříček, 2014)

Stav nebezpečí *„se jako bezodkladné opatření může vyhlásit, jsou-li ohroženy životy, zdraví, majetek, životní prostředí, pokud nedosahuje intenzita ohrožení značného rozsahu, a není možné odvrátit ohrožení běžnou činností správních úřadů, orgánů kraje a obcí, složek integrovaného záchranného systému nebo subjektů kritické infrastruktury.“* (Česko, 2000)

Riziko se vždy odvozuje od konkrétní hrozby, která může nastat. Míru rizika lze posoudit analýzou rizik vycházející z připravenosti těmto hrozbám čelit. Riziko nám tedy vystihuje určitou pravděpodobnost, že dojde k události, jež způsobí škody neboli výsledek míry dané hrozby, jejíž následek je negativní vůči danému objektu. Riziko vychází pokaždé z nějaké hrozby. Pod pojmem rizika můžeme také chápat situaci, kdy s největší pravděpodobností nastane událost, která se výrazně odlišuje od toho, co si přejeme. (Smolík, Šmíd, 2010)

Kriminalita může být vnímána jako jednání, které trestní právo posuzuje jako trestné činy. Jedná se o synonymum ke slovu zločinnost. Kriminalitu máme dvojího druhu. Registrovaná, což je kriminalita zjištěná a kriminalita latentní, což je protiprávní jednání, které nikdy nebo málokdy je evidováno.

Informační kriminalita je definována jako trestná činnost, ve vztahu k softwaru, k datům, uloženým informacím, a jedná se o aktivity, které vedou k neautorizovanému čtení, nakládaní, vymazaní, zneužití, změně nebo jinému nakládání s daty. (MV ČR, 2016)

Bezpečnostní politika státu je soubor opatření a postupů, které mají chránit národní zájmy a bezpečnost státu před různými hrozbami a výzvami, včetně vojenských hrozeb, terorismu, kybernetických útoků, ekonomických nebezpečí, migrace a dalších. Cílem bezpečnostní politiky je minimalizovat rizika a zajistit stabilitu, bezpečnost a prosperitu země. (MV ČR, 2023)

Terminologický slovník obsahuje specializované termíny a jejich definice v určitém oboru. Jeho hlavním účelem je poskytnout uživatelům přesnou a konzistentní terminologii pro konkrétní obor, aby bylo možné komunikovat mezi odborníky a zabezpečit porozumění mezi nimi.

2 PRÁVO BEZPEČNOSTI

Právní normy bezpečnosti ČR jsou souborem právních předpisů, které stanovují způsoby ochrany obyvatel a majetku. Jde o složitý soubor právních předpisů a opatření, které slouží k zajištění bezpečnosti obyvatelstva a ochrany zájmů státu.[1] Cílem je zajistit bezpečnost obyvatel a majetku v souladu se zákony a mezinárodními dohodami, kterých je ČR signatářem. Cílem je také zachování lidských práv, svobod a ochrana demokratického právního řádu.

Zabývá se oblastmi a zejména právem krizového řízení a civilní obrany, ochrany kritické infrastruktury a dalšími. Hlavním zákonem v oblasti bezpečnosti je ústavní zákon č. 110/1998 Sb. o bezpečnosti České republiky a balíček krizových zákonů.[2] Vedle ústavních zákonů má ČR také strategické dokumenty.[3]

Bezpečnostní strategii ČR 2015 na jejímž zpracování se společně podílelo Ministerstvo zahraničních věcí společně s kanceláří prezidenta České republiky a parlamentem.[4]

Bezpečnostní strategie *„představuje přístupy, nástroje a opatření k zajištění bezpečnosti, obrany a ochrany občanů státu.“* (MZV ČR, 2015)

Jedná se o strategický dokument, který vytváří rámec pro zabezpečení a ochranu národních zájmů ČR v oblasti bezpečnosti. Zaměřuje se na ochranu veřejného pořádku a bezpečnost občanů, včetně boje proti terorismu, extremismu a organizovanému zločinu. V případě kybernetické bezpečnosti se zabývá ochranou informačních systémů, sítí a dat před kybernetickými útoky a zneužitím. Řeší otázky týkající se dodávek energií a zajištění energetické soběstačnosti. (MZV ČR, 2015)

Obraná strategie byla 13. března 2017 aktualizována. Strategii vypracovalo Ministerstvo obrany České republiky a nahrazuje Vojenskou strategii z roku 2008.

Hlavním cílem obranné strategie je zajištění bezpečnosti a obrany území ČR a ochrana jejich obyvatel. Definuje způsoby, jakými se bude ČR bránit proti vnějším hrozbám. Věnuje se

[1] Ústavní zákon č. 1/1993 Sb. Ústava České republiky, ústavní zákon č. 2/1993 Sb. Základní listina práv a svobod.
[2] Zákon č. 239/2000 Sb., o IZS, zákon č. 240/2000 Sb. O Krizovém řízení, zákon č. 241/2000 Sb., o HOPKS, zákon č. 219/1999 Sb., o ozbrojených silách a zákon č. 222/1999 Sb. O Zajišťování obrany
[3] V současné době prochází legislativa v oblasti vnitřní bezpečnosti novelizačním procesem, kde v roce 2023 by měla projít revizí legislativa krizového řízení a měla by být zveřejněna nová Bezpečnostní strategie a obranná strategie.
[4] První bezpečnostní strategie byla přijata vládou v roce 1999, následovaly aktualizace v letech 2001, 2003, 2011 a poslední v roce 2015.

rozvoji a modernizaci ozbrojených sil ČR, aby byly schopné účinně plnit své úkoly. Klade důraz na spolupráci s mezinárodními spojenci, jako jsou NATO, OSN nebo EU. Strategie se také věnuje boji proti hybridním hrozbám[5], jako jsou kybernetické útoky, dezinformace a propaganda.

Cíle obranné strategie jsou průběžně aktualizovány v závislosti na vývoji bezpečnostních hrozeb a změnách v mezinárodním prostředí. (MO ČR, 2017)

Audit národní bezpečnosti (dále jen „ANB“) je proces posouzení a hodnocení bezpečnostních opatření a strategií, které jsou aplikovány na národní úrovni. Cílem auditu je identifikovat potenciální hrozby a rizika pro národní bezpečnost a navrhnout opatření, která by měla být přijata k minimalizaci rizik. (Vláda ČR, 2016)

Koncepce ochrany obyvatelstva do roku 2025 s výhledem do roku 2030 byla schválena vládou České republiky dne 21. června 2021. Obecně se zabývá zajištěním bezpečnosti a ochrany obyvatelstva v případě krizových situací, jako jsou například přírodní katastrofy, teroristické útoky, válečné konflikty nebo epidemie. Zaměřuje se na prevenci, přípravu, reakci a obnovu.

Strategie ČR pro boj proti terorismu je součástí celoevropského rámce boje proti terorismu. Strategie zahrnuje prevenci, zvládání a reakci na teroristické útoky. Zaměřuje se na identifikaci a vyšetřování teroristických aktivit, zajištění bezpečnosti KI a posilování schopností záchranných složek.

Národní strategie kybernetické bezpečnosti ČR (dále jen „NSKB“) na období 2021-2025 navazuje na předešlou NSKB. Byla vypracována v souladu s bezpečnostními zájmy, které jsou popsány v Bezpečnostní strategii ČR. Jedná se o dokument, ve kterém jsou uvedeny nástroje, principy a vize, jakými chce stát zajišťovat kybernetickou bezpečnost.

V roce 2022 NKÚ provedl na MV kontrolu zaměřenou na OO a jeho financování. K zajištění úkolů ochrany obyvatelstva přistupuje MV GŘ-HZS ČR prostřednictvím strategických dokumentů, které jasně definují, před jakými hrozbami je nutné obyvatelstvo chránit. Nedávno ČR čelila pandemii Covid-19, tornádu a v současné době výrazně ovlivňuje geopolitické dění Ruská agrese na Ukrajině. Na základě definovaných vnějších ohrožení,

[5] Hybridní hrozby jsou kombinací vojenských a nevojenských prostředků a technik, jako jsou kybernetické útoky, propaganda a dezinformace. Využívají se k dosažení politického, ekonomického nebo strategického cíle.

kterými naše republika může čelit, odpovídá i v ochraně obyvatelstva přístup k zajištění finančních prostředků. (MV GŘ-HZS, 2023)[6]

I přesto, že Česká republika se neřadí k zemím, které jsou řazeny mezi ty, jenž jsou nebo by měly být bezprostředně ohroženy bezpečnostními hrozbami jakéhokoliv charakteru, tak i přesto disponuje náš stát bezpečnostní politikou, ve které je zaneseno mnoho právních a strategických dokumentů, které jsou zpracovávány na základě nejnovějších poznatků a analýz současných a nových hrozeb, které by mohly narušit bezpečnostní prostředí České republiky.

[6] Informace o stavu ochrany obyvatelstva a krizového řízení z pohledu MV viz:https://www.hzscr.cz/clanek/zpravodajstvi-2023-brezen-ochrana-obyvatelstva.aspx .
Tisková zpráva NKÚ k dispozici na: https://www.nku.cz/cz/pro-media/tiskove-zpravy/system-ochrany-obyvatelstva-v-cr-ma-radu-zasadnich-nedostatku--lide-nejsou-dostatecne-informovani--chybeji-masky-i-ukryty-id13084/.

3 BEZPEČNOSTNÍ PROSTŘEDÍ

Bezpečnostní prostředí může být ovlivněno různými faktory, jako jsou přírodní katastrofy, teroristické útoky, kybernetické útoky, nebo kriminální aktivity. Bezpečnostní prostředí se stává stále důležitějším tématem pro společnost a věnuje se mu více pozornosti v podobě studia a vylepšování s cílem snížit riziko a zlepšit bezpečnost.

Bezpečnostní prostředí může být definováno jako prostředí *„ve kterém mohou probíhat jakékoliv bezpečnostní děje a události, tj. děje a události s potenciálním nebo reálným dopadem do bezpečnosti pro zúčastněné objekty či subjekty, se vznikem škod nebo újem.“* (Porada, 2019)

Může být také vnímáno jako prostředí, ve kterém dochází k realizaci a střetu zájmů státu se zájmy států a aktérů mezinárodních vztahů. Bezpečnostní prostředí ČR je tvořeno především okolními státy[7]. Blízké bezpečnostní prostředí zahrnuje evropské státy a bezpečnostní seskupení v rámci EU a NATO. [8]

Vzhledem k rozmanitosti a vývoji společnosti se oblast bezpečnosti rozšířila i do ostatních oblastí. To bylo reflektováno v rámci Kodaňské školy o nové sektory, jako jsou sektor vojenský, společenský, politický, ekonomický a enviromentální. O daném rozšíření se zmiňují Barry Buzan a jeho spolupracovníci v publikaci „Bezpečnost: nový rámec pro analýzu“. (Buzan, 2005)

3.1 Bezpečnost státu

Bezpečnost státu může být zajišťována různými způsoby, včetně politické, hospodářské, vojenské a technologické ochrany. Politická ochrana může zahrnovat udržování stability a míru, zajištění právního řádu a lidských práv. Hospodářská ochrana zahrnuje zabezpečení dostatku potravin, energie a dalších zdrojů. Vojenská ochrana může zahrnovat posilování obrany a zajištění vojenské síly. Technologická ochrana zahrnuje kybernetickou bezpečnost a sledování komunikací.

Je významnou součástí mezinárodní politiky a je často řešena prostřednictvím spolupráce na mezinárodní úrovni. Státy spolupracují na posílení obrany, ochrany zdrojů, boji proti

[7] Slovensko, Polsko, Německo a Rakousko

[8] NATO (North Atlantic Treaty Organization) – Mezinárodní vojenská organizace, založena 4. dubna 1949 podpisem Washingtonské smlouvy 12 státy. „*Smluvní strany se zavazují, jak je uvedeno v Chartě OSN, urovnávat veškeré mezinárodní spory, v nichž mohou být účastny, mírovými prostředky tak, aby nebyl ohrožen mezinárodní mír, bezpečnost a spravedlnost, a zdržet se ve svých mezinárodních vztazích hrozby silou nebo použití síly jakýmkoli způsobem neslučitelným s cíli OSN“* (Washingtonská smlouva, čl. 1, 1949)

terorismu a dalších bezpečnostních otázkách. Mezinárodní organizace (OS, NATO) hrají důležitou roli v řešení globálních bezpečnostních výzev a v poskytování pomoci státům v nouzi.

3.2 Vnější a vnitřní bezpečnost státu

Vnější bezpečnost zahrnuje opatření, která mají za cíl chránit stát před vnějšími hrozbami, které mohou ohrozit bezpečnost státu z vnějšku. [9] Lze ji definovat jako: *„stav kdy jsou na nejnižší možnou míru eliminovány hrozby a rizika ohrožující stát a jeho zájmy z vnějšku a kdy je tento stát k eliminaci hrozeb vybaven.“* (Porada, 2019) Tyto hrozby mohou být ekonomického, vojenského nebo politického původu a mohou být způsobeny špatnými mezinárodními vztahy. Mezi tyto hrozby patří migrační vlny, přerušení dodávek energetických a potravinových surovin, terorismus a kybernetické hrozby.

Vnitřní bezpečností se zaměřuje na ochranu chráněných zájmů uvnitř státu a zahrnuje využití ozbrojených bezpečnostních sborů, záchranných sborů, havarijních služeb, státních a územních orgánů a dalších subjektů, kteří mají své povinnosti stanoveny zákonem. [10] Vnější bezpečnost je definována jako *„stav kdy jsou na nejnižší možnou míru eliminovány hrozby a rizika ohrožující objekt a jeho zájmy zevnitř.“* (Porada, 2019)

Z výše uvedeného vyplývá, že ČR má zájem prostřednictvím bezpečnostní politiky aktualizovat právo bezpečnosti a strategické dokumenty ve vztahu k dynamicky se měnícímu bezpečnostnímu prostředí. Na základě vzniku nových hrozeb provádí analýzy a statistiky, díky kterým reaguje na aktuální situaci. V daném pohledu lze uvést, že Česká republika je na vysoké úrovni v zajišťování bezpečnosti státu a svých občanů.

[9] Vnější hrozby jsou např. vojenské hrozby, teroristické a kybernetické útoky a další formy nebezpečí způsobené vnějším prostředím.
[10] Zákon č. 110/1998 Sb. O Bezpečnosti ČR

4 CHARAKTERISTIKA BEZPEČNOSTNÍCH HROZEB PRO ČESKOU REPUBLIKU

Bezpečnostní hrozby mají vliv na celosvětové společenské prostředí a ohrožují životy, zdraví, majetek, kulturní statky a životní prostředí. Dané hrozby mají globální charakter a zahrnují terorismus, ZHN a nelegální migraci, což je pro společnost jako celek největším problémem. (Řehák, Martínek, Legierská, 2015)

Při hodnocení hrozeb je nutná jejich identifikace za užití analýz, díky kterým jsme schopni rozpoznat jejich vlastnosti, kterými mohou negativně působit na chráněný zájem.

4.1 Členění bezpečnostních hrozeb

Bezpečnostní hrozby můžeme členit na hrozby naturogenní[11], přičemž tyto jsou vzhledem ke svému charakteru a původu vzniku velmi složitě ovlivnitelné, jelikož jsou způsobeny v závislosti na přírodních jevech. Hrozby antropogenní[12]dělíme na vnější a vnitřní, které jsou vždy odrazem konání lidského faktoru. (Řehák, Martínek a Legierská, 2015)

Koncepce ochrany obyvatelstva do roku 2025 s výhledem do roku 2030 stanovila úkol zpracovat analýzu hrozeb pro ČR a začlenit výsledky této analýzy do metodických a strategických dokumentů.

Analýza hrozeb pro Českou republiku zahrnuje identifikaci a hodnocení potenciálních hrozeb a rizik, kterým může být stát, jeho občané, hospodářství a infrastruktura vystaveny. Následně na základě této analýzy přijímají opatření na zajištění bezpečnosti a ochrany před těmito hrozbami. (Paulus et al., 2015)

Výsledkem analýzy hrozeb je celkem 72 typů nebezpečí, které byly rozčleněny a podle kategorií zaneseny do registru. Z celkového počtu hrozeb bylo u 21 zjištěno nízké riziko. Bylo provedeno podrobné zhodnocení 49 typů hrozeb, z čehož vyplívá, že hrozby narušení kritické infrastruktury a narušení finančního a devizového hospodářství státu velkého rozsahu jsou velmi rizikové a byly identifikovány jako největší nebezpečí.

[11] Naturogenní hrozby jsou klimatologické, biologické a geologické
[12] Antropogenní hrozby vnější (klimatologické, biologické a geologické) a vnitřní (personální, procesní a technické).

