UNIVERZITA PARDUBICE

FAKULTA EKONOMICKO-SPRÁVNÍ

# BAKALÁŘSKÁ PRÁCE

2021 Oliver Mach

Univerzita Pardubice
Fakulta ekonomicko-správní

# Vývoj kybernetické bezpečnosti v České republice

Bakalářská práce

2021 Oliver Mach

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2020/2021

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

| | |
|---|---|
| Jméno a příjmení: | **Oliver Mach** |
| Osobní číslo: | **E18040** |
| Studijní program: | **B6208 Ekonomika a management** |
| Studijní obor: | **Management ochrany podniku a společnosti** |
| Téma práce: | **Vývoj kybernetické bezpečnosti v České republice** |
| Zadávající katedra: | **Ústav podnikové ekonomiky a managementu** |

## Zásady pro vypracování

Práce vymezí problematiku kybernetické bezpečnosti v kontextu nástupu kybernetické kriminality a kybernetického terorismu. Se zaměřením na prostředí České republiky analyzuje ukotvení kybernetiky v základních bezpečnostních dokumentech a institucionální zajištění této problematiky ústředními orgány státní správy. Cílem práce je popsat a zhodnotit vývoj kybernetické bezpečnosti a posoudit připravenost České republiky v tomto kontextu.

Osnova:
- Vymezení problematiky kybernetické bezpečnosti.
- Ukotvení kybernetiky v základních bezpečnostních dokumentech České republiky.
- Analýza vývoje kybernetické bezpečnosti v České republice.
- Vyhodnocení výsledků a formulace závěrů.

Rozsah pracovní zprávy: **cca 35 stran**
Rozsah grafických prací: **–**
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

BROOKS, CH. J., GROW, CH., CRAIG, P., SHORT, D. Cybersecurity essentials. Indianapolis, Indiana: Sybex, John Wiley, 2018. 758 s. ISBN 978-1-119-36239-5.
JIROVSKÝ, V. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. 284 s. ISBN 978-80-247-1561-2.
KOLOUCH, J., BAŠTA, P. CyberSecurity. Praha: CZ.NIC, 2019. 556 s. ISBN 978-80-88168-31-7.
SAK, P. Úvod do teorie bezpečnosti: nekonvenční pohledy na minulost, přítomnost a budoucnost lidstva. Praha: Petrklíč, 2018. 271 s. ISBN 978-80-7229-652-1.
ŠULC, V. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. 147 s. ISBN 978-80-7380-737-5.

Vedoucí bakalářské práce: **Ing. Pavel Zdražil, Ph.D.**
Ústav ekonomických věd

Datum zadání bakalářské práce: **1. září 2020**
Termín odevzdání bakalářské práce: **30. dubna 2021**

L.S.

**prof. Ing. Jan Stejskal, Ph.D.**
děkan

**doc. Ing. Marcela Kožená, Ph.D.**
vedoucí ústavu

V Pardubicích dne 1. září 2020

Prohlašuji:

Práci s názvem vývoj kybernetické bezpečnosti v České republice jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 24. 11. 2021

Oliver Mach

## PODĚKOVÁNÍ

Tímto bych rád poděkoval mému vedoucímu práce Ing. Pavlu Zdražilovi, Ph.D. za jeho rady, ochotu, odbornou pomoc, a především trpělivost při zpracování bakalářské práce.

## ANOTACE

*Bakalářská práce se zabývá problematikou kybernetické bezpečnosti. Cílem práce je popsat a zhodnotit vývoj kybernetické bezpečnosti a posoudit připravenost České republiky v tomto kontextu. První kapitola diskutuje o bezpečnostní vědě a bezpečnosti jako takové a následně definuje kybernetickou bezpečnost. Druhá kapitola shrnuje řízení kybernetické bezpečnosti. Třetí kapitola popisuje dokumenty České republiky, ve kterých je problematika kybernetické bezpečnosti ukotvena. Čtvrtá kapitola se zabývá analýzou kybernetické bezpečnosti a na závěr diskutuje o připravenosti České republiky na tuto bezpečnost. Z analýzy vyplývá, že počet kybernetických útoků se konstantně zvyšuje, zejména v kategoriích phishing a spam.*

## KLÍČOVÁ SLOVA

*bezpečnostní věda, bezpečnost, kybernetická bezpečnost, kybernetické útoky, kyberprostor, Česká republika*

## TITLE

*Development of cyber security in the Czech Republic*

## ANNOTATION

*This Bachelor's thesis deals with issues of cyber security. An aim of this work is to describe the development of cyber security in the Czech Republic. The first chapter discusses the science of safety and safety as such, and consequently defines cyber security. The second chapter recapitulates cyber company management. The third chapter describes documents of the Czech Republic which anchor the issues of the cyber security. The fourth chapter pursues an analysis of cyber security and in conclusion discusses preparedness of the Czech Republic for this security. The analysis shows, that number of cyber attacks increases, especially in phishing and spam categories.*

## KEYWORDS

*safety science, safety, cyber security, cyber attacks, cyberspace, Czech Republic*

# OBSAH

ÚVOD ..... 11
1. Kybernetická bezpečnost v rámci bezpečnostní vědy ..... 13
1.1 Předmět bezpečnostní vědy ..... 15
1.2 Kybernetická bezpečnost ..... 16
1.3 Kyberprostor ..... 17
1.4 Kybernetické útoky ..... 19
2. Řízení kybernetické bezpečnosti ..... 22
2.1 Riziko ..... 23
2.2 Aktiva ..... 25
2.3 Hrozby a zranitelnost ..... 26
2.4 Základní bezpečnostní opatření ..... 28
3. Ukotvení kybernetiky v bezpečnostních dokumentech České republiky ..... 29
3.1 Bezpečnostní dokumenty ČR ..... 29
3.2 Národní úřad pro kybernetickou a informační bezpečnost ..... 32
4. Analýza vývoje kybernetické bezpečnosti ..... 36
4.1 Analýza kybernetických útoků ve světě ..... 36
4.2 Analýza kybernetických útoků v České republice ..... 42
4.3 Vyhodnocení výsledků analýzy a připravenost ČR ..... 48
ZÁVĚR ..... 51
POUŽITÁ LITERATURA ..... 53

# SEZNAM TABULEK A ILUSTRACÍ

Tabulka 1 – Pravděpodobnost výskytu rizika ..... 24
Tabulka 2 – Dopad rizika ..... 24
Tabulka 3 – Matice základních typů hrozeb ..... 26
Tabulka 4 – Strategické cíle národní strategie kybernetické bezpečnosti 2021-2025 ..... 32
Tabulka 5 – Prvních pět států s největším počtem bezpečnostních týmů CERT/CSIRT ..... 34
Tabulka 6 – Poměr škodlivého spamu na nejvíce napadené země 2020 ..... 39
Tabulka 7 – Osoby ve věku 16-74 let v zemích EU, které obdržely podvodný e-mail v roce 2019 ..... 40
Tabulka 8 – Osoby ve věku 16-74 let v zemích EU, které byly přesměrovány na podvodné webové stránky v roce 2019 ..... 40
Tabulka 9 – Měsíční podíl počítačů podléhajících kybernetickým útokům v evropských státech v roce 2020 ..... 41
Tabulka 10 – Počet vybraných incidentů řešených CSIRT týmy v létech 2016-2020 ..... 45

Obrázek 1 – Bezpečnostní roviny kodaňské školy ..... 14
Obrázek 2 – Fáze kybernetického útoku ..... 21
Obrázek 3 – Počet bezpečnostních týmů v ČR v letech 2004-2019 ..... 35
Obrázek 4 – Vývoj kybernetických útoků v letech 2016-2020 ..... 37
Obrázek 5 – Vývoj pěti nejčastějších kybernetických útoků v letech 2016-2020 ..... 38
Obrázek 6 – Hrozby spojené s Covid-19 v 1. čtvrtletí roku 2020 (v procentech) ..... 38
Obrázek 7 – Počet domácností v ČR vlastnící počítač s internetem v letech 2016-2020 (v milionech) ..... 42
Obrázek 8 – Počet osob starší 16 let používající internet v letech 2016-2020 (v milionech) ..... 42
Obrázek 9 – Počet domén v ČR v letech 2011-2020 ..... 43
Obrázek 10 – Počet doménových registrací v jednotlivých měsících v letech 2017-2020 ..... 44
Obrázek 11 – Vývoj síly DDoS útoků v letech 2012–2020 ..... 46
Obrázek 12 – Vývoj počtu pokusů připojení zachycených IDS v letech 2016-2020 ..... 47

# SEZNAM ZKRATEK

| | |
|---|---|
| CCTV | Uzavřený televizní okruh |
| CERT | Skupina pro reakci na počítačové hrozby |
| CSIRT | Skupina pro reakci na počítačové bezpečnostní incidenty |
| ČR | Česká republika |
| DDOS | Odepření služby (Danial of Services) |
| EU | Evropská unie |
| FBI | Federální úřad pro vyšetřování |
| IA | Informační aktiva |
| IC3 | Centrum pro stížnosti na internetovou kriminalitu |
| ICT | Informační a komunikační technologie |
| IDS | Systém pro odhalení průniků (Intrusion Detection Systém) |
| IS | Informační systémy |
| IT | Informační technologie |
| MIMT | Člověk uprostřed (Man in the Middle) |
| MVČR | Ministerstvo vnitra České republiky |
| NAS | Chytrá datová uložiště |
| NATO | Severoatlantická aliance |
| NBÚ | Národní bezpečnostní úřad |
| NÚKIB | Národní úřad pro kybernetickou a informační bezpečnost |
| OSINT | Zpravodajství z otevřených zdrojů |
| RAT | Vzdálený přístup |
| SAN | Dedikovaná datová síť |
| SCADA | Dispečerské řízení a sběr dat |
| SQL | SQL injeciton |
| TCP/IP | Primární přenosový protokol/protokol síťové vrstvy |
| USA | Spojené státy americké |
| XSS | Cross-site scripting |
| ZOKB | Zákon o kybernetické bezpečnosti |

# ÚVOD

V současné době se problematika kybernetické bezpečnosti stává stále více probíraným tématem, a to nejen na úrovni českých institucí a firem, ale také v jednotlivých domácnostech. Se stále zvyšujícím se tempem rozvoje informačních a komunikačních technologií, je současná společnost nucena převést většinu svých aktivit do kyberprostoru. Toto tempo růstu se stává těžce sledovatelným, nejen z pohledu běžného uživatele, ale také odborníků v oblasti kybernetické bezpečnosti. Vývoj informačních a komunikačních technologií a pohyb v kyberprostoru přináší usnadnění některých aktivit, ale na druhou stranu pohyb v kyberprostoru s sebou nese určitá úskalí v podobě kybernetických hrozeb a útoků.

Především od roku 2020 došlo k urychlení přesunu aktivit do kyberprostoru v důsledku pandemie Covid-19. Krom toho, problematika kybernetické bezpečnosti se velmi rychle vyvíjí, a proto v souvislosti s tím dochází i k vývoji bezpečnostních prvků a systémů. Uživatelé, kteří se neadaptují na tyto změny, se stávají zranitelnými vůči kybernetickým útokům, jelikož používají zastaralé aplikace či software, a na ty jsou často vedeny kybernetické útoky. Mezi tyto uživatele především patří veřejný sektor, zdravotnictví a školství, na které se v posledních letech zvýšil počet kybernetických útoků.

V návaznosti na výše uvedené je **cílem této práce je popsat a zhodnotit vývoj kybernetické bezpečnosti a posoudit připravenost České republiky v tomto kontextu.**

Práce se skládá ze čtyř kapitol, z toho první tři kapitoly se zabývají teoretickým vymezením problematiky kybernetické bezpečnosti a poslední kapitola je věnována analytickému pohledu. Problematika kybernetické bezpečnosti je celosvětovým problémem, proto se analýza zabývá nejen Českou republikou, ale také zbytkem světa.

Kybernetická bezpečnost je podmnožina bezpečnosti jako takové, proto se začátek první kapitoly věnuje vymezení samotné bezpečnosti. Také se zabývá bezpečnostními studii, které s bezpečností úzce souvisí a jsou klíčová pro její vymezení. Mimo jiné kapitola nabízí pohled na vývoj pojetí bezpečnostních studií. Závěr této kapitoly se zabývá vymezením již samotné kybernetické bezpečnosti, ve kterém je nastíněna její definice, definice kyberprostoru a jsou představeny nejčastější kybernetické útoky.

Druhá kapitola je věnována řízení kybernetické bezpečnosti a s ní souvisejícím činitelům, které jsou základními prvky řízení bezpečnosti. Mezi tyto prvky patří aktiva, rizika, hrozby a zranitelnost, které jsou v této kapitole podrobněji představeny. Řízení bezpečnosti se většinou vymezuje v souvislosti s podnikem a na základě tohoto řízení mohou podniky lépe zajišťovat

svoji bezpečnost. Obdobně probíhá řízení kybernetické bezpečnosti. Mimo jiné kapitola nabídne vymezení doporučených postupů při řízení bezpečnosti v této oblasti.

Třetí kapitola nabídne pohled do problematiky kybernetické bezpečnosti prostřednictvím dokumentů České republiky, ve kterých je tato problematika ukotvena. V kapitole jsou uvedeny dokumenty dle časové posloupnosti, kdy byly vydávány. Nejzásadnějším okamžikem je vydání Zákona o kybernetické bezpečnosti a vzniku Národního úřadu pro kybernetickou a informační bezpečnost. V kapitole je nastíněn obsah jednotlivých dokumentů a přestavena činnost Národního úřadu společně s týmy pro reakci na počítačové hrozby a incidenty.

Čtvrtá kapitola se zabývá analýzou kybernetické bezpečnosti a skládá se ze tří částí. Tato analýza využívá prezentaci zpracovaných dat do podoby grafických a tabulkových výstupů. V první části se zaměřuje na okolní svět a kybernetické útoky, kterým podléhá. Druhá část analýzy se zaměřuje na Českou republiku, která není výjimkou pro cíl kybernetických útoků. Poslední část čtvrté kapitoly vyhodnotí provedenou analýzu a vymezí připravenost České republiky z hlediska kybernetické bezpečnosti. Na skrz celou kapitolou se prolíná současná situace ohledně pandemie onemocnění Covid-19, která do problematiky přinesla nové cíle, zranitelnosti a rizika.

# 1. Kybernetická bezpečnost v rámci bezpečnostní vědy

Rozpracováním obecné teorie bezpečnosti a analyzováním rizik, bezpečnostní věda zpracovává koncepce, kterými zmírňuje, nebo dokonce eliminuje bezpečnostní rizika systému. Pro bezpečnostní vědu a teorii bezpečnosti je definování samotné bezpečnosti klíčové. Od raných počátků lidstva jsou opatření a jednání z úvah o bezpečnosti součástí lidské historie. Tyto úvahy byly vždy v souladu s dosaženou materiální, technologickou úrovní, úrovní poznání a úrovní bezpečnostní reflexe. Bezpečnostní reflexe se zaměřuje na společnost a civilizaci jako celek. Její úroveň se mění vývojem a proměnou společnosti a civilizace. (Sak, 2018)

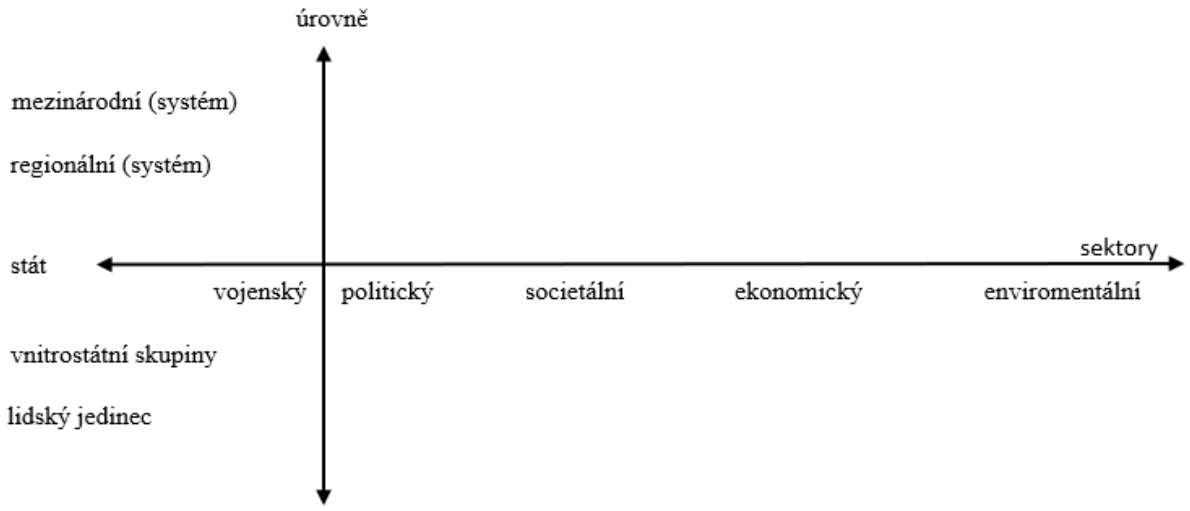
Podle Petra Saka (2018, 42): *„Bezpečnostní věda se zabývá ohrožením a riziky pro existenci systému, její struktury a naplňování jeho funkcí.“*

*„Proměny společnosti a lidské civilizace směřující k vyšší komplexitě, planetarizaci, virtualizaci a medializaci kladou na reflexi bezpečnosti výrazně jiné požadavky, které v úhrnu vedou ke vzniku vědní disciplíny, jejíž reflexe bezpečnostní problematiky odpovídá potřebám lidské civilizace v nové etapě jejího vývoje.“* (Sak, 2018, 15)

Stephen Walt (1991, 212) ve své definici charakterizoval bezpečnostní vědy jako *„studium hrozby, užití a kontroly vojenské síly.“* V této definici bezpečnostní vědy jsou tématem bezesporu válka a zní vyplývající hrozby a rizika. Bezpečnost se zajišťuje a udržuje pomocí vojenské síly.

