MASARYKOVA
UNIVERZITA

FAKULTA SOCIÁLNÍCH STUDIÍ

Potírání ransomwarových útoků v České republice

Diplomová práce

BC. PAVLÍNA MACHOVÁ

UČO: 471445

Vedoucí práce: Mgr. Aneta Pinková, PhD.

Katedra politologie
Program Bezpečnostní a strategická studia

Brno 2022

MUNI
FSS

Bibliografický záznam

Autor: Bc. Pavlína Machová
Fakulta sociálních studií
Masarykova univerzita
Katedra politologie

Název práce: Potírání ransomwarových útoků v České republice

Studijní program: Bezpečnostní a strategická studia

Vedoucí práce: Mgr. Aneta Pinková, PhD.

Rok: 2022

Počet stran: 210

Klíčová slova: ransomware, kyberbezpečnost, kyberútoky, kyberkriminalita, policy analysis, Česká republika

Bibliographic record

Author: Bc. Pavlína Machová
Faculty of Social Studies
Masaryk University
Department of Political Science

Title of Thesis: Combating ransomware attacks in the Czech Republic

Degree Programme: Security & Strategic Studies

Supervisor: Mgr. Aneta Pinková, PhD.

Year: 2022

Number of Pages: 210

Keywords: ransomware, cybersecurity, cyberattacks, cybercrime, policy analysis, Czech Republic

Anotace

Ransomwarové útoky představují jednu z nejvýznamnějších kybernetických hrozeb, s nimiž se státy v současnosti potýkají. Diplomová práce prezentuje policy analysis potírání této hrozby v ČR. Vzhledem k absenci explicitně vyřčené policy pracuje s rámcem závazků představeným zástupci zemí, které se v roce 2021 zúčastnily virtuálního setkání Counter Ransomware Initiative zorganizovaného Národní bezpečností radou Bílého domu. Na jeho základě a za využití informací z otevřených zdrojů a expertních rozhovorů identifikuje a hodnotí koncepční a legislativní ukotvení potírání ransomware v ČR, stejně jako jeho praktickou aplikaci. Směrem k identifikovaným slabým místům policy potírání ransomware v ČR diplomová práce představuje také doporučení k jejich eliminaci.

Abstract

Ransomware attacks are one of the most relevant threats for states all over the world. This diploma thesis presents a policy analysis of the Czech Republic's approach towards combating ransomware. For the absence of explicit policy, the thesis works with framework of commitments from the Counter Ransomware Initiative meeting organized by the National Security Council of the White House in 2021. Based on aims and commitments presented there and information from open sources and expert interviews, the thesis identifies and evaluates conceptual and legislative anchoring of Czech policy towards combating ransomware, same as its practical application. Concerning identified weak spots of analysed policy, recommendations for their elimination are proposed.

Čestné prohlášení

Prohlašuji, že jsem diplomovou práci na téma **Potírání ransomwarových útoků v České republice** zpracovala sama**.** Veškeré prameny a zdroje informací, které jsem použila k sepsání této práce, byly citovány v textu a jsou uvedeny v seznamu použitých pramenů a literatury.

V Brně 31. května 2022 .....

Bc. Pavlína Machová

Poděkování

Za odborné vedení diplomové práce a nesmírnou ochotu děkuji vedoucí práce Mgr. Anetě Pinkové, PhD. Dále děkuji také všem respondentům za poskytnutí rozhovorů, bez kterých by tato práce nemohla vzniknout.

Obsah

Seznam tabulek **10**

Seznam pojmů a zkratek **11**

1 Úvod **13**

2 Konceptualizace pojmů **16**

2.1 Kyberbezpečnost ... 16

2.2 Ransomware ... 24

2.3 Policy ... 37

3 Metodologie **42**

3.1 Policy analysis ... 42

3.2 Aplikovaný přístup k policy analysis ... 44

3.3 Výzkumný design ... 45

3.4 Metody sběru dat ... 47

3.5 Limity a etické aspekty ... 52

4 Policy analysis **55**

4.1 Kontext boje proti ransomware ... 55

4.2 Policy potírání ransomware v ČR ... 62

4.3 Slabá místa policy potírání ransomware v ČR ... 105

4.4 Doporučení ... 123

5 Závěr **135**

Použité zdroje **138**

Příloha A Přepis rozhovoru s Expertem č. 1 **176**

Příloha B Přepis rozhovoru s Expertem č. 2 **183**

Příloha C Přepis rozhovoru s Expertem č. 3 **196**

Příloha D Přepis rozhovoru s Expertem č. 4 **199**

Příloha E Přepis rozhovoru s Expertem č. 5 **202**

Příloha F Přepis rozhovoru s Expertem č. 6 **204**

Příloha G Přepis rozhovoru s Expertem č. 7 **208**

Počet znaků: 200 375

Seznam tabulek

Tab. 1: Respondenti expertních rozhovorů (vlastní tabulka) 50
Tab. 2: Shrnutí identifikovaných slabých míst policy potírání ransomware v ČR (vlastní tabulka) 122
Tab. 3: Informace o rozhovoru s Expertem č. 1 (vlastní tabulka).....176
Tab. 4: Informace o rozhovoru s Expertem č. 2 (vlastní tabulka).....183
Tab. 5: Informace o rozhovoru s Expertem č. 3 (vlastní tabulka).....196
Tab. 6: Informace o rozhovoru s Expertem č. 4 (vlastní tabulka).....199
Tab. 7: Informace o rozhovoru s Expertem č. 5 (vlastní tabulka).....202
Tab. 8: Informace o rozhovoru s Expertem č. 6 (vlastní tabulka).....204
Tab. 9: Informace o rozhovoru s Expertem č. 7 (vlastní tabulka).....208

Seznam pojmů a zkratek

BIS	–	Bezpečnostní informační služba
CEPOL	–	Agentura Evropské unie pro vzdělávání a výcvik v oblasti prosazování práva
CERT	–	Computer Emergency Response Team
CSIRT	–	Computer Security Incident Response Team
ČR	–	Česká republika
EUROPOL	–	Evropský policejní úřad
EMPACT	–	Evropská multidisciplinární platforma proti kriminálním hrozbám
FAÚ	–	Finanční analytický úřad
FBI	–	Federal Bureau of Investigation
ICT	–	informační a komunikační technologie
INTERPOL	–	Mezinárodní organizace kriminální policie
KB	–	kybernetická bezpečnost
MF ČR	–	Ministerstvo financí České republiky
ML/FT	–	legalizace výnosů z trestné činnosti a financování terorismu
MŠMT ČR	–	Ministerstvo školství, mládeže a tělovýchovy České republiky
MV ČR	–	Ministerstvo vnitra České republiky
MZV ČR	–	Ministerstvo zahraničních věcí České republiky

NCKO	–	Národní centrum kybernetických operací
NCOZ	–	Národní centrála proti organizovanému zločinu služby kriminální policie a vyšetřování
NKÚ	–	Nejvyšší kontrolní úřad
NÚKIB	–	Národní úřad pro kybernetickou a informační bezpečnost
OČTŘ	–	orgány činné v trestním řízení
OSN	–	Organizace spojených národů
OZ	–	organizovaný zločin
ŘSD	–	Ředitelství silnic a dálnic
USD	–	United States Dollar
ÚZSI	–	Úřad pro zahraniční styky a informace
VKB	–	Vyhláška o kybernetické bezpečnosti
VPD	–	veřejné politické dokumenty
VZ	–	Vojenské zpravodajství
ZKB	–	Zákon o kybernetické bezpečnosti

1 Úvod

Je březen roku 2020, lékaři a sestry Fakultní nemocnice u svaté Anny v Brně si však zapisují zdravotnické údaje na papír. Část pacientů musí být odkloněna do okolních nemocnic. Odkládají se také plánové operace. Navrácení chodu nemocnice do původních kolejí bude trvat téměř měsíc. V květnu o dva roky později se v podobné situaci ocitají zaměstnanci Ředitelství silnic a dálnic (dále ŘSD). Nefunguje řada vnitřních systémů a řidiči se jen marně snaží dohledat oficiální informace o aktuálním stavu v dopravě. Řízení dopravy naštěstí funguje i nadále. Očekává se, že obnovení původního chodu ŘSD bude trvat měsíce. Tyto dvě organizace, narušení jejichž chodu by mohlo ohrozit lidské životy, přivedl do této situace společný jmenovatel – ransomware.

Ransomware představuje jednu z nejvýznamnějších kybernetických hrozeb bezpečnosti České republiky (dále ČR) a jejích občanů. Nejen, že působí významné ekonomické škody, ale může ohrožovat i lidské životy. V ČR však i přesto prozatím absentuje explicitně vyslovená policy potírání ransomwarových útoků. Na mezinárodní úrovni však ČR vyslovila své odhodlání bojovat proti ransomware jasně. Při příležitosti virtuálního setkání Counter Ransomware Initiative zorganizovaného Národní bezpečnostní radou Bílého domu ve dnech 13. a 14. října 2021 jeho účastnici včetně ČR vydali Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021 (dále Joint Statement). V tomto prohlášení se zavazují společně i individuálně bojovat proti ransomware zejména ve čtyřech oblastech – skrze budování resilience, potírání nezákonného financování ransomware, vymáhání práva a diplomacii. To, zda je v uvedených oblastech

ČR schopna dostát svým závazkům je předmětem analýzy této diplomové práce.

Diplomová práce psaná v žánru policy analysis se věnuje oblasti kyberbezpečnosti, v rámci níž se zaměřuje na téma potírání ransomwarových útoků v ČR, které prozatím nebylo dostatečně komplexně prozkoumáno. To nicméně představuje zásadní problém, neboť aby mohla být jakákoli policy úspěšná, musí si její tvůrci a vykonavatelé uvědomovat její slabá místa a usilovat o jejich nápravu. Cílem této práce je tedy na základě rámce Joint Statement a informací z otevřených zdrojů a expertních interview identifikovat slabá místa v současném přístupu ČR k boji proti ransomware a navrhnout doporučení pro jejich eliminaci. Toho bude dosaženo skrze zodpovězení následujících výzkumných otázek:

- Je policy potírání ransomware v ČR v souladu se závazky vyslovenými v Joint Statement?
    - Jak je v koncepčních dokumentech ČR vymezena policy potírání ransomware?
        - Jaká jsou slabá místa koncepčního vymezení policy potírání ransomware v ČR?
    - Jak je v ČR legislativně ukotvena policy potírání ransomware?
        - Jaká jsou slabá místa legislativního ukotvení policy potírání ransomware v ČR?
    - Jaké kroky činí ČR za účelem potírání ransomware v praxi?
        - Jaká jsou slabá místa praxe potírání ransomware v ČR?
- Jakým způsobem je možné eliminovat identifikovaná slabá místa policy potírání ransomware v ČR?

Diplomová práce je členěna do několika částí, přičemž první z nich představuje vymezení základních pojmů pojících se s problematikou. Na ni navazuje část dedikovaná představení žánru policy analysis, metodám sběru dat a limitujícím a etickým aspektům práce. Poté je představena samotná policy analysis, která sestává z částí věnovaných deskripci současné policy potírání ransomware, identifikaci jejích slabých míst a doporučením směrem k jejich eliminaci. V závěru práce jsou shrnuty zjištěné poznatky a představeno další možné směřování výzkumu v této oblasti.

2 Konceptualizace pojmů

V rámci kapitoly věnující se vymezení pojmů, se kterými se v rámci tohoto textu pracuje, jsou nejprve objasněny pojmy pojící se s tématem kyberbezpečnosti obecně, tedy kyberprostor, kyberbezpečnost, kybernetická hrozba, kybernetické riziko, kybernetická zranitelnost, aktivum, kyberbezpečnostní incident, kyberútok a kyberkriminalita.
V druhé části této kapitoly je pak blíže představen fenomén ransomware. Text se věnuje definování pojmu ransomware a srovnání různých typů tohoto škodlivého software. Dále představuje zjednodušené typické schéma ransomwarového útoku a charakterizuje útočníky a oběti ransomware. Poté je pozornost věnována platbám výkupného a virtuálním aktivům. Rozebrán je také vztah mezi ransomware a organizovaným zločinem (dále OZ).
Poslední část této kapitoly se věnuje definování pojmu policy, jakožto ohniska zájmu policy analysis, tedy žánru této práce.

2.1 Kyberbezpečnost

2.1.1 Kyberprostor

Pro správné pochopení obsahu pojmu kyberbezpečnost je nejprve nutné objasnit význam pojmu kyberprostor. Jirásek, Bašta a Požár (2013, 59) definují kyberprostor jako *„digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.“* Shodnou definici kyberprostoru uvádí také § 2 písm. a) Zákona o kybernetické bezpečnosti (dále ZKB). Kolouch, Bašta et al. (2019, 36) zjednodušeně uvádějí, že *„kyberprostor je také možné definovat jako prostor kybernetických aktivit, či jako prostor*

vytvořený informačními a komunikačními technologiemi.“ Tyto definice však opomíjí významný faktor kyberprostoru, kterým jsou uživatelé. Ty ve své definici zmiňují Singer a Friedman (2014, 13), kteří kyberprostor chápou jako *„říši počítačových sítí (za kterými stojí uživatelé), kde jsou online ukládány, sdíleny a komunikovány informace.“* Ani tato definice nicméně zcela nevystihuje skutečnou podstatu kyberprostoru. Tu dle Koloucha, Bašty et al. (2019, 37-38) skvěle zachycuje trojdimenzionální pojetí představené v dokumentu Cyberspace Operations Concept Capability Plan 2016-2018 (TRADOC 2010). Kyberprostor se dle něj skládá ze tří vrstev:

- **Fyzická vrstva** se skládá ze dvou komponent – geografických a fyzických síťových. Fyzické síťové komponenty lze chápat jako infrastrukturu, geografické komponenty pak jako její přesné umístění ve fyzickém světě. Uvědomění si fyzických komponent je významné v první řadě proto, že narušuje časté chápání kyberprostoru jako místa bez hranic.
- **Logická vrstva** obsahuje logická propojení mezi síťovými uzly, která jsou realizována skrze síťové komunikační protokoly. Uzly jsou tedy síťová zařízení (např. počítače), která lze obecně nazvat jako logické síťové komponenty.
- **Sociální vrstva** se pak skládá z komponent, které lze nazvat kyberosobnost a osobnost. Osobnost je možné vnímat jako uživatele, který může mít současně více kyberosobností. Ty lze chápat jako identifikaci osoby na síti (např. e-mailová či IP adresa). Současně pak může být jedna kyberosobnost využívána více osobnostmi.

Kyberprostor je pak dle Koloucha, Bašty et al. (2019, 38) možno rozdělit dle dostupnosti a dohledatelnosti dat na Surface, Deep a Dark Web. Dle Sultany a Jilaniho (2021, 86-87) je:

- **Surface Web** označení pro rozměr, kde jsou služby a data dostupné za použití běžných internetových vyhledávačů;
- **Deep Web** vrstva, kde se nachází služby a data, které jsou uživatelům dostupné, nicméně běžnými internetovými vyhledávači přehlížené (např. data ve specializovaných databázích);
- **Dark Web** je pak vrstvou obsahující záměrně skryté služby a data, které jsou často spojené s nelegálními aktivitami. Tato vrstva je dostupná pouze za využití speciálních nástrojů jako třeba TOR, IIP či Freenet.

2.1.2 Kyberbezpečnost

Koulouch, Bašta et al. (2019, 40) uvádí, že k vysvětlení pojmu kyberbezpečnost je vhodné jej rozebrat. Kyber zde odkazuje k vazbě na prvky informačních a komunikačních technologií (dále ICT), či přímo na výše rozebraný kyberprostor. Bezpečnost je pak podobně jako kyberprostor definována různými autory rozdílně, pro účely této práce je přijata definice Mareše (2002a, 13), který bezpečnost chápe jako *„stav, kdy jsou na nejnižší možnou míru eliminovány hrozby pro objekt … a jeho zájmy a tento objekt je k eliminaci stávajících i potenciálních hrozeb efektivně vybaven a ochoten při ní spolupracovat.“*

S ohledem na bezpečnost je tedy třeba se ptát o čí bezpečnost se jedná, jaké hodnoty mají být chráněny, před čím mají být tyto hodnoty chráněny a jaké prostředky je k této ochraně třeba využít (Kolouch, Bašta et al. 2019, 41). Ve snaze zodpovědět tyto otázky představují Kolouch, Bašta et al. (2019, 44-45) vlastní definici kyberbezpečnosti, kterou

chápou jako *„souhrn právních, organizačních, technických a vzdělávacích prostředků, které směřují k zajištění ochrany počítačových systémů a dalších prvků ICT, aplikací, dat a uživatelů“* a zároveň jako *„schopnost počítačových systémů a využívaných služeb reagovat na kybernetické hrozby či útoky a jejich následky, jakož i plánování obnovy funkčnosti počítačových systémů a služeb s nimi spojených.“*

Vzhledem k tomu, že je tato práce zaměřena na kybernetickou bezpečnost ČR, je třeba definovat také pojem národní bezpečnost. Zde je přijata definice Mareše, který uvádí:

> *„Národní bezpečnost je stav, kdy objektu (národnímu státu jako celku nebo jeho podstatným atributům) nehrozí závažné ohrožení svrchovanosti, územní celistvosti, základům politického uspořádání, vnitřního pořádku a bezpečnosti, životů a zdraví občanů, majetkových hodnot a životního prostředí. Ani jeho spojenci nejsou vystaveni hrozbám, které by v případě jejich aktivace vyžadovaly ozbrojenou či jinou rizikovou spoluúčast. Objekt je schopen a ochoten potenciální hrozby rozpoznat a v maximální možné míře jim zamezovat, popřípadě je eliminovat“* (Mareš 2002b, 15).

2.1.3 Kybernetická hrozba

Jirásek, Novák a Požár (2013, 20) uvádí, že kybernetická hrozba je *„potenciální příčina nežádoucí události, která může mít za následek poškození systému a jeho aktiv, např. zničení, nežádoucí zpřístupnění (kompromitaci), modifikaci dat nebo nedostupnost služeb.“* Dle § 2 písm. e) Vyhlášky o kybernetické bezpečnosti (dále VKB) je hrozbou *„potenciální*

příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, která může způsobit škodu.“ Phoha (2002, 129) zase definuje hrozbu jako *„jakoukoli potenciálně škodlivou událost pro systém, která působí skrze neautorizovaný přístup, zničení, zveřejnění či modifikaci dat, nebo skrze odepření přístupu.“* Kolouch, Bašta et al. (2019, 74) pak hrozbu vnímají jako *„něco, co je schopno narušit běžný či řádný stav věcí a zasáhnout do práv jiných subjektů,“* přičemž toto negativní působení může, ale nemusí nastat. Kybernetické hrozby je pak možné dělit několika způsoby, čímž lze ilustrovat jejich značný rozsah.

Jírovský (2017, 21) uvádí, že lze rozeznat čtyři skupiny základních kyberbezpečnostních hrozeb:

- **únik informací** (stav označující zisk chráněných informací neautorizovaným subjektem);
- **narušení integrity** (stav, kdy je porušena konzistence dat neautorizovaným subjektem – může dojít k změně či vymazání chráněných dat, nebo k vytvoření dat nových);
- **potlačení služby** (stav, kdy je úmyslně bráněno přístupu k informacím či systémům subjektu, který je k tomuto přístupu autorizován);
- **nelegitimní použití** (stav, kdy je konkrétní zdroj užíván neautorizovaným či neadekvátním způsobem).

Dle Koloucha, Bašty et al. (2019, 76-79) je kyberbezpečnostní hrozby nicméně možno dělit řadou dalších způsobů. Konkrétně dle jejich zdroje, původu, cíle, motivace či specifické formy.

2.1.4 Kybernetické riziko

Kolouch, Bašta et al. (2019, 68) uvádějí, že *„riziko vyjadřuje pravděpodobnost, s jakou může nastat nechtěná událost.“* Phoha (2002, 115) pak

riziko definuje jako *„pravděpodobnost, že bude zneužita určitá zranitelnost bezpečnostního systému.“* V § 2 písm. h) VKB je riziko definováno jako *„možnost, že určitá hrozba využije zranitelnosti aktiva a způsobí škodu.“*

2.1.5 Kybernetická zranitelnost

Kybernetickou zranitelnost je možno definovat jako *„slabé místo aktiva nebo řízení, které může být využito hrozbou“* (Jirásek, Novák and Požár 2013, 117). VKB je zranitelnost definována v § 2 písm. p) jako *„slabé místo aktiva nebo slabé místo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami.“* Phoha (2002, 140) pak o zranitelnosti hovoří jako o *„zneužitelné slabině bezpečnostních systémů, procedur, designu, kontroly či implementace.“* Kolouch, Bašta et al. (2019, 72) s těmito definicemi v zásadě souhlasí a dodávají, že zranitelnosti je v kybernetické bezpečnosti možno dělit na známé (ty mohou být opravené či neopravené) a neznámé (skryté či neobjevené).

2.1.6 Aktivum

Dle Koloucha, Bašty et al. (2019, 72) může být aktivem cokoli, co má pro určitý subjekt hodnotu. Může se jednat o věc hmotnou (např. počítačový systém) i nehmotnou (např. informace a data). Jako aktivum je však možné vnímat i vlastnost (např. důvěrnost, integritu či dostupnost), reputaci a dobré jméno, nebo konkrétní osoby a jejich znalosti, dovednosti a zkušenosti. VKB jsou aktiva členěna na primární a podpůrná. Primárním aktivem je dle § 2 písm. g) *„informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém.*“ Podpůrné aktivum je pak dle § 2 písm. f) *„technické aktivum, zaměstnanci a dodavatelé*

podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému.“

2.1.7 Kyberbezpečnostní událost

Jirásek, Novák a Požár (2013, 23) uvádějí, že kyberbezpečnostní událost *„může způsobit nebo vést k narušení informačních systémů a technologií a pravidel definovaných k jeho ochraně (bezpečnostní politiky).“* Dle § 7 odst. (1) ZKB je kyberbezpečnostní událostí *„událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.“* Phoha (2002, 49) událost v kontextu kyberbezpečnosti vnímá jako *„příhodu, která může ovlivnit fungování systémů.“* Kolouch, Bašta et al. (2019, 80-81) pak uvádí, že se jedná o *„událost bez zatím reálného negativního následku,“* pro kterou by bylo vzhledem k dosavadnímu nenaplnění potenciálu způsobit nežádoucí následky možné využívat označení kybernetická hrozba.

2.1.8 Kyberbezpečnostní incident

Kyberbezpečnostní incident definují Jirásek, Novák a Požár (2013, 20) jako *„porušení nebo bezprostřední hrozbu porušení bezpečnostních politik, bezpečnostních zásad nebo standardních bezpečnostních pravidel provozu informační a komunikační technologie.“* Phoha (2002, 62) chápe incident jako *„zhodnocenou událost, která může negativně ovlivnit systémy, nebo tak již činí.“* ZKB v § 7 odst. (2) uvádí, že kybernetický bezpečnostní incident je *„narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.“* Dle Kolloucha, Bašty et al. (2019, 81-82) tedy může být kyberbezpečnostní

incident způsoben úmyslným i nedbalostním chování, případně také vyšší mocí. Oproti kyberbezpečnostní události pak představuje incident skutečné narušení bezpečnosti.

2.1.9 Kyberútok

Dříve v práci často citovaní Jirásek, Novák a Požár (2013, 59) definují kyberútok jako *„útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace.“* Kolouch, Bašta et al. (2019, 82-83) však tuto definice kritizují s ohledem na to, že problematiku nepostihuje dostatečně široce. Ve vlastní definici uvádějí, že kyberútok je *„jakékoli úmyslné jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby,“* konkrétněji pak, že se jedná o *„jednání útočníka či skupiny útočníků, které využívá informační a komunikační technologie k útoku na jinou informační a komunikační infrastrukturu, ať už s cílem narušit dostupnost, důvěrnost nebo integritu dat.“* Phoha (2002, 7) pak definuje kyberútok jako *„neautorizovanou zlomyslnou intencionální akci vůči počítači, síti či systému.“*

2.1.10 Kyberkriminalita

Vzhledem k zájmu o problematiku kyberútoků je třeba zmínit také pojem kyberkriminalita. Ten lze dle Koloucha, Bašty et al. (2019, 83) definovat jako *„jednání namířené proti počítačovému systému, počítačové síti, datům či uživatelům nebo jako jednání, při němž je počítačový systém použit jako nástroj pro spáchání trestného činu.“* Singer a Friedman (2014, 85) pak uvádí, že kybernetická kriminalita je nejčastěji definována jako *„využití digitálních nástrojů zločinci ke krádežím či jiným nezákonným aktivitám.“* Směrem k jasnějšímu vymezení kybernetické kriminality pak tito autoři odkazují ke snahám Evropské Komise, která rozlišuje mezi tradičními

zločiny využívajícími kybernetických prostředků a kyberzločiny, které jsou omezeny výhradně na kyberprostor – cíle i prostředky k jejich dosažení náleží do kyberprostoru (Singer and Friedman 2014, 85; European Comission n.d.).

Na tomto místě je pak třeba zmínit, že vzhledem k neustálému rozvoji kyberútoků a často velmi pomalé reakci zákonodárců může docházet k případům, kdy specifické kyberútoky nejsou trestným činem. Naopak každý kybernetický trestný čin dle platné legislativy musí být zároveň kyberútokem (Kolouch, Bašta et al. 2019, 83).

2.2 Ransomware

2.2.1 Ransomware

Než bude definován samotný pojem ransomware, je třeba osvětlit také význam pojmu malware. Ten vzniknul sloučením slov malicious (škodlivý) a software. Jedná se o obecné označení různých typů software, které byly vytvořeny za účelem páchání škody v cílovém výpočetním zařízení (Hassan 2019, 9; Ryan 2021, 20-21).

Ransomware pak DiMaggio (2022) definuje jako *„typ malware, který šifruje data své oběti s cílem získání peněz ve formě výkupného.“* Hassan (2019, xvii) uvádí, že *„ransomware je druhem malware, který brání uživatelům v přístupu k prostředkům jejich výpočetního zařízení a/nebo k osobním datům, typicky jejich zašifrováním,“* k čemuž dále dodává, že *„data ve výpočetním zařízení oběti se stávají rukojmí dokud oběť nezaplatí výkupné.“* Miller (2017, 3) pak uvádí, že *„ransomware je malware využívaný v rámci kyberútoku k zašifrování dat oběti prostřednictvím šifrovacího klíče, který je znám pouze útočníkovi, čímž činí tato data nepoužitelná do doby, než je obětí zaplaceno výkupné.“*

Ransomware je pak možno označit také jako jednu z metod digitálního vydírání. Prostřednictvím těch útočníci usilují o nelegitimní zisk specifických dat, případně o zabránění přístupu legitimním uživatelům k těmto datům s cílem finančního zisku formou výkupného (Hassan 2019, 17).

2.2.2 Typy ransomware

Ransomware v žádném případě není uniformní – existuje mnoho typů, které lze klasifikovat na základě řady různých kritérií. Hassan (2019, 47-67) uvádí, že experti na kyberbezpečnost preferují členění na tzv. ransomwarové rodiny, které spojuje signatura kódu obsahující sekvence příkazů a instrukcí zodpovědných za škodlivou aktivitu. Mezi tyto rodiny můžeme řadit Ryuk, WannaCry, Cerber, Locky, Petya, SamSam, DMA Locker, CyptXXX či CryptoWall. Pro účely této práce se však jako vhodnější jeví vzhledem k větší výpovědní hodnotě dělení Grimese (2021, 10-32) dle specifických znaků ransomware.

V první řadě je dle Grimese (2021, 10-14) třeba rozlišovat mezi **pravým a falešným ransomware,** kdy jako falešný ransomware vnímá programy či aplikace, které se jako ransomware pouze tváří, avšak ve skutečnosti nedochází k zašifrování ani k převzetí skutečné kontroly nad zasaženým zařízením. Tyto lze spolu s ransomware zařadit do skupiny digitálního vydírání (Hassan 2019, 17).

Zde vyvstává otázka, zda je za ransomware možno považovat i tzv. locker. Savage, Coogan a Lau (2015, 5-6), Hassan (2019, 17-19) či Liska a Gallo (2016, 11-15) člení ransomware na dva hlavní typy – crypto (šifruje soubory) a locker (odpírá uživateli určité funkce jeho zařízení). I přes poměrně velkou rozšířenost tohoto přístupu není v této práci na

locker nahlíženo jako na pravý ransomware v důsledku absence šifrování souborů.

Grimes (2021, 10-13) pak ve vztahu k falešnému ransomware zmiňuje různé typy malware tvářící se jako ransomware, avšak bez skutečné schopnosti šifrovat data. Ty vytváří pevná okna či přejmenovávají soubory, jako např. některé verze StrRAT Malware (Nair 2021; The BlackBerry Research & Intelligence Team 2021). Jako ransomware pak dle Grimese (2021, 13-14) nelze označit ani malware žádající výkupné za zpřístupnění určitým způsobem zablokovaných či zničených dat, která však není útočník ve skutečnosti schopen opět zpřístupnit. Tento typ lze označit jako wiper a zřejmě nejproslulejším příkladem je NotPetya (Greenberg 2018; Shepherd 2021).

Dalším bodem, podle kterého Grimes (2021, 14-17) dělí ransomware, je **doba jeho spuštění od proniknutí do systému**. Až donedávna většina ransomwarových programů začala s šifrováním dat v okamžiku svého spuštění – zde např. Kolz (Petcu 2020; Bolton 2020) či CryptoLocker (Laffan, 2015; Belcic 2021). Od roku 2019 je tento typ ransomware spíše výjimkou a převládají programy, které v infikovaném zařízení či síti vyčkávají bez povšimnutí dny, měsíce, někdy dokonce i roky (Grimes 2021, 15). Příkladem vyčkávajícího ransomware může být např. Sodinokibi (Fadilpasic 2020; Heinemeyer 2020). Čím déle se ransomware v zařízení nachází, tím více škody dokáže napáchat. Zejména pokud disponuje schopností rozšířit se v konkrétní síti na další zařízení včetně záloh, případně pokud je schopen plnit i další funkce kromě vlastního šifrování dat (Grimes 2021, 14-17).

Dále lze dle Grimese (2021, 17-18) členit ransomware na **automatický a řízený.** Jednou z nejvýznamnější proměn, kterou ransomware v posledních letech prošel, je dle něj právě možnost řídit jeho činnost na

dálku. Tradiční ransomware učinil to, k čemu byl předem naprogramován – útočník po jeho spuštění neměl možnost ovlivnit jeho chování. Nechvalně proslulým zástupcem neřízeného ransomware je WannaCry (Rosencrance 2021; Davis 2021). Člověkem řízený ransomware je dle Grimese (2021, 17-18) automatizován typicky jen v úvodní fázi proniknutí ransomware do systému. Ve chvíli, kdy program splní svůj úkol přebírá nad jeho dalšími akcemi kontrolu útočník. Tato skutečnost vede k větší flexibilitě ransomware a k možnostem dalšího zneužití již získaného přístupu do zařízení či sítě k jiným škodlivým aktivitám. DiMaggio (2021a) nicméně zdůrazňuje, že i řízený ransomware využívá nástrojů, které jsou automatické a značně tak snižují čas, který musí útočníci strávit v infikovaném systému aniž by byli detekováni.

Dalším možným způsobem rozlišování ransomware je dle Grimese (2021, 18-19) to, zda **zasahuje jedno nebo více zařízení**, tedy je schopen rozšířit se do všech zařízení připojených ke konkrétní síti. Starší nebo velmi jednoduché typy ransomware postihují pouze zařízení, na kterém byly původně spuštěny. Příkladem může být např. Cryptic (Grimes 2021, 18). V současnosti je však pro ransomware typická schopnost automaticky nebo řízeně prozkoumávat a infikovat všechna dostupná zařízení v síti. Příkladem může být třeba Ryuk (Seals 2021; Dinu 2021) či SamSam (Spring 2016; Burgess 2018).

Problematická je v této souvislosti zejména skutečnost, že i když je oběť zasažena okamžitým ransomware napadajícím pouze jedno zařízení, nemůže si tím být jista až do chvíle, kdy jsou zkontrolována všechna zařízení přes síť připojená k tomu původně infikovanému. To významně navyšuje čas a náklady spojené se zotavením z ransomwarových útoků (Grimes 2021, 18-19).

Významných faktorem, dle kterého lze dále rozlišovat ransomware, jsou pak dle Grimese (2021, 19-20) **vektory útoku**. Existuje nespočet metod, kterými může ransomware proniknout do zařízení či sítě. Miller (2017, 7) za nejčastější vektory považuje exploit kity, infikované webové stránky (watering holes), škodlivé reklamy (malwertising) a phishingové e-maily. Hassan (2019, 208) pak v tomto kontextu zmiňuje škodlivé přílohy či odkazy v e-mailech, zranitelnosti webových prohlížečů, makra Microsoft Office, infikované soubory na pirátských stránkách či přenosná USB zařízení. Sám Grimes (2021, 19-20) mezi nejčastější vektory řadí metody sociálního inženýrství, malware (typicky trojské koně či červi), nezazáplatovaný software, zneužití špatné konfigurace, uniklá či slabá hesla, infekce skrze USB a insidery, infikované webové stránky a vyskakovací okna. Tyto způsoby dle něj často pracují současně, o čemž svědčí i skutečnost, že nejčastěji využívanou metodou k šíření a doručení ransomware do zařízení či sítě je využití sociálního inženýrství, typicky phishingových e-mailů, které v příloze obsahují trojského koně (Grimes 2021, 20).

