Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Analýza kybernetických hrozeb pro ČR

Filip Jantač

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Filip Jantač

Informatika

Název práce

Analýza kybernetických hrozeb pro ČR

Název anglicky

Analysis of cybersecurity threats for Czech Republic

Cíle práce

Hlavním cílem práce je zhodnocení kybernetických hrozeb pro ČR, které již v minulosti proběhly nebo teoreticky mohou proběhnout v budoucnu.

Dílčí cíle
- Nejčastější varianty kybernetických útoků
- Zhodnocení angažovanosti vybraných států v kybernetických útocích
- Rozbor závažných kybernetických útoků od roku 2000
- Srovnání nebezpečnosti různých kybernetických útoků
- Doporučení na zlepšení bezpečnosti před kybernetickými hrozbami

Metodika

Bakalářská práce bude obsahovat charakteristiku a různé varianty kybernetických útoků. Zaměří se na závažné kybernetické útoky, které proběhly ve světě od roku 2000. Bude uvedena analýza, jak se v této problematice vybrané státy angažují a práce celkově zanalyzuje, jakým hrozbám je Česká republika vystavena. Dále budou srovnány závažnosti různých kybernetických útoků. Práce v závěru vyvodí doporučení na zlepšení bezpečnosti ČR před kybernetickými hrozbami.

Doporučený rozsah práce

40-50 stran

Klíčová slova

kybernetická bezpečnost; kybernetické hrozby; hybridní válka; hackerský útok; hrozby; ddos; kybernetická válka

---

Doporučené zdroje informací

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

ŘEHKA, Karel. Informační válka. Praha: Academia, 2017. XXI. století. ISBN 978-80-200-2770-2

SINGER, P. W. a Allan FRIEDMAN. Cybersecurity and cyberwar: what everyone needs to know. New York: Oxford University Press, c2014. ISBN 978-0-19-991809-6

Předběžný termín obhajoby

2022/23 LS – PEF

Vedoucí práce

doc. Ing. Jiří Vaněk, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 31. 5. 2022

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 27. 10. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 12. 03. 2023

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Analýza kybernetických hrozeb pro ČR" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 12.3.2023 _____

Poděkování

Rád bych touto cestou poděkoval doc. Ing. Jiřímu Vaňkovi, Ph.D. za odborné rady a připomínky při vedení této bakalářské práce.

Analýza kybernetických hrozeb pro ČR

Abstrakt

Tato bakalářská práce se zabývá analýzou kybernetických hrozeb pro Českou republiku. Práce zkoumá různé typy kybernetických hrozeb, které představují riziko pro kriticikou infrastrukturu, státní orgány nebo vysoce postavené politicky exponované osoby. Autor provedl také výzkum četnosti nejvíce používaných podob kybernetických útoků v rámci celého světa, a zároveň jaké státy se v kybernetickém prostoru nejvíce angažují, ať už v roli útočníka, nebo oběti. Vybrané signifikantní kybernetické útoky jsou detailněji zkoumány z hlediska jejich důsledků a navrhovaných protiopatření. Následně se práce zabývá, co by v budoucnu mohlo hrozit z kybernetického hlediska České republice a autorem jsou navržena doporučovaná opatření, jak riziko co nejvíce minimalizovat. Zjištění této práce mohou nabídnout cenné postřehy pro zlepšení zabezpečení státu před kybernetickými hrozbami.

Klíčová slova: kybernetická bezpečnost; kybernetické hrozby; hybridní válka; hackerský útok; hrozby; ddos; kybernetická válka

Analysis of cybersecurity threats for Czech Republic

Abstract

This bachelor thesis deals with the analysis of cyber threats for Czech Republic. The thesis examines different types of cyber threats that pose a risk to critical infrastructure, state institutions or politically exposed persons. The author has also conducted research on the frequency of the most used forms of cyber-attacks worldwide, as well as which states are most engaged in cyberspace, either as attacker or victim. Selected significant cyber attacks are examined in more detail in terms of their consequences and proposed countermeasures. Subsequently, the thesis examines what cyber threats could be dangerous for Czech Republic in the future and the author proposes recommended measures to minimise the risk as much as possible. The findings of this thesis can offer valuable insights for improving the security of the country against cyber threats.

Keywords: cybersecurity, cyber threats, hybrid war, hacking, threats, ddos, cyber war

Obsah

1 Úvod

Práce se zabývá celkovou problematikou kybernetické bezpečnosti. Téma bylo zvoleno, protože je to rychle se rozvíjející oblast IT a je potřeba dbát stále většího důrazu na bezpečnost dat a informací, a zároveň vzdělávat uživatele, jaké jsou nejlepší praktiky pro zamezení úniku dat. Pro Českou republiku, Evropu, ale i celý svět, se tato sféra stává stěžejní, jelikož kybernetické útoky mohou být ohrožením pro zdravotnictví, infrastrukturu nebo přísně tajná data zpravodajských služeb. Informační válka a kybernetické útoky jsou i nedílnou součástí současného konfliktu na Ukrajině.

V teoretické části této práce jsou uvedeny základy kybernetické bezpečnosti, definice klíčových termínů a různé typy kybernetických útoků.

V praktické části je vytyčeným cílem celkové zhodnocení kybernetické hrozeb pro Českou republiku, které v minulosti proběhly nebo teoreticky mohou proběhnout v budoucnu. Budou analyzovány nejčastější varianty kybernetických útoků a jaké mohou být jejich dopady, ať už minimální, nebo třeba nebezpečné pro celý stát a jeho obyvatele. Obsahem práce bude také srovnání nebezpečnosti různých kybernetických útoků. Bude proveden výzkum, které státy se nejčastěji angažují v kybernetických útocích a informačních válkách. Dále se zhodnotí závažné kybernetické útoky z celého světa od roku 2000 a jejich dopady. Nakonec budou navrženy doporučení na zlepšení bezpečnosti před kybernetickými hrozbami.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem práce je zhodnocení kybernetických hrozeb a útoků na Českou republiku, které již v minulosti proběhly nebo mohou teoreticky proběhnout v budoucnu. Jako dílčí cíle práce byly zvoleny následující body:

- Nejčastější varianty kybernetických útoků
- Zhodnocení angažovanosti vybraných států v kybernetických útocích
- Rozbor závažných kybernetických útoků od roku 2000
- Srovnání nebezpečnosti různých kybernetických útoků
- Doporučení na zlepšení bezpečnosti před kybernetickými hrozbami

2.2 Metodika

Bakalářská práce bude obsahovat charakteristiku a různé varianty kybernetických útoků. Zaměří se na závažné kybernetické útoky, které proběhly ve světě od roku 2000. Bude uvedena analýza, jak se v této problematice vybrané státy angažují a práce celkově zanalyzuje, jakým hrozbám je Česká republika vystavena. Dále budou srovnány závažnosti různých kybernetických útoků. Práce v závěru vyvodí doporučení na zlepšení bezpečnosti ČR před kybernetickými hrozbami.

3 Teoretická východiska

3.1 Definice kybernetické bezpečnosti

Kybernetická bezpečnost je umění chránit sítě, elektronická zařízení a data před neoprávněným přístupem nebo kriminálním užitím.[1] Nedílnou součástí kybernetické bezpečnosti je důvěrnost (confidentiality), integrita (integrity) a dostupnost (availability). Tyto 3 základní principy jsou známé pod názvem CIA triáda.

3.2 CIA triáda

CIA triáda je model, podle kterého se vytváří opatření pro kybernetickou bezpečnost, aby byla zajištěna co nejlepší ochrana dat daného systému. Tento model je oprávněně považován za kriticky důležitý nástroj pro ujištění, že systémy jsou bezpečné a optimálně fungují. Všechny tři pilíře jsou vzájemně propojené a nemohou být efektivně implementovány izolovaně.

3.2.1 Confidentiality

Confidentiality, česky důvěrnost, je zjednodušeně synonymum pro soukromí. Hlavní myšlenkou tohoto pilíře je, že se snaží zabránit jakémukoliv zveřejnění dat bez předchozího schválení autora nebo vlastníka dat.

Jedním z klíčových elementů je šifrování, tedy způsob, kterým je zajištěno, aby byla poslaná informace čitelná jen pro osobu, které je určena. Mezi další klíčové elementy patří například autentizace (ověření identity daného subjektu), kontrola přístupu nebo fyzické zabezpečení dat.

3.2.2 Integrity

Integrita zaručuje, že informace, která byla poslána, nebyla žádným způsobem modifikována. K tomu se používá hashování, což je převod určitého textu na určitý počet číslic a písmen. Jakákoliv změna (i naprosto minimální) v původním textu, má za důsledek, že se celý hash kompletně změní. Toto je hojně využíváno při stahování souborů z internetu – např. při stažení nějakého instalačního balíčku z internetu by se měl porovnat kontrolní součet tohoto souboru se součtem, který se nachází na webu, odkud byl soubor stažen. Pokud je stejný, byl stažen soubor bez jakýchkoliv změn. Pokud se byť jen minimálním způsobem liší, byl soubor při stahování modifikován třetí stranou.

3.2.3 Availability

Jak už z názvu vyplývá, základní princip tohoto pilíře je, aby byla data a informace dostupná vždy, když je potřeba. Příkladem může být zálohování – když se rozbije pevný disk v notebooku a data nejsou nikde zálohována, s největší pravděpodobností budou všechna data ztracena. Nejvíce rozšířeným způsobem zálohování pro obyčejné uživatele se v posledních letech stal tzv. cloud – data jsou přístupná vždy na jakémkoliv zařízení, které je připojeno k internetu.