Dříve bezpečnostní vědy studovaly více nebezpečí, nejistoty a jejich zdroje na základě předpokládaných konfliktů mezi státy. Pomohlo tomu propuknutí první světové války, kdy v roce 1919 vznikla ve Velké Británii první katedra mezinárodních vztahů, ve snaze zkoumat její příčiny, průběh, dopady a možné preventivní nástroje, které by takovému střetu zabránily. (Waisová, 2005)

Nový pohled na bezpečnostní vědy nabízí tzv. Kodaňská škola, která definuje bezpečnostní sektory, v jejichž rámci je vojenský sektor pouze jednou z pěti dimenzí. Kodaňská škola také nabízí odlišný pohled na objekty, kterým má být zajištěna bezpečnost. Zatímco pro kritická bezpečnostní studia je hlavním objektem bezpečnost člověka, tak Kodaňská škola se zaměřuje především na bezpečnost státu, ale i na bezpečnost kolektivů a skupin. (Waisová, 2005) Pohled Kodaňské školy na bezpečnostní studia znázorňuje obrázek č. 1.




Obrázek 1 - Bezpečnostní roviny kodaňské školy

Zdroj: *Vlastní zpracování dle Waisová (2005)*

Z obrázku č. 1 vyplývá, že Kodaňská škola rozšířila pohled na bezpečnost o politický, societální, ekonomický a enviromentální sektor. Tyto sektory jsou zobrazeny na horizontální ose a vyjadřují zdroj hrozby. Dále z obrázku vyplývá, že pro Kodaňskou školu, je nejdůležitějším objektem stát, jelikož jedinec nemá potenciál ohrozit bezpečnost celého státu. Na druhou stranu stát má schopnost ohrozit jeho obyvatelstvo, když není zajištěná bezpečnost. Tudíž můžou být ohroženy mezinárodní a regionální systémy.

Vývoj civilizace a společnosti dozrál do takové úrovně, kde v souvislosti s ním vznikají další výrazná rizika, která samotnou společnost ohrožují. Na tyto rizika je vznik, potřeba a reakce bezpečnostní vědy nezbytnou součástí bezpečnosti. Věda musí dostát celistvému chápání bezpečnostního faktoru civilizace, jelikož reakce pouze na jednotlivé segmenty a subsystémy civilizace a společnosti je nedostačující. (Sak, 2018)

Mezi nejvýznamnější faktory růstu bezpečnostní vědy patří (Sak, 2018, 17-19):

- nárůst komplexnosti společenských systémů,
- snižování diverzity mezi sociálními skupinami,
- technologický vývoj zbraní a jejich systému s planetárním dopadem,
- celkový technologický rozvoj společnosti a jejího moderního způsobu života,
- dopad průmyslu na životní prostředí,
- terorismus,

- demokratické politické systémy,
- nárůst organizovaného zločinu a jeho globalizace,
- stírání hranic mezi černou, šedou a normální ekonomikou.

## 1.1 Předmět bezpečnostní vědy

Předmětem bezpečnostní vědy je samotná bezpečnost. V této souvislosti polemizují autoři o odpovědích na otázky typu: „Co je bezpečnost?“ a „K čemu je bezpečnost vztažena?“ (Sak, 2018)

Holcr, Porada a kol. (2011, 89) vymezují bezpečnost jako *„velmi složitý multidimenzionální sociální fenomén, který se spojuje s rozmanitými formami lidského chování a existence.“* V této definici je bezpečnost zredukována pouze na segment sociální sféry a lidského chování.

Podle Petra Saka (2018, 45) *„je bezpečnost stav entity, v němž není narušena či ohrožena její existence, struktura a funkce. Je to v širším významu stav harmonie a homeostáze.“* Předmětem bezpečnostní vědy je tedy sledování atributu stavu entity[1]. Atribut stavu a entita tvoří pilíře bezpečnosti, které je pro bezpečnostní vědu a teorii důležité formulovat.

V bezpečnosti v určitém čase dochází k oscilaci kolem stavu entity, kde se vytváří odchylky od stavu harmonie. Větší odchylka znamená větší ohrožení, tudíž menší bezpečnost entity. Je tedy vymezena bezpečnost ve fixním stavu entity vůči pevně definované struktuře a funkci. (Porada, 2019) *„Je to stav entity v daném čase a prostoru, nepostihuje vývoj a dynamiku entity. Takto vymezenou bezpečnost nazýváme statickou bezpečností.“* (Sak, 2018, 45)

Největším nebezpečím vzhledem ke statické bezpečnosti je pro existující entity evoluce, vývoj a život. V tomto případě je nutné vzít v úvahu dynamický aspekt a definovat dynamickou bezpečnost. (Porada, 2019) *„Jedná se o takovou bezpečnost entity, v níž nejsou ohroženy nejen její existence, funkce a struktura, ale ani jejich vývoj a vývoj entity jak takové.“* (Sak, 2018, 45)

Bezpečnost entit se z hlediska prostředí dělí na vnější a vnitřní podle toho, zda původ ohrožení pochází zevnitř, nebo z vně entity. Oba tyto pojmy nemají jasně vymezenou a zakotvenou definici, tudíž jejich interpretace je značně obtížná. (Porada, 2019)

[1] *„Entita je jakýkoliv objekt v podobě člověka, zvířete, věci nebo jevu, který tvoří součást reálného světa a který je obsažen v datovém modelu.“* (IT slovník, 2021)

*„Vnitřní bezpečnost je stav, kdy jsou na nejnižší možnou míru eliminovány hrozby ohrožující objekt a jeho zájmy akcemi zevnitř a tento objekt je k eliminaci stávajících i potencionálních vnitřních hrozeb efektivně vybaven a k ní ochoten.“* (Porada, 2019, 51)

Obdobně zní definice vnější bezpečnosti s rozdílem ochoty eliminovat hrozby ohrožující stát a jeho zájmy zvnějšku. O vnitřní bezpečnosti lze uvažovat i v širším pojetí, ve kterém se zahrnují i ostatní prospěšné hodnoty na úrovni celé společnosti, jako přírodní vlivy a neúmyslné důsledky lidské činnosti. (Porada, 2019)

V mezinárodním měřítku se mezi těmito pojmy (vnitřní a vnější bezpečnost) postupně smazává rozdíl na základě poklesu vojenského mezinárodního napětí, nárůstu vlivu transnacionálních aktérů ohrožujících bezpečnost, jako je mezinárodní organizovaný zločin a terorismus, a globalizace ekonomiky. Avšak tyto pojmy přežívají ve státních bezpečnostních dokumentech České republiky, kde se sebou úzce souvisejí a navzájem se prolínají. (Balabán, Nachtmannová, Stejskal, 2006)

## 1.2 Kybernetická bezpečnost

Za posledních 20 let, na základě velkého vývoje informačních a komunikačních technologií (dále jen ICT), se společnost stala na těchto technologiích zcela závislá. Jejich výpadek a život bez nich by byl nemyslitelný, respektive nemožný. V dnešním období, které lze nazvat „obdobím informačním“, člověk, který má přístup k informačním aktivům (dále jen IA), což jsou data, informace, systémy či infrastruktura a odpovídající znalosti, nabývá konkurenční výhody. Proto kybernetická bezpečnost v dnešní době nabývá na významu a je více než žádoucí. Stala se tak jednou z hlavních priorit národních politik. Hlavním cílem této bezpečnosti je uchránit IA nacházející se v kybernetickém prostoru před zničením, odstraněním, zneužitím či zcizením kybernetickými hrozbami a útoky. Její vymezení je do určité míry problematické a nemá jednotnou obecně uznávanou definici. (Bašta, Kolouch a kol, 2019, Šulc, 2018)

*„Kybernetická bezpečnost představuje soubor opatření, která jsou přijata, aby byl ochráněn počítačový systém před neoprávněným přístupem či útokem.“* (Bašta, Kolouch a kol., 2019, 42)

Podle Oxford dictionary (2021b): „*Kybernetická bezpečnost představuje stav, kdy dochází k ochraně před kriminálním či neautorizovaným užitím elektronických dat.“*

Nebo podle Jiráska a kol. (2013, 57) *„kybernetická bezpečnost představuje souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.“*

Všechny tyto definice nejsou jednotné, jelikož se každá definice zaměřuje na jiné IA, a právě tímto se dopouští určitých nepřesností. První definice se zaměřuje pouze na počítače, systémy a pouze dva druhy kybernetických útoků, přitom ignoruje rozmanitost těchto útoků a IA. Druhá definice se zaměřuje pouze na jednotlivá elektronická data a ignoruje systém jako takový. Třetí definice je relativně přesná, avšak se zaměřuje pouze na ICT prvky v kyberprostoru a ignoruje možné ICT prvky v tzv. „offline-kyberprostoru“. (Bašta, Kolouch a kol., 2019) Na základě analýzy těchto definic je možné vymezit kybernetickou bezpečnost jako:

*„Souhrn právních, organizačních, technických a vzdělávacích prostředků, které směřují k zajištění ochrany počítačových systémů a dalších prvků ICT, aplikací, dat a uživatelů.“* (Bašta, Kolouch a kol., 2019, 44)

Tato definice se zdá být nejvhodnější, jelikož se zaměřuje na všechny informační systémy, včetně jejich prvků a uživatelů, které jsou součástí systému. Nutno podotknout, že kybernetická bezpečnost je realizována nejen uvnitř kybernetického prostoru, ale také mimo něj, tudíž nejen v elektronické podobě. Patří sem např. ústní přenos informací účastníků, kteří jsou součástí kybernetického systému. (Bašta, Kolouch a kol., 2019)

## 1.3 Kyberprostor

První síťové propojení čtyř univerzálních počítačů bylo realizováno v roce 1968, kdy vznikla první síť ARPANET. V té době nebyl na kybernetickou bezpečnost kladen důraz tak jako dnes, protože nikdo nepředpokládal obrovský rozvoj síťových technologií. Na základě tohoto rychlého, neočekávaného pokroku a nedůrazu na její bezpečnost, se staly slabiny těchto technologií cílem nelegálních aktivit. (Jirovský, 2007)

Kyberprostor obsahuje prvky informačních a komunikačních technologií, které vytvářejí celosvětovou, globální počítačovou síť pomocí TCP/IP protokolu, a jednotlivě připojené počítačové systémy, které na síť interagují. Stává se tak dynamickým, měnícím a vyvíjejícím se systémem závislým na hardwaru, který je prakticky neomezený. (Bašta, Kolouch a kol., 2019)

Aby bylo možné věnovat se problematice kybernetické bezpečnosti, je nutné si toto tzv. „hrací pole“, zvané kyberprostor, kde se odehrávají „útočné a obranné“ akce, definovat. Oxford

dictionary (2021a) definuje kyberprostor jako *„pomyslné prostředí, ve kterém probíhá komunikace přes počítačové sítě“.* Avšak tato definice nedefinuje kyberprostor tak, aby bylo možné pochopit jeho komplexnost prostředí.

Legislativní definice podle §2 odst. 2 v Zákoně o kybernetické bezpečnosti (181/2014 Sb.) uvádí *„kybernetickým prostorem je digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.“*

Kyberprostor se dělí do tří základních vrstev. Podle dokumentu Cyberspace Operation: Concept Capability Plan 2016-2028 se dělí na vrstvu (The United States Army, 2010):

- fyzickou,
- logickou,
- sociální.

**Fyzická** vrstva zahrnuje fyzické síťové komponenty, kterými je myšlena infrastruktura v podobě kabelů, routerů, switche, řídících prvků sítě a další zařízení, která jsou umístěna na přesném místě ve fyzickém světě. (Bašta, Kolouch a kol, 2019)

**Logická** vrstva zahrnuje logické síťové komponenty. *„Myšlena jsou logická propojení mezi síťovými uzly. Ta jsou realizována prostřednictvím síťových komunikačních protokolů. Uzly mohou být počítače, telefony a další síťová zařízení.“* (Bašta, Kolouch a kol, 2019, 37)

**Sociální** vrstva zahrnuje komponenty nazývané jako „kyberosobnost“ a osobnost. Pojmem kyberosobnost je myšlena komponenta, která může identifikovat samotnou osobnost pomocí e-mailové adresy, IP adresy, telefonního čísla atd. Osobností jsou myšleny skutečné osoby připojené k síti. Každá osoba dnes může mít více kyberosobností, např. má více založených e-mailových účtů, používá více zařízení. (Bašta, Kolouch a kol., 2019)

Kyberprostor se v prostředí internetu rozlišuje podle dostupnosti, dohledatelnosti a přístupu běžného uživatele na (Kolb, 2020):

- surface web,
- deep web,
- dark web.

**Surface Web** se nazývá tzv. „špička ledovce“, jelikož běžný uživatel připojený k síti může dohledat pouze 5 % obsahu celého internetu pomocí indexu vyhledávacího okna. (Kolb, 2020)

**Deep Web** představuje zbylých 95 % obsahu na internetu, kam se běžný uživatel nedokáže pomocí běžného vyhledávacího indexu dostat. Zde je potřeba speciálního hesla. Obsah tohoto webu je předmětem vyšetřování zpravodajství z otevřených zdrojů. (Kolb, 2020)

**Dark Web** představuje nejhlubší vrstvu internetu a byl vždy spojován s nelegálními aktivitami. Nejčastěji s prodejem zbraní, obchodováním s lidmi či obchodováním s drogami. Pro jeho přístup je zapotřebí žádoucí software nebo jejich kombinace. Dark web je označován jako samostatná vrstva, ale je brán spíše jako podvrstva Deep webu. (Kolb, 2020)

## 1.4 Kybernetické útoky

Kybernetické útoky se řadí mezi nejzávažnější rizika, jelikož dnes mají veliký potenciál způsobit vysoké škody v nepoměru s náklady, které jsou potřeba pro jejich realizaci. Uvádí se, že škody při kybernetickém útoku mohou být i vyšší nežli škody přírodní katastrofy či teroristického útoku, jelikož mohou vyřadit kritickou infrastrukturu, na které je společnost závislá. (Šulc, 2018)

Potenciál těchto útoků v dnešní době nadále roste s každým dalším zařízení, které se připojí na internet, a tak se i zvyšuje počet potencionálních útočníků a obětí. S růstem počtu zařízení roste různorodost a složitost těchto zařízení, rychlost a objem přenosu dat. Jediné, co neroste, dokonce i klesá, protože počítač používají dnes běžní uživatelé jako pracovní stanici, je bezpečnostní povědomí. (Šulc, 2018)

Kybernetický útok se definuje jako: *„útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků.“* (Jirásek a kol., 2013, 59) Tato definice se zužuje pouze na poškození IT a získání informací a ignoruje rozmanitost negativních aktivit v kyberprostoru.

Na základě nedostatku této definice, se kybernetický útok definuje jako: *„jakékoliv úmyslné jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby.“* (Bašta, Kolouch a kol., 2019, 82)

Útočníci provádí útoky pomocí programových nebo hardwarových nástrojů. S vývojem ICT se nástroje neustále zdokonalují a pestrost útoků se zvyšuje. Útoky probíhají cíleně nebo plošně.

V případě **plošného útoku** se útočníci snaží proniknout do systému a využít ho co nejjednodušším, nejrychlejším a nejlacinějším způsobem. Doufají, že ve velkém počtu připojených zařízení se najdou taková, která nejsou dostatečně zabezpečena. Předmětem plošného útoku je získání přihlašovacích údajů do např. internetového bankovnictví, platebních systémů, elektronické pošty, nebo jakéhokoliv systému, který obsahuje osobní údaje. Je častější než cílené útoky. Nejčastější příklady plošného útoku jsou phishing a spam. (Šulc, 2018)

V případě **cíleného útoku** se útočníci snaží nalézt systémy s největší zranitelností, aby je mohli využít. Při proniknutí do systému ho útočníci infikují pomocí stroje Remote Access Tool (RAT), kterým systém ovládnou a získají vzdálený přístup. Předmětem cíleného útoku je např. krádež citlivých informací, převod finančních prostředků, znetvoření webových stránek a zneužití infrastruktury pro další útoky. Cílené útoky nejsou tak časté, zato se jim hůře brání, jelikož útočník soustředí veškerou svoji energii na konkrétní oběť. (Šulc, 2018)

Nejčastější typy kybernetických útoků (Kresa, 2018):

- malware,
- phishing,
- SQL Injection a Cross-site scripting (dále jen SQL a XSS),
- Denial of Services (dále jen DoS),
- Man in the Middle a Hijacking.