Následně Grimes (2021, 21-22) uvádí, že je třeba rozlišovat mezi ransomware **šifrujícím běžné soubory a tím, který infikuje boot**. Ransomware běžně usiluje o zašifrování většiny souborů v zařízení, mimořádně se pak soustředí na specifické soubory (např. soubory Microsoft Office). Bootovací[1] soubory a procesy ransomware většinou neinfikuje, díky čemuž může komunikovat s uživatelem ohledně vzniklé

[1] Bootovací proces probíhá po zapnutí počítače. Zahrnuje načtení pokynů pro spuštění počítače a načtení operačního systému. Bootovací soubory jsou soubory potřebné k uskutečnění bootovacího procesu, tedy ke spuštění počítače a načtení operačního systému (TechLib n.d.).

situace, předat zprávu o požadovaném výkupném a případně umožnit vložení dešifrovacího klíče a zpřístupnění souborů.

Existuje však i ransomware, který zašifruje všechny soubory včetně těch bootovacích, případně pouze je – zde např. Petya (Hung and Joven 2017; Belcic 2022). Ransomware napadající boot je nicméně méně častý, neboť infekce těchto souborů je náročnější, avšak zotavení se z ní je pro uživatele snazší i bez získání dešifrovacího klíče (Grimes 2021, 21-22).

U ransomware je pak také důležité rozlišit, zda disponuje **dobrým nebo špatným šifrováním** (Grimes 2021, 22-23). Podobně jako v minulosti, i dnes je možné setkat se s nekvalitním šifrováním, které lze prolomit i bez originálního dešifrovacího klíče. Těchto případů však ubývá a drtivá většina ransomware již pracuje s kvalitním, bez klíče neprolomitelným šifrováním. Liska a Gallo (2016, 13-15) pak rozlišují mezi symetrickým a asymetrickým šifrováním. Symetrické šifrování je možné označit za „špatné," neboť je prolomitelné i bez dešifrovacího klíče. Asymetrické šifrování představuje to „dobré," využívající dvou klíčů – veřejného, prostřednictvím kterého dochází k zašifrování souborů v napadeném zařízení a soukromého, určeného k jejich následnému dešifrování.

Dalším specifickým znakem, dle kterého lze dělit ransomware, je podle Grimese (2021, 13-30) **rozsah jeho schopností** – tedy jestli pouze šifruje soubory, nebo je schopen širšího spektra škodlivých aktivit. Zatímco dříve ransomware pouze zašifroval soubory v infikovaném zařízení, v roce 2019 se vynořil Maze (Shemesh 2021; Cluley 2020), který kromě toho také odcizil data svých obětí a vyhrožoval jejich zveřejněním v případě nezaplacení výkupného. To inspirovalo i ostatní např. REvil/Sodinokibi či Zeppellin (Cimpanu 2019; De Souza 2020) a zcela běžnou se tak stala praktika velmi často označovaná jako dvojí zneužití, či dvojí vydírání.

Grimes (2021, 23-30) nicméně upozorňuje, že tento problém je mnohem rozsáhlejší. Útočníci si totiž již plně uvědomují hodnotu přístupu do zařízení či sítí, kterého dosáhli prostřednictvím ransomware, a snaží se jej co nejlépe využít. Kromě zašifrování souborů tak dochází současně ke krádeži dat a vyžadování výkupného za jejich nezveřejnění nejen od zasažené organizace, ale také od zaměstnanců, zákazníků či dodavatelů. Dále dochází ke krádežím přihlašovacích údajů, k zneužívání přístupu za účelem rozesílání škodlivých e-mailů ze skutečných adres, nebo k DDoS útokům či veřejnému zesměšňování infikované organizace s cílem donutit ji k zaplacení výkupného.

Posledním členícím aspektem ransomware je dle Grimese (2021, 30-32) otázka jeho původu – tedy zda byl **vytvořen útočníkem, nebo se jedná o ransomware jako službu.** Původní ransomware, tedy ten zároveň vytvořený a použitý útočníkem, je na ústupu. V současnosti se rozmáhá trend ransomware jako služby. Je však nutné zmínit, že hotový ransomware bylo možné zakoupit již poměrně dávno. Změna nastala zejména v tom, že v současnosti poskytují tvůrci ransomware svým zákazníkům mnohem rozsáhlejší služby, které jdou daleko za samotný vývoj škodlivého software (Grimes 2021, 30-32). Tvůrci ransomware poskytují útočníkům nejčastěji za počáteční poplatek a procenta ze získaného výkupného. Za to však nabízí mimo samotný škodlivý software také řadu dodatečných služeb, třeba zákaznickou a technickou podporu či asistenci při vymáhání, výběru a legalizaci výkupného (DiMaggio 2022). Mezi nejproslulejší zástupce skupin nabízejících ransomware jako službu patří DarkSide (Baker 2022a; Nuce et al. 2021), REvil/Sodinokibi (Baker 2022a; Cluley 2022) či LockBit (Baker 2022a; Roddie 2021).

2.2.3 Schéma ransomwarového útoku

Vytvoření univerzálního schématu ransomwarového útoku je vzhledem k obrovskému množství různých typů, které se od sebe mohou i významně lišit, téměř nemožné.

Liska a Gallo (2016, 6-17) rozdělují typický ransomwarový útok do pěti fází:

- **nasazení** – využití vektorů k infikování cílového zařízení;
- **instalace** – instalace škodlivého software do cílového zařízení, rozšíření škodlivého software po síti do dalších zařízení, zisk informací o prostředí, ve kterém se škodlivý software nachází;
- **řízení a kontrola** – vytvoření komunikačních kanálů k řídícím serverům a očekávání instrukcí, identifikace a validace útoku, předání šifrovacího klíče;
- **destrukce** – zašifrování souborů;
- **vydírání** – představení požadavků oběti.

Také dle Hassana (2019, 44-45) lze typický ransomwarový útok zjednodušeně vystihnout v pěti fázích, ty se nicméně od těch představených výše mírně liší:

- **zneužití a infekce** – ransomware proniká do systému oběti;
- **doručení a spuštění** – ransomware je instalován do zařízení oběti;
- **zničení záloh** – ransomware hledá zálohy souborů a ničí je;
- **zašifrování** – ransomware šifruje soubory v zařízení oběti a zajišťuje si bezpečné spojení se servery řízení a kontroly;
- **uvědomění oběti a vydírání** – ransomware zobrazuje oběti požadavek výkupného.

Podle Grimese (2021, 32-48) pak zahrnuje jediný ransomwarový útok na šestnáct samostatných fází, přičemž zašifrování souborů je až třináctou z nich. Tento rozdíl mezi zmíněnými schématy je možno vysvětlit mimo případný subjektivní pohled autorů jak rozdílným chováním jednotlivých rodin ransomware, tak zvyšující se sofistikovaností a komplikovaností tohoto typu malware v čase.

2.2.4 Útočníci a oběti ransomware

Ransomwaroví útočníci se podobně jako jejich cíle vyvíjeli v čase. V prvotních fázích rozvoje ransomware se jednalo zejména o jednotlivce či malé neprofesionální skupiny. Ti po nahrání souborů nakažených primitivním ransomware na pirátské stránky či jejich rozeslání tisícům náhodných adresátů e-mailem doufali v nedostatečné zabezpečení zařízení svých obětí (DiMaggio 2022). Ransomware nebyl do rozšíření používání kryptoměn příliš výnosnou záležitostí, tudíž neexistoval dostatečný impuls k pokusům o sofistikovanější kampaně, které by si vyžadovaly vyšší míru profesionalizace útočníků (Grimes 2021, 48).

S příchodem Bitcoinu se transakce staly pro útočníky bezpečnější a také se významně navýšily zisky plynoucí z ransomware (Hassan 2019, 7). To vedlo k většímu zájmu o tuto kategorii kyberkriminality a útočníci se začali profesionalizovat (Grimes 2021, 49). Díky stále se navyšujícím ziskům lákal ransomware nové talenty, začaly vznikat nové skupiny a ty původní se dále rozrůstaly. Grimes (2021, 49-51) uvádí, že se začaly tvořit kyberzločinecké korporace. V současnosti je pak dle něj možno ty nejúspěšnější skupiny označit jako konglomeráty, v rámci kterých existují menší vzájemně provázané úzce specializované profesionální skupiny.

Významnou roli v tomto vývoji pak sehrály také některé státy – zejména Čína, Rusko a Severní Korea, které poskytují kyberzločincům

útočiště a mnohdy také využívají jejich působení k vlastnímu prospěchu (Grimes 2021, 79). Důležité je pak také znovu upozornit na to, že útočníci nemusí být nutně tvůrci daného ransomware, což umožňuje v současnosti hojně se vyskytující model ransomware jako služby (Grimes 2021, 30-32; DiMaggio 2022).

Primární oběti ransomwarových útoků se také postupně proměňovaly a tento vývoj významně kopíruje vývoj samotných kyberzločinců. Před rokem 2015 byli cílem kyberzločinců především náhodní jednotlivci (DiMaggio 2022). S profesionalizací ransomware nicméně došlo k přesunu zájmu na hodnotnější cíle ve formě vládních a nevládních organizací. V roce 2016 se pak oblíbeným cílem útočníků stala zejména zdravotnická zařízení (Hassan 2019, 23).

V současnosti se vzhledem ke schopnostem útočníků může stát obětí téměř kdokoli – od jednotlivce, přes vládní, zdravotnické či vzdělávací instituce, až po nadnárodní korporace či prvky kritické infrastruktury (Vigliarolo 2021). Mimo to je třeba poukázat také na fakt, že ransomware se již netýká pouze osobních počítačů, přičemž ani zde již nehraje téměř žádnou roli využívaný operační systém – obětí se mohou stát uživatelé Microsoft Windows, Apple či Linux. Ransomware v dnešní době může postihnout i mobilní zařízení, zařízení internetu věcí či průmyslové kontrolní systémy a SCADA systémy (Grimes 2021, 262-263).

2.2.5 Platby výkupného

S ransomware je přímo spojena také problematika plateb výkupného. Pro útočníky bylo dříve velice náročné získat od svých obětí bezpečně zaplaceno, což poměrně dlouho bránilo ransomwarovým útokům v rozmachu. Zatímco doktor Popp, tvůrce prvního vyděračského malware, požadoval výkupné v případě AIDS PC Cyborg Trojan zaslat peněžní

poukázku na P.O. Box v Panamě, později se staly populárními voucherové systémy jako Paysafecard, MoneyPack, UKash, CashU či MoneXy (Savage, Coogan and Lau 2015, 22). Pravého rozvoje však dosáhl ransomware až s příchodem Bitcoin a dalších kryptoměn (Hassan 2017, 7; Grimes 2021, 48-49), které jsou ransomwarovými útočníky preferovaným způsobem plateb výkupného do současnosti (DiMaggio 2022).

Kryptoměny představují digitální hotovostní systém fungující jako médium pro směnu využívající kryptografických protokolů k zabezpečení transakcí (Hassan 2019, 179) fungujících na principu blockchainu, tedy určité podkladové transakční distribuované sledovací účetní knihy. V té jsou detailně zaznamenány všechny transakce včetně digitálních identit odesílatelů a příjemců (Grimes 2021, 116). Pohyb kryptoměn je tedy možné skrze blockchain poměrně detailně sledovat, v dnešní době případně také blokovat či přesměrovat, jako se to povedlo americké FBI v případě proslulého ransomwarového útoku na Colonial Pipeline (Uberti 2021; Romo 2021). Aby útočníci o výkupné nepřišli, případně aby se neprozradili při jeho převodu na fiat měnu, využívají metod praní špinavých peněz. Pro tyto účely existují specializované zločinecké skupiny zaměřující se pouze na skrytí transakcí v rámci blockchainu (Grimes 2021, 54).

Kryptoměn existuje v současnosti celá řada, tou nejproslulejší a prozatím nejpoužívanější i v oblasti ransomware je nicméně Bitcoin (Grimes 2022). Směrem k legislativní úpravě kryptoměn mimo jiné i ve vztahu k praní špinavých peněz, se pro kryptoměny využívá označení virtuální aktiva. Ta jsou definována § 4 odst. (9) Zákona o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu (dále Zákon ML/FT) ve vazbě na § 3 odst. (3) písm. c) bodů 4 až 7 a písm. e) Zákona o platebním styku.

Částky požadované ransomwarovými útočníky se různí, v současnosti jsou běžně přizpůsobeny možnostem oběti (Savage, Coogan and Lau 2015, 21-22). Rozpětí požadavků je v tomto ohledu obrovské – od stovek USD v případě jednotlivců, po miliony USD v případě velkých společností. Prozatím nejvyšší zdokumentované výkupné 70 milionů USD požadoval REvil při útoku na společnost Kaseya (Clancy 2021; Winder 2021; Lawler 2021). Dostupné statistiky týkající se požadavků útočníků, případně pak i peněz vyplacených na výkupném, nejsou bohužel přesné. Ne všechny oběti totiž informují o svém napadení či o výši zaplaceného výkupného.[2]

2.2.6 Ransomware a organizovaný zločin

Jak bylo již dříve zmíněno, ransomware je jednou z forem kyberkriminality. Podobně bylo v práci také zmíněno, že současní ransomwaroví útočníci povětšinou nepracují individuálně, nýbrž ve skupinách, které se vyznačují určitou mírou organizace. Na místě je tedy představit vztah mezi ransomware a OZ.

Definic OZ je nespočet. Šmíd (2008, 279) považuje za jeden z nejzdařilejších přístupů Finckenauerův rámec specifikující definiční znaky OZ – absenci ideologie, strukturu/organizaci/hierarchii, kontinuitu,

[2] Unit 42 Palo Alto Networks uvádí, že u jimi řešených případů činil v roce 2021 průměrný požadavek na výkupné 2,2 milionu USD a průměrné zaplacené výkupné dosáhlo na 541 010 USD (Muncaster 2022). Dle Raybouldа (2022) činil průměrný požadavek výkupného u ransomware v roce 2021 celých 220 298 USD. Dle Sophos byla průměrná hodnota zaplaceného výkupného v roce 2021 812 000 USD (Jones 2022) a dle Crowdstrike dokonce 1,79 milionu USD (Baker 2022b). Dle Chainalysis činila celková hodnota plateb za ransomwarové výkupné v roce 2021 jen v kryptoměnách více než 600 milionů USD (Janofsky 2022), přičemž dle Financial Crimes Enforcement Network mohla čítat tato částka ještě před koncem roku 2021 až na 5,2 miliardy USD (De 2021).

násilí/hrozby násilím, omezené členství, nelegální podnikání, pronikání do legitimní ekonomiky a korupci (Finckenauer 2005, 65). Jako další vhodnou zmiňuje Šmíd (2008, 281) také definici dle Hagana (2006, 133), která uvádí, že pojem *„organizovaný zločin odkazuje ke kontinuálně operujícím organizovaným skupinám monopolizujícím nelegální podnikání skrze násilí a hrozby, které si zajišťují beztrestnost skrze korupci."*

Když přihlédneme k definičním znakům dle Finckenauera (2005, 65), je možné konstatovat, že ransomwaroví útočníci naplňují alespoň částečně hned několik z nich. Splnění jednotlivých znaků se nicméně může měnit skupinu od skupiny. Typicky jsou útočníci motivováni finančním ziskem (Grimes 2021, xxxiv; DiMaggio 2022), disponují organizační strukturou (Grimes 2021, 48-55), členství je omezeno národností a/nebo talentem (Grimes 2021, 49; DiMaggio 2022), jejich hlavním zdrojem příjmu je páchání nelegálních aktivit (Grimes 2021, 30-32; DiMaggio 2022), usilují o pronikání do legální ekonomiky skrze legalizaci zisků z výkupného (Grimes 2021, 122) a budují korupční vztahy, díky kterým jsou na území určitých států beztrestní (Grimes 2021, xxxiv). Problematickým bodem je pak kontinuita, neboť poměrně často dochází k rozpadům, reorganizacím či rebrandingu těchto skupin (Patterson 2021). Definiční bod násilí je pak nutné vnímat v dimenzi kyberprostoru, kde své oběti zastrašují např. zničením či zveřejněním dat.

Obecnější definice, jejichž kritéria pak ransomwaroví útočníci splňují již v podstatě bez výhrad, představuje například Organizace spojených národů (dále OSN), Evropské unie (dále EU) nebo Policie ČR (dále PČR). Dle OSN (UNODC 2004, 5) je organizovaná kriminální skupina *„strukturovaná skupina tří či více osob existující po určité časové období a jednající v souhře s cílem spáchat jeden či více závažných zločinů … za účelem finančního či materiálního zisku."* Tuto definici v roce 2008 pro

své účely adaptovala také EU k definování tzv. zločinného spolčení v Rámcovém rozhodnutí Rady o boji proti organizované trestné činnosti. EUORPOL (n.d.) k uvedené definici OSN dodává, že reflektuje konceptualizaci OZ většiny orgánů vymáhajících právo po celém světě. PČR (2016) pak na svých webových stránkách uvádí, že *„organizovaný zločin je druhem skupinové trestné činnosti páchané organizovanou zločineckou skupinou nebo zločineckou organizací."* To dále doplňuje prohlášením, že *„tyto skupiny a organizace mají většinou vícestupňovou vertikální organizační strukturu a je pro ně typické soustavné páchání koordinované závažné trestné činnosti."*

Bez ohledu na naplňování výše uvedených definičních znaků je v médiích zažité označování útočníků jako ransomwarových gangů (např. Palmer 2022; Glover 2021; Burgess 2022), objevují se ale také zmínky o ransomwarových kartelech (Sjouwerman 2021; Patterson 2021; DiMaggio 2021b).

2.3 Policy

2.3.1 Trojdimenzionální dělení politiky

Nežli bude představena policy analýza jakožto výzkumný žánr či pojem policy jako takový, je nejprve třeba objasnit trojdimenzionální pojetí pojmu politika, které je dle Fialy a Schuberta (2000, 14) *„základním předpokladem, z nějž celý výzkum policy vychází."* Toto trojdimenzionální pojetí politiky má původ v anglickém jazyce, kde vedle sebe existují tři pojmy – polity, politics a policy.

Tyto pojmy nicméně nejsou synonymní a používají se pro označení tří analyticky odlišitelných aspektů politiky:

- **Polity** je označení pro dostupný rámec formálních i neformálních pravidel hry, která řídí chování politických aktérů (Pennings, Keman and Kleinnijenhuis 2006, 26). Jedná se o institucionální a normativní stránku politiky (Fiala and Schubert 2000, 17-18).
- **Politics** je pojem využívaný pro procesuální dimenzi politiky, do které dynamicky vstupují různí aktéři (Fiala and Schubert 2000, 18), a kde skrze konflikt či koncensus získávají či ztrácí relevanci různé zájmy a přístupy (Veselý, Drhová and Nachtmanová 2005, 7).
- **Policy** pak zjednodušeně značí politická rozhodnutí, která jsou následně implementována (Pennings, Keman and Kleinnijenhuis 2006, 26). Jedná se o dimenzi, ve které se politické ideje a rozhodnutí proměňují v konkrétní opatření jako zákony a nařízení, programy a další výstupy (Fiala and Schubert 2000, 19).

Trojdimenzionální pojetí politiky nicméně vytváří terminologický problém mimo jiné v českém jazykovém prostředí, kde je pro označení politiky využíván pouze jeden pojem. Ačkoli pro pojem policy v českém jazyce vhodný jazykový ekvivalent neexistuje, lze zde pracovat s konkrétními pojmy strategie, koncepce, plány, programy či třeba zákony (Veselý, Drhová and Nachtmanová 2005, 12).

2.3.2 Policy

Mimo terminologické obtíže s vymezením pojmu policy v českém jazyce vyvstávají také otázky ohledně jeho definice, na které do současnosti nepanuje úplný konsensus. Pro účely této práce je nicméně přijat přístup Veselého, Drhové a Nachtmanové (2005, 10), kteří se pokusili blíže

specifikovat pojem policy ve veřejném sektoru skrze stanovení toho, čím policy je a čím naopak není. Veselý, Drhová a Nachtmanová (2005, 10) uvádějí, že policy je:

- více než rozhodnutí;
- tvořená s určitým záměrem;
- tvorba a deklarace záměru i proces jeho implementace;
- činnost i nečinnost;
- tvořena především veřejnými organizacemi;
- záměr a jeho realizace, nikoli produkt či výsledek tohoto procesu.

„Termín policy je běžně aplikován směrem k něčemu většímu, nežli k jednotlivým rozhodnutím, ale současně menšímu, nežli jsou obecná sociální hnutí," uvádí Heclo (1972, 84). Tuto myšlenku přijímají i Veselý, Drhová a Nachtmanová (2005, 10), kteří tvrdí, že policy je na *„střední úrovni… má větší dosah než jedno rozhodnutí, ale zároveň je na nižší úrovni než plány na radikální změnu společnosti."* Názor, že policy je více než partikulární rozhodnutí pak zastává mimo jiné také Jenkins (1978, 15) a o policy hovoří jako *o „setu vzájemně propojených rozhodnutí přijatých politickými aktéry, která se týkají výběru cílů a prostředků k jejich dosažení v kontextu specifické situace."* Mimo samotného rozsahu Jenkinsova definice upozorňuje i na další aspekt přijatého vnímání policy, tedy že je tvořena s určitým deklarovaným záměrem.

S potřebou záměru či cíle policy pak souhlasí i dva z otců výzkumu policy Lasswell a Kaplan (1970, 71), kteří uvádějí, že policy je *„předpokládaný program cílů, hodnot a postupů."* Anderson (2003, 2) chápe policy jako *„účelný postup,"* a Friedrich (1963, 70) přímo zdůrazňuje, že *„pro policy je nezbytné, aby měla cíl, účel a záměr."* Dle Dye (2013, 12) jsou ale definice podmiňující policy jejím cílem nevhodné, protože si nemůžeme

být nikdy zcela jisti tím, že určitá akce vlády je činěna s konkrétním cílem. Veselý, Drhová a Nachtmanová (2005, 10), však tento přístup odmítají a dokonce staví bezcílnost do protikladu k policy. Mimo to autoři uvádějí, že cíle a záměry policy mohou být explicitní i implicitní, mohou se v čase vyvíjet a měnit, nebo mohou být odhaleny až zpětně. V tomto směru však není vyloučeno, že politici jednají třeba jen s cílem se zviditelnit (Beblavý 2002, 17).

Třetím aspektem policy je, že zahrnuje nejen tvorbu a deklaraci záměru, ale také jeho realizaci. Veselý, Drhová a Nachtmanová (2005, 10) hovoří o tom, že policy často není jasně vymezený a konkrétní jev spočívající na hierarchickém rozdělení politiků, jakožto tvůrců politiky, a veřejné správy, jakožto jejích realizátorů. Beblavý (2002, 16) zastává v tomto směru totožnou pozici, přičemž policy vnímá jako *„společný výsledek mnoha operativních rozhodnutí anebo reakcí na problémy, které se objevily na relativně nízkých úrovních organizace.“* K této myšlence pak Veselý, Drhová a Nachtmanová (2005, 11) dodávají, že formování finální podoby policy může probíhat i během její implementace. S tímto postojem k policy souhlasí třeba i Kraft a Furlong (2017, 38), kteří uvádějí, že policy je spojena i s praktikami dílčích agentur implementujících konkrétní programy.

Mimo to Kraft a Furlong (2017, 38) vnímají policy *jako „vládní činnost či nečinnost v reakci na veřejné problémy,“* což koresponduje s myšlenkou, že policy nemusí být pouze konkrétní aktivitou, nýbrž také pasivitou. Podobně k policy přistupuje i Birkland (2015, 9), který zastává názor, že *„policy jsou prohlášení vlády o tom, co zamýšlí činit … přičemž absenci těchto prohlášení lze téže vnímat jako implicitní prohlášení policy.“* Snad nejznámějším proponentem tohoto vnímání je ale Dye (2013, 3), jehož velmi často citovaná definice uvádí, že *„policy je cokoli, co se vlády*

rozhodnou učinit či neučinit.“ V tomto směru pak Veselý, Drhová a Nachtmanová (2005, 11) představují tři formy nečinnosti. První z nich je nečinnost nevědomá, kdy si zainteresování aktéři neuvědomují potřebu jednat. Další je pak nečinnost záměrná, kdy je rozhodnuto, že určitý problém není hoden další akce. Třetí formou je nečinnost spočívající v absenci snahy o realizaci určitého deklarovaného záměru.

Předposledním zmíněným aspektem policy je, že je *„vytvořena, autorizována nebo schválena veřejnými institucemi“* (Veselý, Drhová and Nachtmanová 2005, 11). Výše zmíněné definice Krafta a Furlonga (2017, 38), Birklanda (2015, 9) či Dye (2013, 3) zmiňují vládu. Ve veřejné sféře se ale může jednat také o ministerstva, parlament, kraje, obce či přímo řízené organizace (poradní orgány, výzkumné ústavy nebo státní agentury) (Veselý, Drhová a Nachtmanová 2005, 11).

Na závěr je třeba poznamenat, že policy není výstup ani výsledek. Chápání policy současně jako záměru i výsledku vede k tomu, že výsledkem policy by byla policy (Veselý, Drhová and Nachtmanová 2005, 11).

3 Metodologie

V rámci kapitoly věnované metodologickému ukotvení jsou představeny možné přístupy k policy analysis jakožto žánru, ve kterém je tato práce pojata. Poté je v kapitole představen přístup k policy analysis využitý pro účely této práce a její výzkumný design odvíjející se od v úvodu představených výzkumných cílů a otázek. Následně se kapitola věnuje již konkrétním metodám sběru a analýzy dat využitým pro zpracování tohoto textu. Na závěr kapitoly jsou představeny limity a etické aspekty.

3.1 Policy analysis

Podobně jako u pojmu policy i u policy analysis narážíme na problém absence konsensu ohledně jejího vnímání. Zatímco někteří autoři (např. Patton and Sawicki 1993, 24; MacRae 1979, 17; Jenkins-Smith 1990, 1; Kraft and Furlong 2017, 199) omezují záběr policy analysis na různorodé zkoumání alternativních policies, další vnímají disciplínu šířeji, což se jeví pochopitelné vzhledem k různorodosti teoretických i metodologických přístupů, s nimiž je možné se v disciplíně policy analysis setkat. Tuto různorodost zachycuje dle Fialy a Schuberta (2000, 13) ve své definici Dye (2013, 11). Ten uvádí, že *„policy analýza je odhalování toho, co vlády dělají, proč to dělají, a jaký rozdíl to vytváří."* Zájmem policy analysis je tedy obsah (co vlády dělají), rozhodující faktory, důvody, příčiny (proč to dělají) a účinky, výsledky a souvislosti policy (jaký rozdíl či změnu to vytváří) (Fiala 1995, 137).

Dále i Dunn (2018, xxvii) poukazuje ve své definicí na různorodost policy analysis když říká, že *„policy analysis je aplikovanou sociálně-vědní disciplínou využívající mnoha metod zkoumání k řešení praktických*

problémů." Své vnímání policy analysis Dunn (2018, 3) dále rozvádí prohlášením, že se jedná *„o proces multidisciplinárního šetření s cílem vytvářet, kriticky hodnotit a komunikovat znalosti relevantní pro policy."*

Bližší pochopení policy analysis je možné také skrze její typy, které někteří autoři specifikují. Enserink, Koppenjan a Mayer (2013, 13) např. dělí policy analysis na analýzu akademickou a praktickou. Akademická policy analysis může být deskriptivní, interpretativní či explanatorní a zaměřuje se na zkoumání policy. Autoři uvádí, že se jedná v podstatě o případové studie policy. Praktická policy analysis pak sestává z aktivit, metod a nástrojů, které jsou využity k podpoře vytváření policy.

Veselý (2007, 21) také zmiňuje, že je možné rozlišit několik typů policy analysis, přičemž jako jedno z hlavních kritérií této typologizace vnímá *„zda je policy analysis prováděna před anebo po implementaci určité policy."* Této otázce se detailně věnují Patton, Sawicki a Clark (2016, 22-23), kteří identifikují dva hlavní typy policy analysis – deskriptivní (ex-post) a prospektivní (ex-ante). Ty dále člení na retrospektivní a evaluační u typu ex-post a prediktivní a preskriptivní u typu ex-ante.

Deskriptivní policy analysis se věnuje buďto historické analýze existujících či minulých policies, případně evaluaci nových policies v době jejich implementace. Historickou analýzu policy je možné nazvat analýzou retrospektivní. Evaluační analýza je pak označení pro analýzu zaměřenou na zhodnocení výsledků policy (Patton, Sawicki and Clark 2016, 22).

Policy analysis zaměřená na možné výsledky navrhovaných policies, tedy do budoucnosti, je nazývána analýzou prospektivní. Pokud se zaměřuje na projekci budoucích stavů, které mohou vzniknout v důsledku přijetí určitých alternativních policies, označuje se jako prediktivní. V případě, že se zaměřuje na doporučení určitých akcí s cílem dosáhnout

konkrétního výsledku, jedná se o analýzu preskriptivní (Patton, Sawicki and Clark 2016, 23).

3.2 Aplikovaný přístup k policy analysis

V rámci představených přístupů ke zkoumání policy je tuto práci možné zařadit do žánru policy analysis. Dle typologizace policy analysis Enserinka, Koppenjana a Mayera (2013, 13) je možné ji chápat konkrétně jako případovou studii policy. Cílem této práce je analyzovat policy zaměřenou na potírání ransomware v ČR, přičemž výzkumné otázky se zaměřují primárně na charakteristiky této policy. Díky tomu je tedy design této práce možné označit jako případovou studii.

Případové studie jsou charakteristické tím, že usilují o detailní studium, tedy popis a rozbor jednoho nebo několika málo případů (Hendl 2005, 103) – v tomto případě policy potírání ransomwarových útoků na území ČR. Hendl (2005, 109-110) zmiňuje možnost rozlišit případové studie dle Yina (1994) na exploratorní, explanatorní, deskriptivní a evaluační. Vzhledem ke svému zaměření je tato práce kombinací případové studie deskriptivní, neboť usiluje o kompletní popis zkoumaného jevu, a případové studie evaluační, protože se zároveň snaží o hodnocení tohoto jevu na základě určitých kritérií.

V rámci rozdělení policy analysis dle Pattona, Sawickiho a Clarkové (2016, 22-23) je práce zaměřena primárně ex-post, neboť se věnuje jak popisu, tak evaluaci v současnosti platné a implementované policy. Jelikož je však součástí práce také navržení doporučení pro vylepšení zkoumané policy, je tuto její specifickou část možno vnímat jako preskriptivní policy analysis spadající do kategorie ex-ante.

3.3 Výzkumný design

Předložený text se věnuje oblasti kyberbezpečnosti, v rámci níž se zaměřuje na téma potírání ransomwarových útoků v ČR. Cílem této práce je identifikovat slabá místa v současném přístupu ČR k potírání ransomware a navrhnout doporučení pro jejich eliminaci.

Policy analysis v tomto textu sestává ze čtyř na sebe navazujících částí. V první části je nastíněn vývoj ransomware jako bezpečnostní hrozby ve světě a následně v ČR. Dále je v krátkosti představen přístup ČR k boji proti ransomware a závazky vyslovené ČR v Joint Statement (The White House 2021). Tato část práce je založena na analýze primárních a sekundárních zdrojů a jejím cílem je představit kontext boje proti ransomware v ČR.

V druhé části je prostřednictvím analýzy koncepčních dokumentů a informací získaných skrze expertní rozhovory provedena deskripce policy potírání ransomware v ČR dle rámce závazků vyslovených ČR v Joint Statement (The White House 2021). Tato část práce usiluje o zodpovězení otázek:

- Je policy potírání ransomware v ČR v souladu se závazky vyslovenými v Joint Statement?
    - Jak je v koncepčních dokumentech ČR vymezena policy potírání ransomware?
    - Jak je v ČR legislativně ukotvena policy potírání ransomware?
    - Jaké kroky činí ČR za účelem potírání ransomware v praxi?

Třetí část je možno označit jako evaluaci policy. Evaluace se může týkat jak výsledků konkrétní policy, tak procesu její implementace (Wollmann 2017, 393), který je středem zájmu evaluace policy v této práci. Evaluace policy provedena v tomto textu se zaměřuje na identifikaci slabých míst

policy boje proti ransomware v ČR zejména s ohledem na její soulad se závazky vyslovenými v Joint Statement (The White House 2021). Mimo to jsou ale v této části zohledněny také názory dotazovaných expertů. Tato část tedy dále rozvádí odpověď na otázku:

- Je policy potírání ransomware v ČR v souladu se závazky vyslovenými v Joint Statement?

A zodpovídá také otázky:

- Jaká jsou slabá místa koncepčního vymezení policy potírání ransomware v ČR?
- Jaká jsou slabá místa legislativního ukotvení policy potírání ransomware v ČR?
- Jaká jsou slabá místa praxe potírání ransomware v ČR?