3.2.4 Názorný příklad

Při úspěšném útoku na data uživatele je v každém případě porušen některý nebo více z pilířů CIA triády. Příkladem může být Man-in-the-middle attack (MITM, česky člověk uprostřed). Při tomto útoku se dostane mezi dvě komunikující strany třetí osoba, která upraví zprávu, jenž byla odeslána první osobou druhé osobě. V tomto případě byly porušeny hned 2 pilíře CIA triády. Třetí osoba, tedy útočník, se dostal k informacím, ke kterým neměl mít přístup, a které měla vidět jen první a druhá osoba – byl porušen pilíř confidentiality. Třetí osoba dále upravila původní zprávu, a tudíž byl porušen pilíř integrity.

3.3 Základní termíny

V této kapitole budou představeny základní termíny, které jsou v této práci využívané a jsou klíčové pro porozumění problematice kybernetické bezpečnosti. Některé termíny mohou být pro osoby, které se nepohybují v oblasti informačních technologií, matoucí. Tudíž je nezbytné poskytnout jasnou a stručnou definici těchto termínu, aby měl každý dostatečný základ pro pochopení této práce.

Mezi základní termíny relevantní pro tuto práci patří vulnerability, threat, exploit, risk a dvoufázové ověření. V následujících podkapitolách jsou stručně a výstižně charakterizovány.

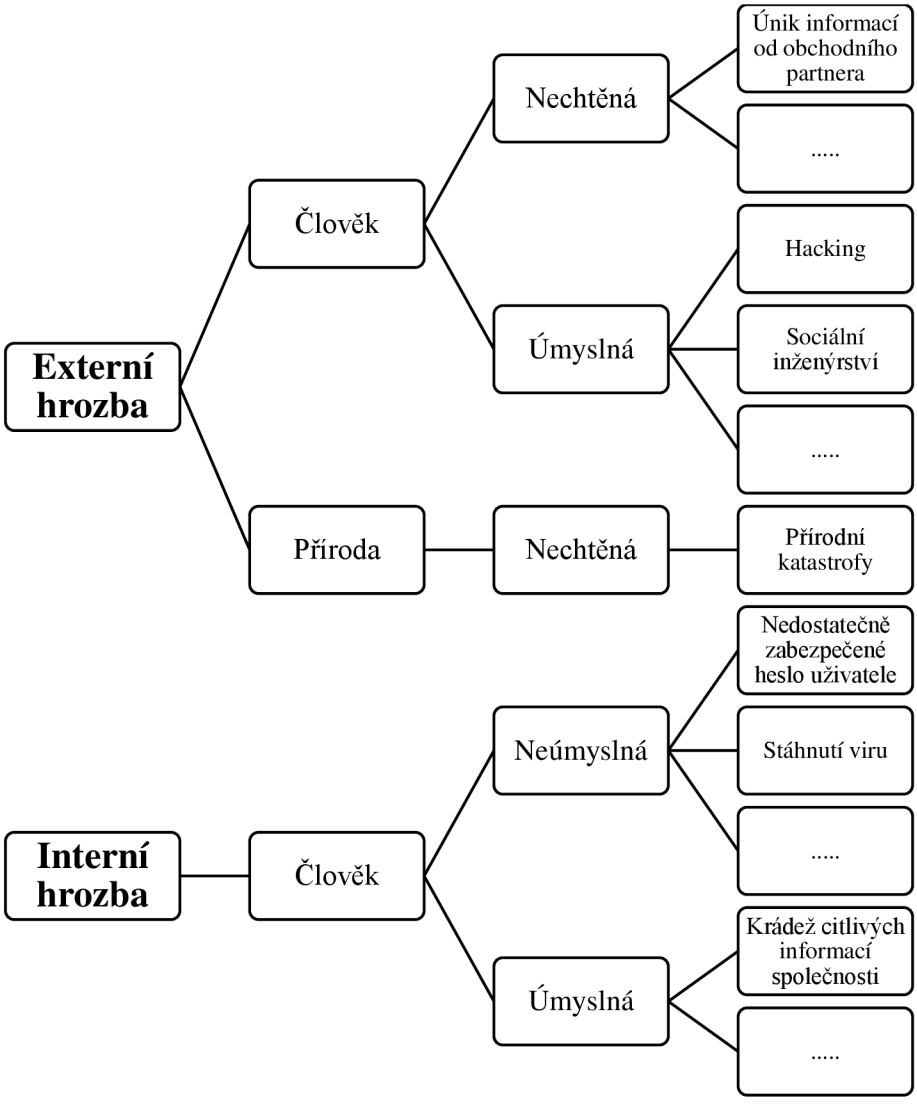
3.3.1 Vulnerability

Vulnerability, česky zranitelnost, je jakákoliv slabina, chyba nebo vada v zabezpečení, která by mohla ohrozit bezpečnost systému a útočník kvůli ní získat přístup k sensitivním informacím. Těchto zranitelnosti existuje nespočitatelné množství – od chyby v kódu nebo programech až po napsaná hesla na papíru připnutá k monitoru.

Je mnoho různých způsobu, jak se zranitelnostem vyhnout. Mezi nejčastější patří aktualizace softwaru operačních systému, programů a antivirů. Neméně důležité je vzdělávat uživatele v oblasti kybernetické bezpečnosti.

3.3.2 **Threat**

Threat je určitá hrozba – vytvořená člověkem nebo přírodou – která může mít negativní důsledek pro firmu a zapříčinit poškození nebo únik důvěrných informací. Z pohledu CIA triády je to cokoliv, co má za důsledek porušení jednoho z jejích pilířů. Hrozeb existuje nevyčíslitelné množství a mohou být rozděleny dle následující zjednodušené hierarchie.



Obrázek 1: Klasifikace hrozeb (zdroj: autor)

3.3.3 **Exploit**

Exploit je určitý způsob, jak narušit zabezpečení systému skrz zranitelnost (vulnerability). Často je předpřipravený, dostupný na internetu a využívaný k tomu, by útočník získal neautorizovaný přístup do IT systémů, sítě, softwaru apod.

Výrobci softwaru provádějí pravidelné aktualizace, aby v programech bylo co nejméně chyb a zranitelností. Pokud chyba není nahlášena a opravena, stává se z ní vstupní místo pro kybernetické zločince. V dnešním moderním světě, kde je propojeno obrovské množství různých zařízení, nejsou v případě úspěšně provedeného exploitu ohrožena jen jednotlivá zařízení, ale i celá síť, na kterou jsou zařízení připojeny.[2]

3.3.4 **Risk**

Riziko je ve smyslu kybernetické bezpečnosti pravděpodobnost vystavení se ztrátě kritických aktiv nebo citlivých informací v důsledku kybernetického útoku. Tyto rizika přicházejí v různých formách a neustále se vyvíjí.[3] Cílem každé entity je tedy co nejvíce minimalizovat toto riziko. V posledních letech se rozšířil tzv. CSaaS (Cybersecurity as a service), kdy si společnost zaplatí, aby se o snížení kybernetických rizik postarala jiná firma, která je na tuto oblast specializována.

3.3.5 **Dvoufázové ověření**

Dvoufázové ověření je bezpečnostní mechanismus, který od uživatele vyžaduje kromě jeho hesla další způsob ověření své identity před tím, než mu bude poskytnut přístup do požadovaného systému nebo aplikace.

„Faktorem ověřování je způsob, jak potvrdit vaši identitu při pokusu o přihlášení. Například heslo je jedním z faktorů, je to věc, kterou znáte. Tři nejběžnější typy faktorů jsou:

- *Něco, co znáte – třeba heslo nebo zapamatovaný PIN kód.*
- *Něco, co máte – třeba smartphone nebo zabezpečený USB klíč.*
- *Něco, co jste – třeba otisk prstu nebo rozpoznávání obličeje.”*[4]

V případě, že se útočník dostane k heslu své oběti, nebude útočníkovi poskytnut přístup, pokud by jeho oběť nepotvrdila např. na svém mobile schválení přístupu.

3.4 Kybernetická válka a její různé podoby

V posledních několika dekádách se kybernetické útoky proti celým státům stávají stále více frekventované a sofistikované. S tím, jak se kybernetické útoky vyvíjí a rozšiřují, je stále důležitější pochopit jejich mnoho podob, ve kterých se mohou vyskytovat.

3.4.1 Špionáž

Špionáž je forma kybernetického útoku proti jinému státu, která má za cíl ukrást tajná data nebo informace k získání ekonomické, politické či vojenské výhody nad tímto státem.[5] Určitý typ špionáže byl přítomný v každé době, ale s rozmachem informačních technologií se forma, jakou je špionáž prováděna, postupně mění – informace mohou být ukradeny vzdáleně. Cílem se stává především know-how, armáda, politici a politické strategie.

3.4.2 Sabotáž

Kybernetická sabotáž je způsob doručení určité hrozby v kybernetickém prostoru, která má za cíl narušit normální fungování procesů a funkcí, nebo zničení vybavení a informací vybraného státu. Hrozby sabotáže jsou jak externí, tak interní – nejčastější formy jsou přes internet, při výrobním procesu nebo fyzickým kontaminováním předmětu sabotáže.[6] Útočník tím dokáže vyřadit z provozu kritickou infrastrukturu, a proto je to pro bezpečnost každého státu stále důležitější záležitost.

3.4.3 Propaganda a falešné zprávy

V moderním světě, kde je vše propojeno informačními technologiemi a sociální sítě jsou všudypřítomné, se propaganda a falešné zprávy ukazují jako obrovské příležitosti pro ovlivňování názoru běžné populace, všech druhů voleb, hodnot akcií apod.

Jako příklad může být uvedeno, když na sociální platformě Twitter útočníci nelegálně převzali kontrolu nad účtem americké tiskové agentury Associated Press a následně přes něj šířili falešné zprávy o výbuchu v Bílém domě, který měl zranit tehdejšího prezidenta Obamu. V reakci na to utrpěl akciový trh Dow Jones obrovské ztráty v podobě 136 miliard amerických dolarů. Falešná zpráva měla tím pádem za důsledek přímou ztrátu bohatství investorů.[7]

3.4.4 **Útok na infrastrukturu státu**

Kybernetické útoky na infrastrukturu státu mohou mít velmi závažné důsledky, mezi něž patří například narušení nezbytných služeb poskytovaných státem, ztráta důležitých dat a ohrožení národní bezpečnosti.