**Malware** je škodlivý software, jehož cílem je proniknout do zařízení uživatele, kde jeho činností může dojít ztrátě dat, získání přístupu k účtům či úplnému převzetí kontroly nad zařízením. Způsobů, kterým se malware dostane do zařízení, je spousty, ale nejčastěji se tak děje samotnou aktivitou oběti, která klikne na podezřelý odkaz, nebo si nakažený soubor stáhne. (Kresa, 2018)

Malware je obecný název pro podmnožinu jednotlivých škodlivých softwarů, které malware obsahuje. Jsou to např. trojanizované aplikace, virus, marcovirus, worm (červ), trojan horse (trojský kůň), spyware, scareware, ransomware, adware atd. Dalšími kybernetickými útoky jsou např. backdoors, skenery, sniffery, rootkitty, debugerry atd. a s dalším vývojem informační a komunikační technologie přibývají další a dokonalejší útoky. Přesto, že se útoky od sebe liší, probíhají stejnými, po sobě jdoucími fázemi, jak je uvedeno v následujícím obrázku č. 2.


Obrázek 2 – Fáze kybernetického útoku

*Zdroj: Vlastní zpracování dle Axians (2021)*

**Phishing**, do češtiny přeloženo jako „rybaření“, je metoda, jak dostat škodlivý kód do koncových zařízení nebo získat citlivé informace pomocí podvodných e-mailů. Tyto e-maily obsahují odkaz či přílohu, kdy při jejím otevření dojde k nakažení zařízení, nebo přesměrování na podvodné stránky. V dnešní době mají problém rozpoznat phishingové e-maily od těch legitimních i samotní experti. (Šulc, 2018)

Pomocí **SQL** se útočníci snaží dostat do databází s největší zranitelností, způsobenou špatným vývojem databáze samotnými vývojáři. Nejčastěji spadají pod útok databáze, které obsahují citlivá data a osobní údaje uživatelů. **XSS** funguje na podobném principu, s rozdílem, že napadají webové stránky, pomocí kterých se snaží dostat ke koncovým uživatelům. (Kresa, 2018)

**DoS**, česky odepření služby, je takový útok, který zabraňuje ve fungování prvků informačních a komunikačních infrastruktur. Dočasně nebo trvale zabraňuje přístupu k určitým službám oprávněných uživatelů. Cílem je intenzivně klást na službu tolik legitimních požadavků, až se úplně zahltí a přestane fungovat. Rozlišuje se útok DoS a DDoS podle počtu počítačů, ze kterých útok pochází. (Smejkal, 2018)

**Man in the middle (MIMT)** útok používají útočníci, aby se stali „člověkem uprostřed“ mezi adresáty soukromé konverzace bez toho, aniž by si toho obě strany všimly. Poté může útočník nahlížet do konverzace a libovolně ji upravovat. Pomocí **hijackingu** útočník získá unikátní ID oběti, kdy se poté může přihlásit do jejich účtů, v podstatě se za ně vydává. (Kresa, 2018)

# 2. Řízení kybernetické bezpečnosti

*„K řízení informační bezpečnosti lze přistoupit různými způsoby. Zpravidla se ale začíná jmenováním osoby, která bude za řízení informační bezpečnosti odpovědná, a dále pak zavedením základních bezpečnostních opatření organizační a technické povahy. Následně by se mělo pokračovat analýzou rizik a návrhem vhodného způsobu jejich zvládání.* (Šulc, 2018, 86)

Následná opatření by se měla pravidelně prověřovat a vyhodnocovat a v případě včas reagovat na nesoulady s jejími požadavky. Tohoto postupu by se měla držet každá firma bez ohledu na to, v jakém odvětví podniká, jaký je její předmět podnikání, a jaká je její velikost. (Šulc, 2018)

Podle doporučeného postupu s řízením kybernetické bezpečnosti Evropského parlamentu a Rady na základě směrnice ISO/IEC 27002 by se mělo postupovat následovně (Šulc, 2018, 87-88):

- **stanovit rozsah a hranice ISMS** a kde bude zaváděno,
- **definovat metodiku hodnocení rizik**,
- **provést analýzu rizik**, identifikovat a kvantifikovat aktiva, hrozby, zranitelnosti a výsledné riziko,
- **zvolit vhodný způsob zvládání rizik,** vybrat vhodná bezpečnostní opatření a způsob jejich měření,
- **získat souhlas vedení organizace** se způsobem zvládání jednotlivých rizik a zavádění vybraných opatření,
- **formulovat plán zvládaní rizik** vycházející ze souhlasu vedení organizace,
- **zavést bezpečnostní opatření**,
- **zpracovat bezpečnostní politiku, standardy a směrnice**, které vychází z rizik, opatření a cílů organizace,
- **zvyšovat bezpečnostní povědomí** zaměstnanců formou školení, kurzů atd,
- **monitorovat a vyhodnocovat funkčnost zavedených opatření**,
- **opakovat analýzu rizik v pravidelných intervalech**,

- **provádět interní audity**,
- **zavádět nová a účinnější opatření** na základě analýzy rizik, interních auditů,
- **aktualizovat a optimalizovat** jednotlivé postupy.

Hlavními aktéry v kyberprostoru jsou informační systémy (dále jen IS), které jsou tvořeny IA. Tato aktiva jsou zranitelná a podléhají určitým rizikům a hrozbám. Proto se tyto pojmy staly jedním z hlavních témat politiky bezpečnosti v oblasti kybernetické bezpečnosti. Vymezení těchto pojmů a uskutečnění navazujících činností je pro tuto bezpečnost klíčové.

## 2.1 Riziko

**Riziku** podléhají v kyberprostoru jak počítačové systémy, tak uživatelé a aplikace, které je využívají. Jeden z hlavních kroků řízení kybernetické bezpečnosti, je analýza a vyhodnocení rizik. Výkladový slovník kybernetické bezpečnosti definuje riziko jako: *„Nebezpečí, možnost škody, ztráty, nezdaru. Účinek nejistoty na dosažení cílů. Možnost že určitá hrozba využije zranitelnosti aktiva nebo skupiny aktiv a způsobí organizaci škodu.“* (Jirásek a kol., 2013, 85)

Při práci s rizikem se stanovují tři základní otázky (Bašta, Kolouch a spol., 2019):

- Co nežádoucího se může stát? Co může selhat?
- Jaká je pravděpodobnost, že se to stane?
- Jak závažné mohou být dopady?

Analýza rizik, která definuje jednotlivá rizika, jejich pravděpodobnost a dopady, je pro zodpovězení těchto otázek klíčová. Po jejím zhotovení se stanoví stupeň významnosti rizika, který lze vyjádřit následující rovnicí (1), respektive (2) pro portfolio rizik:

$$R = p * X \quad (1) \qquad \text{neboli} \qquad R = \sum p_i * X_i \quad (2)$$

R … riziko

p … pravděpodobnost

X … dopad

Pravděpodobnost výskytu se hodnotí např. v pětibodové stupnici, jak znázorňuje tabulka č. 1.

Tabulka 1 – Pravděpodobnost výskytu rizika

| **Body** | **Pravděpodobnost výskytu** | **Popis výskytu** |
|---|---|---|
| 5 | JISTÉ | Riziko se téměř vždy vyskytne nebo s pravděpodobností 90–100 % |
| 4 | PRAVDĚPODOBNÉ | Riziko se pravděpodobně vyskytne |
| 3 | MOŽNÉ | Riziko se někdy může vyskytnout (např. za specifických podmínek |
| 2 | NEPRAVDĚPODOBNÉ | Riziko se někdy může vyskytnout, ale je to nepravděpodobné |
| 1 | VYLOUČENÉ | Riziko se vyskytne pouze ve výjimečných případech a za specifických podmínek |

*Zdroj: Vlastní zpracování dle Střelec (2015)*

Dopady rizika se hodnotí v pětibodové stupnici, jak znázorňuje tabulka č. 2.

Tabulka 2 – Dopad rizika

| **Body** | **Dopad rizika** | **Popis dopadu** |
|---|---|---|
| 5 | KRIZOVÉ | Situace zásadně omezí nebo ukončí provoz firmy |
| 4 | VÝZNAMNÉ | Situace velmi nebezpečně ovlivňuje vnitřní i vnější chod firmy (vznik významných finančních ztrát) |
| 3 | STŘEDNÍ | Situace nebezpečně ovlivní vnitřní i vnější chod firmy (ztráty vzniknou, ale firma je schopná dále fungovat) |
| 2 | NEVÝZNAMNÉ | Situace omezuje vnitřní chod firmy (dojde k časovým zpožděním) |
| 1 | ZANEDBATELNÉ | Situace sice negativně omezuje chod firmy, ale nezpůsobuje ztráty větší než 5 % |

*Zdroj: Vlastní zpracování dle Střelec (2015)*

*„Analýza rizik je značně obtížná a vyžaduje znalost aktiv, hrozeb a zejména je třeba mít v této oblasti jíž nějaké zkušenosti. Na základě analýzy rizik je možné stanovat opatření za účelem minimalizace nebo úplného odstranění rizik.“* (Bašta, Kolouch a kol., 2019, 71)

## 2.2 Aktiva

*„**Aktivum** je všechno, co má pro subjekt hodnotu, která může být zmenšena působením hrozby.“* (Kodl, Sokol, Smejkal, 2019, 294)

Subjektem se rozumí určitá organizace, která aktiva vlastní. Dělí se na hmotná (např. cenné papíry, nemovitosti) a nehmotná (informace, morálka a kvalifikace zaměstnanců), nebo podle úrovně jednotlivé organizace na primární, podpůrná a technická. Uvědomění si existence aktiv a jejich významu je pro organizace klíčové. (Kodl, Sokol, Smejkal, 2019)

Aktiva se v kybernetické bezpečnosti označují jako informační aktiva (IA), která jsou důležitými prvky tvořící informační systémy (IS), kde jsou uchovávány, zpracovávány a přenášeny data a informace. Právě IA podléhají nejčastěji kybernetickým hrozbám a útokům. K zjištění a lepšímu pochopení, na která aktiva mohou být vedeny útoky, a která aktiva chránit, je nutné zavést tzv. dekompozici systému. (Šulc, 2018)

IS zpravidla tvoří tyto IA (Šulc, 2018, 89-90):

- **koncová zařízení**: (stolní počítače, přenosné počítače, tablety, smartphony),
- **servery**: webové (zpravidla vystaveny do internetu nebo intranetu), aplikační (zde probíhá zpracování zadaných dat), databázové (zde jsou uložena data a informace), souborové (zde se nachází adresáře a soubory, dokumenty, tabulky atd.), tiskové (slouží pro tisk),
- **průmyslové systémy** (slouží k řízení výroby): SCADA, roboti (hardware i software),
- **pasivní a aktivní síťové prvky**: (switche, routery, kabely),
- **zabezpečovací systémy**: (kamerové systémy, CCTV, čidla),
- **IoT** (internet věcí): (bíla elektronika, televize, hodinky, termostatické hlavice, auta, kardiostimulátory),
- **prostory**: (společné prostory, serverové místnosti, technické místnosti nacházejí se zde aktivní i pasivní prvky),
- **zálohy**: (zálohovací servery, NAS, SAN, cloud),
- **dokumentace**: (v elektronické a papírové podobě),
- **lidé**: (uživatelé, správci, vývojáři, dodavatelé).

V dnešní době existují i organizace, které mají zavedená bezpečnostní opatření na vysoké úrovni, a přesto se stávají oběťmi cílených útoků. ICT už je natolik rozvinutá, že útočníci mají schopnosti zneužít skutečnosti, že zaměstnanci vlastní chytrá zařízení, kterými se připojují do podnikové sítě, a prostřednictvím těchto zařízení provést útok. (Šulc, 2018)

## 2.3 Hrozby a zranitelnost

Aby bylo možné čelit **hrozbám**, kterým je vystaven každý IS, je nutné nejdříve jednotlivé hrozby identifikovat. V kyberprostoru je možné hovořit o tzv. obecných neboli generických hrozbách, jelikož všechny IS většinou podléhají stejným hrozbám. (Šulc, 2018)

*„Hrozbu můžeme definovat jako náhodnou nebo úmyslně vyvolanou událost, která může mít negativní dopad na důvěrnost, integritu a dostupnost aktiv.“* (Šulc, 2018, 90)

Hrozby se dělí podle úmyslu a umístění zdroje hrozby.

Podle úmyslu (Šulc, 2018, 91):

- náhodné hrozby – hrozby, které byly způsobeny náhodně a bez úmyslu,
- úmyslné hrozby – hrozby, které byly způsobeny úmyslně.

Podle zdroje (Šulc, 2018, 91):

- vnitřní hrozby – zdroj hrozby se nachází uvnitř organizace,
- vnější hrozby – zdroj hrozby se nachází mimo organizaci.

Na základě těchto dělení a jejich kombinací, se vytvoří matice základních typů hrozeb, kterou lze pozorovat v následující tabulce č. 3.

Tabulka 3 – Matice základních typů hrozeb

| **Hrozby** | **Náhodné** | **Úmyslné** |
|---|---|---|
| **Externí** | přírodního původu | hacking |
| **Interní** | technické selhání | sabotáž |

*Zdroj: Vlastní zpracování dle Šulc (2018)*

Pro stanovení míry hrozby se musí zohlednit následující faktory (Šulc, 2018, 91-92):

- Četnost výskytu – ze statistik, průzkumů kybernetické bezpečnosti a vlastní evidence bezpečnostních incidentů se stanoví pravděpodobnost výskytu hrozby.

- Příležitost – např. když denně přichází zaměstnanec s přístupem do systému, který není monitorován, ke styku s důvěrnými informacemi, je větší pravděpodobnost, že přístupu zneužije a dojde k úniku informací.
- Motiv – větší pravděpodobnost realizace hrozby je v době krize, fúzování, outsourcingu, kdy mají útočníci větší motiv.
- Schopnosti – čím větší speciální znalosti, schopnosti a dovednosti, tím větší pravděpodobnost realizace hrozby.
- Peníze – pravděpodobnost hrozby je vyšší, čím nižší jsou náklady na její realizaci.
- Vybavení – čím nižší nároky na hardware a software vybavení útočníka, tím vyšší pravděpodobnost hrozby.
- Čas – čím kratší čas je potřeba na realizaci hrozby, tím vyšší je její pravděpodobnost, jelikož když je útok proveden rychle, je možné, že si přípravy a samotného útoku nikdo nevšimne.
- Atraktivitu aktiva – pravděpodobnost hrozby se zvyšuje s atraktivností aktiva. Např. u defacementu (průnik na webové stránky a změna jejich obsahu či vizuálního vzhledu) si útočník vybere systém, který je dosti frekventovaný a znám.
- Počet osob – čím více osob přijde do styku s aktivem, tím větší je pravděpodobnost, že bude hrozba realizována.

Při počátku rozvoje internetu, kde působili spíše osamocení hackeři, bylo stanovení míry pravděpodobnosti hrozby o dost jednodušší nežli dnes. Osamocení hackeři totiž nedisponovali příležitostmi, schopnostmi, ani potřebnými zdroji, zvlášť u cenných aktiv. Proto se dalo hrozbu označit jako málo pravděpodobnou. V dnešní době z důvodu zformování virtuálních organizovaných skupin, které stojí za velkou většinu útoků a operující celosvětově, není stanovení výsledné míry hrozby tak triviální.

**Zranitelnost** je nežádoucí vlastnost označující nedostatek či slabinu aktiva, softwaru, hardwaru a lidí v IS, které je využito jednou nebo více hrozbami. V oblasti kybernetické bezpečnosti se rozeznávají zranitelnosti známé a neznámé, které se zaměřují na software. U známých zranitelností záleží, zda vydavatel nebo správce softwaru jednotlivé zranitelnosti identifikoval a vydal aktualizaci, která je ošetří. Podle toho, zda jsou nebo nejsou ošetřeny, se dělí zranitelnosti na opravené a neopravené. U neznámých zranitelností je významné, kterým

subjektem jsou objeveny. Zda jsou objeveny vydavatelem, osobou zabývající se penetračním testováním, bezpečnostním analytikem či dokonce samotným útočníkem. (Bašta, Kolouch a kol., 2019)

Zranitelnost objevená útočníkem se nazývá tzv. zranitelnost nultého dne. Tuto zranitelnost útočníci záměrně vyhledávají, a to nejčastěji používáním aplikace takovým způsobem, který vývojáři nepředpokládali. Při úspěšném nalezení následně zranitelnost podléhá útoku tzv. zero-day attack. Jedná se o takový útok, který zneužívá zranitelnosti v softwaru, která není známá samotným vydavatelem či správcem, a na kterou dosud nebyla vydaná aktualizace. (Brooks, Craig a kol., 2018)

## 2.4 Základní bezpečnostní opatření

S pojmy bezpečnost a riziko úzce souvisí také pojem bezpečnostní opatření. Aby bylo možné snižovat či eliminovat rizika, je nutností nacházet a implementovat bezpečnostní opatření k zajištění větší bezpečnosti objektu.