Čtvrtá část je věnována doporučením pro úpravu zkoumané policy směrem k eliminaci identifikovaných slabých míst. Zohledněn je v tomto případě jak soulad či nesoulad s Joint Statement, tak názor dotazovaných expertů či benchmarking. Benchmarking byl původně metodou využívanou v korporátním světě – společnosti se srovnávaly s těmi, které jsou považovány za nejlepší v oboru a na základě tohoto srovnání a identifikace možností k vlastnímu zlepšení upravovaly své operace. Jedná se tedy o učení na základě srovnání, které se z korporátního světa rozšířilo i do oblasti zkoumání a vytváření policy (Malecki 2007, 639). Touto prací představená doporučení jsou tedy formulována na základě dat získaných expertními rozhovory, a také rešerší primárních a sekundárních zdrojů. Cílem této části je tedy zodpovědět otázku:

- Jakým způsobem je možné eliminovat identifikovaná slabá místa policy potírání ransomware v ČR?

3.4 Metody sběru dat

Vzhledem k tomu, že policy analysis nabízí poměrně otevřený prostor nejen v oblasti teoretických východisek, ale také v metodologických přístupech (Fiala and Schubert 2000, 38), je výběr konkrétních metod pro zodpovězení představených otázek možno přizpůsobit charakteru výzkumu. Pro účely této práce se jako nejvhodnější výzkumná strategie jeví kvalitativní přístup, jenž dle Reichela (2009, 40) *„představuje řadu rozdílných postupů, které se snaží najít porozumění zkoumanému sociálnímu problému“* a *„pokoušejí se určitý fenomén (prvek, aspekt, proces apod.) nahlížet v pro něj autentickém prostředí a vytvářet jeho obraz v co možná nejkomplexnější podobě.“* S ohledem na konkrétní vyšetřovací techniky Fiala a Schubert (2000, 41) uvádějí, že u policy analysis je běžně využíváno dotazování, angažovaného pozorování a obsahové analýzy. V rámci této práce bude využito dotazování ve formě částečně standardizovaných expertních rozhovorů a také nestandardizované kvalitativní analýzy dokumentů.

3.4.1 Analýza dokumentů

Data získaná analýzou dokumentů tvoří základní datový podklad této práce. Jako dokument pak vnímáme *„data, která vznikla v minulosti, byla pořízena někým jiným než výzkumníkem a pro jiný účel, než jaký má aktuální výzkum“* (Hendl 2005, 204). Otázce dokumentů využitelných pro policy analysis se věnují Veselý, Drhová a Nachtmanová (2005, 13). Ti uvádějí, že u policy je velmi komplikované identifikovat její konkrétní začátek, lze však identifikovat určité okamžiky, kdy je policy explicitně formulována. Tak se děje nejčastěji formou písemného dokumentu. Tyto

dokumenty lze dle autorů nazývat veřejné politické dokumenty (dále VPD), které jde členit na:

- **strategické VPD** (např. strategie, koncepce, akční plány, plány rozvoje, národní politiky),
- **legislativní VPD** (např. ústavní zákony, zákony, nařízení, vyhlášky, mezinárodní dohody),
- **výzkumné VPD** (např. veřejné politické analýzy, policy briefs),
- **deklarativní a advokační VPD** (např. programová prohlášení vlády).

Cílem analýzy VPD pro účely této práce je identifikace konkrétních prohlášení majících vztah k předmětu jejího zájmu. Na základě této identifikace bude následně provedena jak deskripce zkoumané policy, tak částečně i její evaluace. Významné pro evaluaci budou však zejména expertní rozhovory.

Pro účely této práce byly primárně analyzovány v současnosti platné strategické VPD, které vymezují policy ČR v oblasti bezpečnosti, kyberbezpečnosti, boje proti trestné činnosti, potažmo organizované kyberkriminalitě. Mezi tyto dokumenty patří zejména:

- **Bezpečnostní strategie České republiky 2015** (dále Bezpečnostní strategie) vydaná v roce 2015 Ministerstvem zahraničních věcí ČR (dále MZV ČR),
- **Národní strategie kybernetické bezpečnosti České republiky na období let 2021-2025** (dále Národní strategie KB) vydaná v roce 2020 Národním úřadem pro kybernetickou a informační bezpečnost (dále NÚKIB),
- **Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025** (dále Akční plán) vydaný v roce 2021 NÚKIB,

- **Koncepce boje proti organizovanému zločinu do roku 2023** (dále Koncepce boje proti OZ) vydaná v roce 2018 Ministerstvem vnitra ČR (dále MV ČR).

Dále byly analyzovány legislativní VPD upravující kyberbezpečnost, boj proti organizované kyberkriminalitě či legalizaci výnosů z ní, a také legislativní VPD vymezující role významných aktérů v těchto oblastech působících. Mezi tyto dokumenty patří zejména:

- **Zákon č. 181/2014 Sb., o kybernetické bezpečnosti** (dále ZKB)
- **Zákon č. 273/2008 Sb., o Policii České republiky** (dále Zákon o PČR)
- **Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu** (dále Zákon ML/FT)
- **Zákon č. 40/2009 Sb., trestní zákoník**

3.4.2 Expertní rozhovory

Kromě rešerše a analýzy dokumentů jsou pro tuto práci významná taktéž data získána formou expertních rozhovorů. Expertní rozhovory jsou charakteristické tím, že středem zájmu nejsou samotní dotazovaní, nýbrž jejich expertíza, tedy orientace, zkušenosti a znalosti v konkrétní oblasti (Flick 2009, 165). Definování experta se odvíjí od problematiky, která je studována. Pro účely této práce vnímáme experta jako osobu se specifickými profesními zkušenostmi a znalostmi.

Pro účely této práce plnily expertní rozhovory dle typologie Bognera a Menze (2009, 46-48) především funkci systematizující, sekundárně pak také funkci exploratorní. Systematizující funkce rozhovorů spočívala v získání přístupu k exkluzivním znalostem, kterými experti

disponují. Exploratorní funkci pak plnily směrem k získaní ucelenějšího obrazu zkoumané problematiky.

Dále je rozhovory možno členit dle míry jejich standardizace na rozhovor nestrukturovaný, strukturovaný a polostrukturovaný (Reichel 2009, 108-112). Rozhovory využívané k zisku dat pro tuto práci měly formu rozhovorů polostrukturovaných, před rozhovorem byl tedy sestaven soubor otázek, který byl ale v průběhu rozhovorů upravován či doplňován.

Vzorek expertů byl sestaven na základě referenčního výběru metodou sněhové koule (Disman 2002, 114-115). Nejprve byli osloveni experti, na které bylo možné získat kontaktní informace z otevřených zdrojů. Ti byli následně požádání o zprostředkování kontaktu na další experty ve zkoumané oblasti. Experti byli oslovování skrze e-mail a vzhledem k jejich značné pracovní vytíženosti byla forma rozhovoru ponechána na jejich preferenci. Přepis jednotlivých rozhovorů se nachází v přílohách této práce. V tabulce č. 1 se nachází konkrétní výčet expertů, s nimiž byly vedeny rozhovory pro účely této práce.

Tab. 1: Respondenti expertních rozhovorů (vlastní tabulka)

Expert č. 1	
Označení ve zdrojích	Anonymní zdroj č. 1
Pracoviště	NCOZ[3]
Délka praxe	7 let
Forma rozhovoru	Korespondenčně via e-mail
Datum provedení rozhovoru	20. 5. 2022

[3] Národní centrála proti organizovanému zločinu služby kriminální policie a vyšetřování (dále NCOZ).

Expert č. 2	
Označení ve zdrojích	Plecitý, David
Pracoviště	FAÚ[4] – Analytické oddělení 042
Délka praxe	28 let
Forma rozhovoru	Osobní, Praha
Datum provedení rozhovoru	11. 5. 2022
Expert č. 3	
Označení ve zdrojích	Sikora, Vojtěch
Pracoviště	NÚKIB – Oddělení reaktivní
Délka praxe	4 roky
Forma rozhovoru	Korespondenčně via e-mail
Datum provedení rozhovoru	20. 5. 2022
Expert č. 4	
Označení ve zdrojích	Anonymní zdroj č. 2
Pracoviště	NÚKIB – Oddělení vzdělávání
Délka praxe	-
Forma rozhovoru	Korespondenčně via e-mail
Datum provedení rozhovoru	10. 5. 2022
Expert č. 5	
Označení ve zdrojích	Anonymní zdroj č. 3
Pracoviště	NÚKIB
Délka praxe	15 měsíců
Forma rozhovoru	Korespondenčně via e-mail
Datum provedení rozhovoru	10. 5. 2022

[4] Finanční analytický úřad (dále FAÚ).

Expert č. 6	
Označení ve zdrojích	Švéda, Martin
Pracoviště	NÚKIB – Oddělení regulace soukromého sektoru
Délka praxe	6 let
Forma rozhovoru	Korespondenčně via e-mail
Datum provedení rozhovoru	23. 5. 2022
Expert č. 7	
Označení ve zdrojích	Anonymní zdroj č. 4
Pracoviště	NÚKIB – Oddělení cvičení
Délka praxe	6 let
Forma rozhovoru	Korespondenčně via e-mail
Datum provedení rozhovoru	25. 5. 2022

3.5 Limity a etické aspekty

Důležité je představit také limity a etické aspekty této práce. Prvním limitujícím faktorem je skutečnost, že řada pro provedenou analýzu potenciálně hodnotných informací není zveřejňována, případně je ze své povahy dokonce utajována. S cílem získat mimo jiné také z otevřených zdrojů nedostupné informace o činnosti významných aktérů byly provedeny expertní rozhovory. I zde se nicméně vyskytly případy, kdy se expert zdržel zodpovězení otázky třeba z důvodu zachování služebního tajemství.

Dalším významným limitujícím faktorem je fakt, že ne se všemi oslovenými experty se z důvodu jejich značného pracovního vytížení podařilo uskutečnit plánovaný rozhovor. S cílem eliminovat tuto překážku bylo osloveno současně více expertů specializujících se na v práci

analyzovanou problematiku, nicméně ani toto opatření nebylo úspěšné. Analýza a její závěry se tedy v některých bodech opírají pouze o informace z otevřených zdrojů a absentují expertní náhled na věc.

Omezené množství expertů a nedostupnost řady informací dále také značně omezují možnost triangulace dat, což představuje další limitující faktor zejména s ohledem na to, že některé informace získané od expertů plní v případě této práce i systematizující funkci.

Za další limit práce je možné považovat také nejednotnou formu provedených rozhovorů. Expertům byla vzhledem k jejich pracovnímu vytížení nabídnuta možnost zvolit si preferovanou formu vedení rozhovoru. Většina expertů zvolila možnost korespondenčního rozhovoru skrze e-mailovou komunikaci. Jeden expert pak upřednostnil rozhovor vedený osobně. I přes zachování základních aspektů polostrukturovaných rozhovorů, zejména tedy možnosti doptávat se na odpovědi, je nicméně možné pozorovat větší otevřenost experta při vedení rozhovoru osobně, na rozdíl od poměrně stručných, byť hodnotných odpovědí získaných korespondenční formou.

Při provádění rozhovorů byl důraz kladen zejména na etické aspekty vědecké práce. Respondenti byli předem informováni o účelu provedeného rozhovoru, způsobu jeho záznamu, nakládání s tímto záznamem a následné publikaci získaných informací jak v samotném textu práce, tak formou přepisu v jejích přílohách. Respondenti byli požádáni o výslovný souhlas s publikací rozhovorem získaných informací, přičemž jim byla nabídnuta možnost anonymizace, které řada z nich využila. V práci jsou tedy uvedeny pouze ty informace, s jejichž publikací experti výslovně souhlasili.

Významné je pak také uvést, že informace získané expertními rozhovory pro účely této práce nereprezentují oficiální postoj organizací, ve kterých dotazovaní experti pracují – tedy NÚKIB, PČR a FAÚ.

4 Policy analysis

V rámci této kapitoly je nejprve představen kontext boje proti ransomware v ČR. Tato část pojednává o rozvoji hrozby ransomware ve světě, na což přímo navazuje podkapitola věnovaná rozvoji této hrozby v ČR. Poté je představena Counter Ransomware Initiative a závazky vyslovené zástupci států v Joint Statement (The White House 2021).

Na to navazuje další část, která se věnuje analýze policy potírání ransomware v ČR. Vzhledem k již zmíněné absenci jasného vymezení této policy na základě rámce Joint Statement (The White House 2021) text představuje koncepční závazky, legislativní ukotvení a aktivity obecnějšího charakteru, které mohou tuto nevyřčenou policy v ČR suplovat.

V další části této kapitoly jsou představena slabá místa analyzované policy, na což navazuje část věnující se doporučením směrem k jejich eliminaci.

4.1 Kontext boje proti ransomware

4.1.1 Ransomware ve světě

Prvním zdokumentovaným programem, který je běžně označován jako ransomware, byl AIDS PC Cyborg Trojan. Jeho tvůrce, biolog Joseph Popp, jej v roce 1989 rozesílal poštou na disketách (Grimes 2021, xxi-xxvii). Byť poměrně neúspěšný, vzbudil tento program obavy, že se budou podobné pokusy opakovat a stupňovat. Ty se nicméně po dlouhou dobu nenaplnily. V průběhu následujících let se sice postupně objevovaly ransomware využívající zejména pokroků v šifrování, útoky ale nedosahovaly významného úspěchu a ransomware tak byl spíše okrajovou záležitostí (Liska and Gallo 2016, 4).

K přelomu však došlo v roce 2013 s příchodem CryptoLocker, který požadoval platby výkupného v Bitcoin, jenž byl vynalezen roku 2009 (Miller 2017, 5; Grimes 2021, 48-49). Mnohamilionový úspěch CryptoLockeru inspiroval další skupiny a spustila se lavina ransomwarových útoků včetně Torrentblockeru, Cryptowall a Teslascript. Rok 2016 pak zaznamenal obrovský nárůst co do různých typů ransomware, mezi které patřily i nechvalně proslulé Locky, Petya a SamSam (Hassan 2019, 7). Rok 2017 se zase zapsal do historii díky WannaCry, který se samovolně šířil po síti jako červ (Dossett 2021).

V roce 2018 útočníci ustoupily od masivních kampaní a zaměřili se na mnohem cílenější a sofistikovanější útoky vůči velkým organizacím (Freed 2021). V roce 2019 se pak spolu s Maze ransomware skupiny REvil objevila taktika dvojího vydírání (Grimes 2021, 23-24). V současnosti je nejvýznamnějším trendem zejména ransomware jako služba, kterou nabízí např. Maze/Egregor, Ragnar Locker, Lockbit, REvil či Darkside, přičemž nejznámějším využitím ransomware jako služby je útok na americkou Colonial Pipeline z května roku 2021 (DiMaggio 2022; Javers 2021).

4.1.2 Ransomware v ČR

Jak ilustroval výše představený historický vývoj ransomware, tento typ škodlivého software si začal získávat pozornost širší veřejnosti zejména až s příchodem CryptoLocker, který požadoval zaplacení výkupného v Bitcoin (Grimes 2021, 48-49). I v ČR se stal CryptoLocker prvním rozšířenějším ransomware (Novinky 2017; Suchánková 2014), kterému předcházel pouze vyděračský locker – tzv. policejní vir, jinak známý také jako Reveton (CSIRT.CZ 2017; Štrbáková 2012; NCKB 2013, 4). V roce

2015 zaznamenala ČR dokonce několik případů infekce počítačů státní správy ransomware (NBÚ 2016, 36).

V lednu roku 2015 pak společnost ESET varovala před v Evropě se šířícím ransomware CTB-Locker (NCKB 2015, 5; Novinky 2015), který se o přibližně rok a půl později ukázal být za celou čtvrtinou všech detekovaných útoků v ČR (NCKB 2016a, 5; ESET 2016). Dalším ransomware, který si získal pozornost ČR v roce 2016 byl přes Facebook či nevyžádaný e-mail se šířící Locky (NCKB 2016b, 4; Novinky 2016). Ten páchal značné škody i v roce následujícím (AEC 2017; Houser 2017). Ransomware v tomto roce stál za značnou částí kyberbezpečnostních incidentů řešených národním a vládním CERT (NBÚ 2017, 44-45).

Rok 2017 byl co se ransomware zaměřeného na české uživatele týče poměrně plodný. Příkladem může být Crypt0L0cker, který se šířil česky psanými phishingovými e-maily (Křoustek 2017; Kasík 2017a), RANSOM_CZCRYPT.A, jenž zobrazoval požadavek na výkupné v lámané češtině (Trend Micro 2017; Checkmal 2017), nebo přes phishingové e-maily využívající skutečnou identitu jednatele české společnosti se šířící JScript Ransomware RPG (Minařík 2017). Česku se pak v roce 2017 nevyhnuly ani celosvětové kampaně WannaCry (Kalátová and Sassmanová 2017; Šafář and Potůček 2017a), wiperu NotPetya (Šafář and Potůček 2017b; ČTK 2018) či Bad Rabbit (VKR 2017; Kasík 2017b). NÚKIB (2018a, 10-12) nicméně uvádí, že žádné hlášení incidentů týkající se těchto kampaní od povinných subjektů dle ZKB neobdržel.

Rok 2018 zaznamenal ústup ransomwarových útoků jak ve světě, tak v ČR (NÚKIB 2019a, 2). Tento trend byl způsoben zejména navýšením vysoce sofistikovaných cílených útoků na úkor masových kapaní (Freed 2021; Sangani 2018). ČR v tomto roce nicméně zaznamenala útok na Léčebnu tuberkulózy a respiračních nemocí v Janově (NÚKIB 2019a,

36; Sedlák 2018), který předznamenal budoucí trend ransomwarových útoků na zdravotnická zařízení.

V roce 2019 se do ČR významněji promítly přetrvávající tendence světového vývoje ransomware – tedy že útoky jsou sofistikovanější a míří na velké organizace, případně do zdravotnictví (NÚKIB 2020b, 2). Dle průzkumu u subjektů povinných dle ZKB se s ransomwarovým útokem či pokusem o něj setkalo v tomto roce 32 % respondentů (NÚKIB 2020b, 11). Nejvýznamněji pak zasáhl ČR pravděpodobně ransomware Ryuk, který na téměř měsíc vyřadil z plného provozu Nemocnici Rudolfa a Stefanie Benešov (NÚKIB 2020b, 18; Magdoňová 2020), nebo na čtyři dny zastavil těžbu společnosti OKD (NÚKIB 2020b, 11; Mazal 2020).

Covidový rok 2020 se v ČR opět nesl ve znamení ransomwarových útoků na zdravotnická zařízení. NÚKIB (2021b, 14) za jím nejvýznamnější řešený incident označil útok na Fakultní nemocnici u sv. Anny v Brně. Za útokem stál ransomware Defray, přičemž zotavení z něj trvalo nemocnici měsíc (Avast Threat Labs 2021; ČT24 2020). Ransomware pak postihl také Psychiatrickou nemocnici Kosmonosy (NÚKIB 2021b, 14; Avast Threat Labs 2021), Povodí Vltavy (NÚKIB 2021b, 16; Haller 2020) či radnici městské části Prahy 3 (NÚKIB 2021b, 16; Sedlák 2020). NÚKIB (2021b, 14) dále uvádí, že více než třetinu všech řešených incidentů v roce 2020 způsobil škodlivý kód, přičemž ransomware stál za téměř polovinou z nich.

V roce 2021 jsou pak v ČR viditelné případy ransomware jako služby, zejména ve vazbě na skupinu REvil (NÚKIB 2021c, 2) či LockBit (NÚKIB 2021d, 4). Objevily se ale také útoky Avos Locker, Makop, Loki Locker, BlackCat, Hive či Phobos (NÚKIB 2021e, 4; NÚKIB 2021f, 4). Vyzdvihnout pak lze např. útok ransomware Avaddon na Magistrát města Olomouce, který trval několik týdnu. Vzhledem k odmítnutí zaplacení

výkupného přistoupili útočníci také k taktice dvojitého vydírání a začali zveřejňovat ukradená data z počítačů úředníků na Dark Webu (Magdoňová 2021; Hejtman 2022). Ransomware Avaddon v období od dubna do června 2021 napadl také řadu dalších organizací a státních institucí (Fišer 2022; ČT24 2021). Dle studie společnosti Sophos zasáhl v roce 2021 v ČR ransomware na 77 % dotazovaných organizací a zaplacené výkupné se pohybovalo mezi 100 až 500 tisíci USD (Bičíková 2022; ČTK 2022a).

V roce 2022 zatím tvoří ransomware přibližně pětinu incidentů řešených NÚKIB (2022d, 4). Z loňského roku do současnosti přetrvává trend ransomware jako služby (NÚKIB 2022d, 4), objevují se ale také vysoce sofistikované útoky velkých organizovaných skupin (NÚKIB 2022c, 4). Útoky i nadále míří jak na státní, tak na soukromé organizace (NÚKIB 2022a, 4; NÚKIB 2022b, 4; NÚKIB 2022c, 4; NÚKIB 2022d, 4). V ČR se v tomto roce prozatím objevil např. Jigsaw a NightSky (NÚKIB 2022a, 4), LockBit (NÚKIB 2022c, 4) či Phobos a LokiLocker (NÚKIB 2022d, 4). Velice aktuálním je pak ransomwarový útok na ŘSD, který je v době psaní práce již několik dní v řešení. Útok je dle NÚKIB na profesionální úrovni, přičemž útočník je prý také znám, z taktických důvodů však není zveřejněn (ČTK 2022b). Dle generálního ředitele ŘSD útok způsobil organizaci zásadní škody a bude se z něj zotavovat ještě několik měsíců. Dle jeho slov se naštěstí podařilo odizolovat mýtný systém či systém řízení dopravy v tunelech (ČTK 2022c), jehož vyřazení by mohlo mít katastrofické důsledky.

Ransomware tedy patří mezi nejzávažnější původce kyberbezpečnostních incidentů v ČR (NÚKIB 2021b, 9). Útoky míří jak na pro ekonomiku země významné podniky či pro fungování státu zásadní instituce, tak na zdravotnická zařízení, čímž ohrožují nejen citlivá data a chod těchto organizací, ale také lidské životy. I přesto na národní úrovni ČR

absentuje jasné vymezení policy směřující k potírání této pro bezpečnost země zásadní hrozby.

Na mezinárodní úrovni však ČR své odhodlání bojovat proti ransomware vyslovila jasně. Explicitní vyjádření odhodlání bojovat proti ransomware obsahuje např. Brussels Summit Communiqué vydané čelními představiteli zemí Severoatlantické aliance (dále NATO) v červnu roku 2021 (NATO 2021a). Dále se ČR podílela na přípravě Cyber Diplomacy Toolboxu EU, kterého bylo poprvé využito mimo jiné právě vůči ransomwarovým útočníkům (Lenzu 2020). K jasnému vyslovení cílů ČR v oblasti potírání ransomware však došlo zejména na setkání Counter Ransomware Initiative (Neuberger 2021), které bude představeno v následující podkapitole.

4.1.3 Counter Ransomware Initiative

Ve dnech 13. a 14. října 2021 se ČR zúčastnila mezinárodního virtuálního setkání Counter Ransomware Initiative zorganizovaného Národní bezpečnostní radou Bílého domu. Cílem tohoto setkání bylo akcelerovat kooperaci směrem k potírání ransomware (Neuberger 2021). Meetingu se kromě ČR a USA zúčastnili také zástupci Austrálie, Brazílie, Bulharska, Dominikánské republiky, Estonska, Francie, Indie, Irska, Itálie, Izraele, Japonska, Jihoafrické republiky, Jižní Koreje, Kanady, Keni, Litvy, Mexika, Německa, Nigérie, Nizozemska, Nového Zélandu, Polska, Rumunska, Singapuru, Spojeného království, Spojených arabských emirátů, Švédska, Švýcarska, Ukrajiny a EU (The White House 2021).

Setkání bylo završeno vydáním Joint Statement (The White House 2021). V tomto společném prohlášení účastníci setkání rozpoznávají ransomware jako eskalující globální bezpečnostní hrozbu se závažnými ekonomickými a bezpečnostními důsledky, která si žádá společnou

odpověď. Účastníci si dle prohlášení uvědomují potřebu rychlé akce založené na společných prioritách a vzájemně se doplňujících snahách směrem k potírání ransomware ve čtyřech rovinách – **resilience, nezákonného financování, vymáhání práva** a **diplomacie**.

Kategorie **resilience**, tedy odolnosti, zdůrazňuje potřebu efektivního zarámování policy a konzistentně prosazovaného zákonného a regulatorního režimu. Dále zmiňuje potřebu jasné vládní struktury, adekvátních zdrojů a pracovní síly, dobře nacvičených postupů, spolupráce se soukromým sektorem, sdílení informací mezi oběťmi ransomware, orgány vymáhajícími právo a kyberbezpečnostními autoritami a také osvěty zaměřené na základy kyberhygieny. Dále se účastníci shodli na potřebě budování technické odolnosti skrze zavádění základních technických opatření, tedy skrze udržování offline datových záloh, používání silných hesel a vícefaktorové autentizace, a také skrze pravidelné aktualizování a záplatování software (The White House 2021).

Vzhledem k tomu, že útočníci jsou motivováni primárně finančním ziskem a k zužitkování plateb výkupného často využívají sítí praní špinavých peněz, je dle Joint Statement (The White House 2021) třeba zabývat se taktéž **nezákonným financováním** ransomware. Za vhodné aktivity jsou v tomto směru identifikovány náležitá péče zákazníků, reportování podezřelé aktivity a monitoring transakcí. Důraz je pak účastníky setkání kladen primárně na virtuální aktiva a poskytovatele služeb spojených s virtuálními aktivy s ohledem na potřebu jejich zahrnutí do národních rámců boje proti praní špinavých peněz. Účastníci setkání se v prohlášení také zavazují, že navýší kapacity národních autorit za účelem regulace, dohledu, vyšetřování a potírání zneužívání virtuálních aktiv. Zmíněna je pak také potřeba spolupráce s poskytovateli služeb spojených

s virtuálními aktivy v oblasti sdílení informací spojených s ransomware (The White House 2021).

V oblasti **vymáhání práva** se účastníci setkání shodují, že je třeba stíhat ransomwarové útočníky, byť rozpoznávají, jak je tato činnost vzhledem k transnacionální povaze ransomware komplikovaná. K tomu, aby byla úspěšná, je třeba spolupráce mezi orgány vymáhajícími právo, kyberbezpečnostními autoritami a finančními zpravodajskými jednotkami na národní i mezinárodní úrovni. V prohlášení státy dále zdůrazňují, že musí přijmout vhodné kroky k boji proti kyberkriminalitě vycházející z jejich území (The White House 2021).

Poslední oblastí, které se zástupci států v prohlášení věnují je **diplomacie**. Uvádějí, že skrze diplomacii je možno prosazovat chování založené na pravidlech a pomáhat státům k adekvátnímu adresování ransomware na jejich území. Státy se pak také zavazují, že budou koordinovaně využívat diplomatických nástrojů k redukci existujících ransomwarových útočišť (The White House 2021).

4.2 Policy potírání ransomware v ČR

Na základě výše představeného rámce Joint Statement (The White House 2021), který zdůrazňuje potřebu efektivního zarámování policy a konzistentně prosazovaného zákonného a regulatorního režimu, bude v této části kapitoly pozornost věnována koncepčnímu a legislativnímu ukotvení v něm vyřčených závazků v ČR, přičemž bude představena současně také rovina jejich praktické aplikace.

4.2.1 Resilience

V této části práce bude představeno koncepční, legislativní a praktické ukotvení jasné vládní struktury, adekvátních zdrojů, personálního zajištění, cvičení, spolupráce se soukromým sektorem, sdílení informací, osvěty a technických opatření. Tedy bodů, které identifikovali zástupci států v Joint Statement (The White House 2021) za zásadní faktory potírání ransomware v kategorii resilience.

A) Jasná vládní struktura

a. Koncepční ukotvení

Problematika vládní struktury boje proti ransomware není v ČR nikterak jasně vymezena. Avšak vzhledem k tomu, že ransomware představuje hrozbu národní kyberbezpečnosti, je za tuto vládní strukturu obecně možno považovat systém zajišťování kyberbezpečnosti v ČR. Ten přehledně a detailně rozvádí Národní strategie KB (NÚKIB 2020a, 7-8):

- **Vláda ČR,** jakožto vrcholný orgán moci výkonné, je *odpovědná „za zajišťování národní bezpečnosti, a za řízení a funkčnost celého bezpečnostního systému ČR.“*
- **NÚKIB** je *„gestorem kybernetické bezpečnosti a ústředním správním orgánem pro oblast kybernetické bezpečnosti“* a jeho ústřední činnost představuje *„zajišťování kybernetické bezpečnosti ve smyslu ochrany kritické informační infrastruktury a dalších důležitých informačních a komunikačních systémů a sítí,“* přičemž za tímto účelem byl zřízen **vládní CERT** (Gov.CERT). Mimo to se NÚKIB věnuje koordinaci výzkumu a vývoje, ale také vzdělávání a osvětě v oblasti kyberbezpečnosti.
- **Národní CERT** je pod názvem CSIRT.CZ provozován sdružením CZ.NIC a úzce spolupracuje s vládním CERT.

- **MZV ČR** společně s NÚKIB a dalšími orgány státní správy koordinuje *„zahraniční politiku, vztahy ČR s ostatními státy a mezinárodními organizacemi.“*
- **Zpravodajské služby** *„zabezpečují, zpracovávají a analyzují informace důležité pro kybernetickou, potažmo národní bezpečnost“* a patří mezi ně **Bezpečnostní informační služba** (dále BIS), **Vojenské zpravodajství** (dále VZ) a **Úřad pro zahraniční styky a informace** (dále ÚZSI).
- **PČR,** konkrétně pak **NCOZ** je národním kontaktním bodem pro kyberkriminalitu. Problematika prevence a potírání kyberkriminality náleží primárně orgánům činným v trestním řízení (dále OČTŘ).
- **VZ**, konkrétně pak **Národní centrum kybernetických operací** (dále NCKO)**,** je zodpovědné za budování systému kybernetické obrany.
- **Armáda ČR,** jmenovitě **Velitelství kybernetických sil a informačních operací,** se podílí na kybernetické obraně.

Mimo výše zmíněných institucí disponujících specifickým bezpečnostním mandátem a agendou jsou dle dokumentu (NÚKIB 2020a, 8-9) součástí systému zajišťování kyberbezpečnosti v ČR jmenovitě také:

- **Ministerstvo průmyslu a obchodu**, konkrétně pak **Český telekomunikační úřad**, který se věnuje problematice digitální ekonomiky a rozvoje telekomunikačního trhu.
- **MV ČR** zejména s ohledem na budování bezpečného eGovernmentu.
- **Ministerstvo školství, mládeže a tělovýchovy** (dále MŠMT ČR) vzhledem k jeho podílu na zajišťování vzdělanosti nové generace občanů v oblasti kyberbezpečnosti.

Dále dokument (NÚKIB 2020a, 9) uvádí, že významnou roli zastávají zástupci z řad povinných subjektů dle ZKB, neboť významně ovlivňují úroveň kyberbezpečnosti v ČR a efektivitu systému. Případně pak také *„další subjekty například z řad soukromého sektoru, akademie, asociací, sdružení a CSIRT týmů mimo veřejnou správu,"* s nimiž je pro zajištění fungování systémů klíčové spolupracovat, byť nejsou postiženy ZKB.

Vzhledem k tomu, že ransomwaroví útočníci v současnosti nejčastěji operují v rámci organizovaných kyberzločineckých skupin, je nutné zohlednit také strukturu boje proti OZ v ČR. Ta je představena Koncepcí boje proti OZ (MV ČR 2018, 4) v následujícím, znění:

- **MV ČR** je ústředním orgánem boje proti OZ v ČR, na jehož aktivním potírání se podílejí zejména **OČTŘ.**
- Na boji proti OZ se pak podílejí i další ministerstva, jejich podřízené složky a další státní orgány:
    - **Ministerstvo financí** (dále MF ČR)
    - **Ministerstvo spravedlnosti**
    - **Úřad vlády**
    - **Ministerstvo životního prostředí**
- Významnou roli v boji proti OZ zastává **PČR** (zejména NCOZ SKPV).
- **Zpravodajské služby** participují v rámci své působnosti.

V oblasti ransomware je vhodné zdůraznit zejména roli **FAÚ,** který v ČR plní funkci finanční zpravodajské jednotky a mimo jiné je *„hlavním gestorem opatření zaměřených na prevenci a boj proti praní peněz"* (FAÚ n.d.).

b. Legislativní ukotvení

Podobně jasné a přehledné vymezení systému zajišťování kyberbezpečnosti však na rozdíl od jeho koncepčního vymezení absentuje v legislativě. Legitimita vládní struktury zajišťování kyberbezpečnosti je značně limitována roztříštěností jednotlivých předpisů stanovujících role zmíněných institucí ve vztahu k zajišťování kyberbezpečnosti, případně pak směrem k potírání ransomware. Konkrétně ZKB má dle § 1 odst. (1) upravovat *„působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti,"* věnuje se nicméně pouze roli NÚKIB, národního a vládního CERT.