Mezi časté cíle útoku může patřit:

- Elektrická síť
- Vodovodní systémy – přerušení kontroly kontaminované vody
- Komunikační sítě
- Dopravní systémy

Častým cílem je právě elektrická síť, která bude rozvedena detailněji. Příčiny výpadku dodávky elektřiny jsou tyto: porucha způsobena přírodními vlivy, významný přetok energie ze zahraničních rozvodných soustav, technické poruchy, lidský faktor, teroristický útok[8] nebo kybernetický útok.

Kybernetický útok na elektrárnu je velice nebezpečný, protože v případě, kdy se elektrárna dostane pod kontrolu útočníků, má situace negativní, v případě jaderných elektráren až katastrofální, vliv na daný stát a jeho občany, podniky, ekonomiku apod. V zájmu každého státu je zabezpečení této kritické infrastruktury na co nejvyšší úrovni, i za cenu vysokých finančních nákladů.

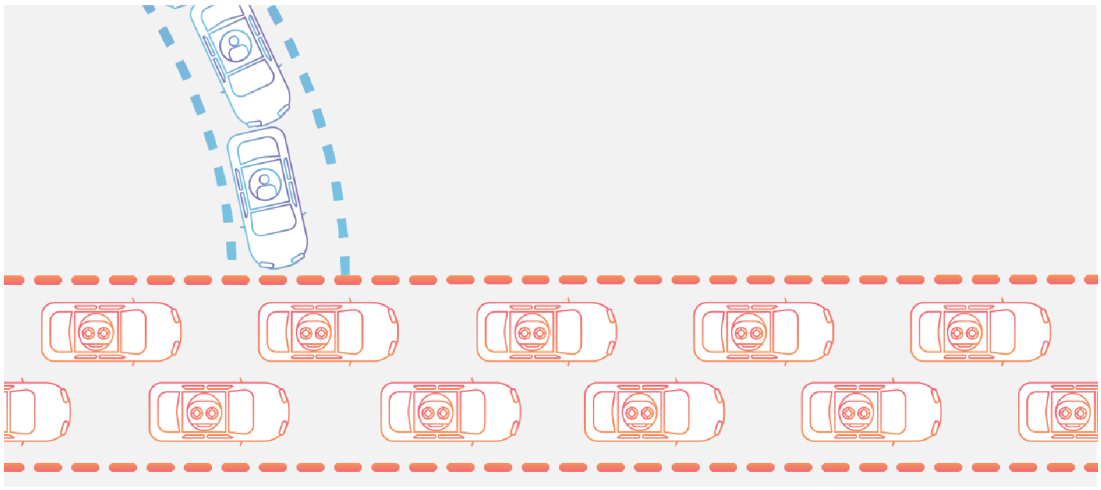
V důsledku těchto obav, byl vytvořen takzvaný blackout simulátor, který porovnává náklady výpadku dodávek elektřiny na ekonomiku s nasazením drahých protiopatření, které by výpadku zabránily. Tato protiopatření obsahují například instalaci záložního elektrického vedení, nebo z IT hlediska zašifrování informací.[9]

3.4.5 **Denial-of-Service**

Cílem DoS útoku je přetížit daný server stále se opakujícími požadavky v takové míře, že server není schopen stíhat posílat odpovědi, což má za důsledek jeho zahlcení a následný výpadek příslušné služby, například webu, který přestane být dostupný.

Podtypem DoS útoku je DDos, anglická zkratka pro Distributed Denial-of-Service, jenž je charakterizován DoS útoky z vícero počítačů, které jsou často hacknuty útočníkem, a z různých lokalit po celém světě. Sofistikovanější DDoS útoky nejsou jen jednoduché požadavky (typu načíst webovou stránku) na cílovou IP adresu serveru, ale požadavky, které simulují reálné chování běžných cílových uživatelů. Tento složitější typ DDoS útoku je pro server mnohem těžší odhalit.

Zjednodušeně by se DDoS útok dal vysvětlit pomocí následujícího obrázku. Oranžová auta jsou autentičtí uživatelé dané služby. Modrá auta, která přijíždějí do oranžového pruhu, jsou v tomto případě DDoS útoky, které následně blokují oranžová auta, tedy opravdové uživatele.



Obrázek 2: What is a DDoS attack? (zdroj: CloudFlare)[10]

Možností, jak se DDoS útokům bránit, je hned několik. Základní pilíře bezpečnosti proti tomuto typu útoku jsou následující:

- Znát provoz dané sítě a v případě podivných schémat provozu začít jednat dle protokolu, který by měla organizace mít vytvořený.
- Automatizované systémy, které zablokuj IP adresu v případě velkého množství podezřelých požadavků z ní přicházejících.
- Servery by měly být rozmístěny v různých lokalitách, aby útočník potřeboval poslat požadavky na více různých IP adres.
- Přesun do cloudu – souvisí s předchozím bodem. Cloud má ve své podstatě rozmístěné servery v nejrůznějších lokalitách. Pro útočníka nesrovnatelně těžší provést úspěšný útok, avšak stále nikoliv nemožný.
- Outsourcing ochrany – specializovaná společnost poskytne nejvyšší možnou formu zabezpečení.

Všechny výše vyjmenované možnosti ochrany jsou velmi důležité. Nejlépe se zabezpečení zvýší kombinací více opatřeními.

3.5 Motivy útoků

Kybernetické útoky mohou mít řadu motivů – od finančních až po politické cíle. Pochopení motivu útoku je stěžejní pro vytvoření efektivní strategie kybernetické bezpečnosti. V této části jsou prozkoumány nejčastější motivy, které za útoky stojí, spolu s cílem, kterého chce útočník dosáhnout.

Motivy se dle společnosti IBM dělí do třech hlavních kategorií:[11]

- Kriminální – např. finanční zisk
- Politické – např. hacktivismus, kybernetická válka
- Osobní – např. bývalí zaměstnanci nebo bývalí partneři

Z těchto kategorií byly autorem vybrány 3 podkategorie, které mohou nějakým způsobem zasáhnout státní orgány – finanční, hacktivismus a kybernetická válka.

3.5.1 Finanční

V moderním světě, kde se většina finančních transakcí přesunula do digitální podoby, toto logicky následovaly i různé kriminální skupiny. Z jejich pohledu je to jednodušší, bezpečnější, méně riskantní a více výdělečné.

Finanční zisk je motivem ale i pro některé státy, které tyto finance poté využívají k jiným, například vojenským, účelům – příkladem může být Severní Korea.[12]

Způsoby kybernetických útoku pro finanční zisk mohou být pro názorný příklad následující:

- Sociální inženýrství – útočník se pomocí sociální interakce a komunikace se svou obětí postupně dostane k citlivým údajům jako například bankovní účty nebo kreditní karty. V tomto případě z toho má přímý zisk jen sám útočník.
- Na takzvaném „dark webu“, což je síť, která je přístupná jen pomocí specializovaného softwaru, nabízejí hackeři získání citlivých údajů oběti dle požadavku objednavatele za úplatu.
- Na zařízení oběti může být nainstalován škodlivý kód, který bez jejího vědomí těží kryptoměny za použití infikovaného zařízení.
- Manipulace s akciovými trhy – útočník se získá přístup k utajovaným informacím nebo rozšíří falešné zprávy, které zmanipulují akciový trh, a tudíž z toho může profitovat

3.5.2 „Hacktivismus“ – Politická motivace

„Hacktivismus“ je slovo stvořené fúzí slov hacking a aktivismus. Cílem „hacktivisty“ je určitým způsobem prosadit svoje politické, náboženské nebo životní názory za použití některých kybernetických útoků na různé entity jako například vláda nebo státní orgány.

„Hacktivismus si typicky klade za cíl splnění jedné nebo více z následujících cílů:

1. Zastavit nebo přerušit financování terorismu
2. Obejít zákony o cenzuře vyhlášené vládou
3. Vyjádřit nesouhlas s válkou
4. Využití sociálních médií k pomoci lidem, kteří jsou cenzorováni nebo jsou porušovány jejich práva
5. Vyjádřit nesouhlas s kapitalismem
6. Zaútočit na vládní webové stránky, které se snaží zastavit státní převrat
7. Podpořit demokracii a svobodu slova
8. Pomoct migrantům dostat se přes státní hranice
9. Pomoct lokálním povstáním
10. Podrýt sílu vybrané korporace
11. Zdiskreditovat vládního představitele“[13]

Většina z výše jmenovaných cílů používá prostředky, které jsou za hranou zákona, a můžou být trestány jak finančně, tak odnětím svobody.

3.5.3 Kybernetická válka

Hlavní motivací mezistátního hackingu, respektive kybernetické války, je získání informační, vojenské nebo ekonomické výhody jednoho státu nad druhým. Používají se k tomu téměř všechny techniky kybernetických útoků, nejčastěji například DDoS útok nebo špionáž.

Dalším důležitým faktem je, kdy tyto útoky probíhají. Pokud se vezme v úvahu špionáž, je pravděpodobné, že probíhá téměř nepřetržitě, aby stát A věděl, co má stát B v plánu nebo co probíhá v jeho vnitřní politice. V dnešní době už není tolik častá fyzická špionáž, ale spíše různé techniky využívající informační technologie.

Když jde o útok na infrastrukturu cizího státu, jedná se naopak spíše o jednorázovou akci. Příkladem může být útok na komunikační technologie a elektrickou síť před plánovanou invazí státu A na stát B, což může státu A dát velkou výhodu a snížit jeho ztráty a na druhou stranu stát B úplně ochromit, snížit jeho obranyschopnost a koordinaci armády.