Obecná definice pro bezpečnostní opatření zní: *„Bezpečnostní opatření jsou opatření vázaná na prostředky odstraňující nebezpečí nebo snižující riziko“* (Hanáková, Král, Malý, 2010)

V oblasti kybernetické bezpečnosti definuje Bašta, Kolouch a kol. (2019, 241) bezpečnostní opatření jako: *„souhrn úkonů jejich cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítích elektronických komunikací v kybernetickém prostoru.“*

Povinnost, která se vztahuje na zavádění a provádění bezpečnostních opatření, obecně neplatí pro všechny orgány. Tato bezpečnostní opatření musí provádět orgány uvedené v zákoně o kybernetické bezpečnosti §3 písm. c) až f) a současně o nich vést bezpečnostní dokumentaci.

Dle zákona o kybernetické bezpečnosti se bezpečnostní opatření dělí na organizační a technická. Do **organizačních opatření** patří *„různé politiky, standardy, procedury a směrnice, které definují závazná pravidla a postupy, dále sem patří aktivity školení v oblasti informační bezpečnosti.“* (Šulc, 2018, 101). Mezi **technická opatření** se řadí *„kontrola pohybu osob ve střežených prostorách, zabránění průniku neoprávněných osob do těchto prostor a opatření týkající se fyzického a logického řízení přístupu informačním zdrojům pomocí identifikace, autentizace, autorizace.“* (Šulc, 2018, 101) Výčet jednotlivých organizačních i technických opatření je uveden v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti §5 odst. 2) a 3).

# 3. Ukotvení kybernetiky v bezpečnostních dokumentech České republiky

V České republice (dále jen ČR) často chybělo bezpečnostní podvědomí vlastníků, manažerů či vedoucích pracovníků organizací. Zvláště v malých podnicích, které si nepřipouštěly, že by se mohly stát cílem útoku. Byly přesvědčeni, s ohledem na velikost jejich firmy a náročnosti provedení útoku, že nejsou pro útočníka dosti zajímaví, tudíž pravděpodobnost útoku je velice nízká. ČR, kromě nedostatečného bezpečnostního povědomí, se potýkala a stále potýká s nedostatkem bezpečnostních odborníků, kteří by dokázali provést kvalitní analýzu rizik a poté zavést organizační a technické opatření. (Šulc, 2018)

Takto se přistupovalo k řízení informační bezpečnosti do roku 2014, který byl pro ČR do počtu a objemu škod přelomový. Do roku 2014 se ČR dlouho kybernetickým útokům vyhýbala, než se začlenila mezi státy, na které nadále mohou být kybernetické útoky vedeny a přestala být vnímána jako tzv. testovací polygon. Na zhoršující situaci česká legislativa reagovala vydáním zákona č. 181/2014 Sb., o kybernetické bezpečnosti a vyhlášky č. 316/2014 Sb., o bezpečnostních opatření. (Šulc, 2018)

## 3.1 Bezpečnostní dokumenty ČR

Kybernetickou bezpečností a její problematikou se ČR zabývala už v roce 2000, kdy ministerstvo vnitra České republiky (dále jen MVČR) publikovalo *„**koncepci boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření**“* Náplní této koncepce je snaha o potírání trestné činnosti v oboru informačních technologií a vytvoření příznivých podmínek pro jejich řešení. (Bašta, Kolouch a kol., 2019)

Následující dokument *„**Státní informační a komunikační e-Česko 2006**“* byl představen v březnu roku 2004. Náplní tohoto dokumentu byla definice čtyř základních oblastí, které byly pro stát prioritní – dostupné a bezpečné komunikační služby, informační vzdělanost, moderní veřejné služby online a dynamické prostředí pro elektronické podnikání. (Bašta, Kolouch a kol., 2019) Z těchto priorit bylo hlavním cílem do konce roku 2004 vytvořit CERT tým a Národní strategii informační bezpečnosti. (Bašta, Kolouch a kol., 2019)

V návaznosti na tento dokument vznikla v roce 2005 první *„**Národní strategie informační bezpečnosti**“*. Ve stejném roce vláda schválila *„**Národní akční plán boje proti terorismu**“*, který řeší koncepci z roku 2000. Na jejím základě byl vydán MVČR dokument *„**Aktuální úroveň zajištění kybernetické bezpečnosti České republiky**“*. Tento dokument byl opakovaně

vracen k jeho dopracování, až byl nakonec v roce 2008 nahrazen *„**Koncepcí boje proti organizovanému zločinu**“*. Tato koncepce totiž lépe odrážela nárůst kybernetických hrozeb a útoků. (Bašta, Kolouch a kol., 2019)

V roce 2011, kdy byl Národní bezpečnostní úřad (dále jen NBÚ) zvolen jako gestor kybernetické bezpečnosti, který měl za úkol aktualizovat doposud vydané Národní strategie a akční plány, vznikla *„**Strategie pro oblast kybernetické bezpečnosti České republiky 2012-2015**“*. Jedním z hlavních cílů této strategie bylo vytvořit legislativní rámec pro kybernetickou bezpečnost ČR. Ze strategie vychází akční plán, který má za úkol rozpracovat jednotlivé strategické cíle a určit subjekty odpovědné za jejich řešení. Plnění cílů vycházejících ze strategie a akčního plánu se následně vyhodnocuje v ročních intervalech. (Doucek, Konečný, Novák, 2019)

Nejzásadnější dokument v problematice kybernetické bezpečnosti, který změnil bezpečnostní povědomí v ČR, vychází z výše uvedené strategie, a je jím **Zákon č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen ZoKB)**. *„Cílem zákona bylo vytvořit zákonné postavení státní instituce, která bude odpovědná za zajišťování kybernetické bezpečnosti státu a oprávněná k regulaci klíčových subjektů.“* (Doucek, Konečný, Novák, 2019, 59) První návrh tohoto zákona předložil NBÚ v roce 2013. ZoKB nabyl účinnosti k 1. lednu 2015 Současně s ním vyšly v platnost následující vyhlášky (Bašta, Kolouch a kol., 2019, 92):

- vyhláška č. 316/2014, o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti,
- vyhláška č. 317/2014, kterou se stanoví významné informační systémy a jejich určující kritéria,
- vyhláška č. 315/2014, novela nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

Jedním z podnětů k vytvoření ZoKB byly požadavky Severoatlantické aliance (dále jen NATO) a Evropské unie (dále jen EU) a závazky ČR vůči těmto institucím. NATO intenzivně vstoupilo do problematiky kybernetické bezpečnosti v roce 2007 v reakci na masivní nárůst kybernetických útoků v Estonsku. NATO, zřízením tzv. **Cooperative Cyber Defence Centre of Excellence** v roce 2010 a schválením **Strategické koncepce NATO Policy on Cyber Defence** v roce 2011, se snaží o rozvoj kolektivní kybernetické obrany. (Bokša, 2018, Jiráček, 2021)

EU naopak usiluje o sblížení právních úprav členských států pro efektivní řešení problematiky kybernetické bezpečnosti pomocí směrnic, nařízení, dokumentů a norem. Mezi nejvýznamnější dokumenty z této oblasti patří *„**směrnice Evropského parlamentu a Rady** (např. 91/250/EHS o právní ochraně počítačových programů; 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systému v Unii), **nařízení Evropského parlamentu a Rady** (např. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu; 679/2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů), **rozhodnutí Rady** (např. 92/242/EHS o bezpečnosti IS), nebo **mezinárodní normy** (např. ISMS řady ISO/IEC 27000).“* (Bašta, Kolouch a kol., 2019, 96-97)

ZoKB, od jeho vzniku, prošel řadou menších úprav a novelizací. Za jednu z největších novelizací se považuje novelizace č. 205/2017 Sb. na základě *„**Směrnice Evropského parlamentu a Rady EU 2016/1148**“*, která zapříčinila vznik Národního úřadu pro kybernetickou a informační bezpečnost. (Bašta, Kolouch a kol., 2019)

Aktualizací předešlé strategie a akčního plánu, vláda roku 2015 schválila usnesení nové *„**Národní strategie kybernetické bezpečnosti České republiky 2015-2020**“* a navazujícího Akčního plánu. *„Oproti minulé strategii, se kvalitativně přesouvá od budování základních kapacit nezbytných pro zajištění elementární míry kybernetické bezpečnosti směrem k jejímu dalšímu hlubšímu a pokročilému zajišťování.“* (Doucek, Konečný, Novák, 2019, 63-64) Celkovým cílem této strategie je zvýšit bezpečnostní povědomí, a to jak u dotčených subjektů, tak i běžných uživatelů. V současnosti se problematice kybernetické bezpečnosti zabývá *„**Národní strategie kybernetické bezpečnosti České republiky 2021-2025**“* a její akční plán. Její hlavní strategické cíle vymezuje následující tabulka č. 4.

Tabulka 4 - Strategické cíle národní strategie kybernetické bezpečnosti 2021-2025

| STRATEGICKÉ CÍLE | | |
|---|---|---|
| **Sebevědomě v kyberprostoru** | **Silná a spolehlivá spojenectví** | **Odolná společnost 4.0** |
| • Celonárodní přístup s důrazem na sdílení informací, koordinaci a spolupráci<br>• Rozvoj schopností a kapacit státu v kybernetické bezpečnosti<br>• Posílení zabezpečení a odolnosti infrastruktury<br>• Rozvoj schopností predikce, detekce a agilní reakce na kybernetický útok<br>• Účinná strategická komunikace<br>• Prevence a potírání kybernetické kriminality | • Efektivní mezinárodní spolupráce<br>• Tvorba spojenců<br>• Prosazování zájmů ČR v zahraničí<br>• Vytváření dialogu v mezinárodním prostředí<br>• Podpora otevřeného a bezpečného chování v kyberprostoru<br>• Export know-how | • Zajištění bezpečnosti digitalizace státní správy / eGovernmentu<br>• Kvalitní systém vzdělávání<br>• Osvětová činnost<br>• Spolupráce státu, soukromé sféry a občanů<br>• Vytváření expertní základny |

*Zdroj: vlastní zpracování dle NÚKIB (2021a)*

## 3.2 Národní úřad pro kybernetickou a informační bezpečnost

Národní úřad pro kybernetickou a informační bezpečnost (dále jen NÚKIB) *„je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany.* (NÚKIB, 2021b) NÚKIB byl zřízen 1. srpna 2017 a převzal veškerá práva a povinnosti Národního bezpečnostního úřadu (NBÚ), které vykonával v oblasti kybernetické bezpečnosti.

NBÚ vznikl 1. srpna 1998. V ČR nebyla instituce, která byla odpovědná za kybernetickou bezpečnost, proto usnesením vlády ČR se dne 19. října 2011 NBÚ stal jednatelem problematiky kybernetické bezpečnosti. Do té doby NBÚ působil pouze jako jednatel problematiky

utajovaných informací. Tato instituce společně s dalšími, jako např. Ministerstvo vnitra, Ministerstvo obrany, byli první, kteří se podíleli na tvorbě ZoKB. Mezi nejvýznamnější úkoly NBÚ spadalo aktualizovat Strategie kybernetické bezpečnosti ČR, aktualizovat Akční plány opatření kybernetické bezpečnosti ČR a být jejich řešitelem, vybudovat Národní centrum kybernetické bezpečnosti a skupinu pro reakci na počítačové hrozby a počítačové bezpečnostní incidenty (dále jen CERT a CSIRT). (Bašta, Kolouch a kol., 2019)

První **CERT** vznikl v USA roku 1988 reakcí na kybernetický útok studenta Roberta Morrisena. Ten se považuje za první útok, který ve velké míře negativně ovlivnil tehdejší internet. Vypuštěním malwaru tzv. červ dokázal vyřadit až 10 % všech připojených zařízení. Účelem CERT je zefektivnit obranu proti kybernetickým útokům, rozpoznání hrozeb, postupy a prostředky, kterými je možné lépe identifikovat pachatele. Z uvedeného incidentu CERT vyvodil, že nejdůležitější je být na takovéto incidenty připraven a spouštět předem definovaný záchranný systém. (Bašta, Kolouch a kol., 2019)

Bezpečnostní týmy **CERT** a **CSIRT** je možné chápat jako jeden a ten samý typ a to: *„tým, který je ve svém jasné definovaném poli působnosti zodpovědný za řešení bezpečnostních incidentů, z pohledu uživatelů nebo jiných týmů tedy místi, na kterém se mohou obrátit se zjištěným bezpečnostním incidentem nebo i jen podezřením.“* (Kropáčová, 2013)

CERT/CSIRT vznikají na základě rozhodnutí jednotlivých organizací. Při rozhodnutí vytvoření týmu, musí mít organizace jasně definované čeho chce vytvořením dosáhnout a jakou bude mít tým roli. Každý tým má jasně vymezené pole působnosti a při práci čerpají ze svých zkušeností, postupů ověřených v praxi a spoluprací s ostatními CERT/CSIRT týmy. Polem působnosti rozumíme roli týmu a za co zodpovídá, a proto se dělí do těchto typů (Bašta, Kolouch a kol.,2019, 509):

- interní – slouží a zodpovídá za konkrétní síť,
- koordinační – hlavní náplní je koordinovat při řešení bezpečnostních incidentů,
- vendor – řeší bezpečnostní incidenty konkrétních produktů (SW),
- národní, vládní – speciální případy interních a koordinačních týmů, pole působnosti závisí na legislativě dané země.

**Národní CERT/CSIRT** mají za úkol koordinovat postup k vyřešení kybernetických incidentů, jelikož nedisponují fyzickou infrastrukturou, tudíž nemají možnost přímého zásahu. Obvykle, k vyřešení incidentů, zprostředkovávají kontakt mezi napadeným a řešitelem. Další funkcí národních CERT/CSIRT týmů je vzdělávat a spolupracovat směrem k veřejnosti v rámci

internetové infrastruktury a pomáhat vytvářet další týmy. První národní CSIRT tým v ČR byl zřízen v prosinci roku 2010 společností CZ.NIC. (Bašta, Kolouch a kol., 2019)

*„**Vládní CERT/CSIRT** se zaměřuje na oblast státní správy a samosprávy a na řešení incidentů, které ohrožují bezpečnost státu a jeho služeb.“* (Kropáčová, 2013) Na rozdíl od národních CERT/CSIRT týmů, při řešení problému, mají možnost přímého zásahu. Jejich působnost podporuje legislativa. První vládní CERT tým v ČR byl zřízen roku 2012. (Bašta, Kolouch a kol., 2019)

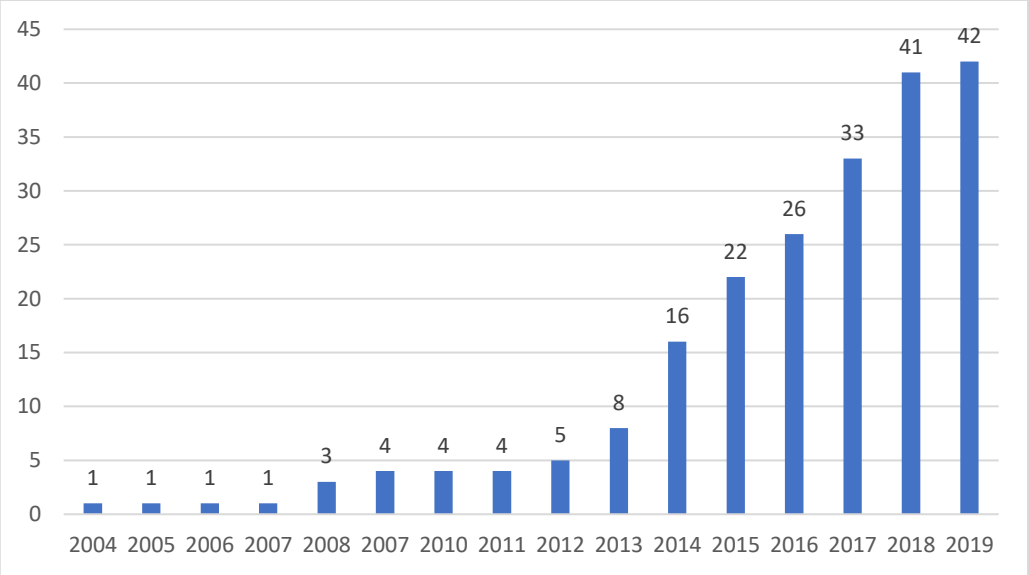
V současné době existuje na světě okolo 430 CERT/CSIRT týmů. Česká republika je označována jako tzv. „světová velmoc“, jelikož má zřízeno největší počet těchto týmů, a to 53. (Trusted Introducer, 2021) Světovou velmoc ČR znázorňuje také následující tabulka č. 5 spolu s dalšími konkurujícími státy, kteří mají více jak 20 bezpečnostních týmů.