Systém boje proti OZ je upraven mimo jiné Kompetenčním zákonem, který § 12 odst. (1) písm. a) stanovuje MV ČR ústředním orgánem pro věci vnitřního pořádku a bezpečnosti, dále pak Zákonem o PČR, který upravuje postavení a činnosti PČR, či Zákonem ML/FT, který mimo jiné upravuje postavení a činnost FAÚ. Důležité je nicméně zohlednit také ustanovení Trestního řádu či Trestního zákoníku. Role dalších institucí, které jsou součástí systému zajišťování kybernetické bezpečnosti jsou upraveny vlastními právními předpisy[5].

c. Praktická aplikace

Z Joint Statement (The White House 2021) vyplývá, že za nejpodstatnější aktéry potírání ransomware je možno považovat zejména orgány vymáhající právo, národní kyberbezpečnostní autority a finanční zpravodajské jednotky – v případě ČR tedy PČR, NÚKIB a FAÚ.

Role PČR v boji proti ransomware dle Experta č. 1 (Anonymní zdroj č. 1 2022) vyplývá z ustanovení § 1 a § 2 Trestního řádu. V případě

[5] Např. Vláda mimo jiné Ústavou ČR; MŠMT ČR, MZV ČR, MF ČR, MV ČR a další Kompetenčním zákonem; BIS, ÚZSI a VZ Zákonem o zpravodajských službách.

podezření z trestné činnosti, tedy v případě *„kdy aplikace škodlivého kódu, který způsobí zašifrování systému a pachatel tohoto jednání požaduje za odšifrování tzv. výkupné … jsou OČTŘ povinny věc prověřit, případně konat i v procesu vyšetřování a následně podat návrh na podání obžaloby dozorovému státnímu zástupci“* (Anonymní zdroj č. 1 2022). Mimo to Expert č. 1 uvádí, že se PČR podílí také na osvětové činnosti v oblasti potírání ransomware, spolupracuje s dalšími národními institucemi (jmenovitě NÚKIB a FAÚ) a účastní se mezinárodních programů zaměřených na prevenci a vzdělávání v dané problematice (Anonymní zdroj č. 1 2022).

Role NÚKIB v boji proti ransomware není nikde jasně vymezena, podílí se na něm však v rámci své role v zajišťování kyberbezpečnosti státu. Vede tedy vládní CERT (NÚKIB n.d.) a dle Experta č. 3 (Sikora 2022) poskytuje subjektům dle ZKB součinnost při řešení incidentů. Konkrétně u ransomware např. zjišťuje typ ransomware, pomáhá při zajišťování dat pro následnou analýzu a v případě závažného incidentu vysílá rapid response tým složený z analytiků a odborníků dle domluvy. Dále NÚKIB spolupracuje s dalšími CERT a CSIRT týmy na národní i mezinárodní úrovni, připravuje bezpečnostní standardy v oblasti kyberbezpečnosti, připravuje a koordinuje kyberbezpečnostní cvičení, vytváří a na mezinárodním poli hájí pozici ČR v oblasti kyberbezpečnosti, připravuje kyberbezpečnostní legislativu a vytyčuje národní strategie v této oblasti (NÚKIB n.d.a). NÚKIB dále také získává a předává svou činností získané informace významné pro činnost OČTŘ (Sikora 2022). Významnou aktivitou NÚKIB je také osvětová činnost, která je zaměřena primárně na základy kyberhygieny (Anonymní zdroj č. 2 2022).

Role FAÚ v potírání ransomware je dle Experta č. 2 (Plecitý 2022) zprostředkovaná – působí tedy v boji proti ransomware odvozenou

formou, ale na hlavním meritu věci se nepodílí. FAÚ se dle Experta č. 2 (Plecitý 2022) *„zabývá tématem legalizace výnosů z trestné činnosti a financování terorismu a s tím souvisejícími zdrojovými trestnými činy.“* Vyhledávací činnost FAÚ je přenesena na Zákonem ML/FT povinné osoby, např. i osoby poskytující služby spojené s virtuálními aktivy, které reportují FAÚ podezřelé obchody. Takto získané informace FAÚ dále analyzuje, přičemž výstupem může být buďto podání trestního oznámení, nebo poskytnutí informace významné pro činnost např. PČR. Mimo to pak FAÚ v rámci součinnosti spolupracuje se svými adresáty, typicky OČTŘ, nebo se zahraničními finančními zpravodajskými jednotkami na poli sdílení informací. Role FAÚ při potírání ransomware tedy spočívá primárně v tom, že získává informace o tocích virtuálních aktiv, které by mohly nějakým způsobem souviset s legalizací výnosů z ransomware (Plecitý 2022).

B) Adekvátní zdroje

a. Koncepční ukotvení

Národní strategie KB (NÚKIB 2020a, 12) zmiňuje, že *„k dosažení vysoké úrovně kybernetické bezpečnosti jsou vyžadovány tomu odpovídající náklady.“* Také Koncepce boje proti OZ (MV ČR 2018, 21) zmiňuje potřebu adekvátních finančních prostředků, a to zejména ve vztahu k pokrytí nových forem trestné činnosti, zejména kyberkriminality. To je dále podtrženo Bezpečnostní strategií (MZV ČR 2015a, 17), která uvádí, že se ČR zaměřuje na zajištění dostupnosti materiálních a finančních zdrojů pro boj proti OZ.

b. Legislativní ukotvení

Jak vyplývá z výše představené vládní struktury, na zajišťování kyberbezpečnosti ČR se podílí celá řada subjektů. Finanční prostředky

k zajištění jejich úkolů v této oblasti však nejsou v ČR samostatnou kapitolou státního rozpočtu, nýbrž součástí rozpočtů jednotlivých subjektů, které s nimi nakládají dle vlastního uvážení. Problematika rozpočtového zajištění těchto subjektů je upravena příslušnými zákony aniž by dále reflektovala výdaje na zajišťování kyberbezpečnosti.

c. Praktická aplikace

V ČR je tedy velice náročné monitorovat a koordinovat zdroje vynakládané na zajišťování kyberbezpečnosti státu, zdroje určené konkrétně na boj proti ransomware nevyjímaje. NÚKIB se dle Nejvyššího kontrolního úřadu (dále NKÚ) snaží získávat informace ohledně zdrojů vynakládaných na kyberbezpečnost skrze dotazníková šetření (NKÚ 2020a). To sice do určité míry umožňuje jejich monitoring, avšak jakákoli strategická koordinace jejich využívání je tímto značně ztížena. To je problematické zejména s ohledem na to, že NÚKIB (2021b, 3; 2020b, 2; 2019a, 27) již několik let upozorňuje na nedostatečné rozpočty sektoru státní správy v oblasti kyberbezpečnosti. Mimo to bylo v roce 2020 dle dat zveřejněných NÚKIB u 43 % jím sledovaných subjektů možno pozorovat dokonce meziroční propad ve výdajích určených na kyberbezpečnost (NÚKIB 2021b, 10).

Co se adekvátnosti finančního zajištění PČR pro boj proti ransomware týče, Expert č. 1 (Anonymní zdroj č. 1 2022) uvádí, že *„v oblasti financování boje proti kybernetické trestné činnosti jsou z minulosti značné rezervy.“* K tomu ale dodává, že *„v současné době je plánovaná sanace potřeb policejních jednotek, které řeší trestnou činnost v oblasti kybernetické kriminality.“* V plánu je tedy nákup zejména speciálních softwarových nástrojů. Expert č. 1 (Anonymní zdroj č. 1 2022) dále uvádí, že jsou požadavky PČR na zajištění speciálních nástrojů pro vyšetřování kyberkriminality postupně zajišťovány, o čemž svědčí např. fakt, že PČR

disponuje softwarovým nástrojem na trasování virtuálních měn. Neadekvátnost finančního zajištění je však možné pozorovat zejména v oblasti platového ohodnocování příslušníků PČR (Anonymní zdroj č. 1 2022), kterému bude pozornost věnována v následující kapitole.

Expert č. 2 (Plecitý 2022) uvádí, že si netroufá hodnotit adekvátnost finančního zajištění činnosti FAÚ, poukazuje nicméně na přetrvávající problém s obsazováním pracovních pozic kvalifikovanými odborníky. Dále také hovoří o tom, že je činnost FAÚ spojena s řadou hrozeb včetně korupčního rizika, neboť analytici FAÚ přichází při své pracovní činnosti do styku s milionovými či miliardovými hodnotami často pocházejícími z prostředí OZ. Proto je třeba finančně zajistit eliminaci hrozeb pramenících z tohoto faktoru a přizpůsobovat mu finanční ohodnocení odborníků z řad FAÚ. Z uvedeného lze tedy vyvodit, že byť současné rozpočtové zajištění FAÚ nepředstavuje významnou překážku jeho činnosti v oblasti boje proti ransomware, vyčlenění většího množství prostředků by těmto činnostem pomohlo zejména směrem k zajištění adekvátních platových podmínek pro zaměstnance, což je nicméně ohniskem zájmu následující kapitoly.

C) Personální zajištění

a. Koncepční ukotvení

Potřeba vysoké odbornosti pracovníků institucí veřejné správy pro zajišťování odpovídající úrovně prevence a potlačování hrozeb je zmíněna už Bezpečnostní strategií (MZV ČR 2015a, 19). Důležitost adekvátně vycvičené a připravené pracovní síly je pak obecně s ohledem na kyberbezpečnost reflektována v jednom ze strategických cílů Národní strategie KB (NÚKIB 2020a, 21). Cílem rozšiřování expertní základny je aktivní vytváření a udržování kvalifikované pracovní síly skrze působení na dvou

úrovních. V rámci první úrovně je důraz kladen na identifikaci talentů a motivaci lidí ke studiu a práci v oblasti kyberbezpečnosti skrze investice do moderních osvětových a vzdělávacích programů a také skrze adekvátní vynakládání prostředků na nábor a vytváření vhodných pracovních podmínek tak, aby byla státní správa konkurenceschopná na trhu práce v této oblasti. Další úrovní personálního zajišťování kyberbezpečnosti je snaha o udržení si a další vzdělávání současných pracovníků (NÚKIB 2020a, 21).

Do budoucna ČR pak dle Národní strategie KB (NÚKIB 2020a, 20) plánuje institucionalizovat možnost podílet se na zajišťování kybernetické bezpečnosti státu také expertům vně státní správy, tedy ze soukromého, neziskového či akademického sektoru. Vytvoření sítě dobrovolníku na tomto základu bude hodnotné zejména *„pro případy vážného ohrožení ČR, které by si vyžádalo větší množství lidských zdrojů, než je státu standardně k dispozici“* (NÚKIB 2020a, 20). Potřeba vytvoření a udržování expertní základy v oblasti potírání či dopadu kyberkriminality je zejména s ohledem na vzdělávání specialistů a expertů z řad bezpečnostních složek zmíněna i Strategií prevence kriminality (MV ČR 2018, 32).

Tyto cíle jsou dále rozvedeny v Akčním plánu (NÚKIB 2021a, 18) do specifických bodů, které se zaměřují především na vzdělávání a osvětu stávajících zaměstnanců veřejné správy, ozbrojených sil, bezpečnostních sborů či soudců a státních zástupců. Dále pak na pokračování posilování systému kybernetické obrany prostřednictvím budování NCKO mimo jiné skrze jeho personální zabezpečení a o posilování personálních kapacit potřebných pro tvorbu, přípravu a realizaci kyberbezpečnostních cvičení (NÚKIB 2021a, 6).

Akční plán (NÚKIB 2021a) nicméně absentuje zmínění konkrétních kroků k zajištění konkurenceschopnosti státní správy či bezpečnostních sborů na trhu práce, které by vedly k žádoucímu budování expertní základny státu v oblasti kyberbezpečnosti či přímo potírání ransomware. Akční plán (NÚKIB 2021a, 6) dále konkrétně zmiňuje cíl vytvoření a institucionalizace platformy zapojující dobrovolníky z řad expertů do zajišťování kyberbezpečnosti státu.

b. Legislativní ukotvení

Cíle rozvíjení expertní základny zajišťování kyberbezpečnosti a tedy i boje proti ransomware nejsou v ČR nikterak legislativně reflektovány. Co se týče zajištění konkurenceschopnosti na pracovním trhu směrem k platovým podmínkám, v ČR je toto s ohledem na tabulkové platy pracovníků ve státní správě či ve služebním poměru, které se povětšinou ani vzdáleně nepřibližují soukromému sektoru, možno pouze omezeně skrze osobní ohodnocení. Personální a platové poměry jsou jasně specifikovány a vymezeny samostatnými legislativními předpisy.[6] Legislativní ukotvení zmíněné platformy pro dobrovolníky prozatím absentuje.

c. Praktická aplikace

NÚKIB (2021b, 3; 2020b, 2; 2019a, 27) pravidelně hovoří o nedostatku specialistů na kyberbezpečnost ve státní správě, přičemž ani jeho personální zajištění není v současnosti adekvátní (NÚKIB 2021g, 15). Dle Experta č. 5 (Anonymní zdroj č. 3 2022) však NÚKIB o zajištění adekvátní expertní základny usiluje hned v několika rovinách. Jedná se o změnu

[6] Zákon o státní službě; Zákon o služebním poměru příslušníků bezpečnostních sborů; Nařízení vlády o platových poměrech zaměstnanců ve veřejných službách a správě; Nařízení o platových poměrech státních zaměstnanců; Nařízení vlády, kterým se stanoví stupnice základních tarifů pro příslušníky bezpečnostních sborů; Nařízení vlády o služebních tarifech a o zvláštním příplatku pro vojáky z povolání.

patřičné legislativy a tvorbu a připomínkování národních strategických dokumentů, které se touto oblastí zaobírají. Dále o podílení se na změnách vzdělávacích programů středních a vyšších odborných škol či spolupráci s vysokými školami. Mimo to jde také o osvětovou činnost na různých úrovních – např. jen v roce 2020 se NÚKIB podařilo proškolit více než 18 tisíc pracovníků státní správy (NÚKIB 2021b, 3).

Expert č. 5 (Anonymní zdroj č. 3 2022) dále uvádí, že roli v budování expertní základny veřejné správy zastávají také MV ČR, Ministerstvo práce a sociálních věcí ČR a MŠMT ČR. Problémem budování adekvátní expertní základny je pak dle Experta č. 5 (Anonymní zdroj č. 3 2022) zejména nejednotné vedení, roztříštěnost pravomocí a absence flexibility jednotlivých ministerstev a dalších ústředních orgánů státní správy, případně také omezená profesní orientace studijních oborů nabízených vysokými školami. O konkurenceschopnost státní správy na trhu práce dle Experta č. 5 (Anonymní zdroj č. 3 2022) usilováno v praxi není. To bude značně ztěžovat mimo jiné cíle NÚKIB (2021g, 41) do roku 2027 téměř zdvojnásobit současnou personální základnu.

Směrem k adekvátní personální základně PČR je možné pozorovat obecný nedostatek policistů, kterých momentálně chybí více než pět tisíc (ČT24 2022; Lánský 2022). Expert č. 1 (Anonymní zdroj č. 1 2022) uvádí, že personální politika této instituce je jasně legislativně definována. Mimo to ale poznamenává, že o konkurenceschopnosti PČR na trhu práce v oblasti kyberbezpečnosti nelze vůbec hovořit – PČR apeluje na vlastenecké cítění, nicméně *„v rovině finančního odměňování je PČR absolutně nekonkurenceschopná."* Problematické je to zejména i s ohledem na fakt, že se PČR již dlouhodobě nedaří obsadit pozici IT specialisty v rámci celorepublikových útvarů, neboť existuje nerovnováha mezi požadavky na odbornost a nabízenými platovými podmínkami (Anonymní zdroj č. 1

2022). Dle Experta č. 2 (Plecitý 2022) se orgány vymáhající právo dlouhodobě potýkají s personálním deficitem v oblasti kyberkriminality, kdy se dodnes nepodařilo realizovat plánované vytvoření samostatných útvarů, což by se nicméně mohlo uskutečnit ještě v tomto roce.

Expert č. 2 (Plecitý 2022) dále uvádí, že ani personální základna FAÚ není adekvátní. Co se však týče specialistů zaměřujících se na problematiku virtuálních aktiv, personální deficit nevnímá jako závažný. I s ohledem na zvyšující se objem případů by nicméně další experty v této oblasti FAÚ zužitkoval. Dále však Expert č. 2 (Plecitý 2022) poukazuje na značný problém s obsazováním specializovaných pozic na FAÚ, kdy je problematické už pouze najít na pracovním trhu uchazeče s dostačující odborností, přičemž ani současné možnosti jejich platového ohodnocení nejsou zcela ideální.

D) Cvičení

a. Koncepční ukotvení

Význam cvičení pro zajišťování bezpečnosti ČR zmiňuje už Bezpečnostní strategie (MZV ČR 2015a, 23). Národní strategie KB (NÚKIB 2020a, 10-11) následně zmiňuje důležitost cvičení hned ve dvou souvislostech. V první řadě se jedná o civilně-vojenskou spolupráci v zabezpečování kyberprostoru. Ta musí být zajištěna skrze jasně dané a vzájemně se doplňující kompetence jednotlivých složek systému zajišťování kyberbezpečnosti, jejichž kooperace pak má být prověřována mimo jiné také speciálními tréninky a cvičeními (NÚKIB 2020a, 10-11). Dále Národní strategie KB (NÚKIB 2020a, 17) uvádí, že cvičení budou využívána jako nástroj nejen k navyšování kyberbezpečnosti, ale také k prohlubování vztahů s partnery.

To, že si ČR uvědomuje význam cvičení jakožto prostředku k budování odolnosti vůči kybernetickým hrozbám, mezi které patří i ransomware, je však viditelné především z Akčního plánu (NÚKIB 2021a). Dle něj ČR plánuje navyšovat kyberbezpečnost skrze realizaci technických, netechnických i kombinovaných cvičení nejen pro orgány a osoby povinné dle ZKB (NÚKIB 2021a, 5). Dále bude začleňovat prvky kyberbezpečnosti do cvičení primárně zaměřených na jiné oblasti (NÚKIB 2021a, 18) či vytvářet a aktivně se podílet na komunikačních a procedurálních cvičeních zaměřených na efektivní spolupráci mezi aktéry v oblasti kyberbezpečnosti, kriminality a obrany (NÚKIB 2021a, 6).

Dále chce dle Akčního plánu ČR zapojovat národní partnery do mezinárodních cvičení s cílem posilovat spolupráci, nastavovat a koordinovat postupy (NÚKIB 2021a, 6), vytvářet a organizovat cvičení v oblasti kyberbezpečnosti pro zahraniční partnery a také aktivně participovat na organizaci, přípravě a provádění mezinárodních cvičení za účelem posilování sítě významných partnerů (NÚKIB 2021a, 13-14).

b. Legislativní ukotvení

Zatímco koncepčně je problematika kyberbezpečnostních cvičení zachycena velice obsáhle, v legislativě ČR její ukotvení absentuje.

c. Praktická aplikace

I přes absenci legislativně ukotvené povinnosti organizovat kyberbezpečnostní cvičení je v tomto směru NÚKIB poměrně aktivní. Za poslední čtyři roky uspořádal 40 cvičení a pravidelně se účastnil a podílel na organizaci mezinárodních cvičení (NÚKIB 2021b, 29; NÚKIB 2020b, 22-24; NÚKIB 2019a, 42-45; Anonymní zdroj č. 4 2022). NÚKIB pravidelně organizuje národní cvičení CyberCzech a experti z NÚKIB se dále účastní či podílí na organizaci mezinárodních cvičení Crossed Swords, Cyber Coalition a Locked Shields (NÚKIB n.d.b).

Konkrétně na hrozbu ransomware se pak dle Experta č. 7 (Anonymní zdroj č. 4 2022) zaměřují na národní úrovni především cvičení netechnická, tedy tzv. table-top cvičení. Jako příklad uvádí cvičení pro sektor zdravotnictví Health Czech (NÚKIB 2021h), cvičení pro strategické firmy obranného průmyslu (NÚKIB 2021i) či cvičení pro ČEPS[7] (NÚKIB 2021j). Přímo ransomware byl pak také jedním z témat mezinárodního cvičení Cyber Coalition, které proběhlo v roce 2021 (NATO 2021b).

E) Spolupráce se soukromým sektorem

a. Koncepční ukotvení

Národní strategie KB (NÚKIB 2020a) jasně zmiňuje, že kvalitní spolupráce se subjekty ze soukromého sektoru je pro fungování systému zajišťování kyberbezpečnosti klíčová (NÚKIB 2020a, 9), což zdůrazňuje i v jednom z uvedených strategických cílů (NÚKIB 2020a, 21). Spolupráce státu, soukromé sféry a občanů je reflektována jak v oblasti vzdělávací a osvětové (NÚKIB 2020a, 19), tak v již zmíněném plánovaném zapojení expertů ze soukromé sféry do řešení závažných kyberbezpečnostních incidentů formou institucionalizované dobrovolnické platformy (NÚKIB 2020a, 20).

Mimo to Národní strategie KB (NÚKIB 2020a, 15) uvádí, že propojení státní, soukromé a akademické sféry je předpokladem pro úspěšné prosazování národních zájmů ČR v oblasti kyberbezpečnosti v mezinárodním prostředí. Důraz je nicméně kladen zejména na budování vzájemné důvěry a spolupráce za účelem zvyšování odolnosti subjektů povinných dle ZKB, které jsou „*stěžejním pilířem kybernetické, potažmo národní bezpečnosti*“ (NÚKIB 2020a, 11).

[7] ČEPS působí na území ČR jako výhradní provozovatel přenosové soustavy elektrických vedení (ČEPS n.d.).

Podobně jako v předchozích případech, i v oblasti spolupráce se soukromým sektorem rozvíjí zmíněné cíle Akční plán (NÚKIB 2021a). Dílčími závazky v této oblasti jsou rozšiřování a upevňování spolupráce se soukromým sektorem (NÚKIB 2021a, 4), zapojování soukromého sektoru při zajišťování kybernetické obrany či již zmíněné vytvoření dobrovolnické expertní platformy (NÚKIB 2021a, 6).

Co se týče spolupráce se subjekty povinnými dle ZKB, Akční plán (NÚKIB 2021a) uvádí, že ČR bude rozvíjet efektivní a koordinovanou spolupráci mezi NÚKIB, PČR a zpravodajskými službami, včetně spolupráce s orgány a osobami povinnými dle ZKB a to při řešení bezpečnostních incidentů (NÚKIB 2021a, 3), nebo že naváže a prohloubí spolupráci na rozvoji kyberbezpečnosti se zastřešujícími organizacemi poskytovatelů základních služeb (NÚKIB 2021a, 4). Dále bude ČR v rámci spolupráce za účelem budování odolnosti s povinnými subjekty dle ZKB vyhledávat zranitelnosti, provádět penetrační testování, vypracuje metodický dokument k řízení bezpečnosti dodavatelů a připraví návrh aktualizace standardů šifrování (NÚKIB 2021a, 5).

b. Legislativní ukotvení

Spolupráce se soukromým sektorem ve smyslu uvedených cílů není legislativně přímo ukotvena. ZKB v § 22 písm. g) nicméně uvádí, že NÚKIB *„spolupracuje s orgány a osobami, které působí v oblasti kybernetické bezpečnosti a kybernetické obrany,“* a dle písm. j) zajišťuje mimo jiné metodickou podporu v oblasti kyberbezpečnosti. Jistou formu institucionalizace spolupráce soukromého sektoru se státem je nicméně možné spatřit také v regulaci specifických subjektů ZKB a jej doplňujícími předpisy. Povinnými subjekty dle § 3 ZKB jsou:

- poskytovatelé služeb elektronických komunikací či subjekty zajišťující síť elektronických komunikací,
- orgán nebo osoba zajišťující významnou síť,
- správce a provozovatel informačního systému kritické informační infrastruktury,
- správce a provozovatel komunikačního systému kritické informační infrastruktury,
- správce a provozovatel významného informačního systému,
- správce a provozovatel informačního systému základní služby,
- provozovatel základní služby,
- poskytovatel digitální služby.

Tato spolupráce spočívá zejména v hlášení kontaktních údajů a kybernetických bezpečnostních incidentů národnímu či vládnímu CERT, a dále pak v implementaci, provádění a oznámení o provedení bezpečnostních, ochranných či reaktivních opatření dle povinností stanovených ZKB. ZKB dále ukládá, že národní a vládní CERT poskytují zákonem specifikovaným povinným subjektům metodickou podporu a pomoc, případně pak i součinnost při výskytu kyberbezpečnostních incidentů.

Spolupráce se soukromým sektorem v oblasti kyberbezpečnosti, konkrétně pak kyberkriminality, je dále upravena i Zákonem o PČR, který v § 14 mimo jiné uvádí, že *„Policie při plnění svých úkolů spolupracuje … s právnickými a fyzickými osobami“* a dle § 18 je policista *„oprávněn požadovat od orgánů a osob uvedených v § 14 věcnou a osobní pomoc … Tyto orgány a osoby jsou povinny požadovanou pomoc poskytnou“* mimo zákonem specifikované případy. Dle § 17 písm. a) téhož zákona pak PČR spolupracuje s právnickými a fyzickými osobami působícími mimo jiné v oblastech prevence kriminality, vzdělávacích aktivit, podpory a pomoci

obětem trestných činů nebo zmírňování následků trestných činů, zde tedy i ve smyslu kyberkriminality. Součinnost státních orgánů, fyzických a právnických osob s PČR je pak např. stanovena také ustanoveními § 7 až § 8d Trestního řádu.

Otázka spolupráce FAÚ se soukromým sektorem, zejména tedy s osobami poskytujícími služby spojené s virtuálními aktivy, je upravena zejména hlavou III Zákona ML/FT, případně pak také § 24 či § 30 téhož zákona. Spolupráce je legislativně ukotvena zejména v oblasti postupů při podezřelém obchodu, sdílení a získávání informací.

c. Praktická aplikace

Dle Experta č. 3 (Sikora 2022) funguje spolupráce NÚKIB se soukromým sektorem zejména v regulích ZKB. NÚKIB přijímá hlášení o incidentech, která dále vyhodnocuje a poskytuje povinným subjektům součinnost. Ta spočívá v zjištění konkrétního typu ransomware a pomoci při zajišťování dat pro následnou analýzu, případně ve vyslání rapid response týmu složeného z analytiků a odborníků. To ale jen v případě závažných incidentů. Metodická podpora je pak dle Experta č. 3 (Sikora 2022) zajištěna také skrze metodické materiály, přičemž alespoň některé z nich jsou veřejně dostupné (NÚKIB n.d.c).

K spolupráci se subjekty neregulovanými ZKB Expert č. 6 (Švéda 2022) uvádí, že se jedná např. o zodpovídání dotazů, případně bývá odborná veřejnost běžně přizvána také k vytváření legislativy[8] či některých podpůrných materiálů. Mimo to má pak NÚKIB s řadou neregulovaných subjektů ze soukromého sektoru uzavřena memoranda o spolupráci, jako např. s Českou bankovní asociací (NÚKIB 2022f). Expert č. 1 (Anonymní zdroj č. 1 2022) nicméně poukazuje na skutečnost, že by se brzy

[8] Mimo jiné vyzval NÚKIB (2022e) odbornou veřejnost k zasílání návrhů na změny Zákona o kybernetické bezpečnosti.

mělo rozšířit spektrum povinných subjektů s ohledem na očekávanou směrnici NIS II (Evropská komise 2020), z čehož by vyplývalo také navýšení objemu spolupráce NÚKIB se soukromým sektorem např. při řešení kyberbezpečnostních incidentů.

Za formu spolupráce pak lze považovat také služby, které NÚKIB nabízí zejména regulovaným subjektům. Jedná se např. o auditní činnost, penetrační testování a hledání zranitelností, analýzy síťového provozu a detekce závadných komunikací, trénink, cvičení či vzdělávání bezpečnostních a manažerských týmů (NÚKIB 2021g, 14).

Spolupráce se soukromým sektorem z pohledu PČR dle experta č. 1 (Anonymní zdroj č. 1 2022) probíhá např. formou přibrání znaleckého pracoviště v rámci znaleckého zkoumání či vypracování odborného vyjádření. S ohledem na zkoumanou problematiku se nicméně jako důležitější jeví zejména ad hoc spolupráce se společnostmi, které u obětí zajišťují specifické softwarové nástroje, nebo se specializují na kyberbezpečnost. PČR pak dle Experta č. 1 (Anonymní zdroj č. 1 2022) před zahájením úkonů trestního řízení také využívá ustanovení § 18 Zákona o PČR, ve zkoumané oblasti zejména směrem k zjištění napadení. Další spolupráce s takovým subjektem se řídí stanovami Trestního řádu.

Spolupráce FAÚ a osob poskytujících služby spojené s virtuálními aktivy je dle Experta č. 2 (Plecitý 2022) jasně stanovena Zákonem ML/FT, v rámci jehož regulí také probíhá. Spolupráce nad rámec zmíněného zákona probíhala zejména v období od roku 2017 do roku 2020, kdy FAÚ organizoval odborné diskuze pro zástupce FAÚ, Celní správy ČR, PČR, osob poskytujících služby spojené s virtuálními aktivy, právních kanceláří a bankovního sektoru. Tyto diskuze měly pomoci vysvětlit povinnosti vyplývající pro dané aktéry ze zákona, aby byla spolupráce v jeho regulích do budoucna méně problematická. S pandemií COVID-19 se tato

činnost zastavila, avšak dodnes probíhá např. metodické vedení ze strany FAÚ formou zodpovídání ad hoc dotazů.

F) Sdílení informací

a. Koncepční ukotvení

Dalším důležitým aspektem boje proti ransomware je dle Joint Statement (The White House 2021) sdílení relevantních informací mezi oběťmi ransomware, orgány vymáhajícími právo a kyberbezpečnostními autoritami. Národní strategie KB (NÚKIB 2020a) rozpoznává potřebu vylepšování modelu sdílení informací nejen napříč státními institucemi (NÚKIB 2020a, 10), ale i s ohledem na strategickou komunikaci státu směrem k národním partnerům či k široké veřejnosti (NÚKIB 2020a, 12). Jako jeden ze svých strategických cílů uvádí *„celonárodní přístup s důrazem na sdílení informací, koordinaci a spolupráci“* (NÚKIB 2020a, 21).

V Akčním plánu (NÚKIB 2021a) je pak tento strategický cíl dále rozvíjen. ČR si klade za cíl vytvořit a provozovat na národní úrovni zabezpečenou platformu pro komunikaci a sdílení informací o kybernetických hrozbách a zranitelnostech a vytvořit návrh umožňující jednotný postup pro hlášení kyberbezpečnostních incidentů (NÚKIB 2021a, 3). Dalšími cíli ČR jsou zpracování návrhu národní politiky koordinovaného zveřejňování zranitelností a vytvoření metodiky pro strategickou komunikaci pro případ reakce na kyberbezpečnostní incidenty, útoky a jiné hrozby (NÚKIB 2021a, 4).

b. Legislativní ukotvení

Co se legislativního ukotvení problematiky sdílení informací týče, dle § 17 odst. (1) ZKB zajišťuje sdílení informací v oblasti kyberbezpečnosti na národní a mezinárodní úrovni národní CERT. Národní a vládní CERT pak dle § 17 odst. (2) respektive dle § 20 ZKB přijímají oznámení

kontaktních údajů či hlášení kyberbezpečnostních incidentů povinných subjektů dle § 16 a § 8 téhož zákona. Dle § 9 vede NÚKIB evidenci kyberbezpečnostních incidentů, z níž poskytuje údaje orgánům veřejné moci pro výkon jejich působnosti. § 22 písm. t) je pak stanoveno, že NÚKIB informuje veřejnost o kyberbezpečnostních incidentech.

Sdílení informací, zejména nahlášení případů kyberkriminality včetně ransomware je pak v ČR možno i skrze tísňovou linku PČR, která dle § 23 Zákona o Policii ČR zajišťuje bezodkladný příjem volání. Národním kontaktním bodem pro kyberkriminalitu je v ČR dle Národní strategie KB NCOZ (NÚKIB 2020a, 8). Co se týče povinnosti sdílení informací, v ČR existují dva zákonné instituty. Tím prvním je nepřekažení trestného činu dle § 367 Trestního zákoníku, který kriminalizuje nepřekažení specifických trestných činů, přičemž překazit trestný čin lze i jeho včasným oznámením. S ohledem na zkoumané téma se může jednat o případy, kdy by ransomwarový útok naplňoval např. skutkovou podstatu vydírání dle § 175 odst. (3) a (4) či obecného ohrožení dle § 272 téhož zákona. Druhým institutem je pak neoznámení trestného činu dle § 368 Trestního zákoníku, které kriminalizuje neoznámení specifických trestných činů. Ve vztahu k ransomware se může jednat např. o již zmíněné obecné ohrožení dle § 272 téhož zákona. Sdílení informací ze strany PČR je pak jasně definováno § 8a až § 8d Trestního řádu.

Legislativní ukotvení sdílení informací mezi osobami poskytujícími služby spojené s virtuálními aktivy a FAÚ je upraveno Zákonem ML/FT. Významným je zejména § 18, který se věnuje problematice oznamování podezřelých obchodů.

c. Praktická aplikace

Sdílení informací probíhá zejména s ohledem na NÚKIB v několika směrech. Vyzdvihnout lze např. publikování varování před nově

identifikovanými hrozbami a zranitelnostmi často i včetně možných protiopatření nejen na webových stránkách NÚKIB (NÚKIB n.d.d), ale také skrze sociální sítě. Mimo to NÚKIB každý měsíc zveřejňuje přehled a analýzu řešených kyberbezpečnostních incidentů (NÚKIB n.d.e) či každoroční zprávy o stavu kyberbezpečnosti v zemi (NÚKIB n.d.f).