Tabulka 1Typy nebezpečí s nepřijatelným rizikem (zdroj: Paulus et al., 2015)

Kategorie nebezpečí		Typy nebezpečí s nepřijatelným rizikem	Gesce
naturogenní	abiotické	dlouhodobé sucho	MŽP, MZe, MV
		extrémně vysoké teploty	MŽP
		přívalová povodeň	MŽP, MZe, MV
		vydatné srážky	MŽP, MV
		extrémní vítr	MŽP, MV
		povodeň	MŽP, MZe, MV
	biotické	epidemie	MZd
		epifytie	MZe
		epizootie	MZe
antropogenní	technogenní	narušení dodávek velkého rozsahu	MZe, MPO
		narušení funkčnosti významných systémů elektronických komunikací	ČTÚ, MPO
		narušení bezpečnosti informací kritické informační infrastruktury	NBÚ, MV
		zvláštní povodeň	MZe, MV, MŽP
		únik nebezpečné chemické látky ze stacionárního zařízení	MŽP, MV, SÚJB
		narušení dodávek pitné vody velkého rozsahu	MZe
		narušení dodávek plynu velkého rozsahu	MPO, MV
		narušení dodávek ropy a ropných produktů velkého rozsahu	SSHR, MPO
		radiační havárie	SÚJB, MV
		narušení dodávek elektrické energie velkého rozsahu	MPO, MV
	sociogenní	migrační vlny velkého rozsahu	MV, MZV
		narušování zákonnosti velkého rozsahu (včetně terorismu)	MV
	ekonomické	narušení finančního a devizového hospodářství státu velkého rozsahu	MF, ČNB

4.2 Bezpečnostní hrozby prezentované ve strategických dokumentech

Na základě analýz jsou pro Českou republiku charakterizovány bezpečnostní hrozby, které jsou ukotveny ve strategických dokumentech. Přímý vliv na analýzu hrozeb má členství ČR

v mezinárodních organizacích. Každá bezpečnostní strategie obsahuje vymezení a zhodnocení hrozeb, vymezuje zde své schopnosti a nástroje které užívá bezpečnostní politika v rámci zajišťování bezpečnosti. (Lošek, 2013)

Oslabování mechanismu kooperativní bezpečnosti se vztahuje k situaci, kdy země nebo mezinárodní organizace neplní své politické a mezinárodně-právní závazky, které jsou spjaty se spoluprací a kooperací v oblasti bezpečnosti. To může vést k oslabení celkového bezpečnostního klimatu a zvýšení rizika vzniku konfliktů, krizí a hrozeb. (Bezpečnostní strategie ČR, 2015)

Teroristické útoky jsou hrozby velmi závažného charakteru, jejichž cílem je vyvolat co největší strach a paniku k dosažení svých cílů. Jsou hrozbou pro životy a zdraví obyvatelstva, životního prostředí a kritickou infrastrukturu. (Bezpečnostní strategie, 2015) V dnešní době v rámci migrace jsou teroristé snáze zahrnutelní do migračních vln, kdy se mísí mezi uprchlíky, a jejich cesty do Evropy jsou snazší. Útoky teroristů jsou nejčastěji mířeny proti měkkým cílům[13] nebo prvkům kritické infrastruktury.[14] (Smejkal, 2018)

Boj proti šíření zbraní hromadného ničení a kontrola zbrojení a ozbrojení je úzce spjata s bojem proti mezinárodnímu terorismu, zejména s ohledem na šíření jaderných, chemických a biologických zbraní. Uvedené zbraně by mohly vážně ohrozit bezpečnost, proto se vyžaduje aktivní i pasivní opatření na ochranu území ČR a jejich spojenců. (Bezpečnostní strategie ČR, 2015)

Kybernetický útok je definován jak úmyslné jednání pachatele v kyberprostoru, které směřuje proti zájmům jiné osoby. (Kolouch a Bašta, 2019)

Tyto útoky se stávají v současnosti velkou hrozbou pro obyvatelstvo, ale i pro národní organizace. Díky nim může docházet k úniku informací, na základě, kterých jsou zajišťovány základní funkce státu a může dojít k ohrožení strategických zájmů ČR. (MZV ČR, 2015)

Kybernetická kriminalita vysoce roste, zejména ve vztahu k narušení kritické infrastruktury, dětské pornografii, podvodům, průmyslovým špionážím, terorismu a dalších. (Požár, 2018)

Mezinárodní migrace může mít pozitivní dopad na hostitelské země, jako je přínos pro ekonomiku, zvyšování pracovní síly a další. Nicméně, existují také negativní aspekty, a to

[13] Měkké cíle (Soft Targets) – místa s vysokou koncentrací lidí, s nízkou mírou ochrany (nemocnice, kostely, nákupní centra)
[14] Jedná se o stavby, prostředky, zařízení (elektrické vedení, dopravní cesta, produktovody)

sociální a ekonomickou nerovnost, kde bohatší země přitahují kvalifikované pracovníky a vzdělané obyvatelstvo z chudých zemí. Zvyšují se náklady na veřejné služby jako je školství, zdravotnictví a sociální dávky. Mezinárodní migrace může vést k nárůstu sociálního napětí a xenofobie, což může být způsobeno nedostatečnou integrací a porozuměním kultury a jazyka země, kam se migranti přesídlují. A nejzávažnějším aspektem je zvýšen riziko kriminality a terorismu, jelikož někteří přistěhovalci mohou být zapojeni do těchto aktivit. (Eichler, 2019)

Estevens se ve svém článku věnuje bezpečnosti v EU na základě analýzy migrace a vyhodnocuje bezpečnostní a obranné strategie členských států v závislosti na migrační krizi. Uvádí, že migrační krize se bude odvíjet od sociálního a politického dění na Blízkém východě a v severní Africe, odkud do Evropy proudí velké množství migrantů. (Estevens, 2018)

Extremismus a nárust interetnického a sociálního napětí – sociálně vyloučené lokality a skupiny přispívají ke vzniku prostředí, které je příznivé pro kriminalitu, a způsobují mezietnické a sociální napětí, což extremistické skupiny využívají ke svým cílům. (MZV ČR, 2015)

Extremismus se v ČR obvykle spojuje s pravicovýma levicovým extremismem, stejně jako s náboženským a rasovým. Tyto skupiny se většinou snaží uplatňovat své ideologie pomocí násilí a nenávisti vůči jiným skupinám lidí, což může vést k napětí a konfliktům v různých oblastech.

V současné době je **organizovaný zločin** jednou z nevojenských hrozeb. ČR je považována za tranzitní zemi pro obchod s drogami, zbraněmi pašováním lidí. Je také spojena s praním špinavých peněz, korupcí a počítačovými zločiny. Česká republika má pro boj proti organizovanému zločinu vypracovanou strategii[15] a byl zřízen tým Daňová kobra.[16]

Ohrožení funkčnosti kritické infrastruktury (dále jen „KI“) je vážným problémem, který vyžaduje pečlivou přípravu a prevenci. KI zahrnuje soubor klíčových prvků, které jsou nezbytné pro chod společnosti. Ohrožení funkčnosti KI může mít vážné následky pro společnost. K narušení může dojít fyzickým poškozením v důsledku teroristických útoků,

[15] Koncepce boje proti organizovanému zločinu do roku 2023
[16] Jedná se o speciální tým založený v roce 2014, jehož hlavním úkolem je potírání skutků organizovaného zločinu

přírodních katastrof a havárií. Nebo také kybernetickými útoky, které jsou častější a sofistikovanější. (MZV ČR, 2015)

Provozovatelé KI musí reagovat na krizové situace a minimalizovat dopady. Důležité je investovat do zajištění bezpečnosti kritické infrastruktury proti různým hrozbám.

Přerušení dodávek strategických surovin a energie může mít vážné dopady na hospodářství a bezpečnost země. V důsledku zvýšení cen a nedostatku zdrojů může dojít k přerušení dodávek, což by ovlivnilo průmysl i spotřebitele. Na základě snížení konkurenceschopnosti v důsledku ztráty přístupu ke strategickým surovinám a energiím může dojít k úpadku. Pokud by došlo k přerušení dodávek surovin a energií, může to mít za následek snížení obranyschopnosti a zvýšení zranitelnosti. Pro mnoho zemí je závislost na strategických surovinách a energiích kritická, proto je důležité, aby vlády přijímaly opatření ke snížení rizik a diverzifikaci zdrojů. [17]

Pohromy přírodního a antropogenního původu a jiné mimořádné události – přirozené a lidské faktory mohou vytvářet hrozby, které vážně ohrožují bezpečnost obyvatel, jejich zdraví, majetek a životní prostředí. Dané pohromy mohou dalekosáhlý dopad na různé aspekty lidské společnosti a stát. V případě, že hrozby jsou trvalejšího charakteru, mohou narušit kritickou infrastrukturu, zásobování surovinami a vodou, šířit infekční onemocnění a mít další nepříznivé následky. (MZV ČR, 2015)

Ozbrojený konflikt mezi Ruskem a Ukrajinou – v současné době již druhým rokem probíhá ozbrojený konflikt, který trvá od 24.2. 2022, kdy Rusko zahájilo invazi na Ukrajinu, formou nevyprovokovaného a agresivního útoku. Válka mezi oběma zeměmi má celkový vliv na bezpečnost a je jím ovlivněno celé geopolitické dění.

Bezpečnostní hrozby jsou velmi rozmanité a mohou vzniknout z různých zdrojů. Mezi nejvýznamnější řadíme terorismus, kybernetické útoky, kriminalitu, nelegální migraci, extremismus a ohrožení KI. Tyto hrozby mohou mít vážné důsledky pro společnost jako celek a vyžadují pečlivou přípravu a prevenci.

[17] Diverzifikace – snížení závislosti na jednom dodavateli nebo zdroji a rozložení rizika na více zdrojů.

5 HROZBY V KYBERNETICKÉM PROSTORU

V České republice jsou kybernetické hrozby velkým problémem, stejně jako v jiných zemích světa. Stejně jako kriminalita se zvyšují s rostoucí závislostí na digitálních technologiích a sítích.

Vláda a bezpečnostní složky ČR bojují proti kybernetickým hrozbám prostřednictvím realizace ustanovení národní strategie kybernetické bezpečnosti, která zahrnuje prevenci, detekci, reakci a zotavení z kybernetických útoků.

V roce 2022 schválil Evropský parlament novou směrnici (EU) 2022/2255, o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v EU pod názvem NIS2.[18] Hlavní změnou je rozšíření subjektů spadajících do její působnosti. Tyto budou muset přijmout technická, provozní a organizační opatření řízení rizik, která by mohla ohrožovat jejich informační systémy a sítě a minimalizovat dopady potenciálních incidentů. Evropská unie na základě toho požaduje zlepšení národních strategií. (Info.cz, 2023)

Kybernetický prostor známý jako kyberspace, je virtuální prostor, ve kterém se odehrávají digitální komunikace, transakce a interakce. Nacházejí se zde webové stránky, sociální sítě, e-mailové schránky, cloudové úložiště, online obchody a mnoho dalších digitálních platforem. Souhrnně jde o pojem, který zahrnuje nejen svět internetu, jiných sítí a mobilních technologií, ale také mnoho jiných prostředí a prostorů, které se vyskytují ve virtuální rovině.

Kybernetická bezpečnost je oblastí bezpečnosti zaměřenou na ochranu informací, systémů a sítí před neoprávněným přístupem, útoky, sabotáží a jinými hrozbami způsobenými použitím počítačů, sítí a dalších informačních technologií. Věnuje se prevenci, detekci a řešení bezpečnostních incidentů. V rámci kybernetické bezpečnosti se využívají různé metody a nástroje, jako jsou firewally, antiviry, šifrování dat, autentizace a autorizace19, monitorování a analýza logů a další. (Smejkal, 2018)

Kybernetický útok se vyskytuje, když útočník úmyslně napadne zájmy jiné osoby v kyberprostoru. Tento druh útoku se provádí prostřednictvím počítačové sítě a zařízení s cílem způsobit škodu, neoprávněně získat přístup nebo odcizit citlivé informace.

[18] NIS2 – směrnice nabyla účinnosti 16.1.2023 a členské státy jsou povinny ji do 17.10.2023 implementovat do legislativy. V případě ČR to bude znamenat změnu zákona o kybernetické bezpečnosti i prováděcích předpisů.

[19] Autentizace (hesla, biometrika, tokeny) – jedná se o ověřování identity uživatele zařízení. Autorizace je proces, kterým se řídí, co může oprávněný uživatel dělat v systému. Slouží k omezení přístupů před neoprávněným uživatelem.

Zabraňování kybernetickým útokům vyžaduje několik opatření, jako například aktualizace softwaru a operačních systémů, používání silných hesel, omezení přístupu a školení zaměstnanců. (Kolouch a Bašta, 2019)

5.1 Vybrané druhy kybernetické kriminality

Kybernetické prostředí představuje řadu různých bezpečnostních hrozeb, které se v posledních letech zvyšují v souvislosti s rostoucí digitalizací a propojeností našich životů. Mezi největší kybernetické hrozby patří:

Malware, což je program navržený pro útok na počítačové systémy, sítě nebo zařízení. Mohou to být viry, červi, trojské koně, ransomware, adware a další typy softwaru, které mohou poškodit zařízení nebo ukrást citlivé informace.

Phishing je podvodná metoda, kterou útočníci používají k získání citlivých informaci prostřednictvím e-mailů, SMS nebo webových stránek.

DDoS útoky jsou útoky na webové stránky nebo servery, které mají za cíl přetížit je velkým množstvím požadavků, což brání ostatním uživatelům v přístupu k těmto stránkám.

Ransomware je typ malware, který šifruje soubory na počítači a požaduje platbu od uživatele za jejich dešifrování. Pokud uživatel nezaplatí včas data se ztratí navždy.

Krádeže dat jsou kybernetické útoky, které mají za cíl ukrást citlivá data, jako jsou osobní údaje, údaje o platební kartě nebo podniková data.

Sociální inženýrství je podvodná metoda, kterou útočníci používají k získání důvěry a přístupu k citlivým informacím od uživatele.

Botnety jsou využívány k útokům na webové stránky, kyberšikaně nebo ke krádeži citlivých informací.

Kybernetické vydírání spočívá v požadavku na oběť, jinak budou zveřejněny citlivé informace, jako jsou fotografie, videa nebo jiné údaje. (Kolouch a Bašta, 2019)

Kyberterorismus je označení pro útoky a aktivity, které jsou prováděny s cílem zastrašovat, poškozovat a destabilizovat společnost. Hlavním cílem útoků je oslabit schopnost napadeného, způsobit velké škody a vyvolat dlouhodobé následky vlivem narušení prvků kritické infrastruktury.[20] Mohou být také zaměřeny na cíle politické nebo ideologické

[20] Elektrárny, plynovody, ropovody, letový provoz

povahy, jako jsou vládní orgány, vojenské organizace nebo korporace. Tyto útoky mohou být prováděny jednotlivci nebo organizovanými skupinami.[21] (Smejkal, 2018)

Kyberšikana se používá pro popisování opakovaných a záměrných kybernetických útoků, které jsou zaměřeny na jednotlivce, a to zejména na děti a mladistvé. Tyto útoky mohou mít různé formy, jako jsou urážky, šíření falešných informací, zastrašování, vyhrožování, vydírání, a mohou způsobovat velké emoční a psychické trauma. Kyberšikana může mít vážné důsledky pro zdraví a blaho dětí, jako je deprese, úzkost, sebevražedné myšlenky a další problémy. Proto je důležité věnovat čas prevenci, jelikož mladiství a děti jsou nejzranitelnějšími obětmi těchto útoků. Bohužel oběť má jen málo prostředků se bránit, jelikož útočník je většinou schovaný pod cizí identitou. (Smejkal, 2018)

5.2 Významné kybernetické útoky v ČR

21. října 2017

Web volby.cz – výpadky webu způsobil hackerský útok

23. června 2018

Plicní nemocnice v Janově na Rokycansku. došlo k zašifrování dat. Nemocnice odmítla požadavky vyděračů. Data obnovila ze záloh.

11. prosince 2019

Nemocnice v Benešově – napadení počítačového systému. Došlo k rušení operací. Provoz byl obnoven po 19 dnech.

23. prosince 2019

Hackerský útok napadl OKD a ochromil počítačovou síť.

V roce 2020 byly postupně spáchány kybernetické útoky na nemocnice v Brně, Kosmonosech a v Ostravě. Došlo k napadení také společnosti ČEZ.

V roce 2021 byly napadeny například Systém veřejné správy a několik poliklinik v Praze. Masivnímu kybernetickému útoku čelila datová infrastruktura magistrátu v Olomouci. Ransomware napadl více jak 60 větších firem a úřadů.