4 Vlastní práce

Teoretický základ pro praktickou část je uveden v předchozích kapitolách. Orientuje se na základní znalosti z oboru kybernetické bezpečnosti, které jsou nutné k pochopení praktické části.

Tato část práce je věnována komplexnímu prostředí kybernetických hrozeb, ve kterém jako alespoň jeden z aktérů útočník/oběť vystupuje stát. V dnešní době závisí efektivní fungování státu na informačních technologiích, které poměrně rychle nahradily (v některých oblastech ještě nahrazují) předešlý způsob zaznamenávání informací. Spolu s rychlým rozšiřováním informačních technologií začala být hrozba a sofistikovanost kybernetických útoků větší. Z tohoto důvodu jsou v práci nejdříve zanalyzovány nejčastější typy kybernetických útoků a dále jsou prozkoumány kybernetické útoky, které byly v minulosti směřovány na Českou republiku. Dále je k dispozici detailnější analýza nejangažovanějších států na poli kybernetických útoků a vybrané závažné útoky jsou rozebrány do detailu – důvod, důsledek a autorem navrhovaná protiopatření útoku. Na základě informací získaných z těchto analýz, se autor věnuje otázce, co by v budoucnu mohlo České republice z kybernetického pohledu hrozit. Nakonec jsou získané znalosti použity k návrhu konkrétních doporučení na zlepšení kybernetické obrany České republiky.

4.1 Nejčastější typy kybernetických útoků a jejich porovnání

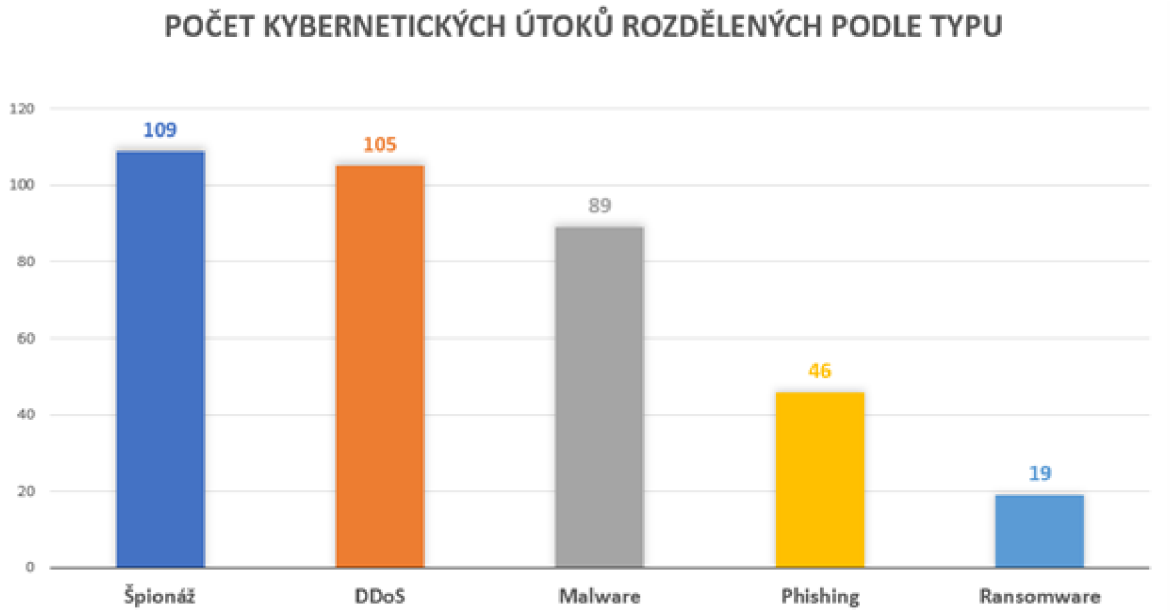
Z veřejně přístupných dat vytvořených organizací EuRepoC (European Repository of Cyber Incidents) byla stažena databáze o kybernetických incidentech (https://eurepoc.eu/databases - EuRepoC Global Database 1.0)[14], které tato organizace dokázala zaznamenat a nashromáždit od roku 2000 do současnosti.

Celkem bylo provedeno 1458 kybernetických útoků. Každý jednotlivý záznam obsahuje následující:

- Název útoku
- Popis útoku
- Datum začátku a konce incidentu
- Z jakého státu útok pocházel
- Do jakého státu útok směřoval
- Kategorie – mohl cílit na vládu, média, kritickou infrastrukturu atd.
- Mnoho dalších informací, které nejsou pro tuto práci relevantní

4.1.1 Statistika typů provedených útoků

Jelikož databáze neobsahuje typ kybernetického útoku, bylo nutné z dat manuálně typ útoku získat. K tomu byly využity sloupce Název útoku a Popis útoku, ve kterých byly vyhledávány typy útoků, respektive tato klíčová slova – Špionáž, DDoS, Phishing a Malware. Z výstupu byla vytvořena kontingenční tabulka, za pomocí které autor provedl součet výskytů jednotlivých klíčových slov. Z tabulky byl následně vytvořen graf, který ukazuje četnost výskytu jednotlivých typů kybernetických útoků.



Obrázek 3 Počet kyb. útoků rozdělených podle typu (zdroj: autor, EuRepoC)

Z výsledného grafu lze vyvozovat, že špionáž se řadí mezi nejčastější typ útoku se 109 incidenty následována DDoS typem útoku se 105 případy. O dvě desítky méně případů bylo malwaru, který je ale též velmi používaný a nebezpečný.

Méně častý je potom phising, který je používaný spíše v soukromé sféře, kdy jde útočníkovi pouze o finanční zisk.

Na posledním místě v rámci autorem analyzovaných typů útoků se nachází ransomware s 19 incidenty. Tato hrozba je také častěji využívána v soukromém sektoru – útočníkovi nezáleží tolik na tom, jakému státu tím způsobí škody, ale spíše kolik uživatelů tím zasáhne. To mohlo být vidět například na ransomware pod označením WannaCry, který uživatelům nezávisle na lokalitě zašifroval data v počítačích a pro získání kódu pro dešifrování vyžadoval platbu v kryptoměně.

4.1.2 Útoky na Českou republiku

Další informace, které se dají z databáze organizace EuRepoC získat, jsou kybernetické útoky vedené proti České republice. K tomu bylo potřeba prohledat celou databázi a zjistit, ve kterých buňkách se nachází klíčové slovo „Czech“. Výsledkem je 5 kybernetických útoků, což se může z databáze o 1458 záznamech zdát poměrně málo. Konkrétně se jedná o tyto útoky:

Hack mailu tehdejšího premiéra Sobotky

Začátek útoku: 1.1.2016

Konec útoku: 1.1.2016

Typ útoku: nespecifikovaný

Krajně pravicová skupina získala přístup k emailovému účtu tehdejšího premiéra České republiky Bohuslava Sobotky a zveřejnila je na krajně pravicovém webu.

Ruský hack českého Ministerstva zahraničí

Začátek útoku: 1.1.2016

Konec útoku: 1.12.2017

Typ útoku: špionáž, malware, phishing

Tato hrozba trvala skoro 2 roky. Jejím původcem byly 2 ruské kyber-špionážní skupiny, které cílily na Ministerstvo zahraničí ČR, Ministerstvo obrany ČR a Armádu ČR. Tato dlouhotrvající hrozba byla odhalena společností BIS (Bezpečnostní informační služba), která uvedla, že útočnici získali přístup k několika osobním emailovým adresám patřícím lidem s vazbami právě na Ministerstvo obrany a Armádu ČR.

Gambling hack

Začátek útoku: 30.5.2016

Konec útoku: 30.5.2016

Typ útoku: DDoS

Hackeři zaútočili na webové stránky Vlády ČR kvůli plánovaném zákazu domén s hazardním obsahem. Pravděpodobně se jednalo o DDoS útok.

DDoS ČSÚ

Začátek útoku: 21.10.2017

Konec útoku: 24.10.2017

Typ útoku: DDoS

Tento útok měl za cíl přehltit dvě webové stránky Českého statistického úřadu, které měly zveřejňovat výsledky voleb do Parlamentu ČR. Dle ČSÚ útok nijak neovlivnil počty hlasů.

Útok na české Ministervo zahraničí

Začátek útoku: 1.6.2019

Konec útoku: 1.6.2019

Typ útoku: DDoS

Útok přehlcením mířený na Ministerstvo zahraničí ČR vykonaný ruskou kybernetickou skupinou Fancy Bear.

4.2 Analýza angažovanosti vybraných států v signifikantních kybernetických útocích

Na základě veřejně dostupných dat[15] od uznávané americké think tank společnosti CSIS (Center for Strategic and International Studies) o signifikantních kybernetických útocích byly autorem práce všechny tyto závažné incidenty zanalyzovány v programu Microsoft Excel. Autor nejprve nakopíroval textovou podobu zdrojových dat do prázdného sešitu a následně byl každý jeden záznam postupně zanalyzován. U každého záznamu se autor zajímal o následující informace:

- Útočník – jaký stát provedl útok
- Oběť – jaký stát byl obětí útoku
- Měsíc – v jakém měsíci roku 2022 se útok odehrál

U některých záznamů mohla být jedna z informací vynechána. Existuje nemalé množství incidentů, kdy za útokem stálo vícero hackerů z různých států světa, nebo neexistovaly důkazy, jaký stát má útok na svědomí. To samé platí pro oběť, protože v některých případech bylo zasaženo tolik států, že ze statistického hlediska by to výsledek spíše zkreslilo.

Jelikož jsou tato data čerpány z americké společnosti, existuje určitá pravděpodobnost, že na ně má nějaký vliv americká vláda, a tudíž můžou být některé incidenty, ve kterých USA figurovalo jako útočník, vynechány z důvodu informační války.