Expert č. 3 (Sikora 2022) dále uvádí, že hlásit incidenty, tedy sdílet informace o nich, je ze ZKB jím upravenými subjekty povinné. Stejně tak mohou nicméně činit také neregulované subjekty, přičemž současná praxe založená na dobrovolnosti sdílení informací neregulovanými subjekty je dle Experta č. 3 (Sikora 2022) adekvátní. Stejný názor pak zastává také Expert č. 6 (Švéda 2022), který dodává, že *„zákon aktuálně stojí na principu minimalizace státního donucení.*" Vynucování hlášení incidentů bez požadavku na plnění dalších povinností nevnímá jako vhodné, v tomto směru by dle něj nicméně bylo možno otevřít diskuzi na téma rozšíření regulovaných subjektů. To by mělo přijít se směrnicí NIS II (Evropská komise 2020).

S již zmíněným nahlašováním kyberbezpečnostních incidentů regulovanými subjekty však dle Experta č. 6 (Švéda 2022) souvisí problém definiční, kdy je pro subjekty náročné uvědomit si šíři toho, co lze chápat jako kyberbezpečnostní incident. K této otázce nicméně již NÚKIB vydal metodický podpůrný materiál (NÚKIB 2022g). Mimo to ale Expert č. 6 (Švéda 2022) upozorňuje, že v současnosti s největší pravděpodobností nejsou regulovanými subjekty nahlašovány všechny incidenty – zdá se mu totiž nepravděpodobné, že by se v rámci jednoho měsíce u stovek

regulovaných subjektů odehrálo v průměru jen 14 kyberbezpečnostních incidentů.[9]

Sdílení informací PČR je jasně vymezeno Trestním řádem, což uvádí i Expert č. 1 (Anonymní zdroj č. 1 2022) a dodává, že je *„sdílení dat vcelku sledováno a nesmí být nahodilé a neuvážené."* Směrem k sdílení informací ze strany obětí Expert č. 1 (Anonymní zdroj č. 1 2022) souhlasí s Expertem č. 3 (Sikora 2022) ohledně adekvátnosti současného nastavení dobrovolnosti nahlašování incidentů včetně útoků ransomware subjekty neregulovanými ZKB. Tento názor pak zdůvodňuje slovy: *„Nelze nutit subjekty k něčemu, co nechtějí. Pokud se jakýkoli subjekt rozhodne, že se nebude cítit jako poškozený, domníváme se, že je to jeho svobodné rozhodnutí a nemělo by se oznámení na něm vynucovat."* Expert č. 1 (Anonymní zdroj č. 1 2022) nicméně dodává, že by bylo *„ideální mít veškerá data ze všech ransomware útoků v jedné databázi."*

Dle informací od Experta č. 2 (Plecitý 2022) probíhá spolupráce mezi FAÚ a osobami provozujícími služby spojené s virtuálními aktivy dle Zákona ML/FT, přičemž lze vyvodit, že i sdílení informací mezi těmito aktéry probíhá v regulích zmíněného zákona, případně skrze expertem zmíněné ad hoc konzultace. Mimo to nicméně FAÚ vydal podobně jako NÚKIB analýzu věnující se případům praní špinavých peněz skrze virtuální aktiva v roce 2020 (FAÚ 2021), přičemž další zpráva za rok 2021 se dle informací od Experta č. 2 (Plecitý 2022) momentálně připravuje.

[9] Za leden 2022 bylo nahlášeno 11 incidentů (NÚKIB 2022a, 2), za únor 2022 také 11 incidentů (NÚKIB 2022b, 2), za březen 2022 pak 14 incidentů, což odpovídá průměru loňského roku (NÚKIB 2022c, 2). Za duben 2022 bylo nahlášeno celkem 20 incidentů (NÚKIB 2022d, 2).

G) Osvětová činnost

a. Koncepční ukotvení

Význam osvěty pro budování odolnosti ČR vůči kybernetickým hrozbám je reflektován Bezpečnostní strategií (MZV ČR 2015a, 16). Ta uvádí, že ČR *„podporuje osvětu zaměřenou na kybernetickou a informační bezpečnost, neboť široká veřejnost může být tím nejzranitelnějším prvkem celého systému."* Vzdělávání a osvěta v oblasti kyberbezpečnosti je pak také jedním ze strategických cílů Národní strategie KB (NÚKIB 2020a, 21). V té stojí, že je třeba začlenit problematiku vzdělávání do všech úrovní vzdělávacího systému (NÚKIB 2020a, 18) a nadále provádět plošné i úzce zaměřené osvětové kampaně (NÚKIB 2020a, 19). Mimo to Národní strategie KB (NÚKIB 2020a, 13) uvádí, že ČR bude posilovat principy digitální hygieny.

Problematika vzdělávání a osvěty v oblasti kyberbezpečnosti je velice detailně rozvedena Akčním plánem (NÚKIB 2021a, 16-17), který hovoří mimo řady dalších o vytvoření národního plánu vzdělávání v oblasti kyberbezpečnosti, tvorbě a nabízení e-learningových kurzů, spolupráci se vzdělávacími institucemi či o vzdělávání odborné i široké veřejnosti v oblasti kyberbezpečnosti formou školení, konferencí či workshopů.

Důležitost osvěty je reflektována také Strategií prevence kriminality (MV ČR 2022, 16), přičemž přímo ve vztahu ke kyberkriminalitě je chápána jako zcela zásadní a nepostradatelná (MV ČR 2022, 31), v tomto smyslu také směrem k *„zvýšení důvěry potencionálních obětí v činnost orgánů činných v trestním řízení"* (MV ČR 2022, 31).

b. Legislativní ukotvení

Legislativní ukotvení osvětových činností je nicméně poměrně omezené. Dle § 22 písm. j) ZKB zajišťuje NÚKIB mimo jiné vzdělávání v oblasti kyberbezpečnosti. Osvětová činnost PČR je pak zmíněna jen ve smyslu

spolupráce s právnickými a fyzickými osobami vykonávajícími činnost v oblasti vzdělávacích aktivit § 17 Zákona o PČR.

c. Praktická aplikace

Dle Experta č. 4 (Anonymní zdroj č. 2 2022) se NÚKIB věnuje osvětě zaměřené na základy kyberhygieny hned ve dvou rovinách. V rámci té první reviduje a připomínkuje projekty organizací, které se věnují vzdělávání v této oblasti, jako např. Datová Lhota od Matematicko-fyzikální fakulty Univerzity Karlovy, České televize a CZ.NIC (Děčko 2020), či Kyberpohádky od Centra kybernetické bezpečnosti (2021). Dále je dle Experta č. 4 (Anonymní zdroj č. 2 2022) NÚKIB součástí řady vzdělávacích konferencí, workshopů či webinářů. Mimo to ale vytváří vlastní vzdělávací aktivity, přičemž jejich preferovanou formou se stal e-learning. Dle Experta č. 4 (Anonymní zdroj č. 2 2022) je vhodné upozornit zejména na kurz Dávej kyber! (Hájek n.d.) či osvětový videokurz Jsem Netvor (NÚKIB n.d.g). Většina e-learningových kurzů NÚKIB je volně dostupná na webových stránkách instituce (NÚKIB n.d.h).

Dále se dle Experta č. 4 (Anonymní zdroj č. 2 2022) věnuje NÚKIB osvětě také přes sociální sítě, třeba prostřednictvím Instagramu @petr.vytrzny (NÚKIB n.d.i), nebo skrze koordinaci Festivalu bezpečného internetu, kde je kyberhygiena jedním z nosných témat (NÚKIB 2020c; NÚKIB n.d.j).

Vzdělávací aktivity NÚKIB se snaží zasáhnout co nejširší spektrum potenciálních kandidátů – od dětí v mateřských školách, přes pedagogy a metodiky prevence, zaměstnance veřejné správy či dalších subjektů dle ZKB, až po seniory (Anonymní zdroj č. 2 2022). Ransomware je konkrétně zmíněn v kurzu Dávej kyber! (Hájek n.d.) a objeví se také na vzdělávacím Instagramu při příležitosti Evropského měsíce kybernetické

bezpečnosti, kde je pro letošní rok ransomware jedním z hlavních témat (Anonymní zdroj č. 2 2022).

Směrem k osvětové činnosti PČR upozorňuje Expert č. 1 (Anonymní expert č. 1 2022) zejména na mezinárodní projekt No More Ransom, na kterém se od roku 2017 NCOZ podílí a postarala se o spuštění jeho webu v českém jazyce. Cílem projektu je šířit osvětu o problematice ransomware a také pomoci obětem ransomware s dešifrováním dat (Randáková 2017; NoMoreRansom n.d.). Mimo to je nicméně možné zmínit také projekt České bankovní asociace Kyberkampaň, na kterém kromě antivirové společnosti Eset spolupracuje právě i PČR (ČBA 2021),

Dle zjištěných informací se FAÚ osvětové činnosti ve zkoumané oblasti nevěnuje. S jistým nadhledem je pak za výjimku možno označit Expertem č. 2 (Plecitý 2022) zmíněné a v této práci již dříve představené odborné diskuze s osobami provozujícími služby spojené s virtuálními aktivy a dalšími aktéry za účelem objasnění jejich zákonných práv a povinností.

H) Technická opatření

a. Koncepční ukotvení

Joint Statement (The White House 2021) dále uvádí, že pro budování odolnosti proti ransomware je třeba dodržovat několik základních technických opatření, kterými jsou udržování offline datových záloh, používání silných hesel, vícefaktorové autentizace a záplatování software (The White House 2021). Bezpečnostní strategie (MZV ČR 2015a, 16) uvádí, že ČR „*upřednostňuje budování systémů pružné odolnosti schopných nejen minimalizovat dopady kybernetického útoku, ale také uvést systém rychle zpět do funkčního stavu.*“ Jedním ze strategických cílů Národní strategie KB (NÚKIB 2020a, 11) pak je i bezpečná infrastruktura, která vysoce

závisí na odolnosti povinných subjektů dle ZKB. Dále zmiňuje Národní strategie KB (NÚKIB 2020a, 18) také závazek budování digitalizované infrastruktury s důrazem na vysokou míru zabezpečení vůči kybernetickým hrozbám.

Akční plán (NÚKIB 2021a, 5) pak rozvádí strategický cíl bezpečné infrastruktury do dílčích cílů zaměřených primárně na metodickou podporu zavádění technických bezpečnostních opatření a vytvoření návrhu jednotné sítě státní správy s cílem navýšení bezpečnosti státních institucí za pomoci plošně aplikovaných standardů zabezpečení. Dále zmiňuje aktualizaci metod analýzy rizik a aktualizaci a vytváření souborů doporučených kyberbezpečnostních standardů (NÚKIB 2021a, 9). Mimo to se Akční plán (NÚKIB 2021a, 15) významně věnuje zabezpečení digitální veřejné správy, zejména zdůrazňuje potřebu zajištění kyberbezpečnosti jednotlivých projektů.

b. Legislativní ukotvení

Legislativně jsou technická opatření pro zajištění odolnosti systémů regulovaných dle ZKB podchycena poměrně detailně VKB. Zálohování je upraveno § 10 písm. k). Problematice hesel a ověřování identit se podrobně věnuje § 19, přičemž zmiňuje i vícefaktorovou autentizaci. Záplatování a aktualizaci software se pak věnují § 21 písm. e) či § 26 písm. a).

c. Praktická aplikace

Zatímco analyzovanými strategickými VPD nejsou základní technická opatření zmíněna, NÚKIB vydal ve spolupráci s AFCEA a NAKIT v roce 2020 dokument Ransomware: Doporučení pro mitigaci, prevenci a reakci, který se zaměřuje přímo na hrozbu ransomware a poměrně podrobně rozebírá všechna technická opatření uvedená v Joint Statement (The White House 2021) a mnoho dalších. Mimo to pak NÚKIB ve spolupráci s NAKIT a MV ČR vydal v roce 2020 pro ZKB neregulované subjekty

také Minimální bezpečnostní standard, který se věnuje již zmíněným technickým opatřením.

Dodržování VKB stanovených technických opatření pak NÚKIB dle Experta č. 3 (Sikora 2022) prosazuje v rámci své kontrolní činnosti. V roce 2019 provedl NÚKIB celkem 15 takovýchto kontrol (NÚKIB 2020b, 21), v roce 2020 pak v důsledku propuknutí pandemie COVID-19 pouze 8 (NÚKIB 2021b, 28), pro rok 2021 prozatím nejsou veřejně dostupná data.

4.2.2 Nezákonné financování

Další kategorií, které se představitelé zemí věnovali v rámci Joint Statement (The White House 2021) je nezákonné financování ransomware. V rámci této podkapitoly bude analyzováno koncepční, legislativní a praktické ukotvení náležité péče zákazníků, reportování podezřelé aktivity a monitoring transakcí v oblasti virtuálních aktiv, stejně jako jejich úprava v rámci národního rámce boje proti praní špinavých peněz. Dále bude analyzován závazek k navyšování kapacit národních autorit za účelem regulace, dohledu a vyšetřování a příslib spolupráce s poskytovateli služeb spojených s virtuálními aktivity.

A) Legalizace výnosů z ransomware

a. Koncepční ukotvení

Oblast virtuálních měn není v ČR téměř nikterak koncepčně ukotvena. Jediný strategický VPD zmiňující tuto problematiku je Koncepce boje proti OZ (MV ČR 2018, 41). Tato zmínka se objevuje v kontextu plateb výkupného ransomwarovým útočníkům v sekci věnované aktivitám organizovaných zločineckých skupin (MV ČR 2018, 41), následně v sekci věnované nástrojům OZ v oblasti legalizace výnosů z trestné činnosti (MV ČR

2018, 56) a také v sekci věnované budoucím trendům OZ (MV ČR 2018, 63). Koncepce boje proti OZ (MV ČR 2018, 15) si dále obecně v oblasti nových metod a nástrojů OZ stanovuje strategický cíl adaptovat OČTŘ na nové metody OZ skrze posilování odborných týmů, auditu požadavků na servisní útvary OČTŘ a také skrze důslednou regulaci nově dostupných nástrojů a reakci orgánů činných v trestním řízení na jejich nástup. Z uvedeného tedy vyplývá, že koncepčně je v ČR ukotvena pouze otázka navyšování kapacit národních autorit, která naopak není jasně ukotvena legislativně.

b. Legislativní ukotvení

Jinak je však legislativní ukotvení problematiky poměrně adekvátní. Dle § 2 odst. (1) písm. l) Zákona ML/FT, je povinnou osobou také osoba, která poskytuje služby spojené s virtuálními aktivy. Touto osobou je dle § 4 odst. (8) ten, kdo *„jako předmět své podnikatelské činnosti kupuje, prodává, uchovává, pro jiného spravuje, převádí nebo zprostředkovává nákup nebo prodej virtuálního aktiva,“* případně také ten, kdo *„poskytuje finanční služby týkající se nabídky nebo prodeje virtuálního aktiva,“* nebo *„poskytuje jiné služby spojené s virtuálním aktivem.“* Virtuální aktivum je definováno v § 4 odst. (9), přičemž do této definice lze obsáhnout aktiva známá jako virtuální měny či kryptoměny.

Pro povinné osoby z téhož zákona vyplývá množství povinností. Primárně se jedná o monitoring transakcí, který je upraven zejména ustanoveními části druhé téhož zákona. Na základě monitorování transakcí je § 18 téhož zákona upravena povinnost reportování podezřelé aktivity FAÚ. Definici podezřelého obchodu představuje § 6, který mimo jiné uvádí, že podezřelým obchodem se rozumí *„obchod uskutečněný za okolností vyvolávajících podezření ze snahy o legalizaci výnosů z trestné činnosti.“* Když nebude zohledněna spolupráce vyplývající ze zmíněných

ustanovení, není spolupráce s poskytovateli služeb spojených s virtuálními aktivy např. s ohledem na sdílení informací týkajících se ransomware legislativně žádným způsobem ukotvena.

Otázce legalizace výnosů trestné činnosti a legalizace výnosů trestné činnosti z nedbalosti se pak věnují také § 216 a § 217 Trestního zákoníku, které je s jistou mírou abstrakce možno chápat jako legislativní ukotvení náležité péče zákazníků zmíněné Joint Statement (The White House 2021).

c. Praktická aplikace

Jak bylo již dříve zmíněno, spolupráce s poskytovateli služeb spojených s virtuálními aktivy probíhá dle Experta č. 2 (Plecitý 2022) až na dříve vedené odborné debaty v regulích Zákona ML/FT, což považuje za adekvátní vzhledem k aktuálním potřebám.

Budování národních kapacit skrze rozšiřování expertní základny není v případě FAÚ v současnosti aktuální, neboť Expert č. 2 (Plecitý 2022) hodnotí současný stav za poměrně vyhovující. Uvádí však, že dalšího experta na problematiku by FAÚ minimálně do budoucna jistě zužitkoval. Poukazuje nicméně na deficit odborníků na kyberkriminalitu obecně a problematiku již zmiňované nekonkurenceschopnosti státní správy, která jakékoli budování národních kapacit významně ztěžuje. Na tomto faktoru se tedy shoduje také s Expertem č. 1 (Anonymní zdroj č. 1 2022), který nicméně uvádí, že alespoň směrem k technickému vybavení jsou postupně národní kapacity vylepšovány, přičemž jako příklad uvádí např. software určený k trasování virtuálních měn.

Spolupráce s OČTŘ je z určité části kryta povinností mlčenlivosti, vzájemná komunikace a sdílení informací s orgány na úrovni skupin či oddělení kyberkriminality a analytických oddělení krajských ředitelství PČR je nicméně Expertem č. 2 (Plecitý 2022) hodnocena jako téměř

bezproblémová. Spolupráce s NCOZ je pak na výborné úrovni, přičemž v případech vyžadujících si urgentní spolupráci fungují komunikační kanály dle slov Experta č. 2 (Plecitý 2022) tzv. 24/7, kdy je za jistý omezující faktor možno označit zejména další aktéry, jmenovitě např. bankovní sektor. Velmi dobrou úroveň spolupráce mezi PČR a FAÚ pak potvrzuje i Expert č. 1 (Anonymní zdroj č. 1 2022). Spolupráce s NÚKIB je pak výrazně nižší. Expert č. 2 (Plecitý 2022) uvedl, že nebude konkrétní a zmínil zejména spolupráci v rámci odborných meziresortních skupin třeba na MV ČR,

V praktické rovině probíhá také spolupráce FAÚ se zahraničními finančními zpravodajskými jednotkami, kdy Expert č. 2 (Plecitý 2022) poukazuje zejména na sdílení informací, které je poměrně nevyrovnané. Zatímco do ČR proudí obrovské množství pouze základně zpracovaných dat, z ČR odesílají zahraniční jednotky FAÚ již zpracované informace. Tuto skutečnost Expert č. 2 (Plecitý 2022) zdůvodňuje objemem těchto dat. Zahraniční partneři pracují často např. s významnými kryptoměnovými burzami, případně monitorují větší objem subjektů, nežli ČR. Takto získané informace jsou pak zpracovávány, případně předávány dále OČTŘ.

Významným úskalím boje proti legalizaci výnosů z trestné činnosti přes virtuální aktiva je dle Experta č. 2 (Plecitý 2022) zejména problematická postižitelnost osob provádějících tuto činnost skrze tzv. peer-to-peer obchody na k tomu určených platformách. Takto obchodující lidé mohou poměrně snadno popřít vědomí o původu obchodovaných prostředků, případně přenést odpovědnost na poskytovatele této služby.

B) Placení výkupného

a. Koncepční ukotvení

I přesto, že Joint Statement (The White House 2021) tuto problematiku přímo nezmiňuje, placení výkupného ransomwarovým útočníkům představuje jedno ze zásadních úskalí v boji proti ransomware. Platby výkupného totiž v podstatě živí útočníky a neutuchající ochota obětí za dešifrování svých dat zaplatit je dále motivuje k činnosti (Grimes 2021, 124; Savage, Coogan and Lau 2015, 24; Hassan 2019, 178). Na úrovni strategických VPD nicméně není problematika placení výkupného nijak řešena, což je vzhledem k absenci řešení problematiky ransomware vcelku pochopitelné.

b. Legislativní ukotvení

Podle Experta č. 3 (Sikora 2022) se v ČR může subjekt zaplacením výkupného dopustit porušení zásad péče řádného hospodáře dle § 159 Občanského zákoníku, povinnosti při správě cizího majetku dle § 220 či předpisů o pravidlech hospodářské soutěže dle § 248 Trestního zákoníku. Případně může být daný subjekt stíhán i za trestný čin zpronevěry dle § 206, zneužití pravomoci úřední osoby dle § 329 či legalizace výnosů z trestné činnosti dle § 216 téhož zákona. Explicitně však není zaplacení výkupného v případě ransomwarového útoku v ČR kriminalizováno.

c. Praktická aplikace

V praxi se nicméně na tuto problematiku názory různí a k stíhání obětí ransomware kvůli platbám výkupného zřejmě nedochází. To lze vyvodit z absence případných medializovaných případů či z vyjádření Experta č. 1 (Anonymní zdroj č. 1 2022). Ten uvádí, že *„nelze kriminalizovat oběť, která je sama v tísni.“* A dodává, že pokud by chtěl stát takto kriminalizovat platby výkupného při incidentech ransomware, musel by přistoupit k reparacím vůči oběti, které v důsledku nezaplacení vznikla

mnohonásobně vyšší škoda, než byla hodnota požadovaného výkupného. Překvapivé je pak zejména další vyjádření Experta č. 1 (Anonymní zdroj č. 1 2022), že v případě většího počtu plateb výkupného je sice možné očekávat také zvýšení intenzity ransomwarových útoků, avšak *„z našeho pohledu není zcela jasně vyhraněna škodlivost tohoto jednání (placení výkupného).“*

Již zmiňovaný dokument Ransomware: Doporučení pro mitigaci, prevenci a reakci (NÚKIB, AFCEA and NAKIT 2020, 14) nicméně jasně uvádí, že oběť by v žádném případě neměla platit výkupné, neboť tím motivuje útočníka k dalším útokům a nemá záruku, že budou po zaplacení data skutečně odblokována, nebo že dojde k odstranění škodlivého kódu, který by mohl vést k opakovanému útoku. Doporučení neplatit ransomwarovým útočníkům pak obsahuje také osvětový kurz NÚKIB Dávej kyber! (Hájek n.d.) či projekt No More Ransom (NoMoreRansom n.d.).

4.2.3 Vymáhání práva

V této části věnované koncepčnímu, legislativnímu a praktickému ukotvení závazků z Joint Statement (The White House 2021) směrem k vymáhání práva bude nejprve analyzován příslib boje proti ransomware vycházejícího z území ČR, zejména tedy příslib stíhání ransomwarových útočníků, a dále také závazek k spolupráci mezi orgány vymáhajícími právo, národními kyberbezpečnostními autoritami a finančními zpravodajskými jednotkami

A) Stíhání útočníků

a. Koncepční ukotvení

Národní strategie KB (NÚKIB 2020a, 21) uvádí jako jeden ze strategických cílů ČR také potírání kyberkriminality, směrem k této problematice

však blíže rozvádí pouze problematiku atribuce, tedy vysoké náročnosti určení totožnosti útočníka v kyberprostoru. ČR se tedy dle Národní strategie KB (NÚKIB 2020a, 13-14) zaměřuje na posilování úsilí a kapacit systému detekce, včasné reakce a atribuce kyberútoků. Koncepce boje proti OZ (MV ČR 2018, 21) zmiňuje zejména potřebu adaptace OČTŘ směrem k navýšení připravenosti na řešení masivně narůstajících případů kyberkriminality.

Závazek k potírání kyberkriminality je dále rozveden Akčním plánem (NÚKIB 2021a, 6-7), který představuje příslib vytvoření, implementace a aktivace efektivního národního rámce atribuce závažných kyberútoků, rozvíjení schopností PČR v oblasti kyberkriminality v souladu s Koncepcí rozvoje Policie ČR do roku 2027 a Strategií boje s kybernetickou kriminalitou,[10] a také analyzování mezinárodně-právních závazků v oblasti kyberkriminality a jejich aplikaci do relevantních metodik.

b. Legislativní ukotvení

Legislativní ukotvení možnosti stíhání pachatelů ransomwarových útoků a aktivit s nimi spojených je v ČR kromě zákonů zmíněných v kapitole věnované nelegálnímu financování zajištěno především ustanoveními v Trestním zákoníku. Dle Experta č. 1 (Anonymní zdroj č. 1 2022) mohou ransomwarové útoky naplňovat skutkové podstaty mimo jiné trestného činu neoprávněný přístup k počítačovému systému a nosiči informací dle § 230 a vydírání dle § 175. Zejména s ohledem na různé taktiky, které útočníci využívají směrem k maximalizaci zisků či k donucení obětí zaplatit výkupné, lze uvažovat také o trestném činu neoprávněné nakládání s osobními údaji dle § 180, porušení tajemství dopravovaných zpráv dle § 182, porušení tajemství listin a jiných dokumentů

[10] Dokumenty nejsou veřejně dostupné.

uchovávaných v soukromí dle § 183, poškození cizí věci dle § 228 či opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle § 230. Na základě zmíněných ustanovení Trestního zákoníku je tedy v ČR ransomwarové útočníky v případě podezření z naplnění skutkových podstat možno vyšetřovat a v případě zjištění naplnění skutkových podstat i stíhat.

c. Praktická aplikace

Z provedených expertních rozhovorů se bohužel nepodařilo zjistit, do jaké míry se v ČR daří ransomwarové útočníky skutečně postihovat. Vyšetřování těchto činů nesporně probíhá, o čemž svědčí informace uvedené např. ve Zprávě o činnosti státního zastupitelství za rok 2019 (NSZ 2020) či za rok 2020 (NSZ 2021), případně také ve Zprávě o činnosti národního korespondenta pro boj proti kybernetické kriminalitě, pro ochranu práv k nehmotným statkům a kybernetickou bezpečnost za rok 2019 (Klement 2020, 5) či za rok 2020 (Foldyna 2021, 2-3).

Vzhledem k tomu, že ransomwaroví útočníci často působí ze zahraničních útočišť je možné předpokládat, že úspěšnost není příliš vysoká. To potvrzuje např. také absence medializovaných případů úspěšného stíhání ransomwarových útočníků v ČR, odložení případů ransomwarových útoků na Nemocnici Rudolfa a Stefanie Benešov či Psychiatrickou nemocnici Kosmonosy (NSZ 2020, 3), nebo na Magistrát města Olomouce (Hejtman 2022).

Expert č. 1 (Anonymní zdroj č. 1 2022) potvrzuje náročnost atribuce či přímo stíhání ransomwarových útočníků, přičemž jako jeho největší překážku vnímá zejména využívání anonymizačních prostředků včetně sítě TOR, využívání plateb v kryptoměnách či možnost registrace domén na smyšlená jména. Jak bylo již dříve uvedeno, s ohledem na stíhání osob legalizujících výnosy z trestné činnost je nejproblematičtějším bodem

dle Experta č. 2 (Plecitý 2022) zejména existence peer-to-peer obchodů, u nichž je náročné prokázat vědomí závadového chování, což platí i u případů spojených s ransomware.

Co se týče zmíněných závazků směrem k rozvoji orgánů vymáhajících právo, např. Expert č. 2 (Plecitý 2022) uvádí, že je v tomto roce možné očekávat vznik samostatných útvarů PČR zaměřených na kyberkriminalitu. Expert č. 1 (Anonymní zdroj č. 1 2022) k tomuto tématu dodává, že co do technického rozvoje je možné pozorovat pozitivní pokrok již nyní, přičemž očekává další zlepšení stavu do budoucna. Aspektem významně ztěžujícím rozvoj orgánů vymáhajících právo je nicméně jejich již několikrát zmíněná nekonkurenceschopnost na trhu práce (Plecitý 2022; Anonymní zdroj č. 1 2022; Anonymní zdroj č. 3 2022).

B) Spolupráce mezi významnými aktéry

a. Koncepční ukotvení

Důležitost spolupráce mezi orgány vymáhajícími právo a kyberbezpečnostními autoritami na národní i mezinárodní úrovni při zajišťování kyberbezpečnosti zmiňuje Bezpečnostní strategie (MZV ČR 2015a, 16), přičemž zdůrazňuje, že ČR *„podporuje posílení mezinárodní soudní a policejní spolupráce s cílem dopadení pachatelů kybernetických útoků.“* Ve vztahu k OZ pak Bezpečnostní strategie (MZV ČR 2015a, 17) uvádí, že se ČR zaměřuje na *„podporu přímé policejní spolupráce na národní i mezinárodní úrovni umožňující rychle reagovat na aktivity kriminálních struktur.“*

Národní strategie KB (NÚKIB 2020a, 10) pak hovoří o potřebě vylepšování modelu spolupráce a sdílení informací napříč jednotlivými státními institucemi, která by měla přispět mimo jiné k nalezení konsenzu v otázkách kyberbezpečnosti. Z takto vytvořené jednotné pozice

bude ČR usilovat o spolupráci na mezinárodní i bilaterální úrovni, neboť si uvědomuje důležitost společné reakce, koordinace a postupu proti kyberbezpečnostním hrozbám a směrem k atribuci kyberútoků (NÚKIB 2020a, 15). Národní strategie KB (NÚKIB 2020a, 16) také uvádí, že ČR bude v oblasti vymáhání práva a potírání kyberkriminality *„podporovat a pomáhat při spolupráci s partnerskými zeměmi při posílení kooperace mezi orgány činnými v trestním řízení a dalšími složkami.“*

Význam spolupráce mezi orgány státní správy a veřejné moci na národní i mezinárodní úrovni v boji proti OZ pak vyzdvihuje také Koncepce boje proti OZ (MV ČR 2018, 16-17), která si jako jeden ze strategických cílů klade *„posílit sdílení informací a spolupráci při řešení případů organizovaného zločinu“* např. skrze vytváření průřezových a ad hoc týmů pro jednotlivé problematiky.

V Akčním plánu (NÚKIB 2021a, 3) je pak představena již dříve zmíněná iniciativa vytvoření a provozování národní zabezpečené platformy pro komunikaci a sdílení informací za účelem řešení kyberbezpečnostních incidentů či rozvoje efektivní a koordinované spolupráce mezi NÚKIB, PČR a zpravodajskými službami. Směrem k mezinárodní spolupráci Akční plán (NÚKIB 2021a, 11-13) hovoří o odhodlání aktivně se podílet na mezinárodních aktivitách v oblasti kyberbezpečnosti a o potřebě vytvoření národní platformy, která by měla tyto aktivity jednotlivých orgánů státní správy koordinovat.

b. Legislativní ukotvení

Legislativně je problematika spolupráce mezi orgány vymáhajícími právo a kyberbezpečnostními autoritami ukotvena např. § 22 ZKB, který stanovuje, že NÚKIB dle písm. g) spolupracuje s orgány a osobami, které působí v oblasti kybernetické bezpečnosti, dle písm. h) zajišťuje mezinárodní spolupráci v oblasti kybernetické bezpečnosti, dle písm. i)

sjednává a uzavírá smlouvy o mezinárodní spolupráci v oblasti kyberbezpečnosti a dle písm. r) je také jednotným kontaktním místem pro zajištění přeshraniční spolupráce v oblasti kybernetické bezpečnosti v rámci EU. Národní CERT pak dle § 17 odst. (1) zajišťuje sdílení informací na národní a mezinárodní úrovni v oblasti kyberbezpečnosti. Národní a vládní CERT pak dle § 17 odst. (2) písm. k) a § 20 písm. n) spolupracují s týmy CSIRT jiných členských států EU.

Zákon o PČR § 14 stanovuje, že PČR při plnění svých úkolů spolupracuje s ozbrojenými silami, bezpečnostními sbory a dalšími orgány veřejné správy. Mezinárodní spolupráce PČR je podrobně upravena hlavou XI Zákona o PČR, který v § 89 uvádí, že PČR při plnění svých úkolů spolupracuje s INTERPOL, EUROPOL, či orgány EU a jejích členských států. Dále také uvádí, že PČR spolupracuje s dalšími *„mezinárodními organizacemi, s mezinárodními trestními soudy, mezinárodními trestními tribunály, popřípadě obdobnými mezinárodními soudními orgány“* a také se *„zahraničními bezpečnostními sbory a dalšími příslušnými zahraničními subjekty,“* přičemž dle § 90 je ústředním orgánem pro mezinárodní policejní spolupráci policejní prezidium. Mezinárodní justiční spolupráce je pak detailně upravena Zákonem o mezinárodní justiční spolupráci ve věcech trestních.

Spolupráce mezi OČTŘ a FAÚ je legislativně zakotvena v § 30 a § 31 Zákona ML/FT a to zejména s ohledem na získávání a zpracování informací. Mezinárodní spolupráce v oblasti legalizace výnosů z trestné činnosti je pak upravena § 33 odst. (1), kde stojí, že FAÚ spolupracuje se zahraničními orgány a mezinárodními organizacemi se srovnatelnou věcnou působností, přičemž dle odst. (2) je obsahem této spolupráce zejména předávání a získávání údajů, které je dále upraveno § 33a téhož zákona.

c. Praktická aplikace

Dříve již představená spolupráce mezi orgány vymáhajícími právo, kyberbezpečnostními autoritami a finančními analytickými jednotkami funguje při řešení trestných činů souvisejících s ransomware v ČR na adekvátní úrovni, přičemž hlavní oblastí je v tomto ohledu dle dotazovaných expertů v práci již zmíněné sdílení informací (Plecitý 2022; Anonymní zdroj č. 1 2022; Sikora 2022).