[21] Al-Káida je extremistická organizace, spojována s útoky po celém světě, ISIS je extremistická skupina s náboženským a politickým základem, ETA je teroristická organizace usilující o nezávislost Baskického regionu a IRA byla aktivní armáda v Irsku a Severním Irsku a usilovala o sjednocení Irska

V roce 2022 bylo provedeno několik DDoS útoků, a to na internetové stránky České televize, aplikaci Ministerstva financí, skupinu Vltava Labe Media. Hackeři zaútočili na České dráhy a tuzemská letiště. (novinky.cz, 2022)

Kybernetická bezpečnost je významným tématem v oblasti IT a je klíčová pro ochranu jak osobních, tak i obchodních dat a informací. Vzhledem k rychle se rozvíjejícímu digitálnímu prostředí je důležité, aby firmy, organizace i jednotlivci věnovali pozornost bezpečnosti svých sítí i zařízení a pravidelně aktualizovali své zabezpečení a sledovali bezpečnostní hrozby.

6 KRIMINALITA A KYBERNETICKÁ KRIMINALITA

Kriminalita se obecně definuje jako porušení zákonů nebo trestných činů, které jsou stanoveny zákonem a jsou trestány soudy. Kriminalita může mít různé příčiny, jako jsou sociální, ekonomické a psychologické faktory. Kromě toho může být kriminalita ovlivněna různými faktory, jako je vzdělání, kultura, politika, společnost a historické události. K boji proti kriminalitě jsou využívány různé nástroje, jako jsou právní předpisy, soudy, policie a další orgány.

Kriminalita představuje potenciální nebezpečí pro bezpečnost jedinců, skupin a celých společností, a může ohrozit stabilitu státu a jeho bezpečnostní zájmy. Tento problém se vyskytuje ve většině zemí světa a je důležité jej řešit. Spolupráce mezi zeměmi a mezinárodními organizacemi (interpol, Europol) je jedním z hlavních přístupů k boji proti kriminalitě, který by měl být prioritou pro vlády a bezpečnostní síly. [22]

Tabulka 2 Vývoj struktury kriminality v ČR podle druhu kriminality, 2016–2021 (zdroj: Český statistický úřad, 2023)

Rok		druh kriminality						
		Celková kriminalita	v tom:					
			násilná	mravnostní	majetková	ostatní	hospodářská	zbývající
		počet trestných činů						
2016		218 162	14 233	2 241	117 934	26 058	28 306	29 233
2017		202 303	13 672	2 363	108 497	25 635	26 294	25 829
2018		192 405	13 553	2 655	98 670	26 703	24 837	25 974
2019		199 221	13 606	2 733	102 136	27 354	24 589	28 682
2020		165 525	12 247	2 605	82 116	25 013	18 528	24 946
2021		153 233	11 958	3 049	77 562	24 780	12 510	23 312
Změna za 5 let (2016–2021)	*počet*	*-64 929*	*-2 275*	*808*	*-40 372*	*-1 278*	*-15 796*	*-5 921*
	v %	*-29,8 %*	*-16,0 %*	*36,1 %*	*-34,2 %*	*-4,9 %*	*-55,8 %*	*-20,3 %*

Kybernetická kriminalita je kriminální činnost, která se odehrává v kybernetickém prostoru, tedy na internetu, v počítačových sítích a digitálních zařízeních.

Zásadními body v nárůstu trestné činnosti spojené s počítači jsou uváděny jako:

- ✓ nástup osobních počítačů,

[22] Interpol je mezinárodní organizace sloužící pro spolupráci mezi policejními orgány různých zemí. Europol je policejní organizace Evropské unie, jejímž úkolem je podporovat a koordinovat spolupráci mezi členskými zeměmi.

- ✓ vznik počítačových sítí a vzdáleného přístupu k počítačům,

a dále zde můžeme uvést třetí faktor, kterým je masivní rozmach mobilních telefonů a využívání předplacených karet. (Smejkal, 2018)

Boj proti kybernetické kriminalitě je velmi obtížný, jelikož pachatelé mohou operovat anonymně z různých míst na celém světě. V reakci na tuto hrozbu se objevují nové iniciativy, včetně zvýšené spolupráce mezi státy a mezinárodními organizacemi.

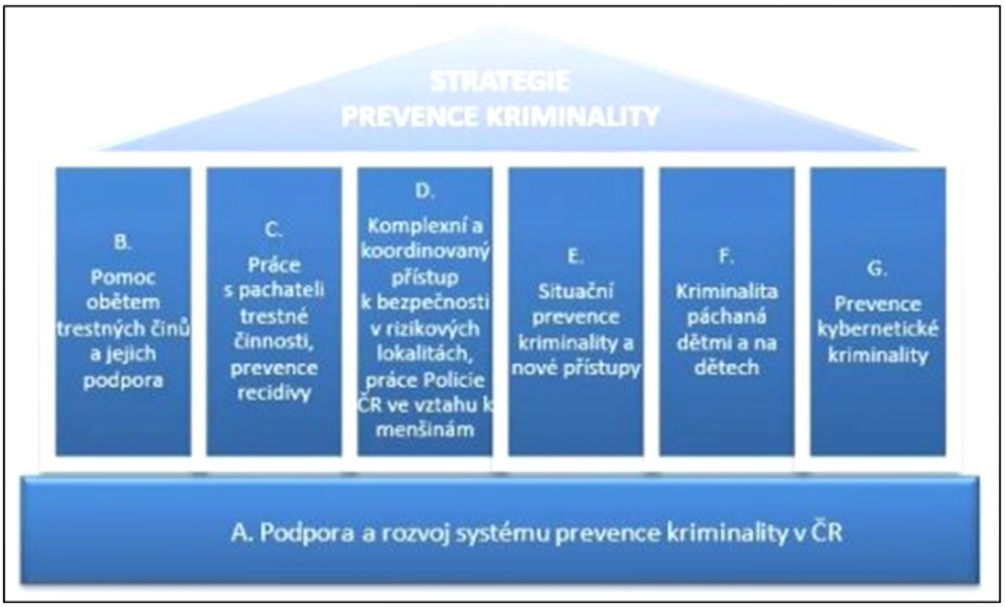
7 PREVENCE KRIMINALITY

Prevence kriminality je soubor opatření, která mají za cíl snížit výskyt kriminality a zlepšit bezpečnost obyvatelstva. Je důležitým tématem, které se týká celé společnosti. Kriminalita může mít negativní dopady na bezpečnost a stabilitu společnosti, ekonomický růst, zdraví a blaho občanů.

Prevence kriminality je nedílnou součástí vládní politiky v České republice již od roku 1993. První strategie prevence kriminality byla schválena v roce 1996 a současná strategie navazuje na další strategické dokumenty ČR a zohledňuje cíle a doporučení mezinárodních dokumentů. Mezi tyto dokumenty patří AGENDA 2030 a její cíle udržitelného rozvoje, které byly začleněny do Strategického rámce ČR 3030 a mají významný dopad na mnoho politik včetně prevence kriminality.

V současné době jsou jednotlivými Krajskými úřady České republiky vydávány Koncepce prevence kriminality na období 2023-2028, které jsou plně v souladu se Strategií prevence kriminality ČR na léta 2022-2027. Jednotlivé koncepce Krajské úřady prezentují na svých webových portálech.

Priority strategie, která byla přijata v dubnu roku 2022, která navazuje na hodnocení předešlé strategie určuje priority a cíle vyobrazené na následujícím obrázku.



Obrázek 1 Strategie prevence kriminality (zdroj: MV ČR, 2022)

Strategie se zaměřuje na nejzávažnější a organizované formy trestné činnosti, jako je terorismus, organizovaný zločin, kybernetická kriminalita a další.

Prevenci kriminality máme trojího typu (primární, sekundární a terciární). V případě primární prevence mluvíme o činnosti výchovné, vzdělávací, osvětové zaměřené na širokou veřejnost a její ovlivňování. Sekundární prevence je již zaměřena na jedince či skupiny osob, se zvýšenou pravděpodobností, že budou páchat trestnou činnost. Terciární forma ji působí na kriminálně narušené osoby, kde usilují formou práce, rekvalifikací a poradenstvím o jejich začlenění do běžného života. (MV ČR, 2023)

Mezi hlavní opatření v prevenci kriminality můžeme uvést:

Osvěta a vzdělávání, tedy informování lidí o rizicích spojených s kriminalitou a naučit je, jak se chránit a chovat v různých situacích.

Zlepšení fyzického prostředí což zahrnuje například instalaci kamerových systémů a osvětlení ulic v nočních hodinách a úpravy veřejných prostranství.

Přítomnost policie v místech s vysokou kriminalitou, kontrola ulic v nočních hodinách a spolupráce s občany.

Programy pro prevenci recidivy, kde by se již dříve trestaní lidé mohli účastnit programů, které jim pomohou zlepšit se a snížit riziko opakování trestné činnosti.

Omezení dostupnosti nelegálních látek, což sebou nese omezení přístupu k drogám a alkoholu, což může mít v důsledku snížení rizika kriminality.

Prevence kriminality by měla být celospolečenskou záležitostí a měla by být realizována pomocí koordinovaného úsilí vládních i nevládních organizací a samotných obyvatel.

Existuje několik evropských programů a iniciativ, které se zabývají prevencí kriminality a posilováním bezpečnosti občanů. Mezi tyto programy patří například:

Evropský program pro prevenci kriminality (European Crime Prevention Network – EUCPN). Tento program podporuje spolupráci mezi evropskými zeměmi a rozvíjí inovativní přístupy ke snižování kriminality a zlepšování bezpečnosti občanů. EUCPN se zaměřuje na témata jako jsou organizovaný zločin, násilí vůči ženám a dětem, prevence extremismu a terorismu a další.

Programy Evropské unie pro boj proti kriminalitě a terorismu. Tyto programy mají za cíl podporovat spolupráci mezi evropskými zeměmi a koordinovat úsilí v boji proti kriminalitě a terorismu. Programy zahrnují financování výzkumu a vývoje, spolupráci mezi orgány činnými v trestním řízení, vzdělávání a osvětu a další.

Evropské monitorovací středisko pro drogy a drogovou závislost (EMCDDA). Tento program se zabývá monitorováním situace v oblasti drog v Evropě a podporuje rozvoj politik a programů na prevenci drogové závislosti a snižování drogově motivované trestné činnosti.

Výše uvedené programy a iniciativy mají za cíl posilovat spolupráci mezi evropskými zeměmi a podporovat inovativní a účinné přístupy k prevenci kriminality a zlepšování bezpečnosti občanů.

Cílem prevence kriminality je vytvořit bezpečnější prostředí a zlepšit kvalitu života. Toho lze dosáhnout identifikací kořenů zločinu a zamezení jeho vzniku, například plánováním architektury a rekonstrukcí městského prostředí s ohledem na koncepty prevence kriminality a osvědčené postupy. [23]

Závěrem je třeba uvést, že se jedná o dlouhodobý proces, který vyžaduje spolupráci různých organizací, občanů a institucí. Cílem prevence kriminality je snížit výskyt kriminality, ale také zlepšit kvalitu života obyvatel a zvýšit pocit bezpečí v oblastech, kde se lidé pohybují.

[23] V říjnu 2022 MV ČR uspořádalo konferenci „Městské prostředí – bezpečnostní hrozba, nebo příležitost pro prevenci?“. Byly zde představeny normy EN 14383-2 a EN 14383-6, které se týkají budování veřejného prostranství a plánování městské výstavby a navrhování budov v rámci prevence kriminality.

8 ZÁVĚR TEORETICKÉ ČÁSTI BAKALÁŘSKÉ PRÁCE

Ke zpracování teoretické části bakalářské práce jsem čerpal z odborné literatury, webových stránek a časopisů, které byly plnohodnotně využity k přípravě a jejímu zpracování

Závěrem lze tedy říct, že bezpečnost státu je základním předpokladem pro stabilitu a prosperitu společnosti. Pro zajištění bezpečnosti státu je nezbytné mít v platnosti koncepční a strategické dokumenty, které umožňují koordinaci a spolupráci všech zainteresovaných subjektů.

Právo bezpečnosti stanovuje pravomoci státních orgánů a institucí, které se zabývají ochranou bezpečnosti státu a jeho obyvatel. Tyto pravomoci jsou upraveny zákony a musí být dodržovány v souladu s ústavou a lidskými právy.

Koncepční a strategické dokumenty slouží k tomu, aby byla bezpečnost státu plánována a řízena s dlouhodobou perspektivou. Dané dokumenty obsahují analýzu bezpečnostních hrozeb a výzev, definují cíle a priority, stanovují opatření a určují zodpovědnost za jejich realizaci.

Cílem těchto koncepčních a strategických dokumentů je zvýšení efektivity a efektivnosti opatření k zajištění bezpečnosti státu, snížení rizik a zlepšení reakce na krizové situace. Směřují tedy k tomu, aby byla bezpečnost státu zajištěna co nejlepším způsobem a aby byla zaručena ochrana životů, majetku a svobod občanů.

II. PRAKTICKÁ ČÁST

9 STATISTICKÁ ANALÝZA KYBERNETICKÉ KRIMINALITY

Statistika kriminality podává nejpřesnější a nejúplnější obraz o jejím rozsahu. Jedná se o data, která jsou dána a rozlišena podle neměnných, stálých a kontinuálně sledovatelných kriminalistických hledisek. Registrovaná kriminalita zahrnuje trestné činy, které byly oznámeny, zjištěny nebo vyhledány ve sledovaném období, a v těchto případech bylo zahájeno trestní stíhání.

V následující tabulce je zobrazen počet skutků spáchaných v kybernetickém prostředí v zemích EU za období 2011–2019, tak jak jej uvádí ČSÚ.[24]

Tabulka 3 Kybernetická kriminalita – počet registrovaných skutků na 100 tisíc obyvatel v zemích EU, 2011–2019 (zdroj: Český statistický úřad, 2023)

Území	2011	2012	2013	2014	2015	2016	2017	2018	2019
	na 100 tis. obyvatel								počet
Belgie	.	.	.	.	.	.	.	.	.	.
Bulharsko	.	.	.	.	.	0,8	1,0	0,8	0,9	66,0
Česko	.	.	.	**6,3**	**6,7**	**6,0**	**7,4**	**8,4**	**10,2**	**1 092,0**
Dánsko	.	.	.	3,3	2,8	6,0	8,0	8,5	0,8	47,0
Estonsko	.	.	.	0,5	2,4	2,5	2,3	2,4	2,8	37,0
Finsko	.	.	.	6,6	7,1	7,8	8,0	9,2	14,4	794,0
Francie	.	.	.	.	.	11,6	11,8	10,3	10,9	7 086,0
Chorvatsko	.	.	.	.	.	2,7	0,2	0,4	0,4	15,0
Irsko	.	.	.	.	.	.	.	.	.	.
Itálie	.	.	.	16,1	13,7	14,6	14,8	19,2	23,9	14 472,0
Kypr	.	.	.	.	.	.	.	.	.	.
Litva	.	.	.	27,6	31,7	13,7	18,2	12,5	13,1	362,0
Lotyšsko	.	.	.	.	.	0,1	0,2	0,5	0,1	2,0
Lucembursko	.	.	.	.	.	.	.	.	.	.
Maďarsko	.	.	.	.	.	.	.	.	.	.
Malta	.	.	.	.	.	44,3	42,7	51,0	42,5	187,0
Německo	.	.	.	.	.	.	.	.	.	.
Nizozemsko	.	.	.	12,1	13,1	11,0	13,6	17,2	28,1	4 810,0
Polsko	.	.	.	0,3	0,4	0,3	0,5	0,3	0,6	230,0
Portugalsko	.	.	.	.	.	.	.	.	.	.
Rakousko	.	.	.	.	.	5,9	4,8	5,2	8,3	742,0
Rumunsko	.	.	.	.	.	.	3,4	4,0	3,6	695,0
Řecko	.	.	.	1,3	1,6	1,3	1,8	2,7	2,3	238,0
Slovensko	.	.	.	0,4	0,4	0,3	0,5	0,4	0,5	29,0
Slovinsko	.	.	.	.	.	.	.	.	.	.
Španělsko	.	.	.	.	.	3,1	3,3	3,3	3,9	1 817,0
Švédsko	.	.	.	.	.	.	.	.	.	.

9.1 Vývoj kybernetické kriminality v letech 2019–2022

Vzhledem k rostoucímu pronikáním informačních technologií do všech oblastí života a společnosti, lze označit kybernetickou kriminalitu a její hrozby za jev moderní doby. Tento

[24] Na následující roky 2020–2022 nejsou u ČSÚ vedeny doposud vyhodnocené statistické ukazatele

trend vede k nárůstu rizik souvisejících s technologickými inovacemi a k nárůstu kriminality.