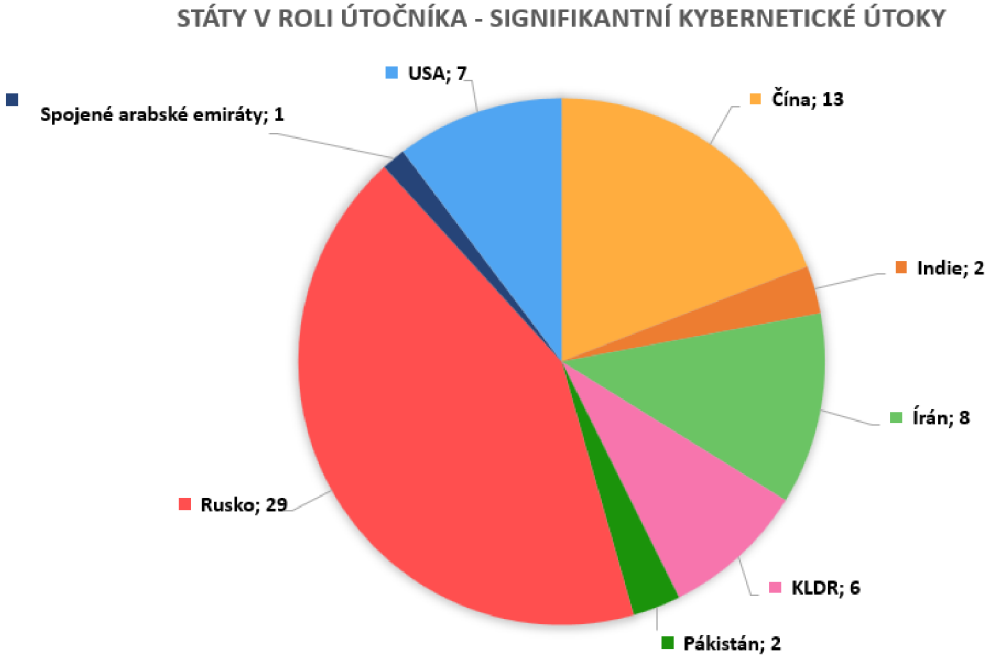
Printscreen autorem vytvořené tabulky, ve kterých je definován Popis útoku, který byl získán z CSIS databáze signifikantních kybernetických útoků, Útočník, Oběť a Měsíc, kdy byl útok proveden:

Popis	Útočník	Oběť	Měsíc útok
November 2022. The UAE hired three former U.S. intelligence and military officials to help the government break into computers in the United States and other countries.	Spojené arabské emiráty	USA	Listopad
November 2022. Microsoft attributed cyberattacks aimed at transportation and related logistics industries in Ukraine and Poland to a Russian GRU hacking group. The campaign began in late September 2022.	Rusko	Ukrajina Polsko	Listopad
November 2022. Hackers targeted Bahraini government websites with DDoS attacks prior the country's parliamentary and local elections.		Bahrajn	Listopad
November 2022. Iranian government-sponsored hackers compromised the U.S. Merit Systems Protection Board, exploiting the log4shell vulnerability as early as February 2022. After breaching the network, hackers installed cryptocurrency-mining software and deployed malware to obtain sensitive data.	Írán	USA	Listopad
November 2022. Hackers damaged Danish State Railways' network after targeting an IT subcontractor's software testing environment. The attack shut down train operations for several hours.		Dánsko	Listopad
November 2022. An Indian-based hacking group targeted Pakistani politicians, generals and diplomats, deploying malware that enables the attacker access to computer cameras and microphones.	Indie	Pákistán	Listopad
November 2022. State-sponsored hackers with possible ties to the Chinese government targeted multiple Asian countries in an espionage operation since March 2022, compromising a digital certificate authority in one country.	Čína		Listopad
November 2022. Hackers disabled digital services of the Vanuatu government in a cyberattack. The attack affected all government services, disabling emails, websites, and government systems, with only partial access restored a month later. Australian sources stated the hack was a ransomware		Vanuatu	Listopad

Obrázek 4 Printscreen tabulky signif. útoku v roce 2022 (zdroj: autor, CSIS)

4.2.1 Útočník

Z předchozí tabulky byla autorem vytvořena kontingenční tabulka, která odhaluje četnost, kolikrát se který stát angažoval v těchto signifikantních útocích. Následně byl z kontingenční tabulky vytvořen koláčový graf, kde vidíme vybrané státy a kolikrát byly v roli útočníka v roce 2022 v signifikantních kybernetických útocích.



Obrázek 5 Státy v roli útočníka - signifikantní kybernetické útoky (zdroj: autor)

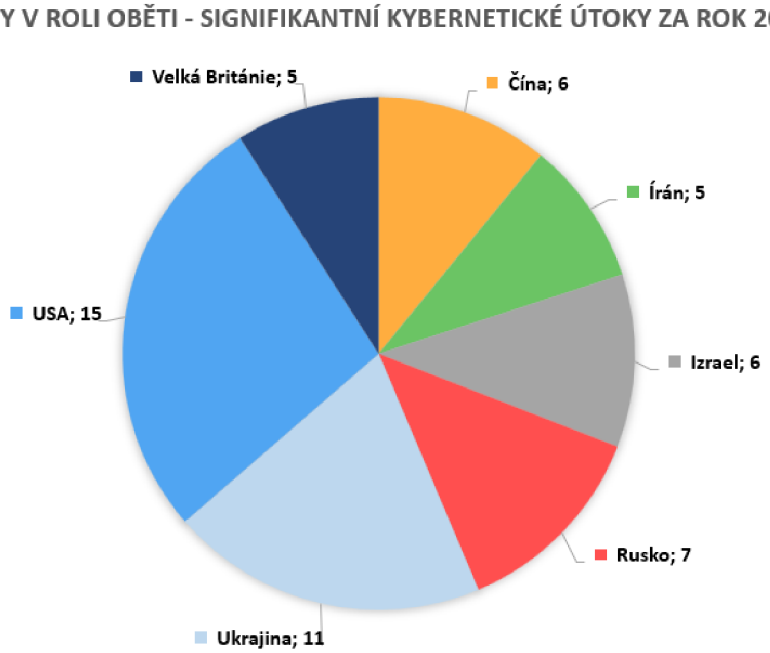
Z grafu jednoznačně vyplývá, že Ruská federace je nejčastějším původcem signifikantních kybernetických útoků. V minulosti bylo Rusko v tomto odvětví velmi aktivní, ale rok 2022 překonává minulé roky, kdy Rusku konkurovalo USA, Čína nebo Írán. Hlavním důvodem nepochybně bude únorová ruská invaze na Ukrajinu, která byla koordinována právě s kybernetickými útoky, které jsou v dnešním způsobu vedení války naprostou nezbytností.

Na druhém místě v četnosti úspěšných signifikantních útoků byla Čína, jejíž kybernetické útoky byly rozesety po celém světě. Čína už tradičně cílila hlavně na USA, ale také na státy v jihovýchodní Asii, kde chce posilovat svůj vliv. Dále se také angažovala v útocích na Taiwan, kde bylo v průběhu roku 2022 z důvodu čínské expanzivní politiky neustálé politické a vojenské napětí. Čínská vláda nezapomněla ani na Austrálii nebo některé státy Evropy jako například Německo a Belgii.

V neposlední řadě stojí za zmínku Írán a KLDR, kteří se angažuji na poli kybernetického zločinu ve velké míře a v podobném měřítku. Dle autorova názoru by se íránská kybernetická aktivita dala přisoudit reakci na červ Stuxnet, který měl pro Írán závažné následky, a tudíž se rozhodl vylepšit své působení v kybernetickém oboru.

4.2.2 **Oběť**

Z analýzy dat mezistátních signifikantních kybernetických incidentů byla autorem práce vytvořena kontingenční tabulka, ve kterém byla pro každý stát spočítána četnost, kdy se stal obětí kybernetického zločinu. Některé státy byly vynechány, protože se obětí staly jen výjimečně, a tudíž nemá smysl je ve statistice uvádět. Byl nastaven filtr pouze na hodnoty větší než 3. Výsledkem bylo 7 států.



Obrázek 6 Státy v roli oběti - signifikantní kybernetické útoky (zdroj: autor)

Z grafu můžeme vidět, že nejčastěji byly kybernetické útoky vedeny proti Spojeným státům americkým. Cílilo na ně především Rusko a Čína, což už je tradičně vzájemné. Jak už bylo jednou řečeno, z důvodu dat získaných od společnosti, která je financována Spojenými státy, nemusí být data 100% spolehlivá, jelikož USA logicky bude chtít „vypadat dobře“ a spíše se bude tvářit jako častější oběť.

Na druhém místě v četnosti kybernetických útoků se nachází Ukrajina, na níž byla valná většina útoků mířená z Ruska pro zvýšení šance na úspěch své vojenské invaze, kterou často koordinuje právě s vojenskými akcemi.

Rusko se logicky také stávalo terčem kybernetických útoků ze strany Ukrajiny, potažmo USA, které Ukrajinu v obraně před ruskou agresí podporují.