Zahraniční spolupráce z pohledu NÚKIB probíhá v rámci pracovních skupin na evropské i světové úrovni, přičemž i zde je dle Experta č. 3 (Sikora 2022) stěžejním aspektem především sdílení jak kontextuálních, tak technických informací, které je ve značné míře automatizováno. Bližší expertní informace týkající se spolupráce NÚKIB se zahraničními institucemi se bohužel nepodařilo získat. Koncepce rozvoje NÚKIB (NÚKIB 2021g, 26) v tomto směru uvádí, že intenzita i význam mezinárodní spolupráce narůstají, přičemž ČR navazuje pracovní vztahy, díky nimž získává NÚKIB včas informace o hrozbách, které jsou vyhodnocovány a sdíleny s dalšími institucemi na národní úrovni.

Z pohledu PČR vyzdvihuje Expert č. 1 (Anonymní zdroj č. 1 2022) zejména podíl ČR na aktivitách EUROPOL, CEPOL či INTERPOL. Specifika či zapojení ČR do konkrétních iniciativ dle Experta č. 1 (Anonymní zdroj č. 1 2022) není z jeho strany vhodné rozebírat. Lze nicméně poukázat na zapojení ČR do operací EUROPOL v rámci EMPACT, tedy Evropské multidisciplinární platformy proti kriminálním hrozbám (EUROPOL 2022a), pod jehož záštitou se NCOZ podílela na přerušení provozu VPNLab.net, tedy platformy zaštiťující komunikaci a přístup k Internetu, která byla běžně využívána ransomwarovými útočníky (EUROPOL 2022b). Pod záštitou EMPACT se pak v loňském roce zřejmě bez přímého zapojení ČR podařilo zadržet pět osob napojených na REvil/Sodinokibi (EUROPOL

2021a), dvanáct osob páchajících ransomwarové útoky např. s využitím ransomware LockerGoga, MegaCortex či Dharma (EUROPOL 2021b), nebo ukrajinský ransomwarový gang bez doposud uveřejněné afiliace (EUROPOL 2021c). INTERPOL pak v oblasti boje proti kyberkriminalitě vytvořil dvě platformy – Cybercrime Knowledge Exchange, která je určena ke sdílení informací, a Cybercrime Collaborative Platform, jejímž účelem je podpora operací orgánů vymáhajících právo (INTERPOL n.d.a). O tom, zda je ČR součástí těchto platforem se nepodařilo získat informace. Avšak s ohledem na fakt, že ČR patří to sítě národních ústředen INTERPOL (INTERPOL n.d.b) je její zapojení možno předpokládat.

Zahraniční spolupráce FAÚ je pak dle Experta č. 2 (Plecitý 2022) založena zejména na sdílení informací, které bylo rozebráno již v jemu dedikované kapitole.

4.2.4 Diplomacie

Poslední oblastí, které se zástupci států v Joint Statement (The White House 2021) věnují, a jejíž koncepční, legislativní a praktické ukotvení v ČR bude analyzováno je oblast diplomacie. Diplomacie může významně přispět v boji proti ransomware a to zejména skrze prosazování chování států založeného na pravidlech, pomoci státům k adekvátnímu adresování ransomware na jejich území a také skrze koordinované využívání diplomacie k redukci ransomwarových útočišť (The White House 2021).

A) Eliminace ransomwarových útočišť, prosazování chování založeného na pravidlech a podpora dalších států

a. Koncepční ukotvení

Význam diplomacie při zajišťování bezpečnostních zájmů ČR reflektuje Bezpečnostní strategie (MZV ČR 2015a, 14). Ta uvádí, že ČR klade důraz

na řešení bezpečnostních výzev diplomatickými prostředky, a že „*významnou roli při zajišťování bezpečnostních zájmů ČR sehrává diplomatická služba*“ (MZV ČR 2015a, 21). Národní strategie KB (NÚKIB 2020a, 13) pak zmiňuje, že ČR je připravena využít dostupných diplomatických prostředků k adresování hrozeb v kyberprostoru. Dále si dle Národní strategie KB (NÚKIB 2020a, 15) ČR uvědomuje důležitost společné reakce, koordinace a postupu proti kyberbezpečnostním hrozbám.

Směrem k prosazování chování založeného na pravidlech pak rozvíjí pozici ČR Akční plán (2021a, 13), který hovoří o aktivní kybernetické diplomacii zaměřené na prosazování stávajícího mezinárodního práva a dodržování nezávazných norem odpovědného chování států v kyberprostoru. Mimo to se chce ČR podílet na rozvoji norem zaměřených na kyberbezpečnost na půdě EU, spolupracovat na implementaci politiky kyberbezpečnosti s NATO, spoluvytvářet a implementovat opatření pro zvyšování důvěry mezi státy v kyberprostoru na půdě OBSE, podílet se na tvorbě strategických dokumentů a doporučení OECD či spoluvytvářet mezinárodní diskuzi na téma bezpečnosti a stability kyberprostoru na půdě OSN (NÚKIB 2021a, 11-13).

K bodu pomoci státům k adekvátnímu adresování ransomware na jejich území je možné vztáhnout Národní strategií KB (NÚKIB 2020a, 17) zmíněné odhodlání ČR aktivně podporovat budování kapacit kyberbezpečnosti v partnerských zemích. ČR si uvědomuje, že posilováním schopností jednotlivých států k zajišťování kyberbezpečnosti na národní úrovni se zvýší odolnost celého systému, neboť se tak alespoň částečně předejde možnosti páchání škodlivé činnosti z jejich území. Za tímto účelem je ČR ochotna sdílet svůj legislativní a strategický rámec kyberbezpečnosti či schopnosti a expertízu se státy, které v této oblasti prozatím zaostávají. V tomto směru pak hovoří Akční plán (NÚKIB 2021a, 14)

o posilování kapacity třetích zemí v oblasti kyberbezpečnosti za využití nástrojů zahraniční rozvojové spolupráce a ekonomické diplomacie v souladu se Strategií zahraniční rozvojové spolupráce (MZV ČR 2017) a Koncepcí zahraniční politiky ČR (MZV ČR 2015b), které však problematiku kyberbezpečnosti explicitně nezmiňují.

b. Legislativní ukotvení

Diplomatické styky na bilaterální úrovni i vzhledem k mezinárodním organizacím jsou upraveny řadou samostatných zákonných předpisů. Významným je v problematice diplomacie zejména Kompetenční zákon, který upravuje okruh působností a zásady činnosti ústředních orgánů státní správy. § 6 odst. (2) Kompetenčního zákona pak stanovuje, že MZV ČR *„zabezpečuje vztahy České republiky k ostatním státům, mezinárodním organizacím a integračním seskupením, koordinuje aktivity vyplývající z dvoustranné a mnohostranné spolupráce.“* Dle § 6 odst. (3) mimo jiné dle písm. a) koordinuje činnost ministerstev a jiných ústředních orgánů státní správy v oblasti zahraničních vztahů. Významným je pak ale zejména písm. b) odst. (3) § 6 téhož zákona, které uvádí, že MZV ČR zajišťuje ochranu práv a zájmů ČR a jejích občanů v zahraničí.

S ohledem na podporu budování kyberbezpečnostní odolnosti třetích států je pak významný zejména Zákon o zahraniční rozvojové spolupráci a humanitární pomoci poskytované do zahraničí. Vzhledem k tomu, že diplomacie významně souvisí s mezinárodní spoluprací, je třeba zohlednit i § 22 písm. h) a j) ZKB, která uvádí, že NÚKIB *„zajišťuje mezinárodní spolupráci v oblasti kybernetické bezpečnosti“* a v této oblasti také *„sjednává a uzavírá smlouvy o mezinárodní spolupráci.“*

c. Praktická aplikace

Zájmy ČR na mezinárodním poli, zejména na půdě mezinárodních organizací a integračních uskupení (např. EU, NATO, OSN), zastupuje NÚKIB

společně s MZV ČR a Ministerstvem obrany (NÚKIB 2021b, 31). Platí však, že koordinační roli sehrává především MZV ČR a NÚKIB zodpovídá zejména za zastupování ČR v odborných skupinách, případně v rámci pozic určených k bilaterální spolupráci (NÚKIB 2021g, 23).

Akčním plánem (NÚKIB 2021a) zmíněné cíle identifikované v části věnované koncepčnímu ukotvení se téměř plně shodují s informacemi o prováděných činnostech v této oblasti zmíněných již Zprávou o stavu kybernetické bezpečnosti ČR za rok 2020 (NÚKIB 2021b). Z toho lze usoudit, že se ČR skutečně aktivně podílí v oblasti kybernetické diplomacie zejména směrem k prosazování na pravidlech založeného chování v kyberprostoru, a její budoucí cíle vychází z již nyní prováděných činností.

V tomto ohledu je na úrovni EU možno zdůraznit zejména existenci tzv. Cyber Diplomacy Toolboxu, na jehož přípravě se podílela i ČR (NÚKIB 2020b, 26; NÚKIB 2021b, 31). Cyber Diplomacy Toolbox byl ustaven v květnu roku 2019 a rámuje možné využití cílených restriktivních opatření členskými státy EU, tedy i ČR, za účelem odstrašení či reakce na kyberútoky (Lenzu 2019). Tohoto rámce bylo poprvé využito v červenci roku 2020 mimo jiné vůči osobám spojeným s ransomware WannaCry či wiperem NotPetya. Sankce obsahovaly zákaz přicestování a zmrazení majetku dotčených osob, stejně jako zákaz zpřístupnění finančních prostředků dotčeným osobám občany a společnostmi na území EU (Lenzu 2020).

V oblasti sdílení informací s cílem budovat větší odolnost zahraničních partnerů pak NÚKIB vysílá národní experty či tzv. kybernetické přidělence do mezinárodních organizací, kde je jejich primárním cílem sdílet svoji expertízu a znalosti (NÚKIB 2021g, 26). Mimo to lze poukázat na účast zástupců ČR včetně expertů z řad NÚKIB na sympoziu Africa Endeavor v letech 2018 (NÚKIB 2018b) a 2019 (NÚKIB 2019b), kde se

podělili o zkušenosti ČR např. s legislativním ukotvením kyberbezpečnosti a pro další účastníky zorganizovali kyberbezpečnostní cvičení.

4.3 Slabá místa policy potírání ransomware v ČR

V rámci této časti policy analysis bude zhodnoceno, zda jsou cíle ke kterým se ČR vyslovila v Joint Statement (The White House 2021) v souladu se závazky, jež jsou stanovené národními koncepčními dokumenty ČR, zda jsou tyto závazky adekvátně vymezeny v národní legislativě, a také zda je adekvátní jejich praktická aplikace. Cílem této kapitoly je tedy shrnout zjištění představená v předchozí části a identifikovat slabá místa současné policy potírání ransomware v ČR.

4.3.1 Resilience

A) Jasná vládní struktura

V kategorii resilience je nejprve zmíněna potřeba jasné vládní struktury. Této otázce se věnuje Národní strategie KB (NÚKIB 2020a), která představuje systém zajišťování kyberbezpečnosti v ČR, a pak také Koncepce boje proti OZ (MV ČR 2018), která představuje institucionální strukturu boje proti OZ. Potírání ransomware je nicméně velice komplikované a žádný z analyzovaných dokumentů nezachycuje dostatečně komplexně všechny subjekty a jejich role v této oblasti. Úlohy a vzájemné vazby kyberbezpečnostních institucí (NÚKIB), finančních analytických jednotek (FAÚ), orgánů činných v trestním řízení (PČR – konkrétně NCOZ) a diplomatického aparátu nejsou tedy v ČR koncepčně adekvátně ukotveny, což je možné označit za nikoli závažné, nýbrž existující slabé místo policy boje proti ransomware ČR.

V oblasti vládní struktury je sice možné říci, že role a povinnosti jednotlivých aktérů jsou zákonně ukotveny, toto ukotvení je však velice nepřehledné. Samostatná legislativní ustanovení upravující role a působnosti aktérů často neadresují přímo a explicitně roli těchto orgánů v zajišťování kyberbezpečnosti či v boji proti kyberkriminalitě. Např. Kompetenční zákon zde stanovuje roli MV ČR, MF ČR či MZV ČR, Zákon o PČR pak upravuje roli PČR, ZKB roli NÚKIB, národního a vládního CERT a Zákon ML/TF upravuje roli FAÚ. Zohlednit je pak také nutno ustanovení Trestního řádu a dalších legislativních VPD. Legislativní ukotvení vládní struktury tedy není jasné a představuje tak slabé místo policy potírání ransomware, které však nelze považovat za závažné.

Z rozhovorů či z informací získaných z otevřených zdrojů nicméně vyplývá, že nejvýznamnější aktéři boje proti ransomware si jsou vědomi své role a působnosti, což dále podtrhuje závěr, že tato slabá místa české policy potírání ransomware nejsou nikterak závažná.

B) Adekvátní zdroje

Dalším bodem kategorie resilience je potřeba vyčlenění adekvátních zdrojů na potírání hrozby ransomware. Potřebu a odhodlání ČR investovat dostatečné zdroje do problematiky kyberbezpečnosti a boje proti OZ zmiňuje Bezpečnostní strategie (MZV ČR 2015a), Národní strategie KB (NÚKIB 2020a) i Koncepce boje proti OZ (MV ČR 2018). Explicitní zmínka o potřebě investovat adekvátní finanční prostředky do boje proti ransomware absentuje, avšak tuto absenci nelze považovat za slabé místo policy, neboť toto odhodlání implicitně vyplývá z obecnějších závazků.

S výše zmíněnou roztroušenou legislativní úpravou vládní struktury pak přímo souvisí také otázka legislativního ukotvení zajištění

adekvátních zdrojů. Zajišťování kyberbezpečnosti ani potírání kyberkriminality, natož tak potírání ransomware, netvoří v ČR samostatnou kapitolu státního rozpočtu, nýbrž je financováno z rozpočtů jednotlivých orgánů vládní struktury dle příslušných legislativních předpisů. To představuje zásadní slabé místo, neboť je v důsledku toho velice komplikované monitorovat a koordinovaně alokovat tyto zdroje, což představuje slabé místo zkoumané policy.

Toto slabé místo dále podtrhuje také fakt, že se v praxi významní aktéři boje proti ransomware potýkají s nedostatečným finančním zajištění jejich činnosti, zejména pak s ohledem na neadekvátní platové ohodnocení specializovaných pozic.

C) Personální zajištění

Zajištění kvalifikované pracovní síly je pak koncepčně zachyceno Bezpečnostní strategií (MZV 2015a), Národní strategií KB (NÚKIB 2020a), či Strategií prevence kriminality (MV ČR 2022). V tomto směru jak k vytvoření konkurenceschopnosti státní správy na trhu práce, tak směrem k rozvíjení schopností současných zaměstnanců. Mimo to chce ČR posílit personální zajišťování kyberbezpečnosti zejména pro řešení závažných incidentů také skrze institucionalizaci spolupráce s experty ze soukromého, neziskového či akademického sektoru. Konkrétní kroky směřující k zajištění kvalifikované pracovní síly jsou dále rozvedeny Akčním plánem (NÚKIB 2021a), avšak zde absentuje jakýkoli cíl směrem k zvýšení konkurenceschopnosti státní správy. To je sice možné považovat za mírný nedostatek, nicméně s ohledem na uvedené cíle strategických VPD nelze koncepční ukotvení problematiky personálního zajištění považovat za slabé místo policy.

Cíl zajištění adekvátně kvalifikované pracovní síly pak legislativně ukotven není. Prohlubování specializace státních zaměstnanců se věnuje např. Zákon o státní službě. Zajišťování konkurenceschopnosti státní správy je pak legislativou v jejím současném stavu spíše ztíženo, neboť se platové podmínky pracovníků musí řídit dle tabulek příslušných nařízení vlády. Ty však neumožňují nabídnout podobné platové podmínky, jaké si může dovolit nabízet soukromý sektor a orgánům státní správy tak zůstávají jen omezené motivační prostředky k náboru. Tato skutečnost představuje poměrně zásadní slabé místo současného legislativního ukotvení zkoumané policy.

Zajišťování adekvátní personální základny, konkrétně pak zejména nekonkurenceschopnost státních institucí jakožto slabé místo policy boje proti ransomware je pak podtrženo expertními informacemi z praxe. Dotazovaní experti se shodují, že státní správa je na současném trhu práce v podstatě nekonkurenceschopná a je náročné obsazovat specializované pozice v rámci jejich institucí, a to zejména v důsledku nabízeného platového ohodnocení (Anonymní zdroj č. 1 2022; Plecitý 2022; Anonymní zdroj č. 3 2022).

D) Cvičení

Otázka nacvičených postupů reakce na kyberbezpečnostní incidenty je v ČR koncepčně dostatečně ukotvena. O odhodlání pořádat pravidelná cvičení hovoří jak Bezpečnostní strategie (MZV ČR 2015a), tak Národní strategie KB (NÚKIB 2020a) a také velmi konkrétně Akční plán (NÚKIB 2021a). Cvičení nejsou řešena jen v rámci státní správy, ale také pro zranitelné sektory či směrem k budování mezinárodních partnerství. Zmínka o cvičení postupů reakce přímo na incidenty spojené s ransomware absentuje, což však nelze považovat za slabé místo policy boje

proti ransomware ČR, neboť i cvičení postupu reakce na jiné kyberbezpečnostní incidenty současně zvyšují připravenost na případy spojené s ransomware.

Závazek k dobře nacvičeným postupům však není ve vztahu ke kyberbezpečnosti v ČR legislativně nijak ukotven. Chybí tedy vymezení toho kdo, kdy, pro koho a jakým způsobem má cvičení zaměřená na kyberbezpečnost organizovat. Absence jasného legislativního podchycení cvičení představuje vzhledem k obsáhlým koncepčním závazkům v této oblasti slabé místo policy potírání ransomware, které je však s ohledem na praxi v oblasti cvičení jen méně závažné.

I přes absenci legislativního ukotvení otázky cvičení je tedy možné pozorovat značnou aktivitu ČR, zejména NÚKIB, směrem k organizaci, ale i účasti expertů na kyberbezpečnostních cvičeních. Na problematiku ransomware pak bylo jedním ze svých scénářů zaměřeno např. mezinárodní cvičení Cyber Coalition 2021 (NATO 2021), či další netechnická cvičení organizovaná NÚKIB (Anonymní zdroj č. 4 2022). Současnou praxi v oblasti cvičení tedy nelze označit za slabé místo policy boje proti ransomware.

E) Spolupráce se soukromým sektorem

Nutnost spolupráce se soukromým sektorem je koncepčními dokumenty ukotvena velice obsáhle. Věnují se jí zejména Národní strategie KB (NÚKIB 2020a) a Akční plán (NÚKIB 2021a). Tyto dokumenty hovoří o potřebě spolupráce se soukromým sektorem obecně, ale také více konkrétně např. směrem k zbudování již zmíněné platformy pro spolupráci s dobrovolníky či specifickým činnostem směrem k subjektům regulovaným dle ZKB. I v tomto případě zcela absentuje zmínka o potřebě spolupráce se soukromým sektorem směrem k potírání ransomware, nicméně

pokud budou analyzované závazky dostatečně naplňovány, nemělo by to představovat slabé místo policy.

Legislativní ukotvení spolupráce se soukromým sektorem je poměrně komplikované. ZKB sice uvádí, že NÚKIB spolupracuje s orgány a osobami působícími v oblasti kyberbezpečnosti, ale soukromý sektor explicitně nezmiňuje. V témže zákoně jsou nicméně ukotveny povinnosti specifických aktérů soukromého sektoru, které lze s určitou mírou abstrakce označit za spolupráci. Zákonem o PČR či Trestním řádem je pak ustanovena spolupráce PČR s právnickými a fyzickými osobami při plnění svých úkolů. Rozsah spolupráce FAÚ se soukromím sektorem je upraven Zákonem ML/FT. Spolupráce se soukromým sektorem vzhledem k regulovaným subjektům je legislativně ukotvena poměrně jasně. Skutečnost, že není explicitně legislativně ukotvena spolupráce s neregulovanými subjekty, nelze považovat za slabé místo zkoumané policy.

V praxi je alespoň dle dotazovaných Expertů (Sikora 2022; Švéda 2022; Anonymní zdroj č. 1 2022; Plecitý 2022) spolupráce se soukromým sektorem zavedena adekvátně vzhledem k potřebám. NÚKIB poskytuje metodickou a případně i praktickou pomoc povinným subjektům dle ZKB při řešení kyberbezpečnostních incidentů (Sikora 2022; Švéda 2022), přičemž spektrum těchto subjektů by se mělo v blízké době rozšířit. Mimo to NÚKIB nabízí další služby posilující spolupráci s regulovanými subjekty i ze soukromého sektoru, jako třeba penetrační testování (NÚKIB 2021g, 14). Se soukromým sektorem pak NÚKIB spolupracuje na přípravě legislativy či metodických materiálů, případně uzavírá memoranda či smlouvy o spolupráci (Švéda 2022). PČR se řídí ustanoveními Zákona o PČR či Trestního řádu (Anonymní zdroj č. 1 2022) a FAÚ dokonce i nad rámec Zákona ML/FT poskytoval a nadále ad hoc také poskytuje metodickou podporu osobám poskytujícím služby spojené

s virtuálními aktivy. Praktickou spolupráci se soukromým sektorem tedy nelze označit za slabé místo české policy potírání ransomware.

F) Sdílení informací

Závazky směrem ke sdílení informací jsou provázány se závazky směrem ke spolupráci. Specificky se této problematice věnuje Národní strategie KB (NÚKIB 2020a) a Akční plán (NÚKIB 2021a). ČR chce vytvořit národní platformu pro sdílení informací, zjednodušit nahlašování kyberbezpečnostních incidentů či vylepšit strategickou komunikaci směrem k národním partnerům i k široké veřejnosti. V tomto ohledu nicméně absentuje explicitní zmínění podpory sdílení informací mezi oběťmi kyberútoků, konkrétně pak ransomware, a kyberbezpečnostními autoritami či orgány vymáhajícími právo. To představuje poměrně závažné slabé místo koncepčního ukotvení policy. Jednotlivé typy ransomware často postihují více obětí, neboť se útočníci snaží maximalizovat zisk. Absence adekvátního systému sdílení informací o útocích (zejména s ohledem na subjekty, které nemají nahlašovací povinnost stanovenou zákonem) významně omezuje možnosti připravenosti celého systému na specifické útoky.

Jisté zakotvení cíle sdílení informací mezi oběťmi ransomwarových útoků, orgány vymáhajícími právo a kyberbezpečnostními autoritami lze identifikovat v ZKB, Zákoně o PČR, Zákoně ML/FT, ale také v Trestním zákoníku, případně i v Trestním řádu. V tomto ohledu se jeví jako nejdůležitější především vzájemné informování o kyberbezpečnostních incidentech. To jsou povinny činit pouze specifické subjekty stanovené ZKB, případně pak i další osoby ve specifických případech dle Trestního zákoníku. Všeobecná povinnost hlásit pokusy či úspěšné kyberútoky včetně ransomware však legislativně ukotvena není. Naopak NÚKIB má ze

zákona povinnost informovat veřejnost o specifických kyberbezpečnostních incidentech. Absence legislativního ukotvení všeobecné povinnosti sdílet informace o kyberútocích nicméně i dle názoru dotazovaných expertů (Anonymní zdroj č. 1 2022; Švéda 2022) nepředstavuje slabé místo policy boje proti ransomware.

Praxe sdílení informací pak v zásadě probíhá v rámci výše uvedených zákonů. Tento stav experti (Anonymní zdroj č. 1 2022; Sikora 2022; Plecitý 2022) vnímají jako adekvátní. Problematickým aspektem je zřejmě nejednoznačný výklad definice kyberbezpečnostních incidentů, přičemž Expert č. 6 (Švéda 2022) upozorňuje na příliš nízké počty hlášených incidentů vůči počtu regulovaných subjektů. Tuto situaci by však mohl pomoci napravit nově vydaný metodický dokument zaměřený na hlášení kyberbezpečnostních incidentů (NÚKIB 2022g). Tato skutečnost tedy představuje slabé místo policy, které však může být díky zmíněnému dokumentu brzy eliminováno.

G) Osvěta

Význam osvěty v oblasti kyberbezpečnosti je v ČR dostatečně koncepčně ukotven. Důležitost tohoto faktoru v budování odolnosti zmiňuje Bezpečnostní strategie (MZV ČR 2015a), Národní strategie KB (NÚKIB 2020a), Akční plán (NÚKIB 2021a) i Strategie prevence kriminality (MV ČR 2022). Osvěta je těmito dokumenty zmíněna jak směrem k pracovníkům státní správy, tak směrem k široké veřejnosti a to i s ohledem na její potenciál budovat důvěru mezi potenciálními oběťmi a státními institucemi. Skutečnost, že není explicitně zmíněna osvěta zaměřená na hrozbu ransomware nepředstavuje slabé místo národní policy, neboť povědomí o základech kyberhygieny působí jako prevence negativního působení v podstatě všech kyberbezpečnostních hrozeb.

Směrem k legislativnímu ukotvení osvětové činnosti v oblasti kyberbezpečnosti a tedy i budování odolnosti vůči ransomware, je ZKB stanoveno, že vzdělávání v oblasti kyberbezpečnosti zajišťuje NÚKIB. Osvětová činnost PČR je pak zmíněna jen směrem ke spolupráci s právnickými a fyzickými osobami, které se jí věnují. Absence detailnějšího ukotvení osvětové činnosti v legislativě ČR tedy představuje pouze méně závažné slabé místo policy potírání ransomware v ČR.

Získané informace týkající se osvětové činnosti v praxi naznačují, že zejména díky aktivitám NÚKIB je tato oblast budování odolnosti státu a jeho občanů vůči kyberbezpečnostním hrozbám poměrně dobře zajištěna. Vzdělávací a osvětové materiály jsou jednoduše přístupné všem, kteří o ně mají zájem. Zároveň je jejich spektrum dostatečně široké tak, aby se v něm našla téměř každá cílová skupina. V současnosti absentují pouze materiály zaměřené na velice zranitelnou skupinu seniorů, i tento nedostatek by však měl být do konce tohoto roku eliminován.[11] Absenci většího přímého adresování ransomware v osvětových projektech NÚKIB skvěle doplňuje projekt No More Ransom, (NoMoreRansom n.d.) na kterém se podílí NCOZ. Osvětová činnost zaměřená na kyberhygienu tedy nepředstavuje slabé místo praxe potírání ransomware v ČR.

H) Technická opatření

Co se posledního bodu kategorie resilience, tedy technických opatření týče, analyzované strategické VPD zmiňují jen velmi obecně potřebu budování odolných a bezpečných systémů, přičemž specifické technické požadavky, které by tyto systémy měly obsahovat zmíněny nejsou. Absence

[11] Do konce roku 2022 by měl být spuštěn e-learningový kurz zaměřený na seniory a měla by také proběhnout e-mailingová kampaň ve spolupráci s organizací SenSen zaměřená na základy kyberhygieny, na které se podílela i autorka této práce.

konkrétní zmínky o odhodlání ČR budovat či podporovat budování systémů na základě specifických technických opatření však nepředstavuje slabé místo koncepčního ukotvení zkoumané policy. Schopnosti ransomwarových útočníků se vyvíjejí s čímž souvisí i vývoj požadavků na technické zabezpečení systémů, což zdůrazňuje také Expert č. 3 (Sikora 2022). Jasná specifikace technických požadavků v koncepčních dokumentech by tedy mohla vzhledem k jejich poměrně dlouhé platnosti rychle zastarat a způsobovat zbytečný chaos.

Technická opatření jsou pak legislativně ukotvena zejména VKB, která se vztahuje na subjekty povinné dle ZKB. Dle Experta č. 3 (Sikora 2022) jsou tyto technické požadavky pro regulované subjekty adekvátní, mimo to téměř ve všech aspektech odpovídají, v některých dokonce převyšují ty, které zmiňuje Joint Statement (The White House 2021). Legislativní ukotvení požadavků na technická opatření tedy nepředstavuje slabé místo policy potírání ransomware v ČR.

Subjekty, které ZKB regulované nejsou se mohou dobrovolně řídit VKB, případně mohou najít oporu v Minimálním bezpečnostním standardu (NÚKIB, NAKIT and MV ČR 2020), nebo v dokumentu Ransomware: Doporučení pro mitigaci, prevenci a reakci (NÚKIB, AFCEA and NAKIT 2020), který je již zaměřen specificky na technická opatření budující odolnost proti ransomware. Za účelem prosazování dodržování technických opatření u povinných subjektů jsou pak NÚKIB uskutečňovány kontroly a audity. Vzhledem k dostupnosti těchto metodických materiálů a uskutečňované kontrolní činnosti nelze ani praxi prosazování základních technických opatření označit za slabé místo české policy boje proti ransomware, byť NÚKIB u regulovaných subjektů nachází určité nedostatky v jejich dodržování (NÚKIB 2021b, 28).

4.3.2 Nezákonné financování

A) Legalizace výnosů z ransomware

V kategorii nezákonného financování téměř úplně absentuje jakékoli koncepční ukotvení této problematiky. Pouze Koncepce boje proti OZ (MV ČR 2018) zmiňuje problematiku kryptoměn a to zejména ve vztahu k potřebě navyšování kapacit národních autorit za účelem negativní důsledky tohoto fenoménu řešit. Nedostatečné koncepční ukotvení nezákonného financování ransomware představuje závažné slabé místo, protože právě nelegálně získané finance z výkupného živí a dále motivují ransomwarové útočníky. Mimo to může absence koncepčního ukotvení národních cílů v této oblasti vyslat nežádoucí signál mezinárodním partnerům ČR.

Na rozdíl od koncepčního je legislativní ukotvení závazků v oblasti nezákonného financování poměrně adekvátní a nepředstavuje tedy slabé místo policy. Jediné, co není legislativou explicitně zmíněno, je závazek k navyšování kapacit národních autorit. Zákon ML/FT upravuje spolupráci mezi FAÚ a osobami poskytujícími služby spojené s virtuálními aktivy, tedy monitoring a reportování podezřelých aktivit. Náležitá péče zákazníků pak s jistou mírou abstrakce vyplývá z Trestního zákoníku. Expert č. 2 (Plecitý 2022) sice zmiňuje, že současná legislativa ve většině případů neumožňuje dosáhnout na osoby legalizující výnosy z trestné činnosti skrze peer-to-peer obchody, její změna v tomto směru by nicméně nemusela být zcela v souladu s demokratickými principy, na kterých si ČR zakládá.

Při praktické aplikaci opatření proti legalizaci výnosů z trestné činnosti, případně tedy i ransomware, probíhá spolupráce s osobami poskytujícími služby spojené s virtuálními aktivy zejména v regulích Zákona ML/FT. Spolupráce mezi FAÚ, NÚKIB a PČR je pak dle dotazovaných

Expertů (Plecitý 2022; Anonymní zdroj č. 1 2022) adekvátní, podobně jako spolupráce FAÚ se zahraničními institucemi. Problematickým bodem a tedy i slabým místem je zejména budování národních kapacit zaměřujících se na tuto problematiku, což však významně souvisí s již řešenou problematikou finančního a personálního zajištění boje proti ransomware.

B) Placení výkupného

Co se týče placení výkupného, tedy bodu, který není zmíněn Joint Statement (The White House 2021), ale představuje významnou otázku v boji proti ransomware, ani ten není na strategické úrovni koncepčně ukotven. Absence zmínky o odhodlání ČR neplatit výkupné, či o vedení svých občanů k neplacení výkupného, představuje další slabé místo koncepčního ukotvení policy.

V otázce legislativního ukotvení plateb výkupného je možné pouze konstatovat, že není explicitně kriminalizováno. Ve specifických případech lze nicméně tento akt klasifikovat dle ustanovení Trestního či Občanského zákoníku. Absenci explicitní kriminalizace placení výkupného ransomwarovým útočníkům nicméně nelze považovat za slabé místo policy potírání ransomware v ČR. Placení výkupného sice motivuje útočníky k dalšímu nelegálnímu chování a financuje jejich operace, avšak pokud zaplacení výkupného nenaplňuje trestní podstatu již vymezených trestných činů, byla by jeho kriminalizace excesivní a stát by musel zvažovat např. Expertem č. 1 (Anonymní zdroj č. 1 2022) zmíněné reparace.

V praxi tedy s největší pravděpodobností nedochází k postihu obětí v případě zaplacení výkupného. Prosazování neplacení výkupného je pak možné identifikovat třeba v dokumentu Ransomware: Doporučení pro mitigaci, prevenci a reakci (NÚKIB, AFCEA and NAKIT 2020, 14),

v osvětovém kurzu NÚKIB Dávej kyber! (Hájek n.d.) či v informacích uvedených na webových stránkách projektu No More Ransom (NoMoreRansom n.d.). Vzhledem k tomu, že snahu prosazovat neplacení výkupného je možno nalézt jak v metodických dokumentech, tak v osvětových projektech významných aktérů, nepředstavuje tento aspekt praxe policy potírání ransomware její slabé místo.