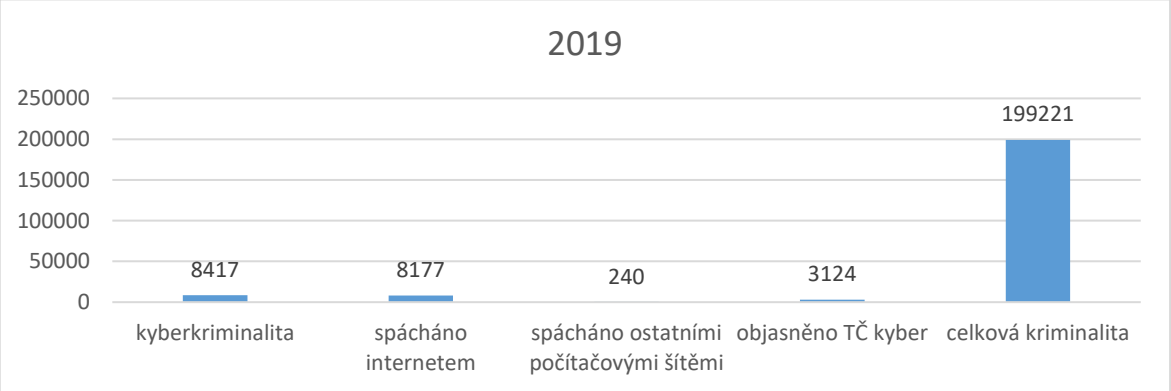
Rok 2019 byl tím posledním rokem, před vypuknutím celosvětové pandemie Covid-19, která zasáhla svět po stránce zdravotní, sociální a v neposlední řadě i v oblasti kriminality a ostatních aspektech společnosti. Opatření, které byly realizovány prostřednictvím vlády České republiky měly svůj vliv i na vývoj trestné činnosti. Kybernetická kriminalita byla významně ovlivněna pandemií Covid-19. S růstem počtu lidí, kteří kvůli omezení sociálních kontaktů tráví více času online, se zvýšila pravděpodobnost kybernetických útoků.

Mezi nejčastější formy kybernetické kriminality v době pandemie patřily phishingové útoky, ransomware, útoky na videohovory a konferenční hovory, krádeže osobních údajů a zneužití online platebních prostředků. Podvodníci využívali nejen obavy lidí z nemocnic, ale také potřebu pracovat a studovat z domova. Velmi často se vydávali za důvěryhodné organizace, jako jsou vládní úřady nebo banky a nabízeli falešné rady, zprávy nebo léky a zdravotnické pomůcky.

Závěrem lze říct, že pandemie Covid-19 představovala zátěžovou situaci bezprecedentní povahy. Zločinci po celou dobu trvání vylepšovali své techniky a taktiky.

9.2 Analýza kybernetické kriminality v roce 2019

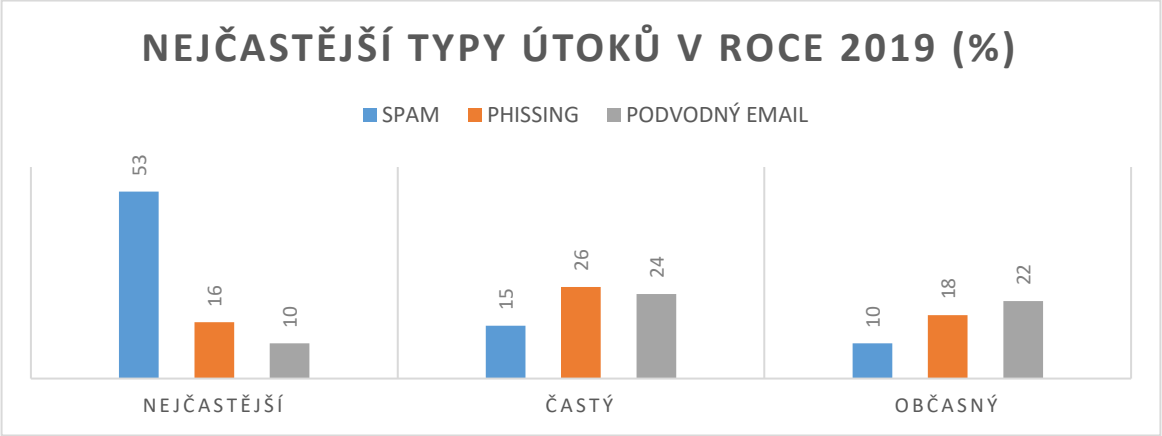
Porovnání statistiky se zaměřuje na kriminalitu páchanou internetem a ostatními sítěmi. Všechen kybernetický zločin bude zahrnut do podrobné analýzy, včetně celkového počtu spáchaných trestných činů, které byly oznámeny na Policii ČR.



Graf 1 Trestná činnost v kyberprostoru v roce 2019 (zdroj: Statistiky kriminality, 2020)

V roce 2019 bylo v České republice evidováno celkem 199 221 trestných činů, což představuje nárůst o 6 816 případů v porovnání s rokem 2018. Z tohoto počtu bylo 8 417

trestných činů spojených s kybernetickou kriminalitou, což znamená nárůst o 1 602 případů oproti roku 2018 (+23,5 %). Objasněno bylo 3 123 případů, což je o 132 méně než v roce 2018 (-4 %). (PP ČR, 2020)



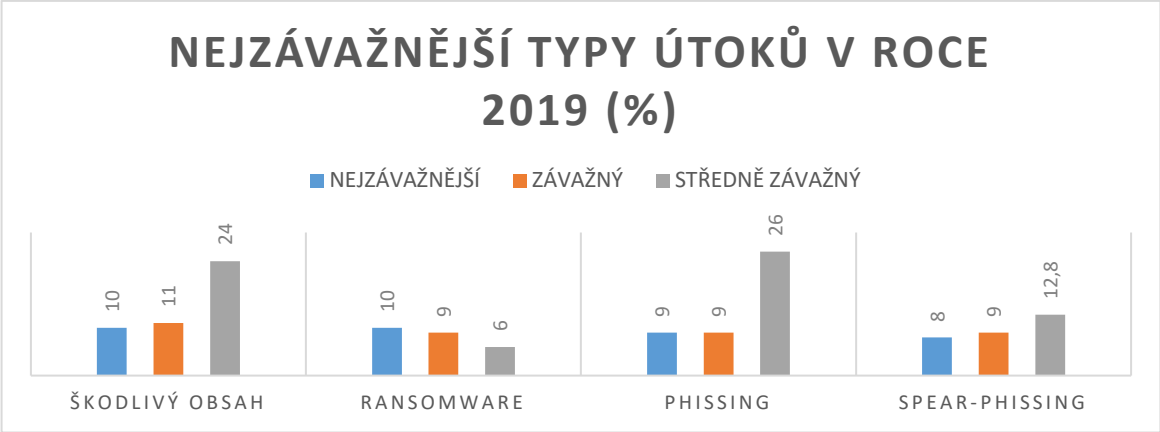
Graf 2 Nejčastější typy útoků 2019 (zdroj: NÚKIB, 2020)

Vzhledem k rychlému rozvoji informačních a komunikačních technologií existuje důvodná obava, že kybernetická kriminalita bude nadále narůstat

Je pravděpodobné, že počet DDoS útoků a útoků prostřednictvím ransomware bude nadále stoupat. Z dlouhodobého hlediska se zaznamenává rostoucí počet případů dětské pornografie a jejího šíření pomocí počítačových systémů a mobilních platforem. V roce 2019 byl zaznamenán větší počet kryptoměn. Česká republika je jednou ze zemí, kde se trh s virtuální měnou rychle etabloval. Hlavním důvodem zvýšené aktivity páchané v kyberprostoru je vidina snadného zisku a malého rizika odhalení této trestné činnosti.

Kybernetické útoky byly také mířeny na státní správu a územní samosprávu, kde nejčastějším typem útoku byl spam, následuje phissing a podvodné emaily. Jako jedna z největší hrozeb je narušení kritické infrastruktury, ale zde nebyl v roce 2019 zaznamenán žádný z útoků.

V ČR došlo ke kybernetickým útokům na MZV neznámými hackery, v důsledku čehož došlo k delšímu výpadku e-mailových služeb. České dráhy byly napadeny v září a došlo k výpadku některých systémů. Cílem útoku měla být francouzská železniční společnost SNFC. Komerční banku byla napadena phishingem, a byly odcizeny citlivé informace. V případě Karlovy univerzity došlo k napadení ransomwarem.



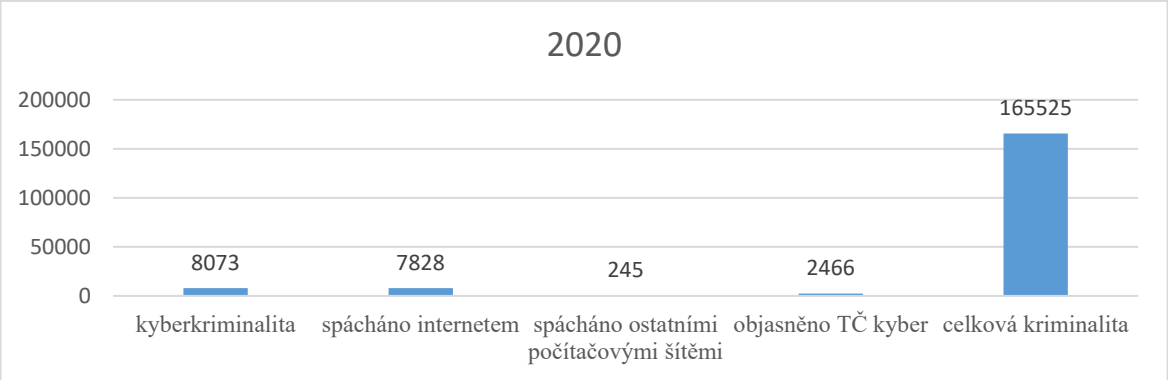
Graf 3 Nejzávažnější typy kybernetických útoků (zdroj: NÚKIB, 2020)

Nejvíce případů kybernetické kriminality bylo zaznamenáno v oblasti podvodů kde se jednalo o 40 % všech případů. Dále se jednalo o útoky na počítače a sítě (21 %), o útoky na webové stránky (16 %), internetové obchody (6 %) a bankovní účty (4 %). (NÚKIB, 2020)

Nejvíce trestných činů spáchaných prostřednictvím internetu a počítačových sítí bylo spácháno v Praze (1685), následuje Jihomoravský kraj (1181) a Středočeský kraj (754). (Statistika kriminality, 2020)

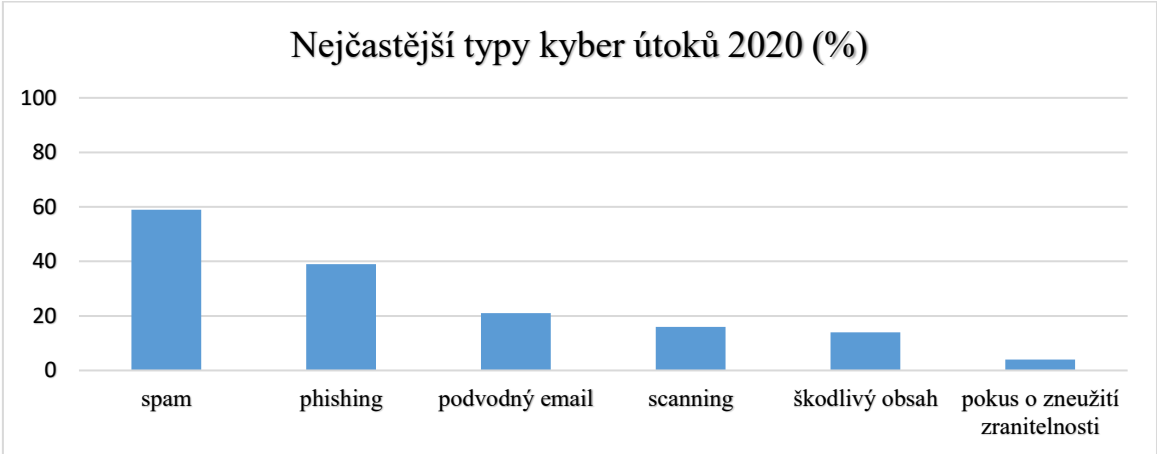
9.3 Analýza kybernetické kriminality v roce 2020

V roce 2020 bylo v České republice zaznamenáno celkově 165525 trestných činů, z toho 8073 bylo spojeno s kybernetickou kriminalitou, což představuje pokles o 344 případů v porovnání s rokem 2019 (- 4 %). Bylo objasněno 2466 trestných činů, což znamená pokles objasněnosti o 685 případů (- 21 %). Podvody byly nejčastějším způsobem páchání trestné činnosti, a to v 3368 případech, což znamená pokles o 45 případů (- 1,3 %), následované poškození a zneužitím záznamu na nosiči informací, kdy bylo zaznamenáno 1160 případů a nárůst o 230 případů (+24,7 %), úvěrovými podvody v 709 případech, což je pokles o 112 případů (- 13,6 %) a mravnostními trestnými činy, kterých bylo evidováno 524 případů, což je o 87 případů (- 14,2 %) méně než v roce předešlém. V roce 2020 byly také zaznamenány útoky na zdravotnická zařízení na velmi profesionální úrovni pokles počtu trestných činů v kyberprostoru může být za částečně způsoben změnou hranice mezi přestupky a trestnými činy kdy byla navýšena z 5000 na 10000 Kč (PP ČR, 2021)



Graf 4 Kriminalita v roce 2020 (zdroj: PP ČR, 2021)

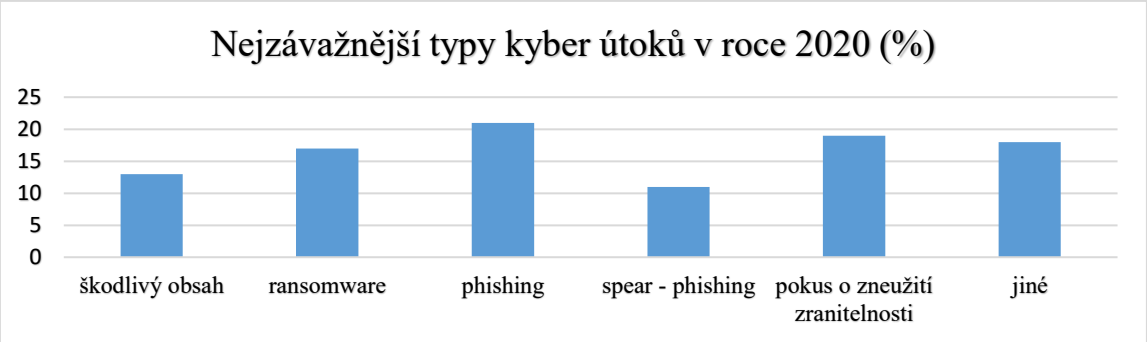
Nejčastějšími formami kybernetických útoků v roce 2020 v ČR byly spamy, phishingové útoky, tedy útoky, při kterých útočníci získávají citlivé informace od uživatelů pomocí napodobených webových stránek a e-mailů. Častými cíli útoků byly banky, finanční instituce a e-shopy.



Graf 5 Kriminalita v roce 2020 (zdroj: PP ČR, 2021)

V ČR došlo v roce 2020 ke kybernetickým útokům na nemocnici v Brně, byla napadena vláda skupinou hacktivistů zvanou Anonymous. Napadena byla i česká pobočka Hondy ransomwarem. Útokem formou DDoS byla napadena společnost O2.

Častými formami kybernetických útoků byly ransomware útoky, při kterých útočníci šifrovali data oběti a požadovali výkupné za jejich obnovení, a DDoS útoky.

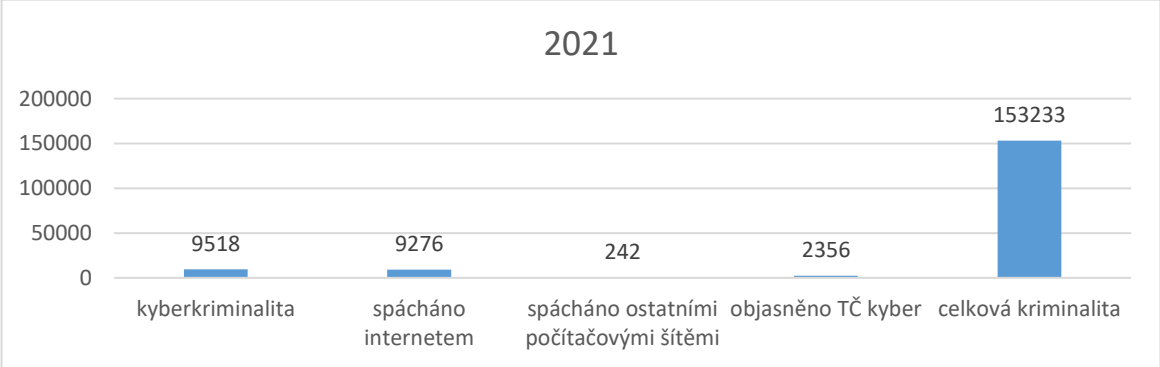


Graf 6 Nejzávažnější typy kybernetických útoků 2020 (zdroj: PP ČR, 2021)

9.4 Analýza kybernetické kriminality v roce 2021

V roce 2021 bylo zaznamenáno několik významných kybernetických útoků na české organizace jako například napadení Ministerstva zahraničí ČR nebo útok na Českou spořitelnu a společnost SolarWinds. Tyto útoky ukázaly, že v kybernetická bezpečnost je stále velkou výzvou pro české organizace a že jsou stále vystaveny vysokému riziku kybernetického napadení.