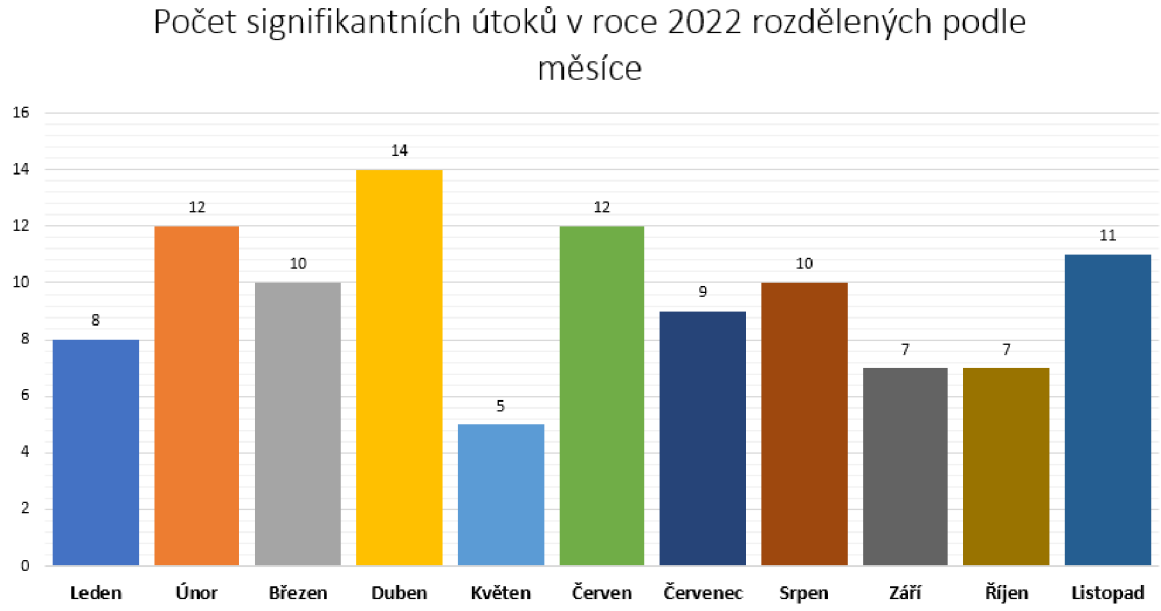
Dále se v grafu se šesti signifikantními incidenty objevil Izrael, který se v první statistice útočících států vůbec nevyskytoval. Podle autorova názoru je hlavním důvodem fakt, že Izrael se vypořádává s problémy zejména v pásmu Gazy, což není oficiální stát, a Palestinci, kteří vlastní stát nemají. S USA má Izrael velmi dobré vztahy a s Ruskem usiluje o udržování co nejdiplomatičtějších vztahů, a proto se kybernetickým útokům na Ruskou federaci snaží vyhýbat.

Nakonec stojí za zmínku Čína a Írán, které mají podobný počet incidentů jako Izrael nebo Velká Británie. V případě Číny byly všechny útoky vedené ze Spojených států amerických. Naopak u Íránu je většina signifikantních incidentů bez jednoznačného viníka, ale dá se odhadovat, že byly pravděpodobně vedeny také pod taktovkou Spojených států amerických. Jen jeden útok byl veden z Pákistánu.

Proti Velké Británii byly útoky vedeny z Ruska nebo Íránu.

4.2.3 **Měsíc útoku**

Následující graf byl vytvořen pro srovnání četnosti útoků v jednotlivých měsících za rok 2022. V grafu je vynechán měsíc prosinec, jelikož pro něj je dostupný jen jeden záznam, který se nedá přisoudit žádnému státu jak v roli útočníka, tak v roli oběti.



Obrázek 7 Počet signif. útoků v roce 2022 rozděl. podle měsíce (zdroj: autor)

Celkem se tedy za rok 2022 uskutečnilo 105 signifikantních kybernetických útoků. Nejčastěji byly provedeny v měsíci únor, duben a červen. Při analýze dat bylo jednoznačně vidět, že v průběhu ruské invaze na Ukrajinu v únoru se počet kybernetických incidentů zvýšil. Vysoké čísla byla i v březnu a následně v dubnu, jenž má za rok 2022 nejvyšší počet incidentů.

Naopak mezi „klidnější" měsíce by se řadilo září a květen, kdy byl v obou měsících počet útoků jen 7. Nejméně signifikantních incidentů se odehrálo v květnu, kdy jich bylo „pouhých" 5. Pokud bychom počítali prosinec, byl to jen 1 incident, ale je možné, že databáze nebyla při psaní práce na začátku ledna 2023 ještě aktualizována.

4.3 Rozbor závažných kybernetických útoků od roku 2000

V této části práce jsou vypsané vybrané kybernetické útoky, které byly provedeny nějakým státem nebo byly proti nějakému státu mířeny. Pro lepší přehlednost jsou útoky u každého kybernetického útoku uvedeny následující informace:

- **Důvod útoku** – Co vedlo útočníka k tomu, aby útok provedl? Čeho chtěl v případě úspěšného provedení dosáhnout?
- **Důsledek útoku** – Jaké byly důsledky a dopady útoku?
- **Protiopatření útoku** – Jaká byla nebo mohla být protiopatření, aby se útok podařilo odrazit nebo jej alespoň minimalizovat?

4.3.1 Operation Aurora – Čínský útok na Google (2009)

Operace Aurora byl útok provedený čínským režimem na americký soukromý sektor, konkrétně byla cílem hlavně společnost Google, která jako jediná veřejně přiznala, že byla obětí úspěšného kybernetického útoku. Mezi další, na které byl útok směřován, bylo více než dvě desítky společností, konkrétně například Yahoo, Adobe, Dow Chemical nebo Morgan Stanley.

Důvod útoku

V případě směřovaného útoku na společnost Google, patřilo mezi hlavní důvod získání informací o čínských lidskoprávních aktivistech a dalších osob, u kterých čínský režim věřil, že by jimi mohl být ohrožen či zdiskreditován. V případě ostatních společnost chtěla Čína získat informace o jejich obchodních tajemstvích.

Důsledek útoku

Tento útok je vnímaný jako milník v kybernetických operacích a jejich použití pro účely špionáže.

Společnost Google veřejně připsala provedený útok čínskému režimu, což bylo do té doby poměrně nevídané, jelikož společnosti se nařknutí celého státu z útoku kvůli obchodním důvodům spíše vyhýbaly (v tomto případě nechtěly přijít o čínský trh). Google v důsledku snížil svoje působení v Číně. V Hong Kongu stále působí.

Všichni uživatelé, u kterých Google věří, že mohli být obětí útoku, byli notifikováni.[16]

Protiopatření útoku

Jelikož se jednalo o útok typu phishing, hlavním protiopatřením mělo/má být hlavně vzdělávání uživatelů v oblasti bezpečného používání internetu a rozpoznávání potenciálně nebezpečných mailů, které mají za cíl z uživatelů dostat jejich citlivé údaje nebo hesla.

Další protiopatření by mohlo být rozpoznávání a označování nebezpečných mailů samotnou mailovou službou Gmail.

4.3.2 Stuxnet (2010)

Stuxnet je počítačový červ, který byl vytvořen, aby získal kontrolu na Íránským jaderným programem, respektive zařízeními, které kontrolují centrifugy. S největší pravděpodobností byl vytvořen vládami Spojených států amerických a Izraelem, ale nikdy to nebylo oficiálně prozrazeno nebo uznáno těmito vládami. Stuxnet je považován za pravděpodobně první kybernetickou zbraň, která poškodila fyzickou infrastrukturu.

Důvod útoku

Spojené státy americké a Izrael byli zneklidněny rychlostí, s jakou se Íránský jaderný program vyvíjí. Zvažovány byly i letecké útoky na jadernou infrastrukturu, ale to se nakonec neuskutečnilo z důvodu obav z konfliktu regionálních nebo dokonce globálních rozměrů. Vlády se proto rozhodly pro méně riskantní útok, tedy kybernetický, který cílil na jadernou infrastrukturu.

Důsledek útoku

Stuxnet se dostal do sítě Íránské jaderného programu a rozšířil se do počítačů a zařízení, které kontrolovaly centrifugy a jiná zařízení, která měla vliv na funkci jaderné infrastruktury. Stuxnet způsobil, že se centrifugy začaly točit příliš rychle po příliš dlouhou dobu. Mezitím program posílal falešná data do Íránských kontrolujících programů, kvůli kterým vypadalo, že vše funguje v pořádku.[17]

Protiopatření útoku

Červ Stuxnet byl s největší pravděpodobností do íránské sítě donesen a připojen přes obyčejný USB flash disk dvojitým agentem, který byl najmut izraelskou vládou.[18]

Před tímto útokem by se dalo chránit určitými restrikcemi u každého počítače nebo zařízení, které má USB porty. I tyto restrikce se však dají jistými technikami obejít, jelikož osoba, která v tomto případě chtěla síť infikovat, byla u zařízení fyzicky přítomna.

Dalším způsobem, kterým se může infikování sítě minimalizovat, je v případě velmi tajných projektů co největší prověřování nových zaměstnanců, kteří mají mít přístup ke kritické infrastruktuře a následně i co největší dozor nad nimi.

4.3.3 Útoky na ukrajinskou elektrickou síť (2015)

Dne 23. prosince 2015 byl proveden kybernetický útok na elektrárnu nacházející se v Ivanofrankivské oblasti, který s největší pravděpodobností spáchán ruskými hackerskými skupina s vazbami na ruskou vládu. Jedná se o první známý úspěšně provedený útok na elektrickou síť. Další podobný útok byl proveden o rok později na severu Kyjeva.

Důvod útoku

Ruská vláda tyto útoky koordinovala se svými politickými a vojenskými zájmy na Ukrajině, které se uskutečnily na pozadí s anexí Krymu a ruskými vojenskými akcemi v Doněcké a Luhanské oblasti.

Dalším důvodem byla větší intenzita destabilizace Ukrajiny a demonstrace síly ve smyslu, že Rusko může udeřit kdekoliv na Ukrajině.