4.3.3 Vymáhání práva

A) Stíhání útočníků

Prvním bodem zmíněným v kategorii vymáhání práva je stíhání ransomwarových útočníků. Tento bod je nicméně analyzovanými koncepčními dokumenty ČR poměrně zanedbán. Národní strategie KB (NÚKIB 2020a) sice zmiňuje odhodlání potírat kyberkriminalitu, věnuje se však především problematice atribuce a o stíhání původců kyberkriminality na území ČR nehovoří. Akční plán (NÚKIB 2021a) pak zmiňuje také pouze snahu o zvýšení schopnosti atribuce. Naopak Koncepce boje proti OZ (MV ČR 2018) zmiňuje jen potřebu adaptace OČTŘ směrem k potírání kyberkriminality, ale ani ona explicitně nezmiňuje odhodlání ČR stíhat útočníky. Absence explicitně vyřčeného závazku stíhat kyberzločince a tedy i ransomwarové útočníky představuje zásadní slabé místo koncepčního ukotvení zkoumané policy.

V ČR je možnost stíhání ransomwarových útočníků působících na jejím území legislativně ukotvena adekvátně. Ransomware může naplňovat řadu skutkových podstat trestných činů dle Trestního zákoníku, na základě kterých mohou být ransomwaroví útočníci vyšetřováni a stíháni. Tato oblast tedy nepředstavuje slabé místo policy.

V praxi však vyvstává problém zejména s ohledem na Národní strategií KB (NÚKIB 2020a) zmíněnou atribuci, v důsledku čehož bývají

případy velmi často odkládány. Vyšetřování a stíhání ransomware stojí v cestě zejména dostupné anonymizační prostředky či nedosažitelnost zákona na peer-to-peer obchody v kryptoměnách (Anonymní zdroj č. 1 2022; Plecitý 2022). Dalším faktorem, který stojí v cestě stíhání ransomwarových útočníků je také nekonkurenceschopnost státní správy a orgánů vymáhajících právo na trhu práce. Vzhledem k tomu, že atribuce není pouze českým problémem, nelze ji vnímat jako slabé místo policy potírání ransomware v ČR. Slabým místem je nicméně omezený rozvoj orgánů vymáhajících právo zejména s ohledem na jejich personální zajištění, což je významným podílem spojeno s dříve identifikovanou nekonkurenceschopností státní správy či orgánů vymáhajících právo na trhu práce.

B) Spolupráce mezi významnými aktéry

Dalším bodem kategorie vymáhání práva je spolupráce mezi kyberbezpečnostními autoritami, finančními zpravodajskými jednotkami a orgány vymáhajícími právo na národní i mezinárodní úrovni. Tomuto bodu se věnuje Bezpečnostní strategie (MZV ČR 2015a), Národní strategie KB (NÚKIB 2020a), Akční plán (NÚKIB 2021a) i Koncepce boje proti OZ (MV ČR 2018). Na základě analyzovaných prohlášení v těchto dokumentech je zřejmé, že ČR je odhodlána podporovat spolupráci zmíněných institucí jak na národní, tak na mezinárodní úrovni. Tento bod je tedy v ČR dostatečně koncepčně ukotven a nepředstavuje tak slabé místo policy.

Spolupráce v oblasti vymáhání práva je legislativně ukotvena zejména ZKB, Zákonem o PČR a Zákonem ML/FT. Tyto normy upravují spolupráci jak na národní, tak na mezinárodní úrovni. Spolupráci na mezinárodní úrovni se dále věnuje také Zákon o mezinárodní justiční spolupráci ve věcech trestních. Legislativní ukotvení spolupráce na

mezinárodní úrovni je adekvátní, na národní úrovni je nicméně velmi obecné. Přesná forma spolupráce tedy významně závisí na pojetí jednotlivých aktérů. To lze označit za slabé místo policy, které úzce souvisí také s nejasným legislativním vymezením rolí jednotlivých aktérů.

V praxi probíhá spolupráce mezi zmíněnými aktéry na národní úrovni dle informací získaných od expertů (Plecitý 2022; Anonymní zdroj č. 1 2022; Sikora 2022) adekvátně a nepředstavuje tak slabé místo zkoumané policy. I rovinu mezinárodní spolupráce je pak možno hodnotit jako adekvátní. NÚKIB je součástí pracovních skupin na evropské i mezinárodní úrovni a účastní se na mezinárodním sdílení informací (Sikora 2022; NÚKIB 2021g, 26). PČR se podílí na aktivitách CEPOL, EUROPOL i INTERPOL, (Anonymní zdroj č. 1 2022). Vyzdvihnout lze zejména účast NCOZ na mezinárodní operaci eliminující jeden z nástrojů využívaný ransomwarovými útočníky (EUROPOL 2022b). FAÚ se směrem k mezinárodní spolupráci účastní zejména sdílení informací (Plecitý 2022).

4.3.4 Diplomacie

A) Eliminace ransomwarových útočišť, prosazování chování založeného na pravidlech a podpora dalších států

Poslední, avšak neméně důležitou kategorií zmíněnou v Joint Statement je diplomacie. Odhodlání využívat diplomacie pro zajišťování bezpečnostních zájmů ČR obecně je zmíněno už Bezpečnostní strategií (MZV ČR 2015a). Národní strategie KB (NÚKIB 2020a) dále zmiňuje závazek ke koordinaci postupu vůči kyberbezpečnostním hrozbám. V tomto smyslu je možné vnímat toto prohlášení i směrem k eliminaci ransomwarových útočišť, což však není explicitně zmíněno a lze tedy tento bod označit za méně závažné slabé místo koncepčního ukotvení policy.

Lépe je koncepčně ukotveno odhodlání ČR prosazovat chování států založené na pravidlech, což je reflektováno zejména v Akčním plánu (NÚKIB 2021a). Ten zmiňuje nejen samotný závazek k aktivní kybernetické diplomacii za účelem prosazování mezinárodního práva a dodržování nezávazných norem chování v kyberprostoru, ale také specifické cíle ČR s ohledem na její působení v mezinárodních organizacích. Tento bod tedy nepředstavuje slabé místo policy potírání ransomware v ČR.

Posledním bodem kategorie diplomacie je pobízení států k adresování ransomware na jejich území. V tomto směru ČR vyslovila zejména závazky pomoci zaostávajícím státům vybudovat odolný systém kyberbezpečnosti, který znesnadní využívání tamní infrastruktury kyberzločincům a ve svém důsledku tak posílí i bezpečnost kyberprostoru obecně. Tyto cíle jsou reflektovány v Národní strategii KB (NÚKIB 2021a) a Akčním plánu (NÚKIB 2021a). Odhodlání směřovat tyto snahy vůči adresování ransomware či kyberkriminality na území těchto států nicméně přímo zmíněno není. To představuje slabé místo policy, které však není ze své podstaty příliš závažné.

Legislativní ukotvení odhodlání ČR bojovat proti ransomware i v diplomatické rovině absentuje. Diplomatické styky jsou v ČR upraveny řadou samostatných zákonných předpisů, významným je však zejména Kompetenční zákon, který jako orgán zajišťující ochranu práv a zájmů ČR v zahraničí ustavuje MZV ČR. Budování kyberbezpečnostní odolnosti třetích států by pak mělo odpovídat ustanovením Zákona o zahraniční rozvojové spolupráci a humanitární pomoci. Tyto zákony však přímo nereflektují odhodlání ČR prosazovat na pravidlech založené chování států, pomáhat státům v adresování ransomware na jejich území či k redukci ransomwarových útočišť. Nicméně, vzhledem k tomu, že s určitou mírou abstrakce lze tyto cíle vnímat jako prosazování zájmů ČR v zahraničí,

nelze absenci jejich explicitního vyřčení v legislativě vnímat jako slabé místo policy.

Směrem k praxi diplomatického úsilí byly vzhledem k absenci expertních informací analyzovány pouze informace dostupné z otevřených zdrojů. Prosazování chování v kyberprostoru založené na pravidlech je možné zpozorovat zejména v Cyber Diplomacy Toolbox EU a jeho aplikaci v roce 2020, kdy došlo k uvalení sankcí i na některé osoby spojené s ransomware (Lenzu 2019; Lenzu 2020). Diplomatické akce s cílem eliminovat ransomwarová útočiště, do kterých by byla přímo zapojena také ČR se nepodařilo identifikovat. Budování kybernetické odolnosti zahraničních partnerů pak probíhá zejména skrze sdílení informací a zkušeností (NÚKIB 2021g, 26; NÚKIB 2018b; NÚKIB 2019b). Je tedy zřejmé, že ČR v tomto směru vyvíjí jisté aktivity, ty však nejsou příliš viditelné. Tento faktor tedy lze považovat za slabé místo policy potírání ransomware ČR.

4.3.5 Shrnutí slabých míst policy

S ohledem na identifikovaná slabá místa je možno konstatovat, že policy boje proti ransomware v ČR je nedostatečná zejména ve třech významných faktorech. Těmi jsou absence explicitního vymezení cílů policy potírání ransomware, její nedostatečné finanční zajištění a nekonkurenceschopnost státní správy a orgánů vymáhajících právo na vysoce kompetitivním trhu práce v oblasti kybernetické bezpečnosti, které je ovlivněno také neadekvátní legislativní úpravou.

Méně zásadní slabá místa zkoumané policy je možné identifikovat v legislativní úpravě, kde se jedná zejména o nejednoznačné vymezení rolí jednotlivých aktérů, s čímž souvisí také absence bližší specifikace spolupráce mezi těmito aktéry či jakékoli úpravy týkající se

kyberbezpečnostních cvičení. Mimo to lze za slabé místo označit i nespecifikování role všech institucí, které by se měly podílet na osvětových aktivitách, případně pak také absence bližšího vymezení formy, kterou by tyto aktivity měly mít.

V praktické rovině je možné kromě neadekvátních zdrojů a nekonkurenceschopnosti státní správy na trhu práce identifikovat slabé místo v oblasti sdílení informací, kde však již byly podniknuty kroky směřující k jeho nápravě. Mimo to je třeba upozornit také na malou dohledatelnost aktivit, které ČR provádí v diplomatické rovině boje proti ransomware. Shrnutí identifikovaných slabých míst je představeno v tabulce č. 2.

Tab. 2: Shrnutí identifikovaných slabých míst policy potírání ransomware v ČR (vlastní tabulka)

	Koncepční ukotvení	**Legislativní ukotvení**	**Praktická aplikace**
Resilience			
Jasná vládní struktura	Slabé místo	Slabé místo	Adekvátní
Adekvátní zdroje	Adekvátní	Slabé místo	Slabé místo
Personální zajištění	Adekvátní	Slabé místo	Slabé místo
Cvičení	Adekvátní	Slabé místo	Adekvátní
Spolupráce se soukromým sektorem	Adekvátní	Adekvátní	Adekvátní
Sdílení informací	Slabé místo	Adekvátní	Slabé místo
Osvěta	Adekvátní	Slabé místo	Adekvátní
Technická opatření	Adekvátní	Adekvátní	Adekvátní

	Koncepční ukotvení	**Legislativní ukotvení**	**Praktická aplikace**
Nezákonné financování			
Legalizace výnosů	Slabé místo	Adekvátní	Slabé místo
Placení výkupného	Slabé místo	Adekvátní	Adekvátní
Vymáhání práva			
Stíhání útočníků	Slabé místo	Adekvátní	Slabé místo
Spolupráce mezi významnými aktéry	Adekvátní	Slabé místo	Adekvátní
Diplomacie			
Eliminace ransomwarových útočišť	Slabé místo	Adekvátní	Slabé místo
Prosazování chování založeného na pravidlech	Adekvátní	Adekvátní	Adekvátní
Podpora dalších států	Slabé místo	Adekvátní	Slabé místo

4.4 Doporučení

V rámci této části práce budou představena doporučení, jejichž cílem je eliminovat slabá místa analyzované policy potírání ransomware v ČR. V tomto ohledu bude nejprve navrženo vytvoření samostatného koncepčního dokumentu, v němž ČR deklaruje odhodlání bojovat proti hrozbě ransomware ve všech bodech, ke kterým se zavázala v Joint Statement (The White House 2021). Dále bude navrženo vytvoření

ransomware dedikované webové stránky, která by tento dokument mohla doplňovat, případně sloužit jako jeho alternativa. Poté budou navržena opatření týkající se rozpočtového zajištění boje proti ransomware a zvýšení konkurenceschopnosti státní správy a orgánů vymáhajících právo na trhu práce v oblasti kyberbezpečnosti. Poslední část této kapitoly bude věnována doplňkovým doporučením, která se týkají identifikovaných slabých míst současné legislativní úpravy a praktické aplikace zkoumané policy.

4.4.1 Akční plán boje proti ransomware v ČR

Ransomware je původce nejzávažnějších kyberbezpečnostních incidentů v ČR (NÚKIB 2021b, 9). Tato hrozba často zasahuje pro stát a jeho občany stěžejní odvětví zdravotnictví či státní správy, kdy nejsou ohrožena pouze velmi citlivá data, ale v nejhorším případě také lidské životy. I přes tuto skutečnost však ČR nemá na národní úrovni explicitně vymezenou policy potírání ransomware. To i přes existenci obecnějších závazků suplujících absenci těch zacílených vůči ransomware představuje slabé místo zkoumané policy.

S ohledem na to, že ČR má řadu velice přesně zacílených koncepčních dokumentů jako je např. Národní strategie boje proti obchodování s lidmi (MV ČR 2020a), Vládní koncepce boje s korupcí (Úřad vlády ČR 2018) či Strategie prevence a potírání trestné činnosti související s odpady (MV ČR 2020b), by se samostatný koncepční dokument dedikovaný hrozbě ransomware nejevil jako neadekvátní. ČR by se bez podobného koncepčního dokumentu jistě obešla, zejména pokud by eliminovala identifikovaná slabá místa již existujících strategických VPD. I v tomto případě by nicméně vyvstal problém v důsledku roztříštěnosti závazků

do různých dokumentů, neboť ransomware je hrozbou, jejíž potírání si vyžaduje široké spektrum aktivit na mnoha úrovních.

V tomto směru by se mohla ČR inspirovat např. Austrálií. Australské Ministerstvo vnitra vydalo v říjnu roku 2021 koncepční dokument nazvaný Ransomware Action Plan (Department of Home Affairs 2021). V tomto dokumentu je představen ransomware jako zásadní hrozba australské národní bezpečnosti, která si žádá koordinovanou a rozhodnou akci (Department of Home Affairs 2021, 2-4). Dále jasně zmiňuje, že *„australská vláda neschvaluje placení výkupného kyberzločincům“* (Department of Home Affairs 2021, 5). Uvádí také konkrétní kroky a připravované změny v oblasti vymáhání práva, legislativy, osvěty, mezinárodní spolupráce a diplomacie, které australská vláda podniká či podnikne, aby co nejvíce ztížila operace ransomwarových útočníků na jejich území (Department of Home Affairs 2021, 6). Výsledná australská policy potírání ransomware je rozdělena do tři pilířů – připravenost a prevence, odpověď a zotavení, narušení a odstrašení, které jsou představeny na základě současných a připravovaných velice konkrétních opatření (Department of Home Affairs 2021, 7-9).

Australský Ransomware Action Plan (Department of Home Affairs 2021) je pojat tak, aby doplňoval již existující národní strategie, zejména v tom směru, že představuje již konkrétní současné či připravované kroky směrem k potírání ransomware. Toto pojetí by pak bylo ideální i v případě vytváření podobného českého dokumentu, jehož základem by se mohla stát aktuální Národní strategie KB (NÚKIB 2020a). Ta své strategické cíle člení také do tří pilířů – Sebevědomě v kyberprostoru, Silná a spolehlivá spojenectví, Odolná společnost 4.0.

V úvodní části navrhovaného Akčního plánu boje proti ransomware v ČR by bylo vhodné explicitně vymezit odhodlání ČR bojovat proti

ransomware a stíhat útočníky na národní i mezinárodní úrovni, představit ransomware jako hrozbu národní bezpečnosti a uvést, že ČR neschvaluje placení výkupného kyberzločincům. Tím by se eliminovalo slabé místo identifikované v koncepčním ukotvení odhodlání ČR stíhat ransomwarové útočníky i otázky placení výkupného. Zmíněním ransomware ve vztahu k virtuálním aktivům a jasné vyslovení odhodlání ČR bojovat proti kyberzločincům i v této rovině, by pak pomohlo eliminovat slabé místo koncepčního ukotvení legalizace výnosů z ransomware.

Dále by bylo na místě identifikovat všechny aktéry, kteří se na boji proti ransomware v ČR podílejí, tedy i včetně těch, kteří se věnují problematice legalizace výnosů z ransomware. Pokud by byly také jasně definovány jejich role a vzájemné vazby, podařilo by se tím eliminovat slabé místo, které v současnosti představuje nejasná vládní struktura. Mimo to by se také snížil význam dalšího identifikovaného slabého místa, tedy v legislativě nedostatečně definovaných rolí některých aktérů ve vztahu k zajišťování kyberbezpečnosti ČR.

V rámci prvního pilíře navrhovaného Akčního plánu by bylo vhodné zmínit současné i připravované kroky, které směřují k budování personálních, technických i dovednostních kapacit aktérů podílejících se na boji proti ransomware, a také kroky směřující k budování či prohlubování spolupráce a komunikace mezi těmito aktéry. Pomohlo by to snížit význam slabého místa nedostatečného legislativního ukotvení spolupráce mezi kyberbezpečnostními autoritami, orgány vymáhajícími právo a finančními zpravodajskými jednotkami. Vhodné by také bylo uvést cvičení, skrze která stát buduje odolnost vůči ransomware. Mimo to by bylo žádoucí definovat aktivity směřující k zabezpečení státní správy a regulovaných subjektů před ransomware a upozornit na doporučená

technická opatření, která jsou navržena za účelem prevence tohoto typu útoku.

Druhý pilíř by pak rozváděl mezinárodní a diplomatickou rovinu boje proti ransomware. Měl by tedy představit současné i připravované kroky směrem k mezinárodní spolupráci a sdílení informací mezi aktéry podílejícími se na boji proti ransomware, či kroky směřující k eliminaci ransomwarových útočišť, prosazování chování založeného na pravidlech v kyberprostoru, nebo aktivity ČR směřující k pomoci dalším státům v boji proti ransomware. Zejména v oblasti diplomacie by se tak podařilo eliminovat nejen slabá místa koncepčního ukotvení, ale částečně také její praktické aplikace, neboť by se tímto významně zviditelnily veškeré aktivity, které v tomto ohledu ČR koná.

Ve třetím pilíři by bylo vhodné uvést současné i plánované aktivity v oblasti osvěty a vzdělávání, a také aktivity týkající se spolupráce se soukromým sektorem a sdílení informací. V tomto směru zejména upozornit na možnost dobrovolného hlášení kyberbezpečnostních incidentů či možnosti spolupráce s národními aktéry na jejich řešení. Tím by se eliminovalo další ze slabých míst současného koncepčního ukotvení policy v oblasti sdílení informací.

Přiblížení současných i plánovaných aktivit směrem k potírání ransomware formou Akčního plánu boje proti ransomware v ČR by tedy bylo možné vnímat jako součást strategické komunikace směrem k budování pozitivního obrazu českých institucí doma i ve světě. Mimo to by však podobný dokument mohl posloužit jako inspirace či motivace pro další státy s ohledem na aktivity, kterými lze bojovat proti ransomware, čímž by mohl dále přispět k budování bezpečnějšího kyberprostoru.

4.4.2 Stopransomware.cz

Skvělým doplněním či alternativou navrhovaného Akčního plánu boje proti ransomware v ČR by se mohla stát potírání ransomware dedikovaná webová stránka po vzoru USA. Na stránce Stopransomware.gov (CISA n.d.) je možné nalézt základní informace o hrozbě ransomware, jak se před ní chránit, jaké aktivity vyvíjí USA v boji proti ransomware a jaké služby nabízí svým občanům. Významným aspektem je pak možnost přímo na této stránce nahlásit případy ransomwarových útoků.

Je nutné poznamenat, že v ČR již existuje velice podobná stránka, která je napojena na projekt No More Ransom (NoMoreRansom n.d.). Svým obsahem je však oproti Stopransomware.gov (CISA n.d.) omezenější. Navrhovaná webová stránka by mohla obsahovat deklaraci odhodlání ČR bojovat proti ransomware a výzvu k neplacení výkupného. Dále také představení této hrozby a veškerých aktivit, které směrem k jejímu potírání ČR vykonává jak na národní, tak na mezinárodní úrovni. Na stránce by mohly být zveřejňovány aktuální varování, doporučení a návody týkající se ransomware, např. i včetně technických opatření. Webová stránka by samozřejmě obsahovala také osvětové materiály týkající se ransomware včetně odkazů na již zmíněné existují e-learningové kurzy a také na webovou stránku projektu No More Ransom (NoMoreRansom n.d.), kde se nachází dostupné dešifrovací klíče pro známé typy ransomware včetně návodů k jejich použití. Významným aspektem Stopransomware.cz by byla možnost online nahlášení incidentů spojených s ransomware pro regulované i neregulované subjekty. Této možnosti by předcházely informace o následném postupu a možnostech spolupráce s kyberbezpečnostními autoritami a orgány vymáhajícími právo při řešení ransomwarových útoků.

Vytvořením této webové stránky by se nepodařilo zcela eliminovat nedostatky analyzované policy v oblasti jejího koncepčního ukotvení, avšak jejich význam by se významně snížil zejména díky jasné deklaraci záměru bojovat proti ransomware a představením aktuálních či připravovaných iniciativ ČR v této oblasti. Nástroj umožňující online nahlašování ransomwarových útoků by přispěl k efektivnímu sdílení informací ze strany ZKB regulovaných i neregulovaných subjektů a napomohl by tak eliminovat slabé místo praktické aplikace současné policy, tedy dle Experta č. 6 (Švéda 2022) jen velmi omezeného nahlašování kyberbezpečnostních incidentů, které nejspíš neodráží reálný stav věci. Usnadnění nahlašování incidentů by mohlo zvýšit počet takovýchto hlášení, což by díky větší dostupnosti informací o aktuálních hrozbách značně přispělo připravenosti dalších institucí na probíhající ransomwarové kampaně.

4.4.3 Rozpočet na kyberbezpečnost

Dalším významným nedostatkem české policy potírání ransomware je neadekvátní rozpočtové zajištění oblasti kyberbezpečnosti obecně. Dle dat zveřejněných NÚKIB se státní správa v minulých letech potýkala s nedostatkem finančních prostředků určených k zajišťování kyberbezpečnosti (NÚKIB 2021b, 3; NÚKIB 2020b, 2; NÚKIB 2019a, 27). V roce 2020 pak dokonce 43 % subjektů sledovaných NÚKIB zaznamenalo meziroční pokles v rozpočtovém zajištění této oblasti.[12] Problematické finanční zajištění svých institucí pak přiznali také Experti č. 1 z NCOZ (Anonymní zdroj č. 1 2022) či Expert č. 2 z FAÚ (Plecitý 2022). Prvním,

[12] Data za rok 2021 nebyla prozatím zveřejněna.

velice obecným doporučením je tedy samozřejmě navýšit investice státu do rozpočtů aktérů, kteří se podílejí na boji proti ransomware.

Vzhledem k současnému negativnímu vývoji národní ekonomiky, která významně utrpěla jak v důsledku pandemie COVID-19, tak kvůli současné krizi na Ukrajině, nelze výrazné navyšování rozpočtů na kyberbezpečnost očekávat. I proto je třeba upozornit na skutečnost, že jsou za současného rozpočtového nastavení výdaje na kyberbezpečnost jen omezeně koordinované a je náročné monitorovat, zda jsou vynakládány dostatečně efektivně. Na tuto skutečnost upozorňuje NKÚ (2020b, 16) přičemž uvádí, že stát *„neměl v průběhu kontrolovaného období informace o celkové výši peněžních prostředků vynakládaných jednotlivými kapitolami státního rozpočtu"* na kyberbezpečnost. Za kontrolované období 2015 až 2020 sice NKÚ (2020b, 14) neidentifikoval nehospodárnost u výdajů na kyberbezpečnost, i přesto však současný systém považuje za nedostatečný (NKÚ 2020b, 5) a směrem k jeho vylepšení upozorňuje na centrálně řízený rozpočet Velké Británie (NKÚ 2020b, 16).

Ve Velké Británii představují prostředky určené na naplňování národní kyberbezpečnostní strategie samostatnou položku státního rozpočtu (NKÚ 2020b; Her Majesty's Treasury 2021, 129) pod kontrolou Úřadu vlády (Committee of Public Accounts 2019, 4). Výdaje dalších orgánů na kyberbezpečnost jsou dále vykazovány samostatně (Her Majesty's Treasury 2021). Ve Velké Británii je tedy nejen jasně stanoveno, jaké prostředky státního rozpočtu jsou vyhrazeny na naplňování cílů tamní kyberbezpečnostní strategie, ale také jsou veškeré do kyberbezpečnosti investované prostředky státní pokladny jasně vykazovány (Her Majesty's Treasury 2021). To pak umožňuje monitorovat a koordinovat výdaje.

V případě, že by se ČR rozhodla inspirovat britským přístupem by bylo nutno v první řadě ustanovit, kdo bude za tento rozpočet zodpovídat. Jako adekvátní volba by se v tomto případě jevil NÚKIB, neboť dle ZKB zodpovídá za kyberbezpečnost ČR. Tato změna by byla jistě spojena s dalšími náklady zejména směrem k zajištění adekvátní personální základny za účelem koordinace a monitoringu vynakládaných zdrojů. I přes tyto výdaje by nicméně úprava současného rozpočtového zajištění umožnila přesnější monitoring výdajů, který by následně mohl pomoci identifikovat místa vyžadující zvýšení investic, stejně jako místa, kde není v současnosti s dostupnými prostředky nakládáno efektivně. Vědomí o těchto rozpočtových aspektech by ČR umožnilo investovat a průběžně redistribuovat své v současnosti omezené zdroje tak, aby mohla efektivně dosahovat svých strategických cílů v oblasti kyberbezpečnosti, případně i konkrétně v boji proti ransomware.

4.4.4 Mzdová tabulka pro kyberbezpečnostní specialisty

Jako jedno z nejvýznamnějších slabých míst policy boje proti ransomware je možno označit nekonkurenceschopnost státní správy a orgánů vymáhajících právo na vysoce kompetitivním trhu práce v oblasti kyberbezpečnosti, což značně brání rozvoji těchto institucí. Dle Joint Statement (The White House 2021) je expertní základna stěžejním aspektem boje proti ransomware. PČR nicméně celkově chybí více než pět tisíc policistů (ČT24 2022; Lánský 2022) a pozice vyžadující si specializaci na IT se dlouhodobě nedaří obsazovat (Anonymní zdroj č. 1 2022). NÚKIB plánuje do roku 2027 navýšit svou personální základnu téměř dvojnásobně (NÚKIB 2021g, 41), avšak dle slov Experta č. 5 (Anonymní zdroj č. 3 2022) v ČR není žádným způsobem usilováno o konkurenceschopnost státní správy na trhu práce v této oblasti. O potřebě výrazně navýšit platy

v NÚKIB pak hovořil již v roce 2019 jeho tehdejší ředitel Dušan Navrátil (2019).

Nekonkurenceschopnost státní správy a orgánů vymáhajících právo významně souvisí s nedostatečným rozpočtovým zajištěním oblasti, vyplývá však také ze současného legislativního ukotvení platových poměrů ve státní správě či v orgánech vymáhajících právo.

Aby se tedy nemusela státní správa a orgány vymáhající právo dle slov Experta č. 1 (Anonymní zdroj č. 1 2022) spoléhat na *„vlastenecké cítění,"* jako jeden z faktorů přispívající jejich konkurenceschopnosti na trhu práce, bylo by vhodné přizpůsobit tabulkové platy platovým poměrům v soukromém sektoru, které jsou často i více než dvojnásobné[13] (Platy.cz n.d.). Vytvoření samostatné tabulky, případně speciální platové třídy v rámci současných tabulek, by i dle Experta č. 5 (Anonymní zdroj č. 3 2022) napomohlo zvýšení konkurenceschopnosti státní správy či orgánů vymáhajících právo na trhu práce. Dále by bylo samozřejmě nutné tabulkové platy pravidelně aktualizovat, aby v případě úspěšného náboru nedocházelo v důsledku nerespektování vývoje pracovního trhu do budoucna ke ztrátě již etablované pracovní síly, tedy i k návratu do současného nevyhovujícího stavu.

[13] Pro ilustraci NÚKIB nabízí plat ve 13. platové třídě tabulky č. 1 Nařízení vlády o platových poměrech zaměstnanců ve veřejných službách a správě, kde plat do 1 roku praxe činí 33 750 Kč a při praxi nad 32 let 49 920 Kč. K platu je následně přičten příplatek za bezpečnostní prověrku a případné osobní ohodnocení. Rozpočtovaný průměrný plat v NÚKIB pak v roce 2020 činil de Vypořádání připomínek k ZKB 52 401 Kč. Dle serveru Platy.cz se nicméně plat v kategorii informačních technologií u 90 % pozic pohybuje okolo 90 000 Kč (Platy cz. n.d.).

4.4.5 Doplňková doporučení

Prozatím jen okrajově adresovaným slabým místem policy potírání ransomware je nejasné legislativní ukotvení vládní struktury. V tomto ohledu by bylo vhodné legislativně jasně definovat role a vzájemné vazby jednotlivých institucí podílejících se na zajišťování kyberbezpečnosti a boji s kyberkriminalitou buďto v jim příslušných právních předpisech, nebo v ZKB.

Toto opatření by pomohlo vyřešit také další identifikované slabé místo legislativního ukotvení policy, tedy příliš obecné definování spolupráce mezi kyberbezpečnostními autoritami, orgány vymáhajícími právo a finančními zpravodajskými jednotkami. Je třeba, aby tato úprava legislativy vycházela z praxe, v rámci které spolupráce funguje alespoň dle dotazovaných expertů adekvátně (Plecitý 2022; Anonymní zdroj č. 1 2022; Sikora 2022). Případné změny je tedy nutné konzultovat s dotčenými aktéry a zohlednit jejich preference a potřeby.

Mimo to by zmíněné opatření pomohlo eliminovat i slabé místo legislativního ukotvení policy identifikované v oblasti osvěty. Ta je podobně jako spolupráce legislativně ukotvena pouze okrajově. Jasné definování toho, kteří aktéři a jakým způsobem se podílejí na osvětových aktivitách, případně také pro koho mají být osvětové aktivity určeny, by jen podpořilo současnou praxi, v níž lze zpozorovat značné úsilí tuto oblast dále rozvíjet.

Na jasnější legislativní vymezení rolí aktérů podílejících se na boji proti kyberkriminalitě, potažmo na zajišťování kyberbezpečnosti, by přímo navazovalo také legislativní ukotvení cvičení, které prozatím absentuje. Zákon by měl obsahovat vymezení aktérů připravujících a organizujících cvičení, aktérů s povinností se cvičení účastnit a také vymezení

formy a frekvence cvičení, jakožto jednoho z významných nástrojů budování kybernetické odolnosti státu.

5 Závěr

Ransomwarové útoky představují pro bezpečnost ČR jednu z nejzávažnějších kybernetických hrozeb. V ČR však prozatím absentuje jasná a explicitně vyřčená policy zaměřená na její potírání. Na mezinárodní úrovni se nicméně při setkání Counter Ransomware Initiative zorganizovaného Národní bezpečnostní radou Bílého domu ve dnech 13. a 14. října 2021 ČR zavázala k naplňování konkrétních cílů představených Joint Statement. Diplomová práce tedy usilovala o zjištění, zda je ČR schopna dostát vyřčeným závazkům, kde se nachází slabá místa její policy na národní úrovni a jakým způsobem je možné tato slabá místa eliminovat. Vzhledem k důrazu Joint Statement (The White House 2021) na potřebu jasného koncepčního a legislativního rámce bylo středem zájmu analýzy zejména koncepční a legislativní ukotvení policy. Žádná policy však nemá smysl bez aplikace v praxi, která se stala dalších předmětem analýzy.

V první řadě bylo zkoumáno, zda je policy potírání ransomware v ČR v souladu se závazky vyslovenými v Joint Statement (The White House 2021), tedy jak je v koncepčních dokumentech ČR vymezena policy potírání ransomware, jak je ukotvena v legislativě a jaké praktické kroky v tomto ohledu ČR činí. V tomto směru bylo zjištěno, že byť na národní úrovni absentuje jasné vyřčení cílů ČR v boji proti ransomware, koncepční závazky, legislativní ustanovení a aktivity povětšinou obecnějšího charakteru na mnoha úrovních odpovídají těm vyřčeným v Joint Statement (The White House 2021).

Podařilo se nicméně identifikovat také slabá místa, která bude muset ČR eliminovat, aby mohla skutečně účinně bojovat proti ransomware. Prozatím absentuje jakékoli jasné koncepční či legislativní vymezení vládní struktury, tedy rolí jednotlivých aktérů v boji proti

ransomware. Na to navazuje v legislativě neukotvená otázka cvičení, jen okrajově ukotvená problematika vzdělávání a osvěty, nebo také absence formalizace spolupráce mezi kyberbezpečnostními autoritami, orgány vymáhajícími právo a finančními zpravodajskými jednotkami.