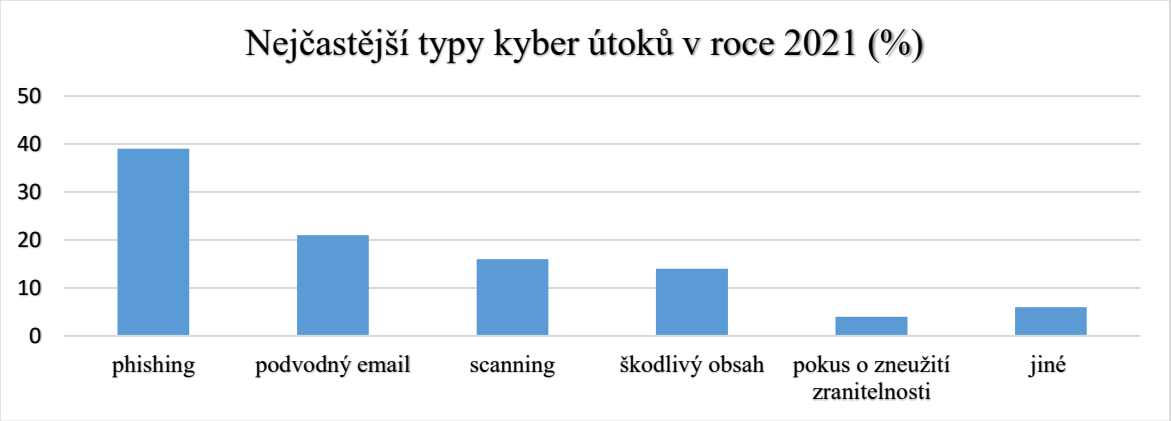
V roce 2021 bylo zaznamenáno 9518 případů trestné činnosti v prostředí internetu a sítí, což je o 1445 skutků více než v roce 2020, což představuje nárůst o 17,8 %. Podvod se stále ukázal jako nejčastější způsob trestné činnosti s 4087 případy, což vykazuje nárůst o 21,3 % oproti roku 2020. Dalšími nejčastějšími způsoby byly poškození a zneužití záznamů na nosiči informaci, přechovávání přístupového zařízení a hesla, kdy počet případů vzrostl o 45 % na 1682. Naopak počet případů úvěrových podvodů klesl o 64,9 % na 645. (PP ČR, 2022)



Graf 7 Kriminalita v roce 2021 (zdroj: PP ČR, 2022)

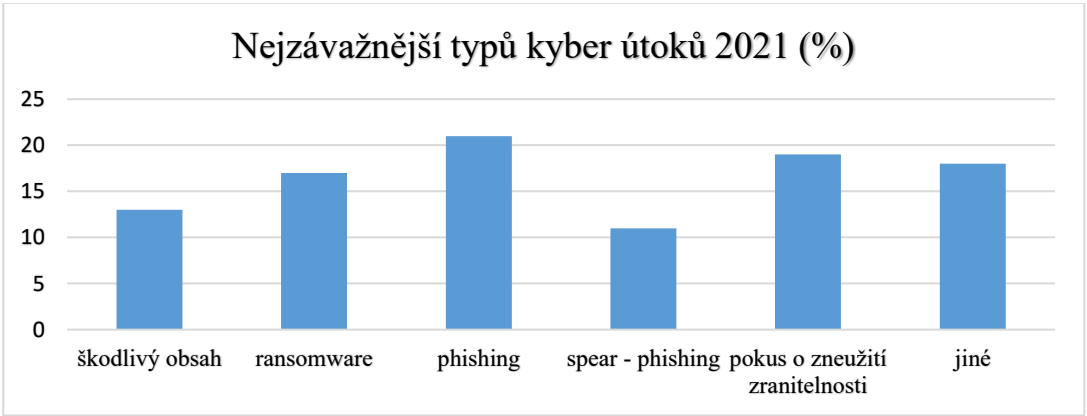
V oblasti trestných činů v kybernetickém prostoru je nejčastější majetková trestná činnost. V roce 2021 došlo k nárůstu tzv. hackingu, tedy útoků na počítačové systémy s následným vydíráním o 45 % ve srovnání s rokem 2020. Nárůst je evidován v oblasti podvodných

emailů nebo zpráv, kdy se pachatelé domáhají z obětí vylákat citlivé údaje osobní údaje a získat přístupy pomocí škodlivých softwarů do jejich zařízení. Další trestnou činností, která zaznamenala nárůst v počtu případů byl vishing v kombinaci se spoofingem telefonních čísel, kde tato jednání jsou spojována s investičními podvody v prostředí kryptoměn.



Graf 8 Nejčastější typy kybernetických útoků 2021 (zdroj: PP ČR, 2022)

V roce 2021 došlo k napadení ministerstva zdravotnictví ransomwarem, což mělo vliv na chod celého systému. Došlo k výpadku v plánování očkování. Napadena byla také Česká spořitelna phishingovou kampaní, kdy se útočníci snažili získat citlivé údaje a data od bankovních účtů. Také došlo k napadení firmy Avast, kde došlo k k úniku citlivých dat uživatelů. Vzhledem k těmto útokům vyšlo varování, že by organizace měly být ostražité a brát v potaz bezpečnostní rizika spojená s kybernetickými útoky.



Graf 9 Nejzávažnější typy kybernetických útoků 2021 (zdroj: PP ČR, 2022)

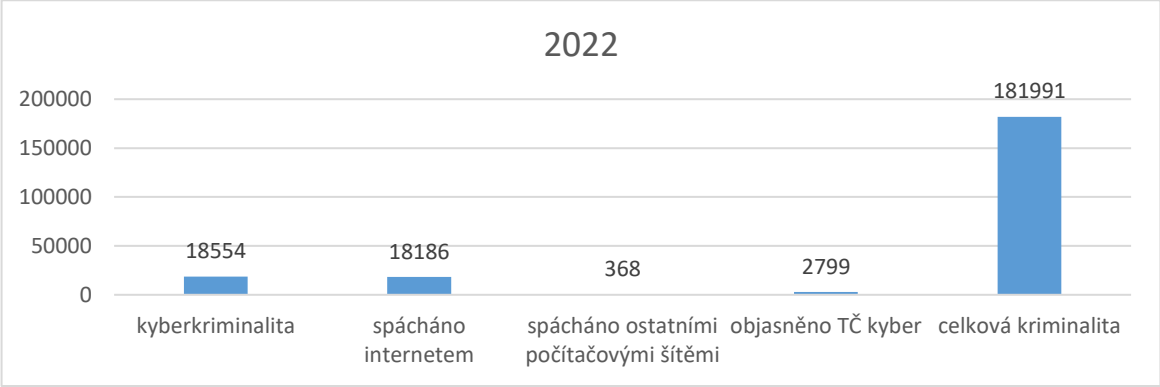
Prověřování a vyšetřování daných činností je velmi zdlouhavé a náročné, ale jelikož převážná část těchto finančních prostředků nabitých výše zmíněnými útoky přechází na zahraniční účty nebo jsou rovnou převedeny do kryptoměn a jsou velmi složitě téměř nemožně dohledatelné. Statisticky jsou již delší dobu vykazovány trestné činy proti

mravnosti, zahrnující zejména šíření a držení dětské pornografie, navazování kontaktu s dětmi a získávání od nich erotického materiálu.

9.5 Analýza kybernetické kriminality v roce 2022

V roce 2022 bylo v České republice z celkového počtu 181991 registrovaných trestných činů zaznamenáno 18554 trestných činů spáchaných na internetu a dalších sítích, což představuje nárůst o 9036 skutků oproti roku 2021 (+94,9 %). Z těchto trestných činů bylo objasněno 2799, což je nárůst v objasněnosti o 443 skutků (+18,8 %). Mezi nejčastější trestné činy patřily podvody v počtu 7272 skutků, což je nárůst o 3640 skutků (+89,1 %), poškození a zneužití záznamu na nosiči informací, přechovávání přístupového zařízení a hesla v počtu 2575 skutků a nárůstem o 893 skutků (+53,1 %) a neoprávněné padělání a pozměnění platebního prostředku, kdy toto bylo zaznamenáno v 4283 případech, což je o 3783 případů více než v roce 2021 (756,6 %). Kriminalita páchaná v kyberprostoru v roce 2022 tvořila 10,2 % z celkové registrované kriminality. (PP ČR, 2023)

V České republice došlo v roce 2022 ke kybernetickým útokům například na internetové stránky České televize, které byly napadeny DDoS útokem. Dále došlo k napadení ministerstva financí, a to aplikace vztahující se na čerpací stanice. A také došlo k hackerským útokům na České dráhy, systémy letišť a Portálu veřejné správy, které má pod svou správou ministerstva vnitra. Na základě vyjádření ministra vnitra za těmito útoky stály ruští hackeři. K útoku se přihlásila proruská hackerská skupina Killnet.



Graf 10 Kriminalita v roce 2022 (zdroj: PP ČR, 2023)

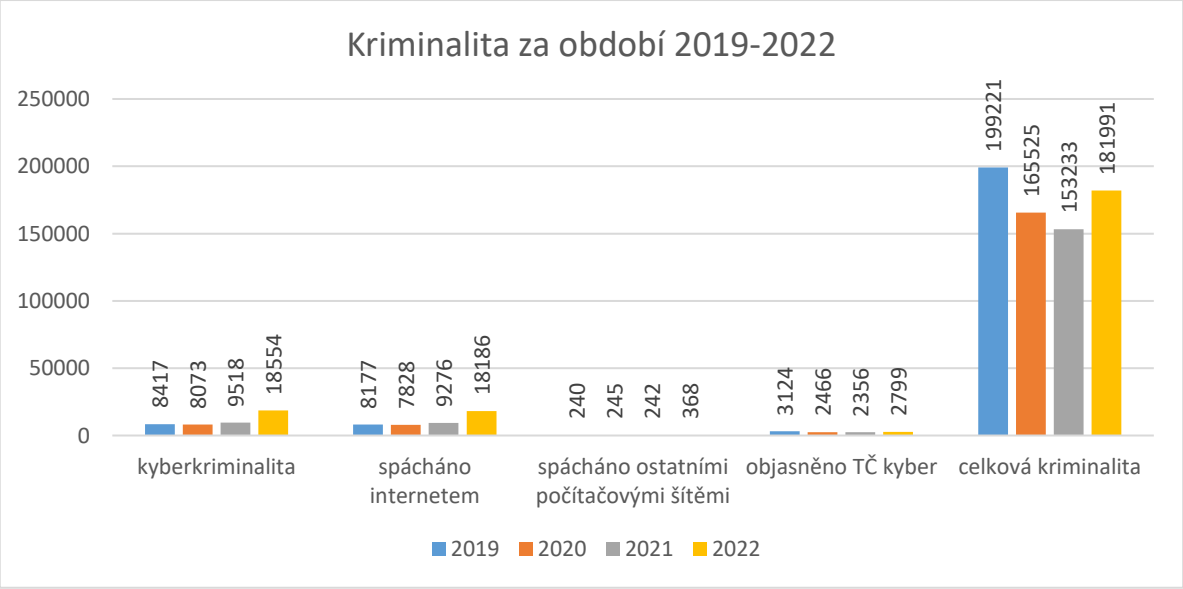
V dané oblasti je setrvalý stav ve formě útoků na počítačové systémy, a jedná se o trvalé bezpečnostní ohrožení. Jednání v kyberprostoru se nesou i v duchu podvodných telefonátů či emailů, za účelem získání přístupových údajů do internetového bankovnictví.

Velmi rozšířeným spektrem trestné činnosti v kyberprostoru je stále více se rozvíjející podvody s legendou výhodných investic do kryptoměn. V důsledku vojenské invaze na Ukrajině docházelo či ještě dochází ze strany proruských hackerských skupin k DDoS útokům na různé cíle v prodemokratických zemích. Jedná se o útoky na mediální instituce, státní instituce a bankovní sektor.

Jednou z největších výzev při odhalování a vyšetřování kybernetické kriminality je skutečnost, že se jedná o boj proti nepříteli, který působí v digitálním prostředí. Ke zlepšení situace v oblasti potýkání se Policie ČR s trestnou činností páchanou v kyberprostoru přijala vláda České republiky 23. 2. 2022 usnesení vlády č. 106, kterým schválila koncepci rozvoje schopností Policie ČR v oblasti kyberprostoru pro léta 2021–2025.

Vliv na kybernetickou bezpečnost v daném roce ovlivnila válka na Ukrajině. Konflikt vyvolal napětí mezi Ruskem a západními zeměmi, což se také projevilo na zvýšeném počtu kybernetických útoků ze strany ruských hackerů a skupin. Kybernetická kriminalita se ve sledovaném období v České republice a po celém světě značně zvýšila a stala se jedním z největších bezpečnostních problémů současnosti.

V roce 2022 byl zaznamenán největší počet trestných činů spáchaných v kybernetickém prostoru, konkrétně 18554 skutků. Kromě toho bylo také zjištěno, že v tomto roce bylo nejvíce trestných činů spácháno prostřednictvím ostatních počítačových sítí v celkovém počtu 368 útoků a v internetovém prostředí bylo spácháno celkem 18186 skutků.



Graf 11 Kybernetická kriminalita za období 2019–2022 (zdroj: PP ČR, 2023)

Vzhledem k celkovému vývoji trestné činnosti páchané v internetovém prostoru, Policie ČR zařadila danou problematiku mezi své hlavní priority pro rok 2023, které je potřeba se věnovat usilovněji.

Celkově lze říct, že kybernetická kriminalita se v posledních letech výrazně zvýšila a stala se stále sofistikovanější a rozmanitější. Je důležité, aby firmy, organizace i jednotlivci přijímali opatření na ochranu proti kybernetickým útokům.

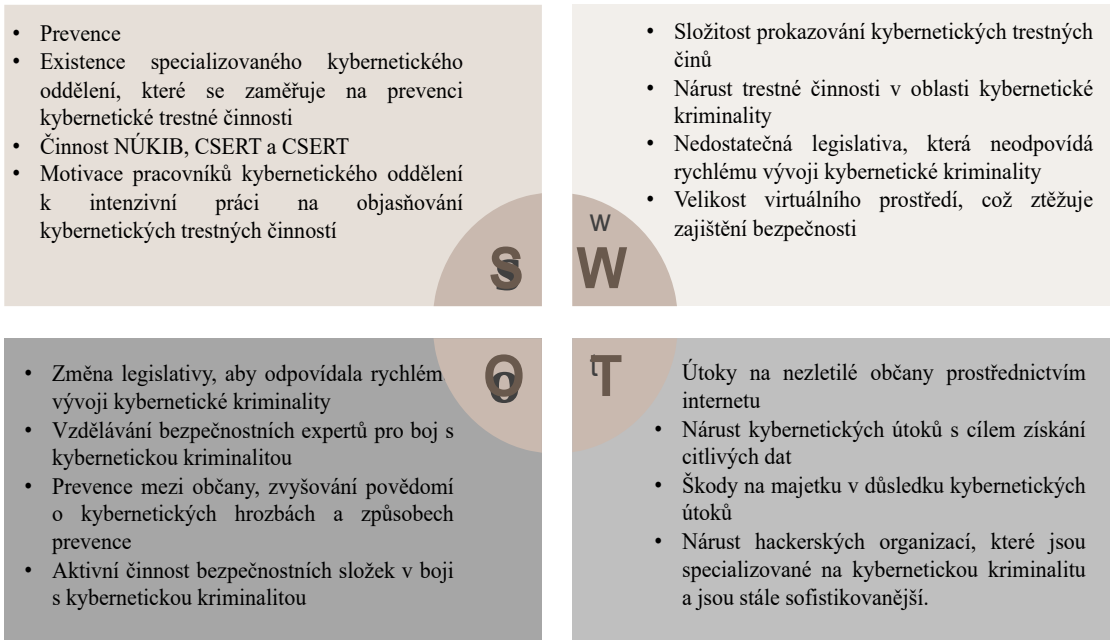
10 SWOT ANALÝZA KYBERNETICKÉ KRIMINALITY

Následující kapitola je zaměřena na analýzu slabých a silných stránek, které mají vliv na objasňování a vyšetřování trestné činnosti související s kybernetickou kriminalitou, a jaké příležitosti a rizika z toho plynou. Analýza se opírá o statistiky týkající se kybernetické kriminality, které jsou shromažďovány Policií ČR, stejně jako o analýzy a sborníky vydávané Policejním prezidiem.