Tabulka 5 - Prvních pět států s největším počtem bezpečnostních týmů CERT/CSIRT

| Pořadí | Stát | Počet bezpečnostních týmů |
|---|---|---|
| 1. | Česká republika | 53 |
| 2. | Francie | 36 |
| 3. | Španělsko | 35 |
| 4. | Německo | 31 |
| 5. | Polsko | 29 |

*Zdroj: Vlastní zpracování dle Trusted Introducer (2021)*

V ČR došlo k největšímu rozvoji CERT/CSIRT týmů po roce 2013, kdy ČR čelila sérii DDoS útoků na veřejné služby. Toto tvrzení podtrhává následující obrázek č. 3.




Obrázek 3 - Počet bezpečnostních týmů v ČR v letech 2004-2019

*Zdroj: vlastní zpracování dle Průša, Průšová (2019)*

Z obrázku č. 3 je zřejmé, že rok 2014 byl pro vznik bezpečnostních týmů zlomový. V tomto roce přibyl dvojnásobek těchto týmů. Jedním z dalších impulzů pro zřízení týmů bylo přijetí ZoKB. Na základě těchto podnětů se i zvýšilo bezpečnostní povědomí v organizacích.

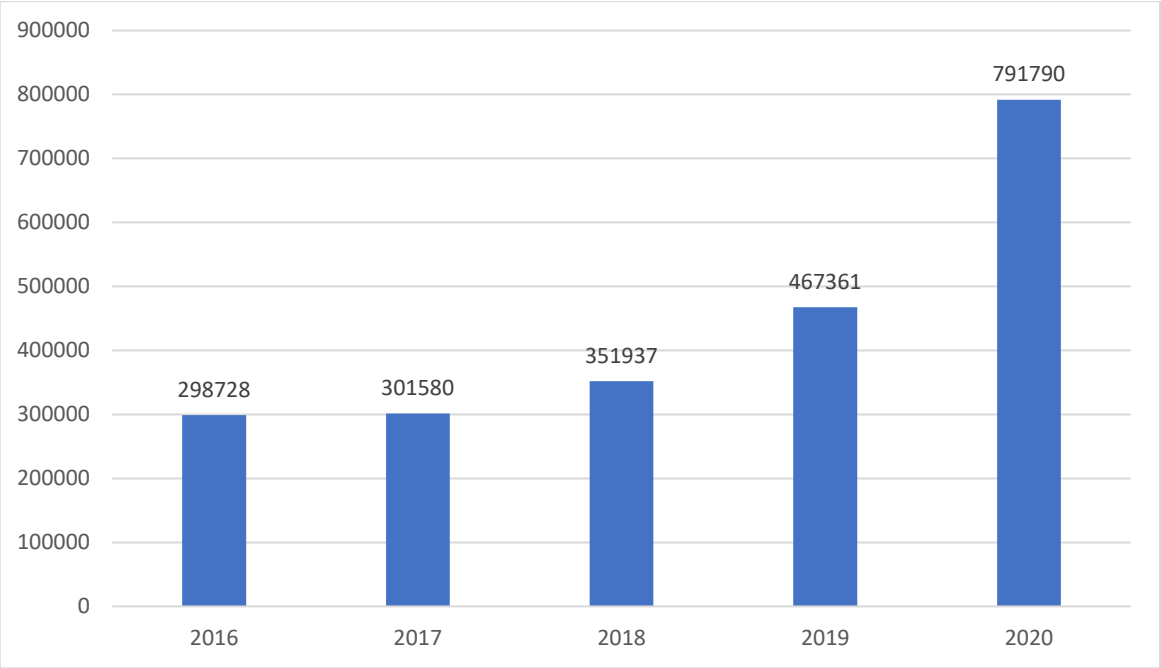
# 4. Analýza vývoje kybernetické bezpečnosti

Následující kapitola se bude zabývat analýzou kybernetické bezpečnosti na světové úrovni a v rámci ČR. V první části budou rozebírány kybernetické útoky v celosvětovém a evropském měřítku. Hlavním zdrojem pro tento rozbor jsou Centrum pro stížnosti na internetovou kriminalitu a Eurostat. Další část analýzy rozebírá stav kybernetické bezpečnosti v ČR. V ČR se problematice kybernetické bezpečnosti věnuje NÚKIB s pomocí CERT/CSIRT týmů, jejichž výroční zprávy jsou zdrojem pro tento rozbor. Výstupy z jednotlivých rozborů jsou prezentovány pomocí tabulek a grafů.

## 4.1 Analýza kybernetických útoků ve světě

V současní době je technologie na takové úrovni, že se na ni dnešní společnost čím dál více upíná a soustřeďuje většinu svých aktivit a povinností do kyberprostoru. Právě proto se útočníci stále častěji zaměřují na odvětví kybernetické kriminality z čehož se kybernetické útoky stávají světovým problémem. Působením v tomto odvětví mohou způsobit vyšší škody nežli dříve. Právě vývoj technologií nabízí útočníkům nové příležitosti k realizaci kybernetických útoků. Člověk totiž může vlastnit více zařízení na které může být veden tento útok. Jedná se o chytrý telefon, tablet, notebook, stolní počítač, a chytrou domácnost, která se stává trendem dnešní doby. V důsledku toho kybernetických útoků stále více přibývá a důkazem toho bude i následující část analýzy.

Následující část analýzy vychází z dat Centra pro stížnosti na internetovou kriminalitu neboli Internet Crime Complaint Center (dále jen IC3). Tento úřad poskytuje veřejnosti spolehlivý a pohodlný mechanismus, kterým mohou nahlašovat kybernetické útoky. Data, která IC3 nashromáždí využívá mimo jiné Federální úřad pro vyšetřování (FBI) pro jejich vyšetřování. Grafické znázornění útoků nahlášených IC3 je možné sledovat v následujícím obrázku č. 4.



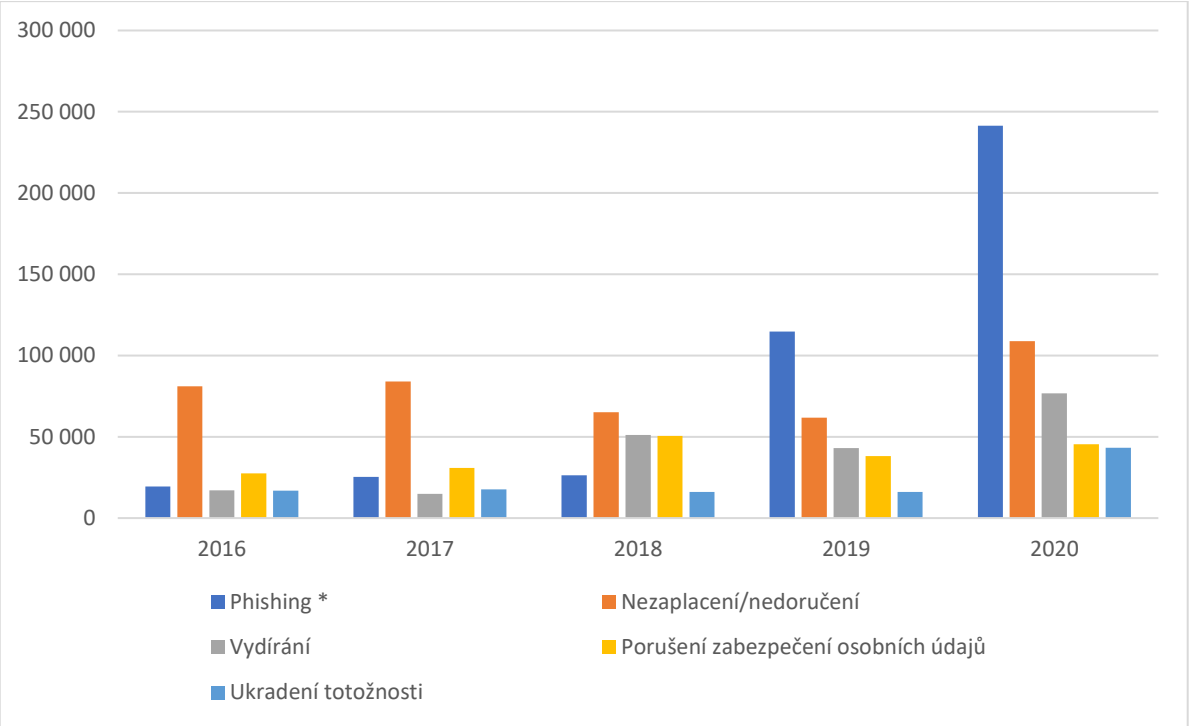

Obrázek 4 - Vývoj kybernetických útoků v letech 2016-2020

*Zdroj: Vlastní zpracování dle Internet Crime Complaint Center (2020)*

Obrázek č. 4 znázorňuje kybernetické útoky a jejich vývoj v posledních 5 letech. Útoky mají rostoucí tendenci. V roce 2016 a 2017 se počet nahlášených útoků pohyboval okolo 300 000 útoků ročně. Větší počty nahlášených útoků, oproti předešlým rokům, byly zaznamenány v letech 2018 a 2019. Největší počet nahlášených útoků zaznamenal rok 2020, a to 791 790. Ve srovnání s rokem 2019 se jednalo téměř o 70% nárůst. Tento nárůst značně souvisí s pandemií Covid-19 a přesunem mnoha aktivit společnosti do kyberprostoru.

Mezi pět nejčastějších útoků zaznamenaných IC3 patří útoky typu phishing, vydírání, ukradení totožnosti, nezaplacení/nedoručení a porušení zabezpečení osobních údajů. Do kategorie phishing spadají také útoky typu vhising, smishing, pharming. Všechny tyto útoku fungují na stejném principu jako phishing s rozdílem toho, že vishing se provádí prostřednictvím telefonních hovorů, kde se útočník představí jménem ověřené společnosti a vyžaduje osobní či bankovní údaje, smishing je prováděn prostřednictvím SMS zpráv a pharming je realizován pomocí falešných bankovních stránek pro získání bankovních údajů.

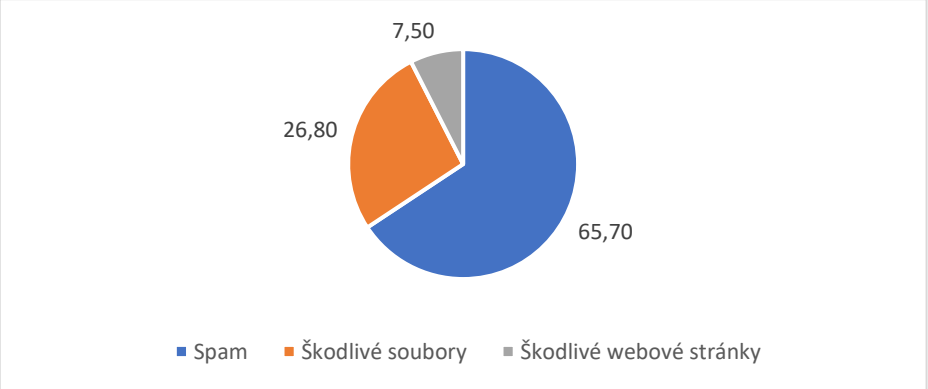
Pod ukradením totožnosti si lze představit situaci, kdy útočník vyzjistí např. přihlašovací údaje Facebooku osoby, na kterou cílí svůj útok a poté se za ní vydává. Nezaplacení je typ útoku, kdy napadená osoba „prodá“ movitou věc útočníkovi za kterou nedostane zaplaceno. Obdobným útokem je nedoručení, kdy napadená osoba za movitou věc zaplatí, ale není ji doručena bez nároku na vrácení peněz. Vývoj těchto pěti útoků je ilustrován v následujícím obrázku č. 5.




Obrázek 5 - Vývoj pěti nejčastějších kybernetických útoků v letech 2016-2020

*Zdroj: Vlastní zpracování dle Internet Crime Complaint Center (2020)*

Z obrázku č. 5 je zřejmé, že počty útoků měly ve všech kategoriích kromě phishingu kolísavý vývoj. V rámci těchto kategorií měl do roku 2019 největší zastoupení útok typu nezaplacení/nedoručení. Naopak útok typu phishing má od roku 2016 rostoucí tendenci. Skokový nárůst byl zaznamenám v letech 2019 a 2020. V roce 2019 bylo nahlášeno více jak čtyřnásobek a v roce 2020 více jak dvojnásobek útoků než v předchozích letech. V roce 2020 zaznamenaly nárůst i ostatní kategorie útoků. Impulzem pro nárůst nahlášených útoků v roce 2020 byla primárně pandemická krize spojená s Covid-19. To, jak se Covid-19 promítl do kybernetických útoků, kterých za první čtvrtletí 2020 přibylo 303 461, znázorňuje následující obrázek č. 6 s jejich procentuální podíl.




Obrázek 6 - Hrozby spojené s Covid-19 v 1. čtvrtletí roku 2020 (v procentech)

*Zdroj: Vlastní zpracování dle Armstrong (2020b)*

Je nutné podotknout, že obrázek č. 6 znázorňuje útoky pouze s tématikou Covid-19 a obsahuje data z tzv. „první vlny“. Největší zastoupení těchto útoků má kategorie spam a to v 199 379 případech. Další kategorií jsou škodlivé soubory obsahující malware. Tyto soubory jsou často součástí e-mailových spamů z předchozí kategorie. V této kategorii bylo nahlášeno 81 315 případů. Kategorie „spam“ a „škodlivý soubor“ jsou rozděleny, protože už samotný spam představuje hrozbu. Nejmenší zastoupení má kategorie škodlivé webové stránky, těch bylo nahlášeno 22 767. Útočníci se snažili využít touhy lidí po informovanosti ohledně této krize. Mnoho e-mailů, údajně od oficiálních organizací, obsahuje aktualizace a doporučení souvisejícím s tímto onemocněním. Následující tabulka demonstruje, na které státy byly nejvíce cíleny útoky typu spam.

Tabulka 6 - Poměr škodlivého spamu na nejvíce napadené země 2020

| | |
|---|---|
| Velká Británie | 20,8 % |
| Francie | 11,5 % |
| Spojené státy americké | 8,2 % |
| Itálie | 5,9 % |
| Belgie | 5,2 % |
| Německo | 5,1 % |
| Indie | 4,9 % |

*Zdroj: Vlastní zpracování dle Armstrong (2020a)*

Z tabulky č. 6 je zřejmé, že největší procento těchto útoků bylo vedeno na Velkou Británii (20,8 %). Mezi další země, na které bylo odesláno již menší procento útoků, se řadí Francie (11,5 %), Spojené státy americké (8,2 %) a Itálie (5,9 %). Dalšími zeměmi jsou Belgie, Německo a Indie, na které byly vedeny útoky s podílem okolo 5 %. V tabulce jsou uvedeny pouze země s více jak 4% podílem.

Kybernetickými útoky v kategorii podvodných e-mailů a podvodných webových stránek se zabývá i následující část analýzy, která je zachycena v tabulkách č. 7 a 8. Tentokrát však bez tématiky Covid-19 a pouze ve státech, které jsou součástí EU. Zdrojem pro tuto analýzu jsou data získaná ze statistického úřadu pro EU neboli z Eurostatu z roku 2019. Tabulka č. 7 obsahuje procentuální vyjádření počtu osob, které v daných zemích obdržely podvodný e-mail. Tabulka č. 8 se věnuje přesměrování podvodné webové stránky. Obě tabulky obsahují výčet prvních pěti pořadí zemí EU a následovně postavení ČR v rámci těchto statistik. V analýze figuruje Velká Británie, jelikož vystoupila z EU až 31. ledna 2020.

Tabulka 7 - Osoby ve věku 16-74 let v zemích EU, které obdržely podvodný e-mail v roce 2019

| Pořadí | Země | Podíl osob |
|---|---|---|
| 1. | Dánsko | 45 % |
| 2. | Francie, Velká Británie, Švédsko | 39 % |
| 3. | Nizozemí | 38 % |
| 4. | Německo, Finsko | 36 % |
| 5. | Rumunsko, Rakousko, Malta | 30 % |
| 10. | Česká republika | 17 % |

*Zdroj: Vlastní zpracování dle Český statistický úřad (2020b)*

Z tabulky č. 7 vyplývá, že největší procento osob, které obdržely podvodný e-mail se nachází v Dánsku. Druhé místo s 39 % sdílí 3 výše uvedené země, stejně tak tomu je i u místa čtvrtého a pátého, všechny uvedené země vždy sdílí stejné procento osob. ČR se nachází na 10. místě se 17% podílem počtu osob. Nejvíce podvodných e-mailů obdržely severské země a země západní Evropy.