Důsledek útoku

Vzhledem k tomu, že to byl první potvrzený úspěšný útok na kritickou infrastrukturu, se některé státy, logicky pak hlavně Ukrajina, rozhodly posílit kybernetickou bezpečnost elektráren a různých energetických zařízení.[19]

Protiopatření útoku

Kybernetické útoky na kritickou infrastrukturu jsou těžko předvídatelné, a tudíž není jednoduché se před nimi bránit. Z tohoto důvodu nemusí být omezení rizika na úplné minimum žádoucí, protože to není nákladově efektivní. Proto je tu snaha vytvořit určité procesy, které by co nejvíce snížili následky těžko předvídatelných útoků.[20]

4.4 Kybernetické hrozby pro ČR

Na základě předchozí kapitoly a analýze úspěšně provedených kybernetických útoků je evidentní, že tento typ hrozeb by v případě, kdy by Česká republika byla obětí, mohl mít velmi závažné důsledky na ekonomickou, vojenskou, bezpečnostní nebo společenskou situaci České republiky. Z tohoto důvodu se kybernetická bezpečnost stává pro stát stále významnějším oborem, a proto byl 1. srpna 2017 založen Národní úřad pro kybernetickou a informační bezpečnost (dále jen NÚKIB), který je ústředním orgánem pro kybernetickou bezpečnost. Mezi jeho hlavní činnosti se řadí následující:

- sledování aktuálních trendů v oblasti kybernetického zločinu
- monitoring kybernetických hrozeb pro ČR
- reakce na kybernetické incidenty a vyhodnocení jejich závažnosti
- zajištění vzdělávání odborníků, firem a občanů v příslušné problematice

Z autorova pohledu a jeho nasbíraných znalostí z analýzy úspěšných kybernetických útoků v kapitolách 4.1 a 4.2, je velmi pravděpodobné, že by se hackeři cizího státu snažili využít nejpoužívanější typy kybernetických útoků, které mají nejlepší poměr nákladu a užitku. Mezi ně patří DDoS, špionáž, phishing nebo malware. V případě zhodnocení závažnosti útoku a jeho důsledků velmi záleží na typu útoku.

Po vyfiltrování kybernetických incidentů zaměřených jen proti České republice z databáze EuRepoC bylo zjištěno, že ve více než 50 procentech se jednalo o DDoS typ útoku. Z toho lze usuzovat, že je vysoká šance, že by se podobný incident mohl opakovat. Útok přehlcením webové stránky naštěstí nemá tak velké následky, a zároveň existuje několik způsobů, jak zranitelnost snížit. Mezi ně patří kontinuální monitoring síťového provozu, díky kterému je možné přehlcení zabránit, protože se útoku zabrání v jeho brzké fázi, kdy ještě není v plném rozsahu. Jelikož se práce zabývá kybernetickou bezpečností pro Českou republiku, bylo by v případě DDoS útoku možné zablokovat veškerý síťový provoz ze zahraničí a zanechat jen provoz pocházející z území České republiky, což by mohlo významně snížit pravděpodobnost úspěšnosti útoku.

Závažnějším typem útoku by pro Českou republiku mohla být špionáž. Ta cílí na citlivá data uživatele a v konečném důsledku může být využita k získání výhody nebo ovlivnění cílové osoby – například v případě získání citlivých dat kohokoliv z vlády, může útočník pod pohrůžkou zveřejnění kompromitující informace ovlivnit rozhodování dané osoby ve vlastní prospěch. Příkladem by mohl být veřejně známý případ z roku 2014, kdy hackeři z KLDR získali přístup k citlivým údajům uživatelů společnosti SONY a následně vyhrožovali jejich zveřejněním v případě uvedení filmu „The Interview“ na trh. Z důvodu těchto a dalších výhružek nakonec film nebyl uveden v kinech, ale jen na streamovacích platformách.

Další významný útok by mohl proběhnout na elektrickou síť, kdy by úspěšně provedená akce mohla mít velké ekonomické, společenské nebo vojenské důsledky. Nejjednodušší pro útočníka je případ, kdy má přístup k rozvodnám elektrické sítě, a tudíž se mu naskýtá lehčí možnost provedení sabotáže. Sofistikovanější útoky mohou proběhnout pomocí počítačového červa, který by byl rozeset po internetové síti na různá IoT zařízení (chytré spotřebiče, kamery, osvětlení), kterých s postupem času enormně přibývá. V případě úspěšného rozesetí červa by do nakažených zařízení mohla být poslána informace, aby mělo každé zařízení co největší spotřebu energie, což by v případě desítek tisíc zařízení způsobilo přetížení elektrické sítě, případně jiné problémy na trafostanicích.

4.5 Doporučení na zlepšení kybernetické bezpečnosti ČR

Na základě informací získaných z teoretické části a autorově analýze kybernetických hrozeb, se tato kapitola věnuje doporučením, která by zefektivnila a zlepšila kybernetické zabezpečení České republiky.

4.5.1 Aktualizování sítí a systémů

Státem by měla být zajištěna neustála kontrola veškerého softwaru a hardwaru, který je používán na denní bázi. Software by měl být vždy aktualizován na nejnovější verzi spolu s instalací všech bezpečnostních „záplat“, které konkrétní výrobce ke svému softwaru vydá. Dobrým zvykem může být také kontrola, zda aktualizace software neobsahuje nějakou zranitelnost (exploit), která by útočníky mohla být využita.

Česká republika by měla mít centralizovaný program a alokovaný tým, který by kontroloval a nařizoval pravidelné aktualizace softwaru a hardwaru napříč všech státních subjektů a kritické infrastruktury.

4.5.2 Vzdělávání zaměstnanců

Pravidelné vzdělávání státních zaměstnanců je jeden z klíčových pilířů kybernetického zabezpečení. Stát může mít software pro podporu kybernetické bezpečnosti na nejvyšší úrovni, ale pokud na tomto poli zaostává ve vzdělávání svých zaměstnanců, bude stále velmi zranitelný.

Proto by měl poskytovat povinné školení svých zaměstnanců na pravidelné bázi. Minimálně jednou ročně by státní zaměstnanci měli mít ze zákona povinnost splnit test na téma kybernetické bezpečnosti – v soukromém sektoru a velkých korporátech se toto z vlastní iniciativy často již děje.

4.5.3 Omezení přístupu k citlivým datům

Přístup k citlivým datům a systémům má být omezen pouze pro pověřený personál, který je vzdělán, jak má s daty nakládat.

Musí být kladen důraz na vytváření silných hesel – vytvořit minimální požadavky pro hesla. Heslo nesmí například obsahovat slova ze slovníku, musí být minimálně o délce 10 znaků a obsahovat minimálně 1 malé písmeno, 1 velké písmeno, číslici a speciální znak. V případě, že by se vytvořilo co nejkratší heslo na základě těchto minimálních požadavků, existuje celkem 53 861 511 409 489 969 152 unikátních kombinací pro vytvoření hesla, a pokud by se všechny kombinace vyzkoušeli na průměrném počítači, zabralo by to nepředstavitelných 43 543 768 dní, tedy 119 218 let.

Ze zákona by mělo být také povinné dvoufázové ověření pro přístup k citlivým datům, což také poměrně razantně snižuje pravděpodobnost úspěšnosti kybernetického útoku.

4.5.4 Monitorování sítě

Dalším důležitým pilířem pro kybernetickou bezpečnost ČR by mělo být kontinuální monitorování sítí a systému v reálném čase. Velmi častým a efektivním řešením jsou systémy SIEM (Security Information and Event Management), které pomáhají při detekci bezpečnostních hrozeb a reagují na ně dříve, než způsobí větší škody.[21]

4.5.5 Vytvoření reakčních plánů na bezpečnostní incidenty

Zefektivnění kybernetické bezpečnosti tkví v tom vědět, co dělat, pokud se útočníkovi kybernetický útok povede a získá přístup například k citlivým datům. V tomto případě by měl reakční tým vědět, co je nutné udělat, aby se co nejvíce minimalizoval dopad útoku. K tomu slouží reakční plány a protokoly.

Pravidelně by se měla provádět cvičení kybernetické bezpečnosti, která by testovala schopnost státu reagovat na kybernetické útoky. Pomohlo by to s vyhodnocením kvality a efektivity reakčních plánu a případným odhalením nedostatků.

4.5.6 Audity

Jednou ročně by mělo probíhat pravidelné posouzení a zhodnocení kybernetických rizik a audit k identifikaci zranitelností a slabých míst kybernetické bezpečnosti. Stát by měl zavést povinné audity v oblasti kybernetické bezpečnosti pro všechny státní subjekty.

4.5.7 **Zálohování kritických dat**

Česká republika by měla pravidelně zálohovat všechna svá kritická data, aby mohla být v případě úspěšného kybernetického útoku a smazání dat, tato data jednoduše obnovena. Zálohy by měly být povinné a uloženy v ideálním případě na serverech na bezpečném místě mimo pracoviště.

5 Výsledky a diskuse

V následující části práci jsou shrnuty všechny výsledky, kterých autor dosáhl. Následuje diskuse, ve které se autor zaměřuje na význam jeho zjištění pro praxi. Dále je vedena diskuse, jaké by mohly být trendy v kybernetických prostoru do budoucna. Nakonec se autor zamýšlí nad limity této práce a navrhuje, jak by na toto téma mohla navazovat následná diplomová práce.

5.1 Výsledky

V praktické části byla nejprve autorem s použitím databáze EuRepoC provedena analýza nejčastějších forem kybernetických útoků, ze které bylo vyvozeno, že nejpravděpodobnější podoba útoku by byla jedna z trojice špionáž, DDoS nebo malware. Z této databáze, která obsahuje 1458 záznamů, byly rovněž extrahovány všechny útoky, které směřovaly přímo na Českou republiku – bylo jich pouhých 5, což je poměrně málo. Ve 3 případech se jednalo o typ útoku DDoS a v 1 případě o špionáž a malware, což podporuje autorovu analýzu nejčastějších podob útoku.

V další kapitole byla autorem provedena analýza nejangažovanějších států v signifikantních kybernetických útocích za rok 2022 za pomoci veřejně dostupných dat v textové podobě od organizace CSIS. Autor se zaměřoval na 2 hlavní kritéria – jaký stát útočil a jaký stát byl obětí útoku. Z této analýzy bylo zjištěno, že v roce 2022 bylo nejčastějším původcem kybernetických útoků Rusko, což se dá přisuzovat koordinaci s jeho únorovou invazí na Ukrajinu. Na druhém místě se s téměř poloviční četností útoků oproti Rusku vyskytovala Čína, která cílila hlavně na USA. Dalšími častými kybernetickými útočníky bylo právě USA nebo Írán a KLDR.