SWOT analýza se zaměřuje na posouzení zkoumaného problému pomocí čtyř prvků: silných stránek (označovaných jako S–strengths), které představují výhody, slabých stránek (označovaných jako W–weaknesses), které se soustředí na nedostatky, příležitostí (označovaných jako O–opportunities), které umožňují rozvoj organizace a realizaci strategických plánů a hrozeb (označovaných jako T–threats), které brání rozvoji a přinášejí rizika. Hlavním cílem SWOT analýzy je identifikovat hrozby, které je třeba minimalizovat, aby bylo dosaženo vysoké úrovně bezpečnosti v dané oblasti. (Managmentmania, 2020)

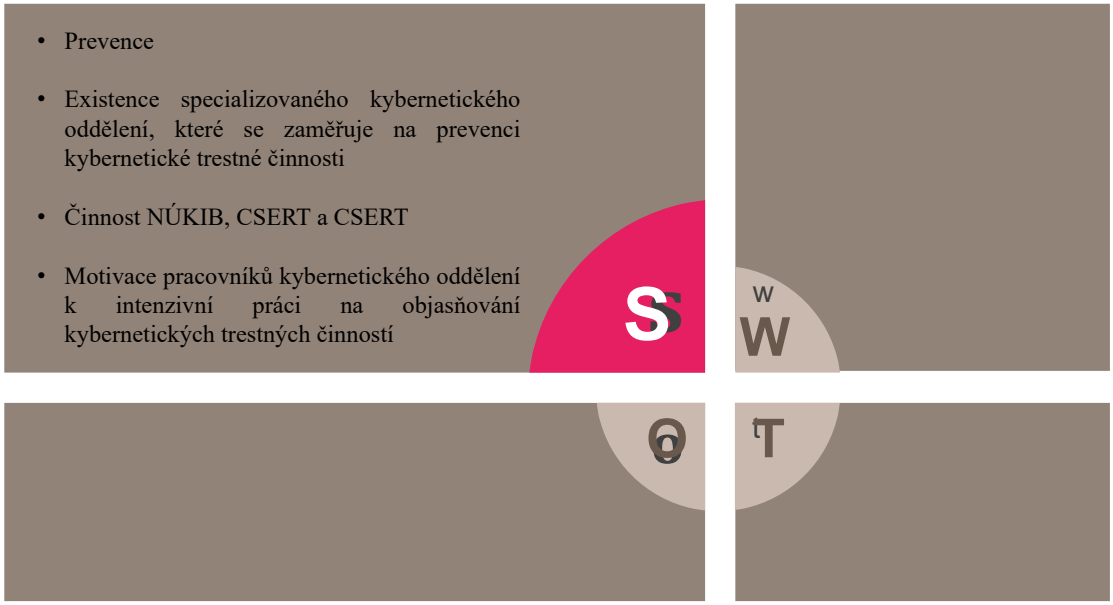
10.1 Analýza kybernetické bezpečnosti

Pro hodnocení jednotlivých kvadrantů jsou využity následující tabulky č. 4–7, kde je použito bodování k posouzení silných stránek a příležitostí, které jsou hodnoceny kladně body od 1 do 5, na druhou stranu slabé stránky a hrozby jsou hodnoceny záporně a získávají body od -1 do -5.



Obrázek 2 SWOT analýza matice (zdroj: vlastní)

Silné stránky (Strengths):

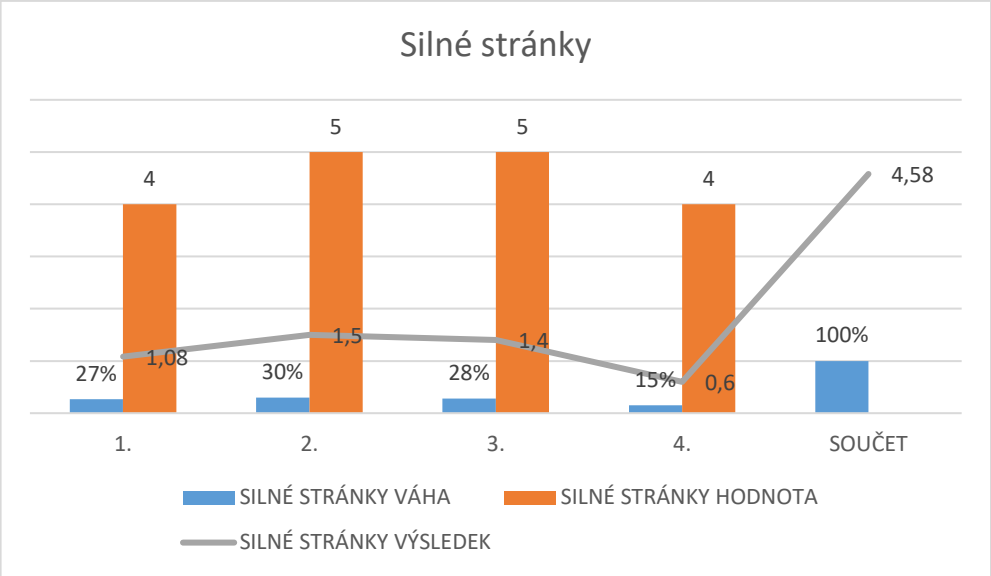


Obrázek 3 Silné stránky (zdroj: vlastní)

1. Prevence kybernetické trestné činnosti je důležitou součástí kybernetické bezpečnosti.
2. Existence specializovaného kybernetického oddělení, které se zaměřuje na prevenci kybernetické trestné činnosti je nedílnou součástí boje proti kybernetickým trestným činům.
3. Činnost NÚKIB, CSIRT a CSERT napomáhají k posilování kybernetické bezpečnosti.
4. Motivace pracovníků kybernetického oddělení k intenzivní práci na objasňování kybernetických trestných činností je klíčová pro úspěšnou prevenci a řešení kybernetických hrozeb a útoků.

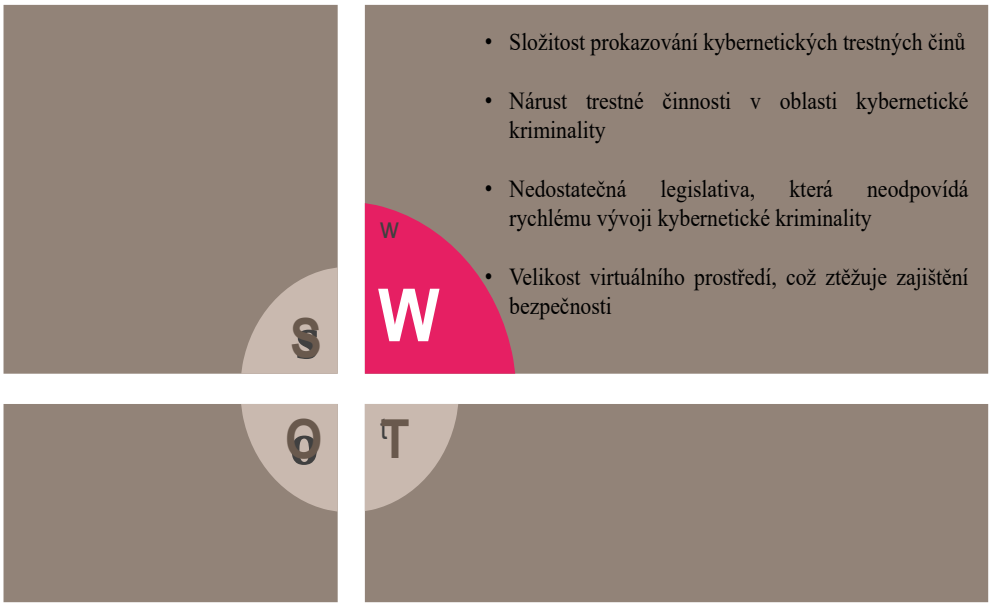
Tabulka 4 SWOT analýza – silné stránky (zdroj: vlastní)

SILNÉ STRÁNKY			
	VÁHA	HODNOTA	VÝSLEDEK
1.	27 %	4	1,08
2.	30 %	5	1,5
3.	28 %	5	1,4
4.	15 %	4	0,6
SOUČET	100 %		4,58



Graf 12 Silné stránky (zdroj: vlastní)

Slabé stránky (Weaknesses):



Obrázek 4 Slabé stránky (zdroj: vlastní)

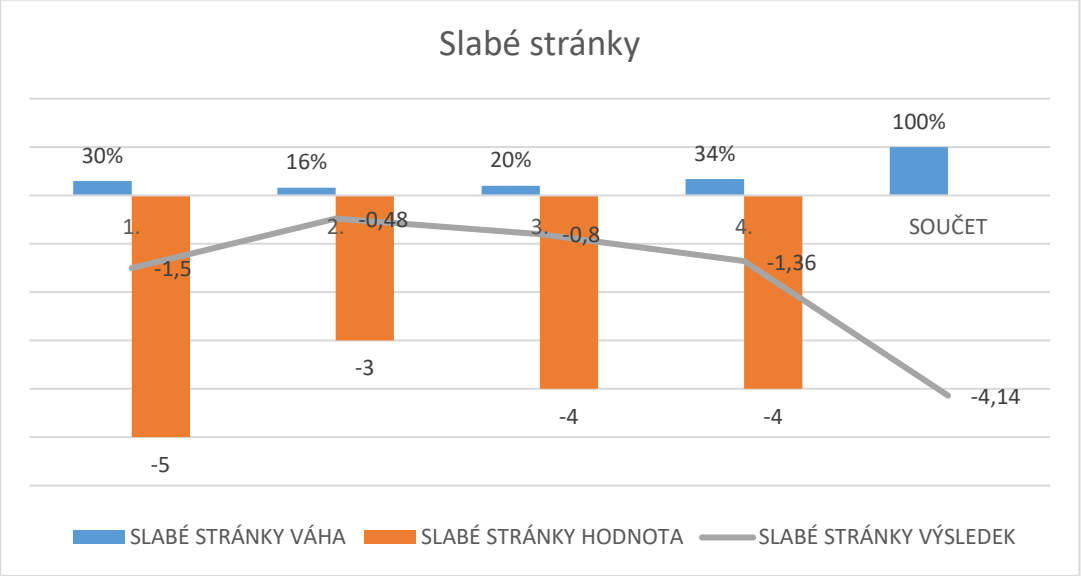
1. Složitost prokazování kybernetických trestných činů – prokazování kybernetických trestných činů je velmi složité kvůli technické a forenzní složitosti těchto zločinů, které se často odehrávají v digitálním prostoru.
2. V oblasti kybernetické kriminality dochází k nárůstu trestné činnosti, což zvyšuje riziko kybernetických útoků a závažných porušení kybernetické bezpečnosti.

3. Nedostatečná legislativa, která neodpovídá rychlému vývoji kybernetické kriminality, a proto je důležité ji aktualizovat a rozšiřovat, aby docházelo k předcházení a řešení kybernetických trestných činů.
4. Velikost virtuálního, v němž se kybernetická kriminalita odehrává, může být obrovská a je obtížné zajistit plnou ochranu proti všem možným hrozbám. To ztěžuje zajištění bezpečnosti a může představovat výzvu pro kybernetickou bezpečnost a prevenci.

Tabulka 5 SWOT analýza – slabé stránky (zdroj: vlastní)

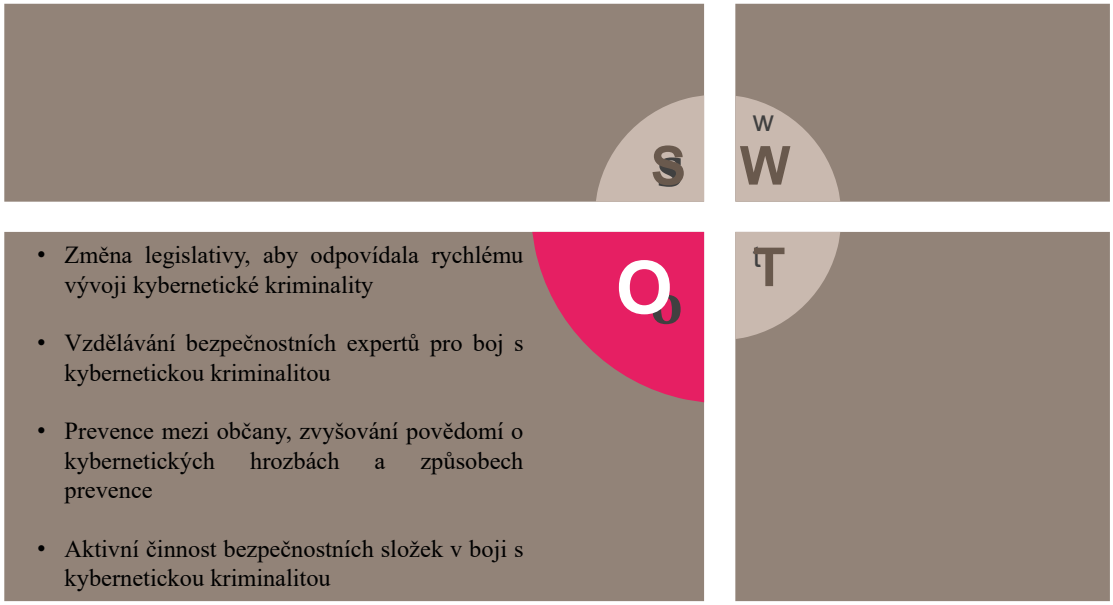
SLABÉ STRÁNKY			
	VÁHA	**HODNOTA**	**VÝSLEDEK**
1.	30 %	-5	-1,5
2.	16 %	-3	-0,48
3.	20 %	-4	-0,8
4.	34 %	-4	-1,36
SOUČET	100 %		-4,14

Celkový součet silných a slabých stránek = 0,44



Graf 13 Slabé stránky (zdroj: vlastní)

Příležitosti (Opportunities):

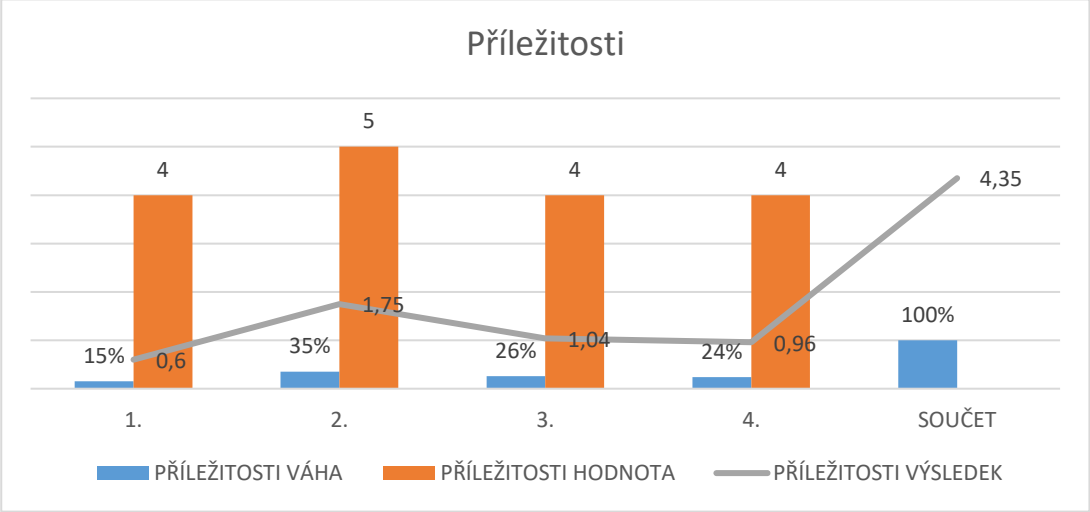


Obrázek 5 Příležitosti (zdroj: vlastní)

1. Změna legislativy, aby odpovídala rychlému vývoji kybernetické kriminality by mohla pomoci přizpůsobit zákony rychle se měnícímu kybernetickému prostředí.
2. Vzdělávání bezpečnostních expertů pro boj s kybernetickou kriminalitou je důležité pro zlepšení schopností zvládat kybernetické hrozby a trestnou činnost v tomto prostoru.
3. Prevence mezi občany, zvyšování povědomí o kybernetických hrozbách a způsobech prevence, například prostřednictvím kampaní a vzdělávacích programů, může pomoci snížit riziko kybernetické kriminality.
4. Aktivní činnost bezpečnostních složek v boji s kybernetickou kriminalitou, jako jsou policie, NÚKIB, CSIRT a další, v boji s kybernetickou kriminalitou je důležitá pro předcházení a řešení kybernetických trestných činů a ochranu kybernetického prostoru.