Tabulka 8 - Osoby ve věku 16-74 let v zemích EU, které byly přesměrovány na podvodné webové stránky v roce 2019

| Pořadí | Země | Podíl osob |
|---|---|---|
| 1. | Malta | 26 % |
| 2. | Velká Británie | 25 % |
| 3. | Francie | 20 % |
| 4. | Španělsko | 17 % |
| 5. | Švédsko | 16 % |
| 15. | Česká republika, Polsko | 4 % |

*Zdroj: Vlastní zpracování dle Český statistický úřad (2020b)*

U tabulky č. 8 lze vyčíst, že přesměrování na podvodné webové stránky bylo největším problémem na Maltě, a to s podílem až 26 %. O pouhé 1 % za Maltou následovala Velká Británie. ČR se nachází na 15. místě se 4 %. Svoji příčku sdílí s Polskem, které má stejný podíl. Menší podíl už zaznamenaly pouze země Litva, Lotyšsko a Bulharsko. Stejně jako

u podvodných e-mailů, tak i tento typ útoku byl v rámci EU v převážné většině směřován na západní a severské země.

Data, která zobrazuje následující tabulka č. 9, se zaměřují na převážnou většinu evropských zemí. U těchto zemí je možné sledovat podíl počítačů, na které byly vedeny kybernetický útoky za rok 2020. Komparací je tak možné zjistit, které z těchto zemí jsou nejvíce zranitelné proti kybernetickým útokům.

Tabulka 9 – Měsíční podíl počítačů podléhajících kybernetickým útokům v evropských státech v roce 2020

| Země | Počet útoků | Země | Počet útoků |
|---|---|---|---|
| Holandsko | 17,64 % | Velká Británie | 3,82 % |
| Bulharsko | 17,55 % | Německo | 3,61 % |
| Bělorusko | 10,83 % | Estonsko | 3,54 % |
| Ukrajina | 10,35 % | Rakousko | 3,47 % |
| Bosna a Hercegovina | 7,06 % | Slovensko | 3,28 % |
| Litva | 6,40 % | Slovinsko | 3,20 % |
| Rumunsko | 6,24 % | Finsko | 3,02 % |
| Francie | 5,41 % | Česká republika | 2,74 % |
| Maďarsko | 4,83 % | Lucembursko | 2,02 % |
| Chorvatsko | 4,55 % | Belgie | 1,99 % |
| Lotyšsko | 4,49 % | Švédsko | 1,85 % |
| Španělsko | 4,47 % | Island | 1,81 % |
| Řecko | 4,28 % | Švýcarsko | 1,69 % |
| Itálie | 4,19 % | Dánsko | 1,60 % |
| Polsko | 3,99 % | Norsko | 1,38 % |
| Portugalsko | 3,83 % | Irsko | 1,08 % |

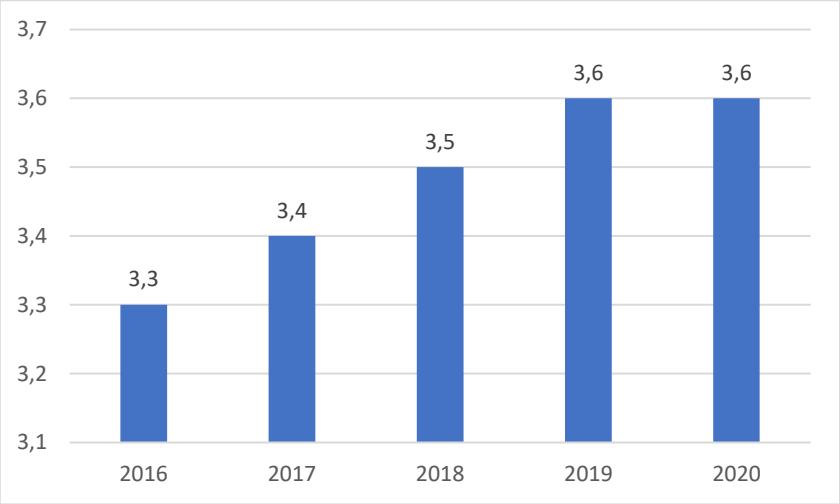
*Zdroj: Vlastní zpracování dle Specops (2020)*

Z tabulky č. 9 vyplývá, že nejzranitelnějšími zeměmi v oblasti kybernetických útoků byly v roce 2020 Nizozemsko a Bulharsko. Tyto země měly podíl vyšší než 17 %. Nad hranicí 10 % se dále pohybovaly Bělorusko a Ukrajina. ČR se nachází na 24. místě s 2,74 %. Nejlépe si v počtu útoků stojí převážně severské země, jako je Švédsko, Dánsko, Norsko a Island. Nejméně zranitelnou zemí v roce 2020 je Irsko, tam bylo napadeno pouze 1,08 % počítačů. Jelikož severní a západní země jsou vyspělejší oproti těm východním, mají tím pádem vyšší

informační gramotnost. Zatímco východní země tuto gramotnost postrádají, proto zde mají útočníci větší úspěšnost kybernetických útoků. Následující část analýzy se zaměří na střed Evropy, a to na ČR.

## 4.2 Analýza kybernetických útoků v České republice

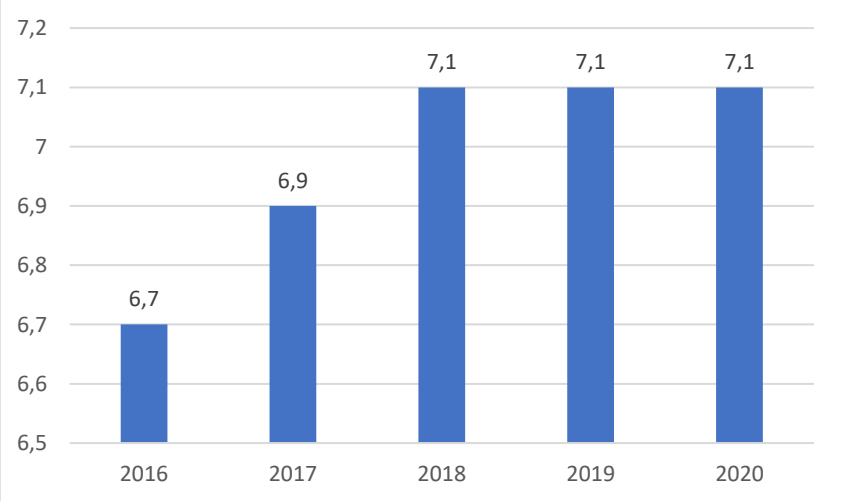
S větším působením na internetu roste pravděpodobnost kybernetických útoků. V předchozí kapitole bylo řečeno, že dnešní společnost stále více upíná svou pozornost na internet a ani ČR toho není výjimkou. Toto tvrzení potvrzují následující obrázky č. 7 a 8.




Obrázek 7 - Počet domácností v ČR vlastnící počítač s internetem v letech 2016-2020 (v milionech)

*Zdroj: Vlastní zpracování dle ČSÚ (2020a,2021a)*

Z obrázku č. 7 vyplývá, že od roku 2016 přibilo okolo 300 000 domácností vlastnící počítač s internetem. V roce 2019 a 2020 se počet domácností nezměnil a pohybuje se kolem 3 600 000 domácností. Jedná se tak o 82 % z celkového počtu domácností.

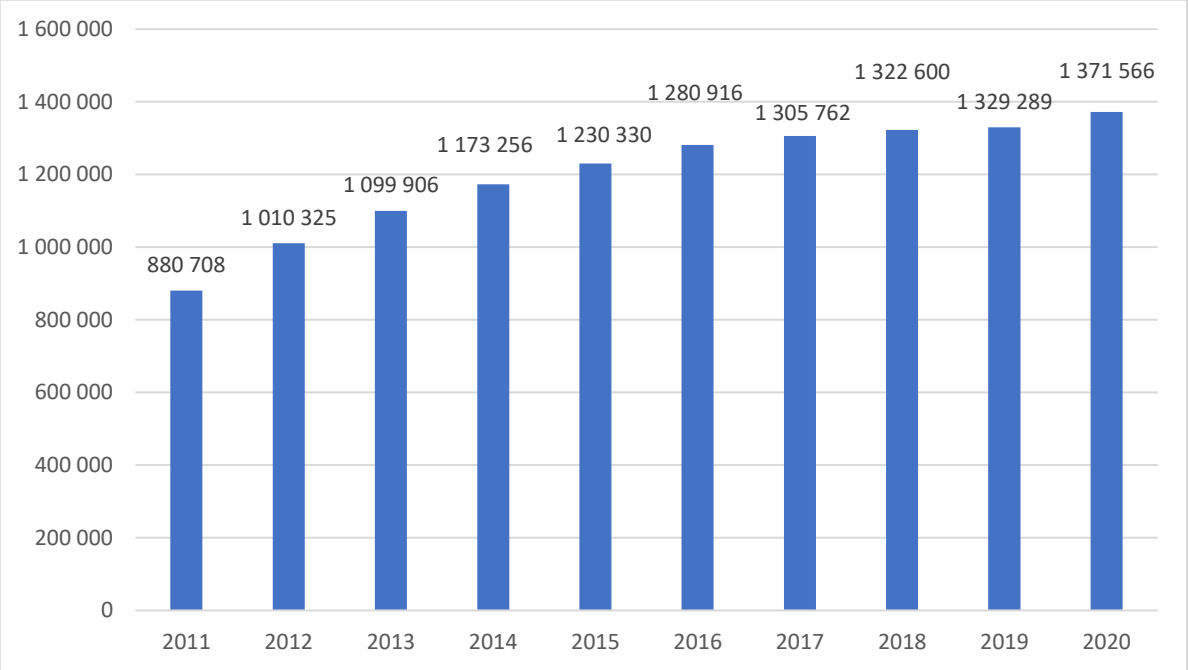



Obrázek 8 - Počet osob starší 16 let používající internet v letech 2016-2020 (v milionech)

*Zdroj: Vlastní zpracování dle ČSÚ (2020b,2021b)*

Z obrázku č. 8 je zřejmé že v průběhu let vzrostl počet uživatelů internetu. V roce 2016 a 2017 vzrostl o 200 000 uživatelů. Od roku 2018 začal stagnovat na hranici 7 100 000 uživatelů. Procentuálně se jedná o 81 % celkového počtu osob starších 16ti let. Lze říci, že uživatelů internetu je mnohem více, jelikož v dnešní době používají internet i osoby mladší 16ti let.

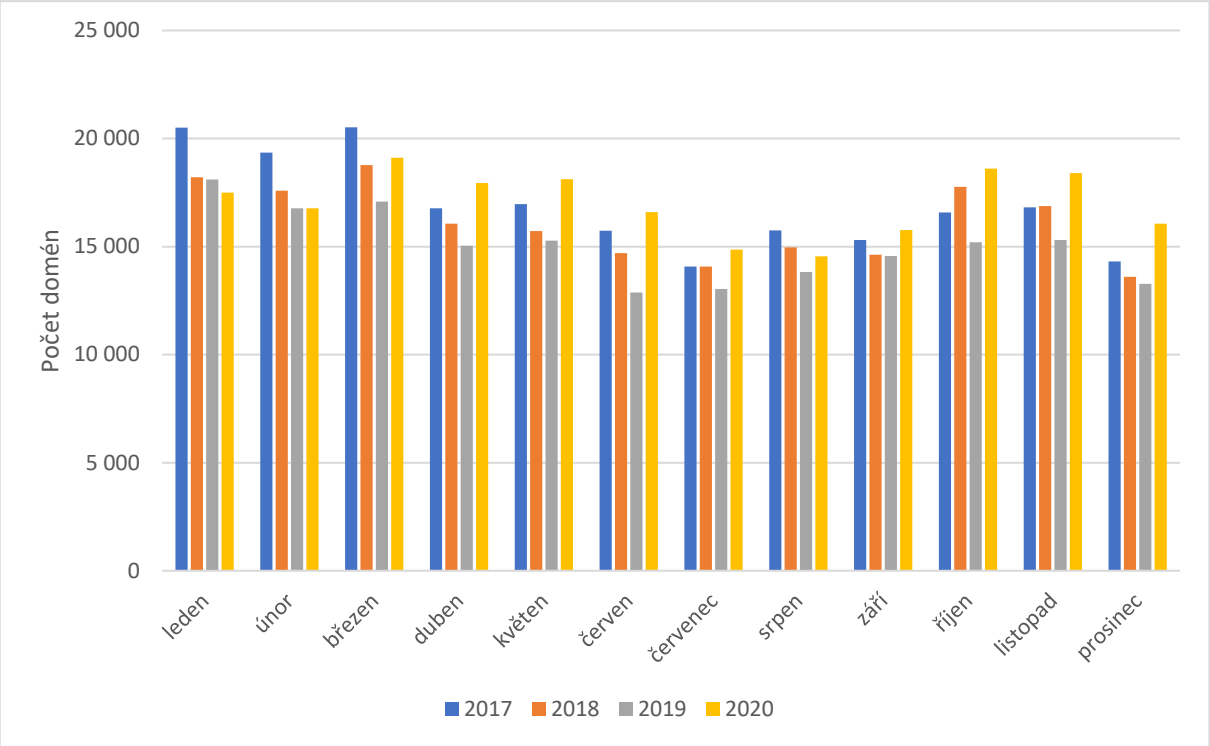
Kromě domácností a jednotlivců svoji působnost na internet přesouvají také organizace a firmy, a to pomocí vytvoření domény.cz na internetu. Domény.cz představují webové stránky vytvořené v ČR. Jejich provozovatelem je zájmové sdružení právnických osob CZ.NIC. Jeho úkolem je provozování registru domén a zabezpečení jejich provozu. Další povinností CZ.NIC je poskytovat statistiky domén, které poslouží pro tuto analýzu jako primární zdroj.




Obrázek 9 - Počet domén v ČR v letech 2011-2020

*Zdroj: Vlastní zpracování dle Domain Report (2017, 2020)*

Největší růst registrovaných domén byl zaznamenám v letech 2011-2015. Od roku 2015 začal růst zřetelně saturovat a v budoucích letech byla očekávána jeho stagnace, či dokonce pokles. Z obrázku č. 9 je zřejmé, že rok 2020 tuto hypotézu vyvrátil. Rok 2020 zaznamenal navýšení domén o 3,2 % oproti roku 2019, a to o 42 277 nových domén. Tento výrazný a nečekaný růst úzce souvisí s pandemií Covid-19. O tom, jak se pandemie promítá v počtu domén je ilustrován v následujícím obrázku č. 10.




Obrázek 10 - Počet doménových registrací v jednotlivých měsících v letech 2017-2020

*Zdroj: Vlastní zpracování dle Domain Report (2019, 2020)*

Za nečekaný nárůst domén v roce 2020 mohou dvě pandemické vlny. Jedna, která proběhla v měsících březen–červen a druhá, která proběhla v měsících říjen–prosinec. V obrázku č. 10 je patrné, že největší nárůst registrovaných domén, byl zaznamenám právě během těchto pandemických vln. Minimálně 2 500 registrovaných domén je přímo spojeno s pandemií, neboť tyto domény obsahují alespoň jedno slovo ze slovních kmenů spojené s Covid-19. Jsou to slova jako např.: korona, virus, respirátor, covid atd. Všechny domény jsou zaregistrovány u tzv. registrátorů. Nejznámějším registrátorem je INTERNET CZ, a. s., který vlastní největší podíl na trhu, a to 21,54 %.

Následující část analýzy vychází z dat CERT/CSIRT týmů, kterým jsou nahlašovány incidenty a události kybernetické bezpečnosti. Jedná se o (CSIRT.CZ, 2020):

- problémy, které mají závažný dopad na infrastrukturu v ČR. Tyto problémy mohou mít plošný charakter a negativně ovlivňovat další sítě, služby a uživatele,
- problémy, u kterých byly vyčerpány veškeré známé způsoby řešení, ale problém přesto přetrvává,
- problémy, u kterých není jednoduché identifikovat, kdo je původcem incidentu, nebo kdo by se jeho řešením měl zabývat a problémy plošného rozsahu.