V roli oběti se nejčastěji za rok 2022 vyskytovalo USA, které bylo hned v závěsu následováno Ukrajinou, která by se v předchozích letech ve statistikách nevyskytovala tak často, ale kvůli Ruské invazi byla na vrchních příčkách. Další země, které se v roli oběti vyskytovali jen asi v polovině případech oproti Ukrajině, bylo Rusko, Izrael, Írán, Čína a Velká Británie.

Dále se autor zaměřil na rozbor vybraných závažných kybernetických útoků, o kterých detailněji zjišťoval důvody, které útočníka motivovaly, důsledky, které byly útokem způsobeny a navrhl protiopatření, která by mohla dopady co nejvíce minimalizovat.

V další sekci byly na základě nasbíraných znalostí z analýz úspěšných kybernetických útoků z předchozích kapitol vybrány nejpravděpodobnější kybernetické hrozby pro Českou republiku, které by v budoucnu mohly proběhnout – ve více než 50 % útoků, které dle organizace EuRepoC na Českou republiku mířily, se jednalo o typ útoku DDoS, z čehož lze vyvozovat, že se jedná o velmi pravděpodobnou hrozbu, na kterou by se stát měl zaměřit. Závažnější důsledky potom může mít například kybernetická hrozba v podobě špionáže, která na Českou republiku v minulosti už také mířila, nebo kybernetická forma útoku na elektrickou síť, která byla v posledních letech hojně využívána Ruskem.

V poslední kapitole praktické části se autor zaměřil na doporučení pro zlepšení kybernetické bezpečnosti České republiky. Mezi nejdůležitější byly zařazeno následující – vzdělávání státních zaměstnanců na poli kybernetické bezpečnosti, kontinuální monitorování sítě, aby se daly předvídat například DDoS útoky a vytvoření reakčních plánů na kybernetické bezpečnostní incidenty.

5.2 Diskuse

Na základě předchozí kapitoly, ve které byly shrnuty výsledky práce, byly hlavní i dílčí cíle splněny. Na základě analýz byly autorem zjištěny nejpravděpodobnější kybernetické hrozby pro Českou republiku – jedna z nich byla i špionáž, která se následně naplnila, jelikož NÚKIB vydal 8. března 2023, tedy v čase, kdy praktická část už byla z většinové části hotová, *„varování před hrozbou v oblasti kybernetické bezpečnosti spočívající v instalaci a používání aplikace TikTok na zařízeních přistupujících k informačním a komunikačním systémům kritické informační infrastruktury, informačním systémům základní služby a významným informačním systémům.“*[22]. Jedná se tedy o bezpečnostní hrozbu v podobě špionáže ze strany Číny.

Je velmi pravděpodobné, že podobné kybernetické hrozby a útoky budou v budoucnu přibývat ve stále větší míře a budou více sofistikované, a proto je nutné se na tyto hrozby připravovat a držet krok s trendy v oboru informačních technologií. Je nezbytné, aby stát alokoval finance a co nejvíce podporoval a zdokonaloval své kybernetické zabezpečení. Užitek v tomto případě velmi přesahuje náklady – v případě zanedbaní své kybernetické bezpečnosti můžou být důsledky katastrofální, což bylo zanalyzováno v praktické části práce.

Limity provedených analýz by mohly spočívat v tom, že veškerá data byla převzata především z evropských a amerických databází, které jsou fundovány právě vládami ze Západu – tudíž se nabízí hypotéza, že západní státy chtějí vypadat na kybernetickém poli jako co nejmenší agresoři a zároveň co největší oběti. Toto by mohla být zajímavá výzkumná otázka pro diplomovou práci navazující na tuto práci – jak by rozdělení útočníků a obětí vypadalo, pokud by se použily čínské nebo ruské databáze kybernetických útoků?

6 Závěr

Práce si kladla za hlavní cíl ponořit se do problematiky kybernetické bezpečnosti na mezistátní úrovni a zhodnotit nejčastější kybernetické hrozby a útoky na Českou republiku, které v minulosti proběhly nebo mohou v budoucnu proběhnout. K zodpovězení těchto výzkumných otázek bylo dosaženo pomocí různých dílčích cílů a analýz provedených autorem, které poskytnuly lepší náhled na různé podoby kybernetických útoků.

V teoretické části byly nejprve specifikovány základní definice a termíny, které se v tomto oboru používají a jsou stěžejní pro pochopení dané problematiky. Jsou výstižně a jasně charakterizované, aby jim byla schopna porozumět i do informačních technologií nezasvěcená osoba. Dále jsou charakterizovány podoby, ve kterých je možné se setkat s kybernetickou válkou a různé motivy, na základě kterých jsou útoky prováděny.

V praktické části byly autorem s pomocí informací o kybernetických útocích volně dostupných na internetu vytvořeny různé analýzy týkající se kybernetických hrozeb, četností nejčastějších podob kybernetických útoků a nejangažovanějších států v kybernetických útocích – ať už v roli útočníka, nebo oběti. Následně autor do detailu rozebral vybrané signifikantní kybernetické útoky a navrhl protiopatření, která by snížila jejich důsledky. Z toho všeho se poté vyvodilo, jaké útoky by České republice mohly v budoucnu hrozit. V poslední sekci praktické části se autor zaměřil na doporučení konkrétních návrhů pro zlepšení kybernetické bezpečnosti České republiky.

7 Seznam obrázků, tabulek, grafů a zkratek

7.1 Seznam obrázků

8 Seznam použitých zdrojů

[1] Security Tip (ST04-001): What is Cybersecurity?. *CISA* [online]. Dostupné z: https://www.cisa.gov/uscert/ncas/tips/ST04-001

[2] What is an Exploit?. *Fortinet* [online]. Dostupné z: https://www.fortinet.com/resources/cyberglossary/exploit

[3] *What is Cybersecurity Risk? Definition & Factors to Consider* [online]. 2021. Dostupné z: https://securityscorecard.com/blog/what-is-cybersecurity-risk-factors-to-consider

[4] Co je: Vícefaktorové ověřování. *Microsoft* [online]. [cit. 2023-03-11]. Dostupné z: https://support.microsoft.com/cs-cz/topic/co-je-v%C3%ADcefaktorov%C3%A9-ov%C4%9B%C5%99ov%C3%A1n%C3%AD-e5e39437-121c-be60-d123-eda06bddf661

[5] What is Cyber Espionage?. *Vmware* [online]. Dostupné z: https://www.vmware.com/topics/glossary/content/cyber-espionage.html

[6] *Cyber Sabotage* [online]. Dostupné z: https://www.military.com/defensetech/2008/02/06/cyber-sabotage

[7] GOSWAMI, Manash. *Fake News and Cyber Propaganda: A Study of Manipulation and Abuses on Social Media* [online]. 2018. Dostupné také z: https://www.researchgate.net/publication/326655516_Fake_News_and_Cyber_Propaganda_A_Study_of_Manipulation_and_Abuses_on_Social_Media

[8] RADY PRO OBČANY - BLACKOUT. *KRIZPORT* [online]. Dostupné z: https://www.krizport.cz/rady/rady-pro-obcany-blackout

[9] Europe's power grids readied against cyber attack. *European Comission* [online]. 2015. Dostupné z: https://ec.europa.eu/research-and-innovation/en/horizon-magazine/europes-power-grids-readied-against-cyber-attack

[10] What is a DDoS attack?. In: *CloudFlare* [online]. Dostupné z: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

[11] Why cyberattacks happen. *IBM* [online]. [cit. 2023-03-11]. Dostupné z: https://www.ibm.com/topics/cyber-attack

[12] North Korea took $2 billion in cyberattacks to fund weapons programme - U.N. report. *Reuters* [online]. [cit. 2023-03-11]. Dostupné z: https://www.reuters.com/article/northkorea-cyber-un-idINKCN1UV1ZC

[13] Hacktivism—A Cyberattack?. *Fortinet* [online]. Dostupné z: https://www.fortinet.com/resources/cyberglossary/what-is-hacktivism

[14] EuRepoC Data. *European Repository of Cyber Incidents* [online]. Dostupné z: https://eurepoc.eu/databases

[15] Significant Cyber Incidents. *Center for Strategic and International Studies* [online]. Dostupné z: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[16] Operation Aurora. *Council on Foreign Relations* [online]. [cit. 2023-01-09]. Dostupné z: https://www.cfr.org/cyber-operations/operation-aurora

[17] Stuxnet: What Is It & How Does It Work?. *Avast* [online]. [cit. 2023-01-10]. Dostupné z: https://www.avast.com/c-stuxnet

[18] Stuxnet virus was planted by Israeli agents using USB sticks, according to new report. *The Verge* [online]. [cit. 2023-01-10]. Dostupné z: https://www.theverge.com/2012/4/12/2944329/stuxnet-computer-virus-planted-israeli-agent-iran

[19] Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks. *The Henry M. Jackson School of International Studies* [online]. [cit. 2023-01-10]. Dostupné z: https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/

[20] Critical infrastructure protection. *European Comission, official website* [online]. [cit. 2023-01-10]. Dostupné z: https://joint-research-centre.ec.europa.eu/scientific-activities-z/critical-infrastructure-protection_en

[21] Co je SIEM?. *Microsoft* [online]. [cit. 2023-03-11]. Dostupné z: https://www.microsoft.com/cs-cz/security/business/security-101/what-is-siem

[22] Aplikace TikTok představuje bezpečnostní hrozbu. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2023-03-12]. Dostupné z: https://www.nukib.cz/download/uredni_deska/2023-03-08_Varovani-TikTok_final.pdf