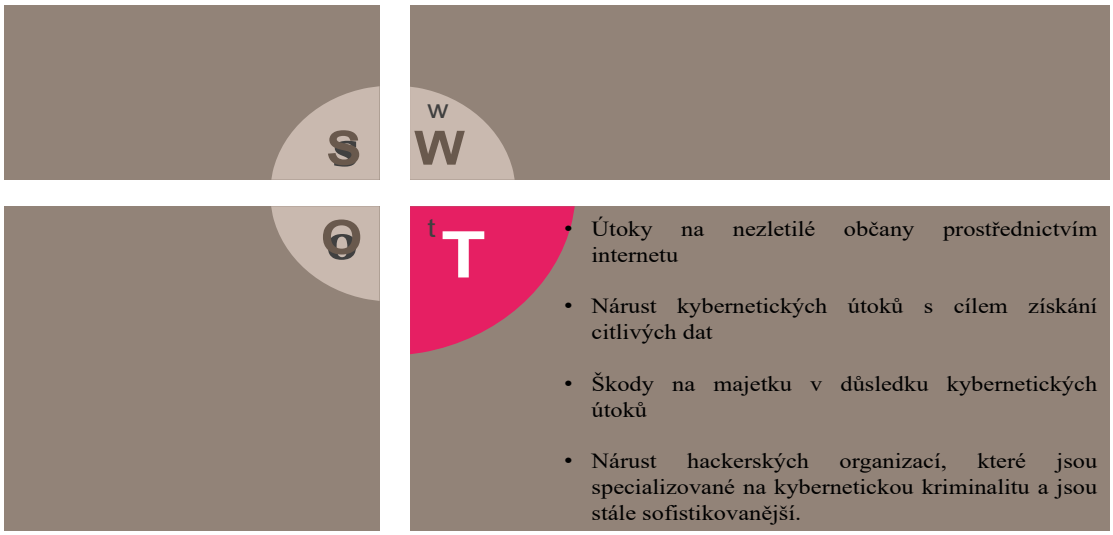
Tabulka 6 SWOT analýza – příležitosti (zdroj: vlastní)

PŘÍLEŽITOSTI			
	VÁHA	HODNOTA	VÝSLEDEK
1.	15 %	4	0,6
2.	35 %	5	1,75
3.	26 %	4	1,04
4.	24 %	4	0,96
SOUČET	100 %		4,35



Graf 14 Příležitosti (zdroj: vlastní)

Hrozby (Threats):



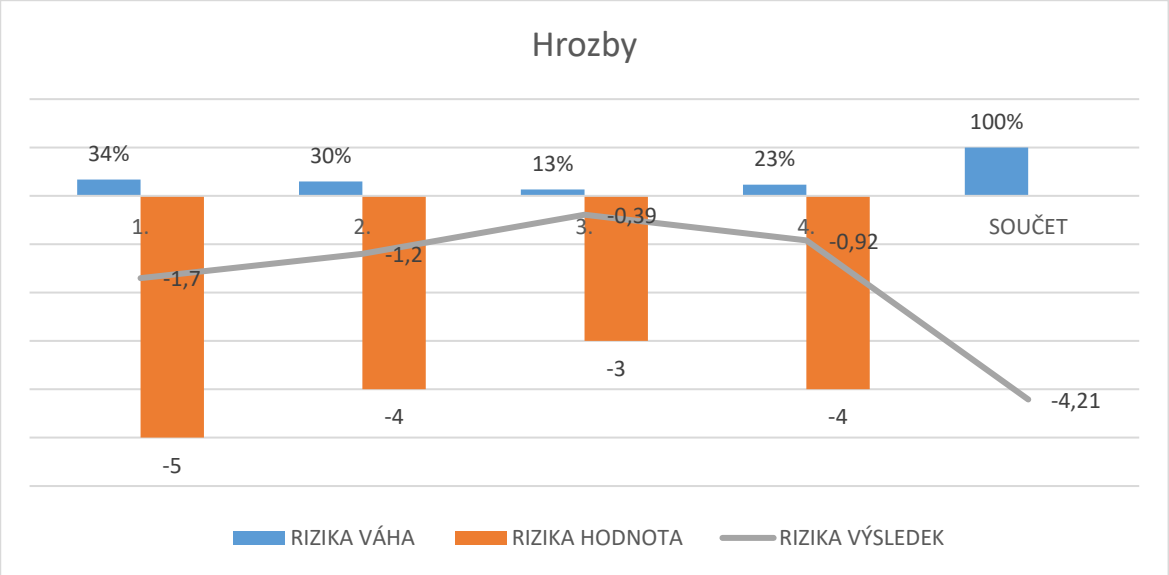
Obrázek 6 Hrozby (zdroj: vlastní)

1. Útoky na nezletilé občany prostřednictvím internetu jsou velkým problémem, protože mlhou mít závažné důsledky na psychické a emocionální zdraví.
2. Nárust kybernetických útoků s cílem získání citlivých dat může mít finanční ztráty jak pro jednotlivce, tak i velké organizace a může vést k ohrožení soukromí a bezpečnosti dat.
3. Škody na majetku v důsledku kybernetických útoků mohou být značné a mohou se týkat jak fyzického majetku, ale i digitálních aktiv.
4. Nárust hackerských organizací, které jsou specializované na kybernetickou kriminalitu a jsou stále sofistikovanější.

Tabulka 7 SWOT analýza – hrozby (zdroj: autor)

RIZIKA			
	VÁHA	**HODNOTA**	**VÝSLEDEK**
1.	34 %	-5	-1,7
2.	30 %	-4	-1,2
3.	13 %	-3	-0,39
4.	23 %	-4	-0,92
SOUČET	**100 %**		**-4,21**

Celkový součet příležitostí a hrozeb = 0,14



Graf 15 Hrozby (zdroj: vlastní)

Mezi silné stránky současného přístupu k potírání kyberkriminality v České republice patří podle předložené SWOT analýzy zaměření na prevenci, existence specializovaných útvarů pro boj s kybernetickou kriminalitou, jako jsou NÚKIB, CSERT a CSIRT a silná motivace pracovníků útvarů pro boj s kybernetickou kriminalitou a vyšetřování.

Na druhou stranu mezi slabé stránky současného přístupu patří obtížnost dokazování kyberkriminality, nárůst kyberkriminální činnosti, nedostatečná legislativa, která nedrží krok s rychlým rozvojem kyberkriminality, a složitost zabezpečení virtuálního prostředí.

Co se týče příležitostí, byly identifikovány možnosti změny a novelizace legislativy pro lepší boj s kyberkriminalitou v souladu s aktuálním děním, vzdělávání a školení bezpečnostních expertů, preventivní a osvětové kampaně mezi širokou veřejností a aktivní úsilí bezpečnostních složek a úřadů v boji proti kyberkriminalitě.

Mezi hrozby patří útoky na nezletilé osoby prostřednictvím internetu, nárůst kybernetických útoků zaměřených na citlivé údaje, škody na majetku v důsledku kybernetických útoků a růst sofistikovaných hackerských organizací.

Celkově analýza SWOT naznačuje, že současný přístup k boji proti kyberkriminalitě v České republice má sice silné stránky, ale také slabé stránky a hrozby, které je třeba řešit, a existují příležitosti ke zlepšení

10.2 Návrh na zlepšení bezpečnostní situace na základě SWOT analýzy

Návrh vychází z analýzy SWOT a bezpečnostní situace týkající se kybernetické kriminality v České republice.

Prvním krokem k dosažení zlepšení bezpečnostní situace a snížení počtu kybernetických útoků trestné činnosti v České republice by mohlo být větší zaměření se na informování obyvatelstva o problematice kybernetické bezpečnosti a rizicích, která jsou spojena s používáním internetu a počítačových sítí. Tím by se lidé mohli lépe chránit před kybernetickými hrozbami a přispět k větší bezpečnosti v digitálním prostředí.

Lidé si veškeré své osobní data ukládají do svých zařízení, která jsou připojena k internetu, a tudíž jsou snadno dostupná hackerským organizacím či jednotlivým útočníkům, kteří své útoky směřují na jejich počítačové systémy, které jsou mnohdy chráněny jen základními a velmi jednoduchými ochranami. S poskytováním informací občanům by se mělo začínat již ve velmi nízkém věku, jelikož dnešní doba je velmi dynamicky se měnící a uspěchaná, a mobilní zařízení, která otevírají přístup do virtuálního světa vlastní již děti v předškolním

věku. Vzdělávání v oblasti prevence při zacházení s počítačovými systémy a dalšími mobilními zařízeními by měly probíhat od základních škol. Ačkoliv se to nezdá, daná skupina mladistvých je v oblasti kybernetické kriminality snadno dostupným cílem pro útočníky. Je důležité dbát na to, aby u dětí byl kladen důraz na opatrnost, aby se vyvarovaly sdílení svých osobních souborů, složek nebo podobných informací pomocí mobilních zařízení. Tento krok je důležitý, neboť takové informace mohou být dále šířeny a zneužívány, což může vést i k vydírání. Tyto situace mohou mít vážné následky nejen na psychiku, ale i na fyzické zdraví dítěte. Je tedy nutné dbát na opatrnost a dávat dětem vhodné informace, aby se dokázaly chránit před riziky v digitálním prostředí.

Kybernetická kriminalita je v současné době jedním z nejvýznamnějších typů kriminality. K zajištění bezpečnosti v kybernetickém prostoru je třeba přijmout řadu právních opatření, která by měla sloužit k prevenci a potírání kybernetické kriminality. Některá z opatření, která lze navrhovat je přijetí nových zákonů specifických pro kybernetickou kriminalitu. Je třeba posílit například trestní zákoník, který by měl být aktualizován, aby reflektoval nové formy kybernetické kriminality. Důležité je také zlepšit mezinárodní spolupráci v oblasti potírání kriminality. Je nutné zvýšit kapacity policie a soudů, což by mělo zahrnovat jejich výcvik, investice do technologií a vybavení a vytvoření specializovaných jednotek pro boj s kybernetickou kriminalitou. Je nutné zlepšit spolupráci mezi státem a podniky v této oblasti.

Na závěr bych tímto návrhem spíše apeloval na poskytovatele, prodejce a další specialisty, kteří vytváří programy pro ochranu počítačových systémů, mobilních zařízení a ochranu v prostředí internetu, že zde by mohlo dojít ze strany vládních bezpečnostních orgánů k regulaci cen u antivirových produktů, jelikož většina těch, které jsou schopny systémy a lidi chránit jsou velmi finančně nákladné a pro spoustu populace nedostupné, proto využívají lidé běžně dostupné free aplikace, ale vzhledem k síle kyberprostoru jsou nedostačující.

11 PŘÍPADOVÁ STUDIE

V této části práce jsem se blíže zaměřil a popsal kybernetický útok ve formě DDoS útoku proti počítačovému systému Bakaláři. Podkladem k vypracování případové studie byl reálný spis, vedený Policií České republiky.

Narušení dostupnosti služeb pomocí DDoS útoku a neoprávněný přístup k počítačovému systému a datům

Neznámý pachatel provedl z blíže nezjištěného místa ve veřejné síti internet kybernetické útoky ve formě DDoS útoků proti počítačovému systému společnosti bakaláři software s.r.o, provozovanému na serverech společnosti fyzicky umístěných v datovém centru DC Tower společnosti České radiokomunikace, přičemž útoky vedl cíleně proti veřejným IP adresám, které jsou využívány pro přístup k internetové aplikaci škola online zahrnující veřejně přístupné internetové stránky dostupné prostřednictvím internetového odkazu https://www.školaonline.cz a informační systém vyžadující přihlášení, dále pro přístup k internetové aplikaci dm software zahrnující veřejně přístupné internetové stránky dostupné prostřednictvím internetového odkazu https://dmsoftware.cz a informační systém vyžadující přihlášení, dále pro přístup k internetové aplikaci zápisy online zahrnující veřejně přístupné internetové stránky dostupné prostřednictvím internetového zápisu odkazu https://zapisyonline.cz a informační sytém vyžadující přihlášení do daného systému a rovněž pro přístup k internetové aplikaci Digiškolka zahrnující veřejně přístupné internetové stránky dostupné prostřednictvím internetového odkazu, a to tak, že pravděpodobně s využitím blíže neurčeného botnetu v době zmíněných útoků několikanásobně zvýšil objem obvyklého síťového provozu za současného i devítinásobného překročení kapacity 1000Mbps připojené linky cílových serverů, které tak nebyly již schopný řádně zpracovávat požadavky oprávněných uživatelů aplikací, tedy data uložená v počítačovém systému dostupná oprávněným uživatelům výhradně prostřednictvím shora uvedených webových aplikací tímto způsobem dočasně potlačil a u jednotlivých útoků k nim omezil dálkový přístup, čímž společnosti Bakaláři software způsobil škodu v podobě nákladů vynaložených na eliminaci útoků a komunikaci s uživateli zmíněných webových aplikací.

K napadenému počítačovému systému, respektive k jednotlivým shora zmíněným aplikacím bylo zjištěno, že se jedná o systém využívaný podle sdělení poškozené společnosti více jak 2400 školami různých stupňů od mateřských až po vyšší odborné školy z celé České republiky a 700000 uživateli z řad zaměstnanců škol, žáků, studentů a jejich zákonných

zástupců. Prostřednictvím těchto aplikací je možné zpracovávat kompletní správu rozsáhlé školní agendy, která je zde rozčleněna do jednotlivých modulů. Aplikace jsou využívány jak registrovanými školami ke správě školní agendy, tak jejich učiteli k prezentaci výukových materiálů, testů, hodnocení žáků, evidenci docházky, tak jejich žáky k práci s výukovými materiály, testy, objednávání stravy a podobně a rodiči žáků těchto škol ke kontrole prospěchu, docházky, omlouvání absence a podobné.

K průběhu a způsobu útoku bylo zjištěno, že tyto útoky měly proběhnout v nočních hodinách, přičemž datový tok, který obvykle během víkendových dnů nepřesahuje 10 Mbps měl v uvedenou dobu několikanásobně narůst, a zcela tak vytížit přenosovou kapacitu 1000 Mbps přípojné linky cílového serveru, na kterém byly jednotlivé aplikace provozovány a omezit dostupnost aplikací pro oprávněné uživatele. Pro detekci útoku aktivované pračce síťového provozu byly odezvy systému výrazně delší a nepodařilo se zcela zabránit ani výpadkům systému. K ukončení útoku došlo samovolně.

Z poskytnutého výňatku logu datového provozu je zřejmé, že v rámci útoku byly kombinovány SYN a UDP útoky konkrétní typy SYN flood, UDP flood, UDP fragment, ICMP flood, přičemž tyto útoky byly vedeny současně, což zvyšovalo jejich efektivitu a bránilo jejich eliminaci. V případě útoku využil pachatel SYN paketů[25] s potvrzenou zdrojovou IP adresou korespondující s jednou z veřejných IP adres využívaných aplikacemi škola online, dm software, zápisy online a digiškolka na různé IP adresy ve veřejné síti internet, které na tyto žádosti o navázání komunikace reagovali odpovědí v podobě SYN ACK paketu zasílaných zpět. Navíc, když útočník neobdržel potvrzení o přijetí odpovědi v podobě ACK paketu, opakoval své odpovědi z důvodů předpokládané ztráty paketů během přenosu přes veřejnou síť internet. To vedlo k výraznému zvýšení síťového provozu směrem k serveru této společnosti, jeho zahlcení a výsledné nedostupnosti pro řádné uživatele. V případě útoku s využitím protokolu UDP, pachatel zasílal velké množství UDP paketů na různé porty serveru, které byly využívány pro provoz aplikací. Tím donutil server k reakci, která spočívala v kontrole využití portů a zaslání odpovědí o nedostupnosti cílového portu. Server také musel provádět defragmentaci nelegitimních paketů, což spotřebovávalo jeho konektivitu a systémové prostředky. To v konečném důsledku způsobilo nemožnost serveru vést jinou komunikaci a jeho nedostupnost.

[25] SYN paket – žádost o navazování komunikace

Neznámý pachatel tímto způsobem dokázal efektivně zamezit oprávněným uživatelům v přístupu k již zmíněnému počítačovému systému a zároveň anonymizovat i svou identitu, neboť ani v případě identifikace koncových přípojných bodů a zařízení, které byly k útoku využity a prakticky nejsou identifikovatelné.

Monitoringem byl zaznamenán útok DOS přesněji podtypu DDoS. Neznámý pachatel umístěn někde na síti internet záměrně dal pokyn k vytvoření takového druhu datového provozu ve směru z internetu na zařízení zákazníka, jehož cílem bylo odstranění tohoto zákazníka od možnosti komunikovat ze sítě internet

Svým jednáním tak neznámý pachatel dočasně potlačil data uložená v počítačovém systému společnosti bakaláři software SRO dostupná oprávněny uživatelů výhradně prostřednictvím shora uvedených webových aplikací a v době jednotlivých útoků k nim omezil dálkový přístup, tedy data uložená v počítačovém systému potlačil úmyslu neoprávněně omezit jeho funkčnost.
V tomto konkrétním případě se cílovou skupinou DDoS útoku staly školská a vzdělávací zařízení, žáci, studenti, učitelé, rodiče a v neposlední řadě poskytovatelé služeb.
Útoky DDoS vznikají tak, že si neznámý pachatel umístěn někde na veřejné síti internet objedná u subjektu, který nabízí za úplatu možnost vytvoření takového datového provozu ve směru z internetu na zařízení, které je identifikováno konkrétní IP adresou.