Tabulka 10 – Počet vybraných incidentů řešených CSIRT týmy v létech 2016-2020

| | **2016** | **2017** | **2018** | **2019** | **2020** |
|---|---|---|---|---|---|
| Phising | 363 | 409 | 518 | 483 | 738 |
| Spam | 290 | 121 | 144 | 128 | 216 |
| Malware | 104 | 99 | 135 | 85 | 109 |
| Trojan | 79 | 94 | 0 | 0 | 0 |
| DoS | 12 | 14 | 7 | 16 | 16 |
| Botnet | 71 | 29 | 20 | 4 | 2 |
| Virus | 0 | 0 | 0 | 0 | 0 |
| Portscan | 6 | 13 | 16 | 3 | 29 |
| Pharming | 2 | 3 | 10 | 9 | 3 |
| **Celkem** | **927** | **782** | **850** | **728** | **1113** |

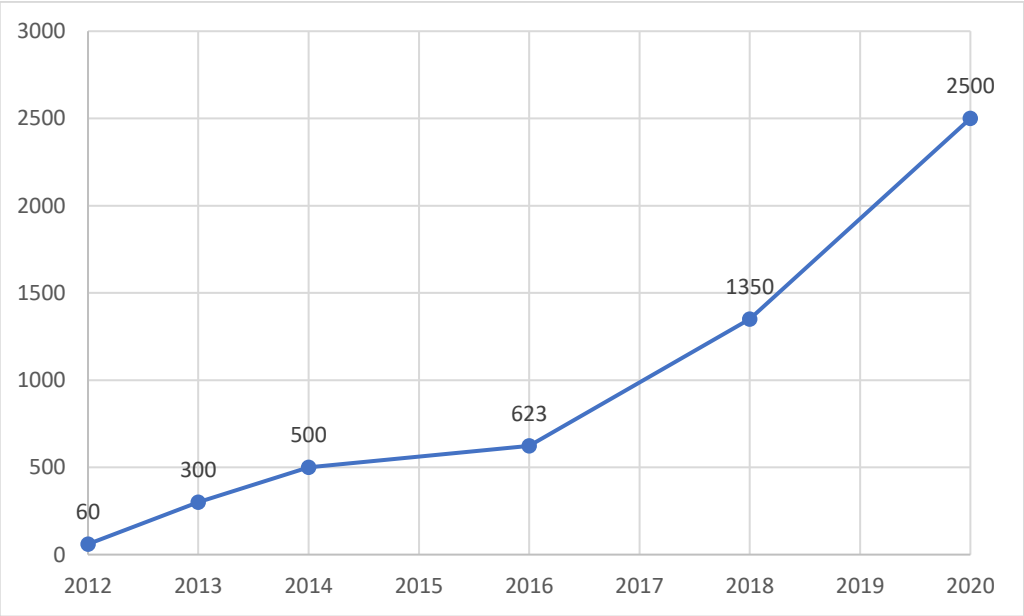
*Zdroj: Vlastní zpracovaní dle CSIRT.CZ (2020)*

Z výše uvedené tabulky č. 10 je patrné, že nejpočetnější zastoupení mají útoky typu phishing, spam a malware. Všechny tyto zmíněné kategorie měly v průběhu let tendenci kolísat. Na druhou stranu mezi nejméně početné incidenty spadaly útoky typu virus a pharming. V rámci posledních pěti let nebyl nahlášen ani jeden útok typu virus. Mezi ně se v roce 2018 přidal i typ incidentu tzv. trojan, který se povedl ČR zcela eliminovat. Jedinou kategorií, která měla od roku 2016 stálý vývoj, a to klesající, byla kategorie botnet. V celkovém úhrnu nejmenší počet útoků přinesl rok 2019. Naopak největší počet útoků byl nahlášen v roce 2020, kdy vzrostl počet útoků o 52 %. V roce 2020 došlo k největšímu nárůstu phishingu. CSIRT uvádí, že už v červnu roku 2020 byl v kategorii phishing překonán počet incidentů za předchozí léta. Mimo jiné došlo také k nárůstu v kategorii spam, portscan a menší nárůst také zaznamenala kategorie malware. V ostatních kategoriích nedošlo k takovému razantnímu nárůstu jako u výše zmíněných, ba naopak došlo k poklesu incidentů.

Razantní nárůst výše uvedených incidentů v roce 2020 není náhodný. Úzce souvisí s pandemií spojenou s Covid-19. Ta pro útočníky přirozeně přinesla nové příležitosti a zranitelnosti. Aby firmy částečně zachovaly kontinuitu činnosti, byli zaměstnanci nuceni přejít z firemního prostředí do prostředí domova neboli tzv. home office, kde byla potřeba připojit se do prostředí firemního. Zaměstnanci se museli připojit do tohoto prostředí pomocí osobních zařízení. S každým dalším připojeným zařízením vzniká pro útočníky nová příležitost otevřeného portu, tudíž dochází k nárůstu incidentů v kategorii portscan. Další příležitosti vznikají v kategoriích phishing a spam. Z předchozí kapitoly 1. 4 „Kybernetické útoky“ vyplývá, že se jedná o plošné

útoky, které jsou technicky nejméně náročné, a proto je velice jednoduché je realizovat. Tudíž je logické, že dochází k jejich nárůstu. Na druhou stranu se proti těmto incidentům lze snadno chránit. Záleží na jednotlivých firmách a jejich bezpečnostním povědomí, zda si jsou jejich zaměstnanci vědomi takových incidentů a jejich následků.

Je nutné zmínit i nárůst DoS útoků v roce 2019, kdy došlo k více než dvojnásobnému počtu těchto incidentů. Po události v roce 2018 se tento typ útoku stal pro útočníky velice sympatický. První významný předěl v síle DDoS útoků mají v zásluze útočníci, kteří v roce 2018 provedli útok na zahraniční službu Github. Jedná se o službu online správce kódů, kterou využívají miliony vývojářů po celém světě. Útočníci na tuto službu provedli DDoS útok se sílou až 1,35 Tb/s. Další významný předěl v síle se stal v roce 2020, kdy útočníci provedli DDoS útok o síle 2,5 Tb/s na společnost Google. Tento incident je zatím považován jako nejsilnější DDoS útok v historii. Útoky DoS (DDoS) fungují na principu posílaní požadavků na určitou síť, do té doby, než dojde k jejímu zahlcení a následnému vyřazení. Síla útoku představuje, kolik požadavků a jakou rychlosti jsou vysílány do napadené sítě.



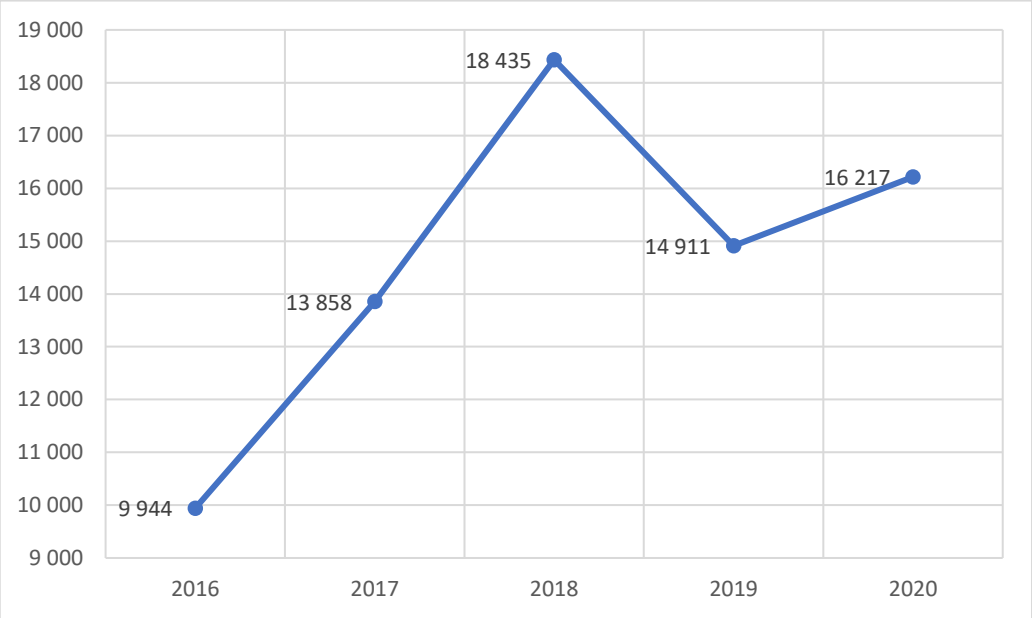

Obrázek 11 - Vývoj síly DDoS útoků v letech 2012–2020

*Zdroj: Vlastní zpracovaní dle NÚKIB (2021c), Nicholson (2021)*

Z obrázku č. 11 je vidět, že roky 2018 a 2020 byly pro sílu DDoS útoků opravdu přelomové. Zatím co do roku 2016 se dosavadní síla DDoS útoků zvedala v průměru okolo 370 Gb/s, v roce 2018 se dosavadní síla zvedla o celých 727 Gb/s a v roce 2020 až o celých 1150 Gb/s. ČR by nebyla schopná odolávat tak silnému útoku. Útok by nenarušil pouze dostupnost napadené služby či stránek, ale také by dokázal narušit kritickou infrastrukturu. Dosavadní DDoS útoky

v ČR se pohybovali na škále několika desítek Mb/s, proti kterým se dokáže efektivně bránit. Nejsilnější útok ČR zaznamenala v roce 2021 na službu WEDOS, a to o síle 300 Gb/s po dobu čtyř dnů. (CN130, 2021)

CSIRT týmy zachycují také incidenty typu IDS (Instrusion Detection System). Jedná se o systém, který zachycuje informace o strojích, ze kterých byly provedeny pouze pokusy o připojení do sítě. *„Využívá adresových bloků, které v internetu dosud nebyli použity, což znamená, že na nich neexistovaly žádné uživatelské stroje. K takovým adresám nemá stroj důvod připojit.“* (CSIRT.CZ, 2020) Následující obrázek č. 12 demonstruje vývoj IDS.




Obrázek 12 - Vývoj počtu pokusů připojení zachycených IDS v letech 2016-2020

*Zdroj: Vlastní zpracování dle CSIRT.CZ (2020)*

Z obrázku č. 12 je zřejmé, že největší nárůst počtu pokusů o připojení do sítě byl zaznamenám v letech 2016-2018. Rok 2018 přinesl téměř dvojnásobné navýšení těchto pokusů oproti roku 2016. V roce 2019 byl zaznamenám pokles těchto incidentů a v roce 2020 nárůst o pouhých 8 %.

## 4.3 Vyhodnocení výsledků analýzy a připravenost ČR

Tato kapitola se zabývá vyhodnocením výsledků analýzy kybernetické bezpečnosti ČR. Z předchozí kapitoly je zřejmé, že kybernetické útoky na ČR stále rostou. Zlomový okamžik, pro věnování větší pozornosti kybernetické bezpečnosti, nastal v roce 2014. Tento rok, viz kapitola 3.1, vznikl ZoKB. Tento zákon reagoval na předešlý rok 2013, ve kterém ČR podléhala rekordnímu počtu kybernetických útoků do roku 2020. V roce 2013 bylo nahlášeno 939 útoků. Po vydání ZoKB a zvýšení pozornosti problematice kybernetické bezpečnosti došlo k značnému úbytku útoků, jelikož v roce 2014 jich bylo nahlášeno pouze 98. (CSIRT.CZ, 2014) Vznik zákona se zasloužil o růst počtu CERT/CSIRT týmů, kterých v roce 2014 přibylo o dvojnásobný počet.

Jediný rok, který počtem útoků předčil rok 2013, byl rok 2020. Z tabulky č. 10 v kapitole 4.2 vyplývá, že v roce 2020 bylo nahlášeno celkem 1113 útoků. V tomto roce se také rozvinul počet útoku na státní správu, a především na zdravotnictví. Co se týče ICT je zdravotnictví zaostalé. Zaostalé jsou především aplikace a software, které ve zdravotnictví používají. Právě na tyto aplikace a software je snadné vést kybernetický útok, proto se zdravotnictví stalo terčem těchto útoků. (NÚKIB, 2021c) Příkladem je fakultní nemocnice v Brně, na kterou byl 13. března 2020 veden kybernetický útok, při kterém vznikly škody v řádech stovek milionů Kč. V reakci na tento incident vydal NÚKIB opatření, kterým *„uložil vybraným subjektům v oblasti zdravotnictví provést nezbytné úkony, které povedou k zabezpečení důležitých informačních a komunikačních systémů před kybernetickým bezpečnostním incidentem. Reaktivní opatření nebylo vydáno plošně a jeho implementace je povinná pouze pro konkrétní subjekty, kterým bylo doručeno.“* (NÚKIB, 2020b) Následující měsíc NÚKIB vydal varování před hrozícími kybernetickými útoky zejména na zdravotnická zařízení. Součástí varování bylo i doporučení NÚKIBu, které se zaměřuje na *„technické a organizační otázky a konkretizuje postupy definované ve varování.“* (NÚKIB, 2021c). Další důležité varování, které vydal NÚKIB v roce 2020, bylo ohledně kybernetických útoků s tématikou Covid-19, které se staly celosvětovým problémem. Konkrétně se jedná o útoky v kategorii podvodné e-maily a spam, ve kterých útočníci rozesílají nakažené soubory s falešnými výsledky testování. (NÚKIB, 2021c)

Jako další opatření NÚKIB, společně s Národní agenturou pro komunikační a informační technologie a MVČR, vydal v roce 2020 dokument **Minimální bezpečnostní standard v1.0**. Tento dokument reaguje na rostoucí trend kybernetických útoků nahlášených CERT/CSIRT týmům v ČR. *„Jeho cílem je pomoci s kybernetickou bezpečností organizacím, které sice nespadají pod zákon o kybernetické bezpečnosti, ale přesto je žádoucí, aby jejich pracovníci*

*znali a respektovali základní pravidla ochrany před hrozbami kyberprostoru. Dokument se dělí na dvě základní části, z nichž první je zaměřená na management organizací a druhá na IT specialisty.“* (NÚKIB, 2020a)

Další činností, kterou se ČR snaží předcházet kybernetickým útokům, je dozorová činnost NÚKIBu tzv. kontrolní audit. Hlavním záměrem kontrolního auditu je sledovat a vyhodnocovat, zda jsou plněny povinnosti plynoucí ze ZoKB. V roce 2019 bylo provedeno celkem 15 těchto auditů. Počet kontrolních auditů v roce 2020 byl ovlivněn situací Covid-19, v důsledku toho jich bylo provedeno pouze 8. V druhé polovině roku 2020 byly tyto audity směřovány na zdravotnický sektor.

NÚKIB každoročně pořádá cvičení kybernetické bezpečnosti. Tato cvičení jsou zdrojem pro nově získané znalosti, zkušenosti a technické schopnosti. Pomocí pořádání těchto cvičení má NÚKIB možnost identifikovat slabiny v kyberprostoru. V roce 2020 pořádal NÚKIB 8 národních a mezinárodních cvičení, kterých se zúčastnilo až 100 účastníků z různých organizací. Mimo jiné se NÚKIB stal koordinátorem jednoho z největších mezinárodních cvičení pořádané NATO. V neposlední řade se NÚKIB snaží o zvýšení bezpečnostního povědomí prostřednictvím vydaných aktualit na svých oficiálních stránkách. Tyto aktuality obsahují varování před aktuálními hrozbami. Tyto informace využívají české instituce a organizace pro školení vlastních zaměstnanců v oblasti kybernetické bezpečnosti.

Podobné aktuality vydávají i antivirové společnosti ve svých tiskových zprávách. Tímto se snaží informovat veřejnost o aktuálních hrozbách a poskytnout rady ohledně toho, jak se proti těmto hrozbám nejlépe chránit. Mezi tyto antivirové společnosti patří např. Eset, Avast, McAfee a NortonLifeLock. Všechny tyto společnosti nabízejí speciální balíčky pro firmy, nebo nabízí svůj antivir zcela zdarma s alespoň minimální ochranou. Nad rámec těchto balíčků společnost Eset nabízí 50% slevu zdravotnickému, školskému sektoru a neziskovým organizacím. (Eset, 2021). V roce 2020 se zvýšil prodej antivirových programů o 1,2 miliardy Kč. Hlavním důvodem byla pandemická opatření, kdy domácnosti musely nakoupit elektroniku pro distanční výuku či home-office a do těchto zařízení si pořídili antivirovou licenci. (Novinky.cz, 2021)

ČR dlouhodobě postrádá odborníky v oblasti kybernetické bezpečnosti. Tento nedostatek je nucena nahrazovat jinými způsoby. Nejčastějšími způsoby jsou využití outsourcingu, nábor absolventů či možnost dalšího vzdělávání. Dalším nedostatkem je alokace zdrojů na kybernetickou bezpečnost v organizacích. Tento nedostatek se odráží právě v nedostatku

odborníků, jelikož organizace nemají dostatek financí pro zaplacení jejich mezd. Ve většině organizací se tyto zdroje pohybují okolo 0-5 % z celkových zdrojů, které organizace uvádí jako nedostatečné. Přestože se tyto zdroje rok od roku zvyšují, tak by bylo potřeba minimálně dvojnásobné navýšení těchto zdrojů. (NÚKIB, 2021c)

I přes výše uvedené nedostatky, ČR disponuje neobyčejným technickým a technologickým know-how a stává se tak relativně bezpečnou zemí v oblasti kybernetické bezpečnosti. Důkazem toho jsou tabulky č. 7,8 a 9, protože ČR se v těchto tabulkách nacházela vždy ve spodních příčkách, ať už v kategorii podvodný e-mail, spam nebo v celkovém podílu napadených počítačů. Aby tomu bylo tak i nadále, musí se ČR adaptovat a reagovat na nejnovější spektrum hrozeb. Musí vytvářet dostatečné kapacity pro analýzu, identifikaci a vyhodnocení současných a budoucích kybernetických hrozeb. Všechny současné a budoucí cíle pro kybernetickou bezpečnost jsou uvedeny v současné Národní strategii kybernetické bezpečnosti České republiky na období let 2021-2025 a akčního plánu.

# ZÁVĚR

Cílem bakalářské práce je popsat a zhodnotit vývoj kybernetické bezpečnosti a posoudit připravenost České republiky v tomto kontextu.

V první kapitole této práce se diskutovalo o bezpečnostních vědách a jejich pohledu na zajištění bezpečnosti. V průběhu let se této problematice věnovalo několik autorů, kteří polemizovali o tom, co je to bezpečnost, a jak jí dosáhnout. Pohledy a definice jednotlivých autorů byly zpravidla odlišné, avšak na základě rozboru těchto pohledů a definic bylo možné stanovit výchozí pohled na problematiku bezpečnosti, který je touto prací využit. Dále kapitola vymezila definici kybernetické bezpečnosti. Po vymezení kybernetické bezpečnosti se kapitola zabývala definováním kybernetického prostoru a jeho vrstev. Následně se kapitola zabývá kybernetickými útoky, které jsou nejvíce diskutovaným tématem problematiky kybernetické bezpečnosti. Rozebírá nejčastější typy útoků, jejich funkci a jednotlivé fáze, ve kterých probíhají.

Druhá kapitola se zabývala řízením kybernetické bezpečnosti. Obsahovala základní a doporučený postup při tomto řízení. Dále kapitola rozebírala základní prvky řízení, kterými jsou aktiva, riziko, hrozby a zranitelnost. Prvním prvkem, který byl vysvětlen bylo riziko a jak s ním nakládat. Dalším prvkem jsou aktiva, která jsou základními prvky kybernetické bezpečnosti, jelikož bez aktiv by nemohly vzniknout informační systémy. Znalost těchto aktiv a systémů je velice důležitá, jelikož právě na tyto aktiva a systémy jsou vedeny kybernetické útoky. Závěrem této kapitoly se rozebíraly poslední dva prvky, a to hrozby a zranitelnost, kde bylo představeno základní dělení hrozeb a definice zranitelnosti.

Třetí kapitola byla věnována ukotvení kybernetické bezpečnosti v jednotlivých dokumentech České republiky. V této kapitole bylo možné sledovat vznik a vývoj těchto dokumentů v časové posloupnosti. Dále byl představen gestor kybernetické bezpečnosti, kterým je Národní úřad pro kybernetickou a informační bezpečnost. Byla nastíněna jeho historie a na základě kterých dokumentů mohl tento úřad vzniknout. V neposlední řadě se kapitola věnuje týmům pro reakci na počítačové hrozby a počítačové bezpečnostní incidenty, jejich rozdělení, funkci a početnímu vývoji.

Čtvrtá kapitola se zabývala analýzou vývoje kybernetické bezpečnosti, a to jak v České republice, tak na světové úrovni. Světové úrovni se věnovala první část analýzy, kde bylo možné sledovat četnost kybernetických útoků a jejich vývoj. Tato část mimo jiné zobrazila útoky, které byly nejvíce zneužívány v době pandemie a na které země byly nejvíce směřovány.

Následující část kapitoly se zaměřila na Českou republiku. Také zde bylo možné sledovat jednotlivé kybernetické útoky a jejich vývoj. Kromě toho bylo ilustrováno, jak je dnešní společnost závislá na informačních a komunikačních technologiích pomocí grafického zpracování celkového počtu domácností vlastníci počítač s připojením na internet a jejich vývoj. Závěrem kapitoly byla diskutována připravenost České republiky v oblasti kybernetické bezpečnosti.

Nejzásadnější dokument, který nejvíce ovlivnil vývoj problematiky kybernetické bezpečnosti v České republice, byl Zákon o kybernetické bezpečnosti. Tento zákon nejvíce přispěl ke zvýšení bezpečnostního povědomí. Veškeré další aktivity v České republice se odvíjeli právě od tohoto dokumentu. V souvislosti se zákonem a doprovázejícími vyhláškami vznikl úřad pro kybernetickou bezpečnosti, vznikly bezpečnostní týmy, strategie a akční plány. Pomocí těchto dokumentů a jejich aktualizací se i nadále Česká republika vypořádává s problematikou kybernetické bezpečnosti dodnes.

Působení v kyberprostoru se stále zvyšuje, a to jak z pohledu domácností, tak z pohledu organizací. To potvrzuje provedená analýza, ze které je zřejmé, že se zvyšuje nejen počet domácností s počítačem s přístupem na internet, ale také počet zaregistrovaných domén na internetu. Součástí analýzy byl rozbor kybernetických útoků vedených na Českou republiku. Zde bylo možné sledovat vývoj útoků, které měly převážně rostoucí tempo růstu, a to v kategorii phishing, spam a portscan. Na druhou stranu bylo možné sledovat vývoj útoků, které Česká republika dokázala zredukovat. I přes rostoucí počet některých kybernetických útoků, je na základě analýzy zřejmé, že se Česká republika v rámci Evropy a Evropské unie řadí mezi bezpečnější země v oblasti kybernetické bezpečnosti. Česká republika se nachází mezi deseti nejbezpečnějšími zeměmi Evropy.

Z analýzy je zřejmé, že rok 2020 zaznamenal nárůst téměř ve všech kategoriích kybernetických útoků. Je třeba zmínit, že tento rok byl velice ovlivněn pandemií a není jasné, jak by vývoj v roce 2020 vypadal, bez přítomnosti Covidu-19. I přesto v předešlých letech počet kybernetických útoků rostl a očekává se nadále potencionální růst těchto útoků v dalších letech s dalším vývojem informačních a komunikačních technologií. Aby se Česká republika mohla efektivně bránit, musí pečlivě sledovat trendy a vývoj těchto technologií a za včas reagovat na případné hrozby a útoky.

# POUŽITÁ LITERATURA


ARMSTRONG, Martin. *The Countries Targeted Most by Malicious Coronavirus Spam* [online]. 2020a [cit. 2021-11-01]. Dostupné z: https://www.statista.com/chart/21291/countries-targeted-most-by-malicious-coronavirus-spam/?fbclid=IwAR0iYA_5GKhGhSJAPAUlKO3JK26qzp4R4_TKa0kZLaZI_DsLOf2sCyBkTvo.

ARMSTRONG, Martin. *The Online Coronavirus Threat* [online]. 2020b [cit. 2021-11-01]. Dostupné z: https://www.statista.com/chart/21286/known-coronavirus-related-malicious-online-threats/?fbclid=IwAR3AMgYVWfy0V5eZhIr3qz0JWALagE42BfKy_8aqdmYdDczcj03eWu4zUfY.

AXIANS. *Jak probíhá kybernetický útok?* [online]. 2021 [cit. 2021-9-30]. Dostupné z: https://www.axians.cz/cs/novinky/jak-probiha-kyberneticky-utok/.

BALABÁN, Miloš, Marta NACHTMANNOVÁ a Libor STEJSKAL. *Proměny konceptu vnitřní bezpečnosti: Changes in the concept of internal security*. Praha: Karolinum, 2006. ISBN 80-246-1175-9.

BOKŠA, Michal, Petr BOHÁČEK, Jakub KUFČÁK a Jonáš SYROVÁTKA. *NATO: naše bezpečnost.* Praha: Asociace pro mezinárodní otázky, 2018. ISBN 978-80-87092--63-7.

BROOKS, Charles J., Christopher GROW, Philip CRAIG a Donald SHORT. *Cybersecurity essentials*. Indianapolis, Indiana: Sybex, John Wiley, 2018. ISBN SBN978-1-119-36239-5.

CN130. *Wedos byl 4 dny pod silnými DDoS útoky, které údajně přesahovaly 300 Gbps* [online]. 2021 [cit. 2021-11-01]. Dostupné z: http://cn130.com/2021/04/wedos-byl-4-dny-pod-silnymi-ddos-utoky-ktere-udajne-presahovaly-300-gbps/.

CSIRT.CZ. *Zpráva o činnosti CSIRT.CZ za rok 2014* [online]. 2014 [cit. 2021-11-01]. Dostupné z: https://csirt.cz/media/filer_public/ca/26/ca266cde-c4c1-47d7-95fe-2d0f35324989/zprava_o_cinnosti_csirtcz2014.pdf.

CSIRT.CZ. *Zpráva o činnosti CSIRT.CZ za rok 2020* [online]. 2020 [cit. 2021-11-01]. Dostupné z: https://www.csirt.cz/media/filer_public/c1/64/c1642df8-32f0-4976-9062-ac259f7a43b4/210304_csirt_vyrocni_zprava_2020.pdf.

CZ.NIC. *Domain Report 2017* [online]. 2017 [cit. 2021-11-01]. Dostupné z: https://stats.nic.cz/reports/2017/.

CZ.NIC. *Domain Report 2019* [online]. 2019 [cit. 2021-11-11]. Dostupné z: https://stats.nic.cz/reports/2019/index_cz.html.

CZ.NIC. *Domain Report 2020* [online]. 2020 [cit. 2021-11-01]. Dostupné z: https://stats.nic.cz/reports/2020/index_cz.html.

ČESKÝ STATISTICKÝ ÚŘAD. *Informační společnost v číslech: Domácnosti a ICT* [online]. 2020a [cit. 2021-11-12]. Dostupné z: https://www.czso.cz/documents/10180/122362632/06100420b.pdf/bd2c09c3-19d9-4934-aeee-e091e09cb65e?version=1.0.

ČESKÝ STATISTICKÝ ÚŘAD. *Informační společnost v číslech: Domácnosti a digitální technologie* [online]. 2021a [cit. 2021-11-12]. Dostupné z: https://www.czso.cz/documents/10180/143060187/06100421b.pdf/7797bed6-fa9b-435e-9fa9-f8e3b1667ff3?version=1.3.

ČESKÝ STATISTICKÝ ÚŘAD. *Informační společnost v číslech: Osoby a digitální technologie* [online]. 2021b [cit. 2021-11-12]. Dostupné z: https://www.czso.cz/documents/10180/143060187/06100421c.pdf/64023ec6-8e3f-4c97-943f-b1dcb143e2d4?version=1.9.

ČESKÝ STATISTICKÝ ÚŘAD. *Informační společnost v číslech: Osoby a ICT* [online]. 2020b [cit. 2021-11-12]. Dostupné z: https://www.czso.cz/documents/10180/122362632/06100420c.pdf/01ab7bd8-1baa-4b8d-854d-81d000d0c953?version=1.2.

DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

ESET. *Standartní ceník produktů pro domácnosti a firmy* [online]. 2021 [cit. 2021-11-01]. Dostupné z: https://www.eset.com/cz/cenik/#slevy-firma.

HANÁKOVÁ, Eva, Miroslav KRÁL a Stanislav MALÝ. *ABC ergonomie*. Praha: Professional Publishing, 2010. ISBN ISBN978-80-7431-027-0.

INTERNET CRIME COMPLAINT CENTRE. *Internet Crime Report 2020* [online]. 2020 [cit. 2021-11-01]. Dostupné z: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

IT SLOVNÍK. *Co je to entita?* [online]. 2021 [cit. 2021-9-30]. Dostupné z: https://it-slovnik.cz/pojem/entita.

JIRÁČEK, Luděk. *Aplikace mezinárodního práva v kybernetickém prostoru a regulace autonomních zbraňových systémů* [online]. 2021 [cit. 2021-9-30]. Dostupné z: http://data.idnes.cz/soubory/na_analyzy/A170626_M02_000_JIRACEK_APLIKACE.PDF.

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary* [online]. 2013 [cit. 2021-11-15]. Dostupné z: https://afcea.cz/wp-content/uploads/2015/03/Slovnik_Final_screen_v2_0.pdf

JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

KOLB, Dirk. *Surface Web is Only the Tip of the Iceberg*. [online]. 2020 [cit. 2021-9-30]. Dostupné z: https://traversals.com/blog/surface-web/?fbclid=IwAR3T-rZEHGq6SI3y8nrAli7Wxnk0_GHpR0kpwLJcqxjOP9z7tr6R0ykkf78.

KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.

KRESA, Dan. *Jaké jsou nejčastější typy kybernetických útoků?* [online]. 2018 [cit. 2021-9-30]. Dostupné z: https://www.kybez.cz/jake-jsou-nejcastejsi-typy-kybernetickych-utoku/.

KROPÁČOVÁ, Andrea. *CERT/CSIRT týmy a jejich role* [online]. 2013 [cit. 2021-9-30]. Dostupné z: https://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/.

LEXICO. *Cyberspace* [online]. 2021a [cit. 2021-11-11]. Dostupné z: https://www.lexico.com/definition/cyberspace.

LEXICO. *Cybersecurity* [online]. 2021b [cit. 2021-9-30]. Dostupné z: https://www.lexico.com/definition/cybersecurity.

NICHOLSON, Paul. *Five Most Famous DDoS Attacks and Then Some* [online]. 2021 [cit. 2021-11-01]. Dostupné z: https://www.a10networks.com/blog/5-most-famous-ddos-attacks/.

NOVINKY.CZ. *Poptávka po antivirech stoupla. I kvůli práci a výuce z domova* [online]. 2021 [cit. 2021-11-01]. Dostupné z: https://www.novinky.cz/internet-a-pc/software/clanek/poptavka-po-antivirech-stoupla-i-kvuli-praci-a-vyuce-z-domova-40374692.

NÚKIB. *Akční plán /Strategie* [online]. 2021a [cit. 2021-9-30]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/.

NÚKIB. *Experti z NÚKIB, NAKIT a Ministerstva vnitra spojili síly kvůli zabezpečení menších organizací* [online]. 2020a [cit. 2021-11-15]. Dostupné z: https://www.nukib.cz/cs/infoservis/aktuality/1601-experti-z-nukib-nakit-a-ministerstva-vnitra-spojili-sily-kvuli-zabezpeceni-mensich-organizaci/.

NÚKIB. *NÚKIB vydal reaktivní opatření pro vybrané subjekty ve zdravotnictví* [online]. 2020b [cit. 2021-11-15]. Dostupné z: https://www.nukib.cz/cs/infoservis/aktuality/1418-nukib-vydal-reaktivni-opatreni-pro-vybrane-subjekty-ve-zdravotnictvi/.

NÚKIB. *O Núkib* [online]. 2021b [cit. 2021-11-11]. Dostupné z: https://www.nukib.cz/cs/o-nukib/.

NÚKIB. *Zprávy o stavu* [online]. 2021c [cit. 2021-11-01]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/.

PORADA, Viktor a Květoň HOLCR. *Policejní vědy*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2011. ISBN 978-807-3803-148.

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

PRŮŠA, Jiří a Lenka PRŮŠOVÁ. *Česko vládne světu v bezpečnosti* [online]. 2019 [cit. 2021-9-30]. Dostupné z: https://www.nic.cz/files/nic/doc/Securityworld_bezpecnostni_tymy_032019.pdf.

SAK, Petr. *Úvod do teorie bezpečnosti: nekonvenční pohledy na minulost, přítomnost a budoucnost lidstva*. Praha: Petrklíč, 2018. ISBN 978-80-7229-652-1.

SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.

SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7.

SPECOPS. *The European Countries Most at Risk of Cyber-Crime* [online]. 2020 [cit. 2021-11-01]. Dostupné z: https://specopssoft.com/blog/european-countries-cyber-crime/?fbclid=IwAR2xklCh1Aq8hzfRv6dmC8IRUNsZeXUD09oFrgHuLUNvHZxhXoWFnutSJ2k.

STŘELEC, Jiří. *Analýza rizik* [online]. 2015 [cit. 2021-11-11]. Dostupné z: https://www.vlastnicesta.cz/metody/analyza-rizik-risk/.

ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

THE UNITED STATES ARMY. *Cyberspace Operations Concept Capability Plan 2016-2028* [online]. 2010 [cit. 2021-10-08]. Dostupné z: https://irp.fas.org/doddir/army/pam525-7-8.pdf.

TRUSTED INTRODUCER. *Searchable Team Database* [online]. 2021 [cit. 2021-9-30]. Dostupné z: https://www.trusted-introducer.org/directory/teams.html#url=c%3DCZ%26q%3D.

WAISOVÁ, Šárka. *Bezpečnost: vývoj a proměny konceptu*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-21-0.

WALT, Stephen M. *International Studies Quaterly: The Renaissance of Security Studies*. 2. vydání. Volume 35, 1991. ISBN ISSN 0020-8833.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181.