Většina DOS útoků jsou podtypu DDoS, protože použití tohoto podtypu útoku je velmi obtížné identifikovat pachatele, to je jak jeho realizátora, a tím pádem i zadavatele.

DDoS útok je koordinovaná snaha velkého množství napadených nebo zranitelných zařízení připojených k veřejné síti internet přetížit požadavky cílového zařízení také připojeného k veřejné síti internet. DDoS útoky provádí botnet, což je síť napadených zařízení. Botnety mohou obsahovat miliony zařízení, většina uživatelů napadených zařízení nemá ponětí, že jejich zařízení je napadeno a jsou součástí botnetu.

Závěrem je třeba říct, že terčem nebo obětí kybernetické kriminality může být kdokoliv z nás, a mnohdy je složité se tomu bránit. I v tomto případě, kdy správci/ provozovateli informačních sítí jsou profesionální firmy, tak se jim nepodařilo, jakkoliv zamezit nebo zmírnit dopady DDoS útoků na výše zmiňované softwary. Provozovatel internetového připojení následně doporučil správci počítačové sítě upravit konfigurace svých zařízení a následně obnovit přístup do sítě internet.

ZÁVĚR

Cílem bakalářské práce bylo zjistit, zda Česká republika má dostatečný bezpečnostní potenciál v rámci zajišťování bezpečnosti, a v jaké míře je připravena bojovat proti kriminalitě a zejména té kybernetické, která je velmi rozšířena a skrývá v sobě mnohé nebezpečí.

Je důležité zmínit, že Česká republika se řadí k těm bezpečnějším zemím Evropy, zvláště díky působení všech státních orgánů, institucí a bezpečnostních složek. Je potřeba na zajišťování bezpečnost stále pracovat a rozvíjet ji, jelikož bez prevence může dojít k ohrožení a napadení. K tomu je potřeba i mezinárodní spolupráce s ostatními státy a mezinárodními organizacemi, při tvorbě legislativy a strategických dokumentů.

Česká republika se v této oblasti spoléhá zejména na strategický dokument Bezpečnostní strategie ČR, která byla naposledy aktualizována v roce 2015. Mezi dalšími dokumenty je třeba zmínit Obrannou strategii a Koncepci ochrany obyvatelstva do roku 2025 s výhledem do roku 2030 a další strategické dokumenty.

Česká republika se v rámci kriminality opírá o právní systém, který zahrnuje zákony a postupy pro trestí stíhání a soudní procesy. Tyto zákony a postupy jsou regulovány především Trestním zákoníkem a Trestním řádem, které určují, co je považováno za trestný čin, jaký je postup při trestním stíhání a jaké jsou tresty za jednotlivé trestné činy.

V ČR existuje řada orgánů a institucí, které se zabývají bojem proti kriminalitě. Patří zde například Policie České republiky, Státní zastupitelství, soudy a vězeňská služba. Tyto orgány spolupracují na detekci, vyšetřování a stíhání trestných činů, a na zajištění trestního řízení a výkonu trestu.

Kromě toho existuje v ČR také mnoho nevládních organizací a občanských sdružení, které se snaží bojovat proti různým formám kriminality a pomáhají obětem trestných činů.

I přesto je třeba neustále v rámci mezinárodní spolupráce přijímat právní předpisy, které umožní účinné stíhání pachatelů jak trestných činů v obecné povaze, tak i kybernetických zločinců. Tyto zákony a normy by měly být přizpůsobeny rychle se měnícím technologiím a kriminálním taktikám.

Cílem teoretické části bylo popsat bezpečnostní prostředí, hrozby a analýzy, na základě, kterých je potřebná bezpečnost zajišťována. Autor se blíže věnoval tématu kybernetické kriminality, na kterou bylo navázáno v praktické části, kde byla provedena statistická

analýza a SWOT analýza kybernetické bezpečnosti, ze které vyplývá, že v České republice je každoročně evidováno mnoho těchto útoků, které jsou vedeny jak proti společnostem, jedincům, ale také zejména proti bezbranným dětem, které jsou terčem útočníků.

Je důležité si uvědomit, že boj proti útočníkům v kyberprostoru je velmi složitý a dopadení těchto pachatelů je mnohdy nemožné. Postupem času se určitě najdou prostředky, jak virtuální prostředí začít lépe a účinně bránit tak, aby bylo chráněno proti různým formám kybernetických útoků, které mnohdy dokážou jedním klinutím ze strany útočníka zničit život oběti na straně druhé. Pro zlepšení bezpečnosti je důležité reagovat na aktuální hrozby, ale i na preventivní opatření. Mezi důležité opatření můžeme zahrnout zvýšení povědomí o kybernetické bezpečnosti formou školení zaměstnanců a uživatelů. Šířit mezi ně formy ochrany před kybernetickými hrozbami. Zdůrazňovat užívání silných hesel, provádět pravidelné aktualizace, nabádat uživatele k užívání antivirových softwarů, pravidelně si zálohovat data na externí disky či jiná uložiště. U velkých organizací a institucí je vhodné spolupracovat s odborníky na kybernetickou bezpečnost, kteří pomohou minimalizovat rizika a zlepšit bezpečnostní opatření. Je důležité usilovat o vytvoření politiky pro síťovou bezpečnost a provádět bezpečnostní opatření.

Daná opatření mohou pomoci snížit riziko kybernetického útoku a minimalizovat škody v případě, že k útoku dojde. Je důležité mít na paměti, že kybernetická bezpečnost by měla být prioritou jak pro jednotlivce, tak organizace a státy.

Počet trestných činů v kyberprostoru vykazuje stoupající tendenci, a jejich provádění je pro společnost velmi nebezpečné. Kybernetická kriminalita se šíří jako epidemie. K řešení problému kybernetické kriminality je důležité, aby trestné činy byly uvedeny v zákoně, zavést zákonná oprávnění v boji proti kybernetické kriminalitě a konat taková opatření, aby byla zajištěna ochrana základních lidských práv a svobod. Je důležité neustále aktualizovat a modernizovat bezpečnostní právo, aby bylo úspěšnější v boji proti těmto nelegálním aktivitám, které mohou být hrozbami.

SEZNAM POUŽITÉ LITERATURY

Knižní zdroje

BUZAN, Barry, Ole WAEVER a Jaap de WILDE, 2005. Bezpečnost: nový rámec pro analýzu. Brno: Centrum strategických studií. Současná teorie mezinárodních vztahů. ISBN 8090333362.

EICHLER, Jan, 2019. Evropská bezpečnost 30 let po skončení studené války. Praha: Oeconomica, nakladatelství VŠE. ISBN 9788024522968

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR, 2013. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze. ISBN 978–80–7251–397–0.

JIROVSKÝ, Václav, 2007. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada. ISBN 978-80-247-.

JUŘÍČEK, Ludvík a Petr ROŽŇÁK, 2014. Bezpečnost, hrozby a rizika v 21. století. Ostrava: Key Publishing. Monografie (Key Publishing). ISBN 9788074182013.

KOLOUCH, Jan a Pavel BAŠTA, 2019. CyberSecurity. Praha: CZ.NIC, z.s.p.o. CZ.NIC. ISBN 978-80-88168-34-8.

LOŠEK, Václav, 2013. Integrovaný záchranný systém. Uherské Hradiště: Univerzita Tomáše Bati ve Zlíně. ISBN 9788074542879.

PORADA, Viktor, 2019. Bezpečnostní vědy: úvod do teorie, metodologie a bezpečnostní terminologie. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-758-0.

PROCHÁZKOVÁ, Dana, 2014. Boj proti terorismu: projekt EU: Improving Security by Democratic Participation – ISDEP. V Praze: České vysoké učení technické, Fakulta dopravní, Ústav bezpečnostních technologií a inženýrství. ISBN 9788001055687.

ŘEHÁK, David, Bohumír MARTÍNEK a Petra LEGIERSKÁ, 2015. Ochrana obyvatelstva v kontextu aktuálních bezpečnostních hrozeb. V Ostravě: Sdružení požárního a bezpečnostního inženýrství. Spektrum (Sdružení požárního a bezpečnostního inženýrství). ISBN 9788073851699.

SMEJKAL, Vladimír, 2018. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 9788073807207

SMOLÍK, Josef a Tomáš ŠMÍD, 2010. Vybrané bezpečnostní hrozby a rizika 21. století. Brno: Masarykova univerzita, Mezinárodní politologický ústav. ISBN 9788021052888.

Elektronické zdroje

Vláda ČR: Audit národní bezpečnosti, 2016. [online]. Praha: Ministerstvo vnitra ČR, odbor bezpečnostní politiky a prevence kriminality [cit. 2023-03-05]. Dostupné z: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf

MZV ČR: Bezpečnostní strategie České republiky 2015 [online], 2015. Praha [cit. 2023-04-12]. Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf

Boj proti terorismu [online], 2022. [cit.2022-12-29]. Dostupné z: https://www.mzv.cz/jnp/cz/zahranicni_vztahy/bezpecnostni_politika/boj_proti_terorismu/index.html

ČESKÁ REPUBLIKA, 2016. Terminologický slovník pojmů z oblasti krizového řízení, ochrany obyvatelstva, enviromentální bezpečnosti a plánování bezpečnosti státu. In: . Praha. Dostupné také z: https://www.mvcr.cz/soubor/terminologicky-slovnik-mv-verze-ke-stazeni.aspx

ČESKO. Ústavní zákon č. 1/1993 Sb., ústava České republiky. In: Zákony pro lidi.cz [online]. © AION CS 2010-2023 [cit. 28. 2. 2023]. Dostupné z: https://www.zakonyprolidi.cz/cs/1993-1

ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: Zákony pro lidi.cz [online]. © AION CS 2010-2023 [cit. 5. 3. 2023]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In: Zákony pro lidi.cz [online]. © AION CS 2010-2022 [cit. 28. 12. 2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

Český statistický úřad: Kriminalita v ČR a EU (2011–2021). In: Český statistický úřad [online]. 2023, 9.1.2023 [cit. 2023-04-08]. Dostupné z: https://www.czso.cz/csu/czso/kriminalita-v-cr-a-eu-20112021

Info.cz: Směrnice NIS2 nabyla účinnosti, 2023. Info.cz [online]. © 2001–2023 Copyright CMI News [cit. 2023-04-01]. Dostupné z: https://www.info.cz/pravo/pravni-

servis/smernice-nis2-nabyla-ucinnosti-cesko-cekaji-velke-zmeny-v-oblasti-kyberneticke-bezpecnosti

Informace o stavu ochrany obyvatelstva a krizového řízení z pohledu MV – Hasičský záchranný sbor České republiky. Úvodní strana – Hasičský záchranný sbor České republiky [online]. Copyright © 2023 Generální ředitelství Hasičského záchranného sboru ČR, všechna práva vyhrazena [cit. 01.04.2023]. Dostupné z: https://www.hzscr.cz/clanek/zpravodajstvi-2023-brezen-ochrana-obyvatelstva.aspx

KOLOUCH, Jan; ZAHRADNICKÝ, Tomáš; KUČÍNSKÝ, Adam. Ransomware Attacks on Czech Hospitals at Beginning of Covid-19 Crisis. In: Trends and Future Directions in Security and Emergency Management. Cham: Springer International Publishing, 2022. p. 303-316.

KOTKOVA, Barbora, 2022. CYBER SECURITY IN THE HEALTHCARE SECTOR – CURRENT THREATS. Proceedings of the International Multidisciplinary Scientific GeoConference SGEM [online]. 22, 11-18 [cit. 2023-03-22]. ISSN 13142704. Dostupné z: doi:10.5593/sgem2022/2.1/s07.02

KREJČÍ, Oskar, 1997. Mezinárodní politika. Praha: Victoria Publishing. ISBN 807187034x.

Kybernetická bezpečnost, 2022. Legislativa.cz [online]. [cit. 2023-03-11]. Dostupné z: https://legislativa.cz/zdroje/kyberneticka-bezpecnost/kyberbezpecnost#cap1

Kybernetická bezpečnost: Hlavní a nově se objevující hrozby | Zpravodajství | Evropský parlament. [online]. Dostupné z: https://www.europarl.europa.eu/news/cs/headlines/society/20220120STO21428/kyberneticka-bezpecnost-hlavni-a-nove-se-objevujici-hrozby

Managmentmania: SWOT analýza [online], 2020. Copyright © 2011-2016 [cit. 2023-04-06]. Dostupné z: https://managementmania.com/cs/swot-analyza

Ministerstvo vnitra České republiky: Bezpečnostní hrozby [online], 2019. [cit. 2022-12-29]. Dostupné z: https://www.mvcr.cz/clanek/bezpecnostni-hrozby-337414.aspx

MINISTERSTVO ZAHRANIČNÍCH VĚCÍ. Czechia Statemen – OEWG ICTs – Current an Emerging Threats [online]. In: . [cit. 2023–
03 13]. Dostupné z: https://www.mzv.cz/un.newyork/cz/zpravy_a_udalosti/kyberneticka_bezpecnost_cr_na_ctvrtem.html

MVČR: Bezpečnostní politika [online], 2023. Praha [cit. 2023-03-23]. Dostupné z: https://www.mvcr.cz/clanek/bezpecnostni-politika-statu.aspx

Novinky.cz: Hackerským útokům čelily v Česku nemocnice, Národní knihovna či volební web, 2022. *Www.novinky.cz* [online]. [cit. 2023-04-09]. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-hackerskym-utokum-celily-v-cesku-nemocnice-narodni-knihovna-ci-volebni-web-40394428

Obranná strategie České republiky: The defence strategy of the Czech Republic, 2017. Praha: Ministerstvo obrany České republiky – VHÚ Praha. ISBN 978-80-7278-702-9.

PAULUS, František et al., 2015. Analýza hrozeb pro Českou republiku: Závěrečná zpráva. Praha.

POLICEJNÍ PREZIDIUM ČESKÉ REPUBLIKY, ÚSKPV, 2022. Zpráva SKPV za rok 2021. Praha.

POŽÁR, Josef. Cyber Attacks on Critical Information Infrastructure: Definitions, Threats and the Czech Perspective. Security in Central and Eastern Europe: Cyberspace, Police, Prisons, Transport, Addictions, the Media, 65.

MV ČR: Strategie prevence kriminality v ČR na léta 2022–2027 [online], 2022. [cit. 2023-04-12]. Dostupné z: https://www.mvcr.cz/clanek/strategie-prevence-kriminality-v-ceske-republice-na-leta-2022-az-2027.aspx

PP ČR: Statistika kriminality: ESSK, Elektronické trestní řízení, 2020. Praha, Policejní prezidium ČR. Dostupné také z: http://10.73.94.250/essk/stav/index.php?cast=kyber

PP ČR: Statistiky kriminality, 2020. Dostupné také z: https://okpk-tw.pcr.cz/SitePages/Spear%20Phishing.aspx

ESTEVENS, João. Migration crisis in the EU: developing a framework for analysis of national security and defence strategies. Comparative migration studies, 2018, 6.1: 28.

Strategie prevence kriminality v ČR 2022 až 2027, 2022. In: Ministerstvo vnitra České republiky [online]. Praha [cit. 2022-12-28]. Dostupné z: https://www.mvcr.cz/clanek/nova-strategie-prevence-kriminality-v-cr-na-leta-2022-2027-byla-schvalena-vladou.aspx

Washingtonská smlouva: článek 1. Www.natoaktual.cz [online]. [cit. 2023-03-25]. Dostupné z: https://www.natoaktual.cz/zpravy/Iwashingtonskasmlouva

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ANB Audit národní bezpečnosti

BIS Bezpečnostní informační služba

BS ČR Bezpečnostní strategie České republiky

ČR Česká republika

ČSÚ Český statistický úřad

ČTÚ Český telekomunikační úřad

DDoS Distribuované odmítnutí služby

EU Evropská unie

KI Kritická infrastruktura

NBÚ Národní bezpečnostní úřad

MF Ministerstvo financí

MO Ministerstvo obrany

MPO Ministerstvo průmyslu a obchodu

MV Ministerstvo vnitra

MZd Ministerstvo zdravotnictví

MZe Ministerstvo zemědělství

MZV Ministerstvo zahraničních věcí

MŽP Ministerstvo životního prostředí

NATO Severoatlantická organizace

NSKB Národní strategie kybernetické bezpečnosti

OBSE Organizace pro bezpečnost a spolupráci v Evropě

OSN Organizace spojených národů

SPTČ Skutková podstata trestného činu

PP ČR Policejní prezidium České republiky

PZV

SSHR Státní správa hmotných rezerv

SÚJB Státní úřad pro jadernou bezpečnost

ÚZSI Úřad pro zahraniční styky a informace

VZ Vojenské zpravodajství

ZHN Zbraně hromadného ničení

ZS Zpravodajské služby

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