Zásadní problém pak představuje nedostatečné finanční zajištění kyberbezpečnosti obecně, které je umocněno skutečností, že prostředky na kyberbezpečnost a potírání kyberkriminality jsou zahrnuty do rozpočtových kapitol jednotlivých aktérů a na centrální úrovni panuje o jejich výši či vynakládání s nimi jen omezený přehled. Tento problém významně souvisí se zajišťováním odborného personálu, který není za současných legislativních ani rozpočtových podmínek možno adekvátně odměňovat, v důsledku čehož jsou státní správa a orgány vymáhající právo zcela nekonkurenceschopné na trhu práce.

Absence koncepčního ukotvení potírání legalizace výnosů z ransomware, otázky placení výkupného či dokonce chybějící explicitní vyřčení odhodlání bojovat proti ransomwarovým útočníkům patří mezi další identifikovaná slabá místa zkoumané policy. K těm dále patří také absence koncepčního ukotvení odhodlání ČR diplomaticky usilovat o eliminaci ransomwarových útočišť, či podporovat další státy v boji proti ransomware, přičemž i praktická aplikace těchto závazků, zejména směrem k jejich nízké viditelnosti, představuje slabé místo policy potírání ransomware v ČR.

S cílem eliminovat uvedená slabá místa byla v práci taktéž představena doporučení. Vytvořením Akčního plánu boje proti ransomware v ČR by se eliminovaly všechny nedostatky aktuálního koncepčního ukotvení problematiky a snížil by se význam některých legislativních slabých míst. Alternativou či doplněním Akčního plánu boje proti ransomware v ČR by mohla být webová stránka Stopransomware.cz, která by

obsahovala varování, doporučení, osvětové materiály a aktuální informace týkající se ransomware. Mimo to by usnadnila sdílení informací mezi kyberbezpečnostními autoritami, orgány vymáhajícími právo a oběťmi útoků, neboť by nabízela možnost jednoduše online nahlásit případný incident. Dalším doporučením byla navržena alternativa k současnému rozpočtovému zajišťování kybernetické bezpečnosti, tedy vytvoření samostatné rozpočtové kapitoly pod centrální kontrolou, která by usnadnila monitoring a koordinaci vynakládaných prostředků. Směrem k eliminaci nekonkurenceschopnosti státní správy a orgánů vymáhajících právo bylo navrženo vytvoření specifické platové tabulky či třídy určené pro specialisty na kyberbezpečnost.

Navrženými doplňkovými doporučeními jsou jasné legislativní vymezení rolí aktérů v oblasti kyberbezpečnosti a potírání kyberkriminality, jejich vzájemné spolupráce, a také role v oblasti cvičení a osvěty.

V případě aplikace zmíněných doporučení by ČR nejen napravila existující slabá místa své současné policy potírání ransomware, ale také vyslala pozitivní signál významným aktérům, široké veřejnosti i mezinárodním partnerům, že svou roli v boji proti ransomware bere vážně a mohou se na ni spolehnout.

Diplomová práce tedy představila koncepční, legislativní i praktické ukotvení policy potírání ransomware v ČR, čímž poskytla výchozí bod pro tvůrce a vykonavatele této policy směrem k její úpravě vedoucí k možné větší efektivitě a srozumitelnosti. Vzhledem k prozatímní absenci akademických prací zaměřujících se na toto téma v prostředí ČR, může práce taktéž představovat výchozí bod pro další výzkum buďto směrem k detailnější analýze jednotlivých aspektů policy, nebo třeba směrem k její komparaci vůči podobným politikám jiných států.

Použité zdroje

1. AEC. 2017. „Ransomware Locky v září masivně útočil ve světě i v ČR.“ *Antivirus.cz,* October 18, 2017. https://www.antivirus.cz/Blog/Stranky/ransomware-locky-v-zari-masivne-utocil-ve-svete-i-v-cr.aspx.

2. Anderson, James I. 2003. *Public Policymaking: An Introduction.* Boston: Houghton Mifflin Company.

3. Anonymní zdroj č. 1. 2022. [Interview]. E-mail, May 20, 2022. Přepis rozhovoru se nachází v příloze A této práce.

4. Anonymní zdroj č. 2. 2022. [Interview]. E-mail, May 10, 2022. Přepis rozhovoru se nachází v příloze D této práce.

5. Anonymní zdroj č. 3. 2022. [Interview]. E-mail, May 10, 2022. Přepis rozhovoru se nachází v příloze E této práce.

6. Anonymní zdroj č. 4. 2022. [Interview]. E-mail, May 25, 2022. Přepis rozhovoru se nachází v příloze G této práce.

7. Avast Threat Labs. 2021. „Nemocnice pod náporem hackerů: Jak proběhly nejznámější kyberútoky na české nemocnice?“ *Avast,* April 29, 2021. https://blog.avast.com/cs/nemocnice-pod-naporem-hackeru-jak-probihaji-kyberutoky-na-ceske-nemocnice.

8. Baker, Kurt. 2022a. „Ransomware as a Service (RaaS) Explained.“ *Crowdstrike,* February 7, 2022. https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/.

9. Baker, Kurt. 2022b. „What Is Ransomware?“ *Crowdstrike,* March 15, 2022. https://www.crowdstrike.com/cybersecurity-101/ransomware/.

10. Beblavý, Miroslav ed. 2002. *Manuál pre tvorbu verejnej politiky.* Bratislava: SGI. https://www.governance.sk/wp-content/uploads/2016/10/Manual.pdf.

11. Belcic, Ivan. 2021. „What is CryptoLocker Ransomware and How to Remove It.“ *Avast,* December 17, 2021. https://www.avast.com/c-cryptolocker.

12. Belcic, Ivan. 2022. „What Is Petya Ransomware, and Why Is It So Dangerous?“ *Avast,* April 30, 2022. https://www.avast.com/c-petya.

13. Bičíková, Zuzana. 2022. „Sophos: Téměř osm z deseti českých organizací zasáhl ransomware.“ ChannelWorld, April 27, 2022. https://www.channelworld.cz/clanky/sophos-temer-osm-z-deseti-ceskych-organizaci-zasahl-ransomware/.

14. Birkland, Thomas A. 2015. *An Introduction to the Policy Process: Theories, Concepts, and Models of Public Policy Making*. New York: Routledge.

15. Bogner, Alexander, and Wolfgang Menz. 2009. „The Theory-Generating Expert Interview: Epistemological Interest, Forms of Knowledge, Interaction.“ In *Interviewing Experts,* edited by Alexander Bogner, Beate Littig and Wolfgang Menz, 43-80. London: Palgrave Macmillan.

16. Bolton, Scott. 2020. „Remove KOLZ Ransomware (Virus Removal Guide).“ *Geek's Advice,* September 22, 2020. https://geeksadvice.com/remove-kolz-ransomware-virus/.

17. Burgess, Matt. 2018. „The Rise of SamSam, the Hacker Group Shutting Down Entire Cities.“ *Wired,* August 1, 2018. https://www.wired.co.uk/article/samsam-ransomware.

18. Burgess, Matt. 2022. „The Workaday Life of the World's Most Dangerous Ransomware Gang.“ *Wired,* March 16, 2022. https://www.wired.com/story/conti-leaks-ransomware-work-life/.

19. Centrum kybernetické bezpečnosti. 2021. *Kyberpohádky.* https://www.kybercentrum.cz/data/kyberpoh%C3%A1dky-cz-nahled.pdf.

20. Cimpanu, Catalin. 2019. „Another Ransomware Strain Is Now Stealing Data Before Encrypting It.“ *ZDNet,* December 18, 2019. https://www.zdnet.com/article/another-ransomware-strain-is-now-stealing-data-before-encrypting-it/.

21. CISA. n.d. *Stopransomware.goc.* Accessed May 29, 2022. https://www.cisa.gov/stopransomware.

22. Clancy, Molly. 2021. „The True Cost of Ransomware.“ *Blackblaze,* September 9, 2021. https://www.backblaze.com/blog/the-true-cost-of-ransomware/.

23. Cluley, Graham. 2020. „Maze Ransomware – What You Need to Know.“ *Tripwire,* April 23, 2020. https://www.tripwire.com/state-of-security/featured/maze-ransomware-what-you-need-to-know/.

24. Cluley, Graham. 2022. „REvil reborn? Notorious Gang's Dark Web Site Redirects to New Ransomware Operation.“ *Tripwire,* April 21, 2022. https://www.tripwire.com/state-of-security/security-data-protection/revil-dark-web-site-redirects-new-ransomware-operation/.

25. Committee of Public Accounts. 2019. *Cyber Security in the UK. Ninenty-Ninth Report of Session 2017-19.* https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/1745/1745.pdf.

26. CSIRT.CZ. 2017. „Historie a vývoj ransomwaru: všechno to začalo s AIDS.“ *Lupa.cz,* July 20, 2017. https://www.lupa.cz/clanky/historie-a-vyvoj-ransomwaru-vsechno-to-zacalo-s-aids/.

27. ČBA. 2021. „Kyberkampaň: Cílem hackera můžete být i vy!“ July 12, 2021. https://cbaonline.cz/kyberkampan-cilem-hackera-muzete-byt-i-vy.

28. ČEPS. n.d. „O společnosti.“ Accessed May 27, 2022. https://www.ceps.cz/cs/o-spolecnosti.

29. ČT24. 2020. „Místo počítače tužka a papír. Po kyberútoku v brněnské nemocnici stále nefungují všechny systémy.“ *Česká televize,* May 21, 2020. https://ct24.ceskatelevize.cz/regiony/3102416-misto-pocitace-tuzka-a-papir-po-kyberutoku-v-brnenske-nemocnici-stale-nefunguji.

30. ČT24. 2021. „Vyděračský program Avaddon napadl šedesát institucí v Česku i zahraničí. Útočí i na veškeré zálohy.“ *Česká televize,* April 28, 2021. https://ct24.ceskatelevize.cz/domaci/3304441-vyderacsky-program-avaddon-napadl-sedesat-instituci-v-cesku-i-zahranici-utoci-i-na.

31. ČT24. 2022. „V Česku chybí tisíce policistů. Noví zájemci o práci ve sboru často nezvládnou psychotesty.“ *Česká televize,* January 16, 2022. https://ct24.ceskatelevize.cz/domaci/3428342-v-cesku-chybi-tisice-policistu-novi-zajemci-o-praci-ve-sboru-casto-nezvladnou.

32. ČTK. 2018. „Za obřím kyberútokem NotPetya stojí ruská armáda, tvrdí USA.“ *Lidovky.cz,* February 2, 2018. https://www.lidovky.cz/svet/za-kyberutok-notpetya-muze-ruska-armada-tvrdi-usa.A180216_072258_ln_zahranici_ele.

33. ČTK. 2022a. „Vyděračské programy loni napadly 77 procent tuzemských firem, velká část zaplatila výkupné.“ *Globe24.cz,* May 18, 2022. https://globe24.cz/byznys/vyderacske-programy-loni-napadly-77-procent-tuzemskych-firem-velka-cast-zaplatila-vykupne.4d9dcf36.

34. ČTK. 2022b. „NÚKIB: Kyberútok na weby ŘSD byl profesionální, zašifroval data.“ *České noviny,* May 20, 2022. https://www.ceske-noviny.cz/zpravy/nukib-kyberutok-na-weby-rsd-byl-profesio-nalni-zasifroval-data/2208924.

35. ČTK. 2022c. „ŘSD se bude z kyberútoku vzpamatovávat měsíce, škody jsou velké, řekl šéf společnosti Radek Mátl.“ *iROZHLAS,* May 23, 2022. https://www.irozhlas.cz/zpravy-domov/rsd-ky-berutok-reditel-matl_2205231628_cen.

36. Davis, Joseph. 2021. „What is Human-Operated Ransomware, and How Does It Differ from Traditional Ransomware?“ *Micro-soft in Bussiness Blogs,* June 22, 2021. https://cloudblogs.micro-soft.com/industry-blog/microsoft-in-business/he-alth/2021/06/22/what-is-human-operated-ransomware-and-how-does-it-differ-from-traditional-ransomware/.

37. De Souza, Tristan. 2020. „Ransomware Operators Now Publicly Leaking Victim Data.“ *Cyjax,* March 3, 2020. https://www.cyjax.com/2020/03/03/ransomware-operators-now-publicly-leaking-victim-data/.

38. De, Nikhilesh. 2021. „Ransomware Payments in 2021 Already Dwarf Last Year’s Total, FinCEN Reports.“ *CoinDesk,* October 15, 2021. https://www.coindesk.com/policy/2021/10/15/ranso-mware-payments-in-2021-already-dwarfs-last-years-total-fin-cen-reports/.

39. Déčko. 2020. „Datová Lhota. V počítači to žije!“ https://decko.ceskatelevize.cz/datova-lhota.

40. Department of Home Affairs. 2021. *Ransomware Action Plan.* https://www.homeaffairs.gov.au/cyber-security-subsite/files/ransomware-action-plan.pdf.

41. DiMaggio, Jon. 2021a. „Ransomware Gangs Move Toward Efficient Self-Automated Attacks." *Analyst1,* April 30, 2021. https://analyst1.com/blog/ransomware-gangs-move-toward-efficient-self-automated-attacks.

42. DiMaggio, Jon. 2021b. „Ransom Mafia – Analysis of the World's First Ransomware Cartel." *Analyst1,* April 7, 2021. https://analyst1.com/blog/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel.

43. DiMaggio, Jon. 2022. *The Art of Cyberwarfare: An Investigator's Guide to Espionage, Ransomware, and Organized Cybercrime.* San Francisco: No Starch Press.

44. Dinu, Cezarina. 2021. „Ryuk Ransomware Now Self-Spreads to Other Windows LAN Devices." *Heimdal Security,* March 1, 2021. https://heimdalsecurity.com/blog/ryuk-ransomware-spreads-to-other-windows-lan-devices/.

45. Disman, M. 2002. *Jak se vyrábí sociologická znalost*. Příručka pro uživatele. Praha: Nakladatelství Karolinum.

46. Dossett, Julian. 2021. „A Timeline of the Biggest Ransomware Attacks: Bitcoin and Other Cryptocurrencies Have Become a Key Tool in Online Crime." *Cnet,* November 15, 2021. https://www.cnet.com/personal-finance/crypto/a-timeline-of-the-biggest-ransomware-attacks/.

47. Dunn, William N. 2018. *Public Policy Analysis: An Integrated Approach.* New York: Routledge.

48. Dye, Thomas R. 2013. *Understanding Public Policy.* Boston: Pearson.

49. Enserink, Bert, Koppenjan, Joop F. M., and Igor S. Mayer. 2013. „A Policy Sciences View on Policy Analysis." In *Public Policy Analysis: New Developments,* edited by Wil A. H. Thissen and Warren E. Walker, 11-40. New York: Springer.

50. ESET. 2016. „Škodlivé přílohy e-mailu ohrožují české uživatele." *Notebook.cz,* June 28, 2016. https://notebook.cz/clanky/tiskova-zprava/2016/0628-eset-malware.

51. European Comission. n.d. „Cybercrime." Accessed May 22, 2022. https://ec.europa.eu/home-affairs/policies/internal-security/cybercrime_en.

52. EUROPOL. 2021a. „Five Affiliates to Sodonikibi/REvil Unplugged." November 8, 2021. https://www.europol.europa.eu/media-press/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged.

53. EUROPOL. 2021b. „Twelve Targeted for Involvement in Ransomware Attacks Against Critical Infrastructure." October 29, 2021. https://www.europol.europa.eu/media-press/newsroom/news/12-targeted-for-involvement-in-ransomware-attacks-against-critical-infrastructure.

54. EUROPOL. 2021c. „Ransomware Gang Arrested in Ukraine with Europol's Support." October 4, 2021. https://www.europol.europa.eu/media-press/newsroom/news/ransomware-gang-arrested-in-ukraine-europol%E2%80%99s-support.

55. EUROPOL. 2022a. „EU Policy Cycle – EMPACT." January 20, 2022. https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact.

56. EUROPOL. 2022b. „Unhappy New Year for Cybercriminals as VPNLab.net Goes Offline." January 18, 2022. https://www.europol.europa.eu/media-press/newsroom/news/unhappy-new-year-for-cybercriminals-vpnlabnet-goes-offline.

57. EUROPOL. n.d. „Defining Serious and Organised Crime." Accessed May 27, 2022. https://www.europol.europa.eu/socta/2017/defining-serious-and-organised-crime.html.

58. Evropská komise. 2020. „Nová Strategie kybernetické bezpečnosti EU a nová pravidla pro větší odolnost fyzických a digitálních kritických subjektů – Otázky a odpovědi." December 16, 2020. https://ec.europa.eu/commission/presscorner/detail/cs/qanda_20_2392.

59. Fadilpasic, Sead. 2020. „Sodinokibi Ransomware Data Available for Purchase on Hacking Forum." *IRProPortal,* March 20, 2020. https://www.itproportal.com/news/sodinokibi-ransomware-data-available-for-purchase-on-hacking-forum/.

60. FAÚ. 2021. *Analýza případů zneužití virtuálních aktiv k ML/FT za rok 2020.* https://www.financnianalytickyurad.cz/files/analyza-pripadu-zneuziti-virtualnich-aktiv-k-ml-ft-za-rok-2020.pdf.

61. Fiala, Petr and Klaus Schubert. 2000. *Moderní analýza politiky: Uvedení do teorií a metod policy analysis*. Praha: Barrister & Principal.

62. Finckenauer, James O. 2005. „Problems Of Definition: What Is Organized Crime?" *Trends in Organized Crime* 8, no. 3, 63-83. https://link.springer.com/content/pdf/10.1007/s12117-005-1038-4.pdf.

63. Fišer, Miloslav. 2022. „Hackerským útokům čelily v Česku nemocnice, Národní knihovna či volební web." *Novinky.cz,* April 21, 2022. https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/hackerskym-utokum-celily-v-cesku-nemocnice-narodni-knihovna-ci-volebni-web-40394428.

64. Flick, Uwe. 2009. *An Introduction to Qualitative Research.* London: SAGE.

65. Foldyna, Tomáš. 2021. *Zpráva o činnosti národního korespondenta pro boj proti kybernetické kriminalitě, pro ochranu práv k nehmotným statkům a kybernetickou bezpečnost za rok 2020.* Brno, February 11, 2021. https://verejnazaloba.cz/wp-content/uploads/2021/06/Kyberkrimi_2020.pdf.

66. Freed, Anthony M. 2021. „A Brief History of Ransomware Evolution." *Cybereason,* November 30, 2021. https://www.cybereason.com/blog/a-brief-history-of-ransomware-evolution.

67. Friedrich, Carl J. 1963. *Man and His Government.* New York: McGraw-Hill.

68. Glover, Claudia. 2021. „Meet the Ransomware Gangs Fuelling a Global Cybercrime Spree.“ *Tech Monitor,* June 28, 2021. https://techmonitor.ai/technology/cybersecurity/top-ten-ransomware-gangs-fuelling-the-global-cybercrime-spree.

69. Greenberg, Andy. 2018. „The Untold Story of NotPetya, the Most Devastating Cyberattack in History.“ *Wired,* August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

70. Grimes, Roger A. 2021. *Ransomware Protection Playbook.* Hoboken: Wiley & Sons.

71. Hagan, Frank E. 2006. „Organized Crime and organized crime: Indeterminate Problems of Definition.“ *Trends in Organized Crime* 9, no. 4, 127-137. https://link.springer.com/content/pdf/10.1007/s12117-006-1017-4.pdf.

72. Hájek, Martin. n.d. „Dávej kyber! Náš on-line kurz základů kybernetické bezpečnosti.“ *NÚKIB.* Accessed May 22, 2022. https://osveta.nukib.cz/course/view.php?id=67.

73. Haller, Martin. 2020. „Jak mohli hackeři napadnout Povodí Vltavy? Průzkum dle OSINT.“ *Lupa.cz,* April 30, 2020. https://www.lupa.cz/clanky/jak-mohli-hackeri-napadnout-povodi-vltavy-pruzkum-dle-osint/.

74. Hassan, Nihad A. 2019. *Ransomware Revealed: A Beginner's Guide to Protecting and Recovering from Ransomware Attacks.* Berkeley: Apress.

75. Heclo, Hugh. 1972. „Policy Analysis." *British Journal of Political Science* 2, no. 1 (January): 83-108. https://www.jstor.org/stable/193311.

76. Heinemeyer, Max. 2020. „Darktrace's Cyber AI Analyst Investigates Sodinokibi (REvil) Ransomware." *Darktrace Blog,* November 30, 2020. https://www.darktrace.com/en/blog/darktraces-cyber-ai-analyst-investigates-sodinokibi-r-evil-ransomware/?utm_source=youtube&utm_medium=social.

77. Hejtman, Libor. 2022. „Kybernetický útok na Magistrát města Olomouce odložen." *Policie České republiky,* February 17, 2022. https://www.policie.cz/clanek/kyberneticky-utok-na-magistrat-mesta-olomouce-odlozen.aspx.

78. Hendl, Jan. 2005. *Kvalitativní výzkum: Základní metody a aplikace.* Praha: Portál.

79. Her Majesty's Treasury. 2021. *Autumn Budget and Spending Review 2021. A Stronger Economy for the British People.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1043688/Budget_AB2021_Print.pdf.

80. Houser, Pavel. 2017. „Ransomware Locky v září masivně útočil ve světě i v ČR.“ *IT Biz,* October 19, 2017. https://www.it-biz.cz/zpravicky/ransomware-locky-v-zari-masivne-utocil-ve-svete-i-v-cr.

81. Hung, Gabriel, and Margarette Joven. 2017. „Petys's Master Boot Record Infection.“ *Fortinet,* July 9, 2017. https://www.fortinet.com/blog/threat-research/petya-s-master-boot-record-infection.

82. Checkmal. 2017. „CzechoSlovak Ransomware (.ENCR / Version Czech).“ *Checkmal,* March 20, 2017. https://www.checkmal.com/video/read/351/.

83. INTERPOL. n.d.a. „Cybercrime Collaboration Services. Secure Information-Sharing Platforms for Law Enforcement and Partners.“ Accessed May 23, 2022. https://www.interpol.int/Crimes/Cybercrime/Cybercrime-Collaboration-Services.

84. INTERPOL. n.d.b. „Czech Republic. How INTERPOL Supports Czech Republic To Tackle International Crime.“ Accessed May 23, 2022. https://www.interpol.int/Who-we-are/Member-countries/Europe/CZECH-REPUBLIC.

85. Janofsky, Adam. 2022. „Ransomware Victims Paid More Than $600 million to Cybercriminals in 2021.“ *The Record,* February 10, 2022. https://therecord.media/ransomware-victims-paid-more-than-600-million-to-cybercriminals-in-2021/.

86. Javers, Eamon. 2021. „Here's the Hacking Group Responsible for the Colonial Pipeline Shutdown." *CNBC,* May 10, 2021. https://www.cnbc.com/2021/05/10/hacking-group-darkside-reportedly-responsible-for-colonial-pipeline-shutdown.html.

87. Jenkins, William I. 1978. *Policy Analysis: A Political and Organizational Perspective.* New York: St. Martin's Press.

88. Jenkins-Smith, Hank C. 1990. *Democratic Politics and Policy Analysis.* Pacific Grove: Brooks/Cole Publishing.

89. Jirásek, Petr, Novák, Luděk, and Josef Požár. 2013. *Výkladový slovník kybernetické bezpečnosti: Cyber Security Glossary.* Praha: Policejní akademie ČR v Praze. https://afcea.cz/wp-content/uploads/2015/03/Slovnik_Final_screen_v2_0.pdf.

90. Jírovský, Václav. 2007. *Kybernetická bezpečnost nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada.

91. Jones, David. 2022. „Ransomware Attacks, Payouts Soared Worldwide in 2021: Report." *Cybersecurity Dive,* April 27, 2022. https://www.cybersecuritydive.com/news/ransomware-attacks-payouts-2021/622784/.

92. Kalátová, Barbora, and Háta Sassmanová. 2017. „Masivní kybernetický útok zasáhl i počítače v Česku. Otázky a odpovědi o viru WannaCry." *Seznam Zprávy,* May 13, 2017. https://www.seznamzpravy.cz/clanek/masivni-kyberneticky-utok-zasahl-i-pocitace-v-cesku-otazky-a-odpovedi-o-viru-wannacry-31382.

93. Kasík, Pavel. 2017a. „Zákeřný ransomware útočí cíleně na Čechy. Láká na fakturu v příloze.“ *iDNES.cz,* April 7, 2017. https://www.idnes.cz/technet/kratke-zpravy/ransomware-cryptolock-crypt0l0ck-cesko-makro.A170407_160258_tec-kratke-zpravy_pka.

94. Kasík, Pavel. 2017b. „Ruská média a ukrajinská města zasáhl vyděračský červ Bad Rabbit.“ *iDNES.cz,* October 25, 2017. https://www.idnes.cz/technet/kratke-zpravy/ransomware-bad-rabbit.A171025_161325_tec-kratke-zpravy_pka.

95. Klement, Petr. 2020. *Zpráva o činnosti národního korespondenta pro boj proti kybernetické kriminalitě, pro ochranu práv k nehmotným statkům a kybernetickou bezpečnost za rok 2019.* Brno, January 29, 2020. https://verejnazaloba.cz/wp-content/uploads/2020/06/NK_kyberkriminalita.pdf.

96. Kolouch, Jan, Bašta, Pavel, Kropáčová, Andrea and Martin Kunc. 2019. *Cybersecurity.* Praha: CZ.NIC. https://knihy.nic.cz/files/edice/cybersecurity.pdf.

97. Kraft, Michael E., and Scott R. Furlong. 2017. *Public Policy: Politics, Analysis, and Alternatives.* Thousand Oaks: CQ Press.

98. Křoustek, Jakub. 2017. „Ransomware Crypt0L0cker intenzivně cílí i na Českou republiku.“ *Avast,* April 7, 2017. https://blog.avast.com/cs/ransomware-crypt0l0cker-intenzivne-c%C3%ADli-i-na-ceskou-republiku.

99. Laffan, Kieran. 2015. „A Brief History of Ransomware.“ *Varonis,* November 10, 2015. https://www.varonis.com/blog/a-brief-history-of-ransomware.

100. Lánský, Tomáš. 2022. „Chybí pět a půl tisíce policistů, slučují se služebny. Starostové obcí se zlobí.“ *iDNES.cz,* May 16, 2022. https://www.idnes.cz/zpravy/domaci/policie-nedostatek-policistu-kraje-sluzebny-maturita-problem-plat.A220515_211144_domaci_albe.

101. Lasswell, Harold D., and Abraham Kaplan. 1970. *Power and Society.* New Haven: Yale University Press.

102. Lawler, Richard. 2021. „Kaseya Ransomware Attackers Demand $70 Million, Claim They Infected Over a Million Devices.“ *The Verge,* July 5, 2021. https://www.theverge.com/2021/7/5/22564054/ransomware-revil-kaseya-coop.

103. Lenzu, Maria Daniela. 2019. „Cyber-Attacks: Council Is Now Ables to Impose Sanctions.“ *Council of the European Union,* May 17, 2019. https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/.

104. Lenzu, Maria Daniela. 2020. „EU Imposes the First Ever Sanctions Against Cyber-Attacks.“ July 30, 2020. https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/.

105. Liska, Allan, and Timothy, Gallo. 2016. *Ransomware: Defending Against Digital Extortion.* Sebastopol: O'Reilly Media.

106. MacRae, Duncan Jr. 1979. „Concepts and Methods of Policy Analysis." *Society* 16, September-October, 17-23. https://doi.org/10.1007/BF02694518.

107. Magdoňová, Jana. 2020. „Na nemocnici v Benešově útočil ruský virus Ryuk. Jermanová odmítá, že by někdo požadoval výkupné." *iROZHLAS,* January 14, 2020. https://www.irozhlas.cz/zpravy-domov/nemocnice-benesov-kyberneticky-utok-ransomware-vykupne-ochrana-osobnich-udaju_2001140615_cha.

108. Magdoňová, Jana. 2021. „Olomoucký magistrát čelí několik týdnů hackerským útokům. Odmítá zaplatit výkupné." *iROZHLAS,* May 22, 2021. https://www.policie.cz/clanek/kyberneticky-utok-na-magistrat-mesta-olomouce-odlozen.aspx.

109. Malecki, Edward J. 2007. „Cities and Regions Competing in the Global Economy: Knowledge and Local Development Policies. *Environment and Planning C: Government and Policy* 25, no. 5 (October 2007): 638–54. https://doi.org/10.1068/c0645.

110. Mareš, Miroslav. 2002a. „Bezpečnost." In *Česká bezpečnostní terminologie: Výklad základních pojmů,* edited by Petr Zeman. Brno: Ústav strategických studií Vojenské akademie v Brně. https://moodle.unob.cz/plugin-file.php/11277/course/section/3043/%C4%8Cesk%C3%A1%20bezpe%C4%8Dnostn%C3%AD%20terminologie.pdf.

111. Mareš, Miroslav. 2002b. „Národní bezpečnost.“ In *Česká bezpečnostní terminologie: Výklad základních pojmů,* edited by Petr Zeman. Brno: Ústav strategických studií Vojenské akademie v Brně. https://moodle.unob.cz/pluginfile.php/11277/course/section/3043/%C4%8Cesk%C3%A1%20bezpe%C4%8Dnostn%C3%AD%20terminologie.pdf.

112. Mazal, Jakub. 2020. „Rozsáhlý útok ransomware RYUK na české firmy. Odborná analýza útoku.“ *Comguard,* February 11, 2020. https://www.comguard.cz/blog/ransomware-ryuk-utok-na-okd.

113. Miller, Lawrence. 2017. *Ransomware Defence for Dummies.* Hoboken: John Wiley & Sons.

114. Minařík, David. 2017. „JScript Ransomware RPG.“ *Computer Incident Response Capability,* February 3, 2017. https://www.nukib.cz/download/hrozby/JScript_Ransomware_RPG.pdf.

115. Muncaster, Phil. 2022. „Ransomware Payments Hit Record Highs in 2021.“ *InfoSecurity,* March 23, 2022. https://www.infosecurity-magazine.com/news/ransomware-payments-hit-record/.

116. MV ČR. 2018. *Koncepce boje proti organizovanému zločinu do roku 2023.* https://www.mvcr.cz/soubor/koncepce-boje-proti-organizovanemu-zlocinu-do-roku-2023.aspx.

117. MV ČR. 2020a. *Národní strategie boje proti obchodování s lidmi v České republice na období 2020-2023.* Praha. https://www.mvcr.cz/soubor/narodni-strategie-boje-proti-obchodovani-s-lidmi-v-cr-na-obdobi-2020-2023-pdf.aspx.

118. MV ČR. 2020b. *Strategie prevence a potírání trestné činnosti související s odpady na období let 2021-2023.* https://www.mvcr.cz/soubor/strategie-prevence-a-potirani-trestne-cinnosti-souvisejici-s-odpady-na-obdobi-let-2021-2023.aspx.

119. MV ČR. 2022. *Strategie prevence kriminality v České republice na léta 2022-2027.* https://www.mvcr.cz/soubor/01-spk-2022-2027-strategie-pk-pdf.aspx.

120. MZV ČR. 2015a. *Bezpečnostní strategie České republiky 2015.* https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf.

121. MZV ČR. 2015b. *Koncepce zahraniční politiky České republiky.* https://www.mzv.cz/file/1565920/Koncepce_zahranicni_politiky_CR.pdf.

122. MZV ČR. 2017. *Strategie zahraniční rozvojové spolupráce 2018-2030.* http://www.czechaid.cz/wp-content/uploads/2016/09/Strategie_ZRS_CR_2018-2030.pdf.

123. Nair, Prajeet. 2021. „StrRAT Masquerades as Ransomware.“ *Bank Info Security,* May 21, 2021. https://www.bankinfosecurity.com/strrat-masquerades-as-ransomware-a-16725.

124. Nařízení vlády č. 304/2014 Sb., o platových poměrech státních zaměstnanců.

125. Nařízení vlády č. 341/2017 Sb., o platových poměrech zaměstnanců ve veřejných službách a správě.

126. Nařízení vlády č. 532/2021 Sb., kterým se stanoví stupnice základních tarifů pro příslušníky bezpečnostních sborů.

127. Nařízení vlády č. 59/2015 Sb., o služebních tarifech a o zvláštním příplatku pro vojáky z povolání.

128. NATO. 2021a. „Brussels Summit Communiqué." June 14, 2021. https://www.nato.int/cps/en/natohq/news_185000.htm?selectedLocale=en.

129. NATO. 2021b. „NATO's Flagship Cyber Defence Exercise Kicks Off In Estonia." November 30, 2021. https://www.nato.int/cps/en/natohq/news_189156.htm?selectedLocale=en.

130. Navrátil, Dušan. 2019. „Platové podmínky máme devastující, hrozí nám zánik, varuje šéf kyberúřadu." Interview by Jan Horák. *Aktuálně.cz,* October 31, 2019. https://zpravy.aktualne.cz/domaci/nukib-platy-navratil/r~ea64d43cfbd611e9ac60ac1f6b220ee8/.

131. NBÚ. 2016. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2015.* https://www.nukib.cz/download/publikace/zpravy_o_stavu/zprava-o-stavu-kyberneticke-bezpecnosti-cr-2015.pdf.

132. NBÚ. 2017. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2016.* https://www.nukib.cz/download/publikace/zpravy_o_stavu/zprava-o-stavu-kyberneticke-bezpecnosti-cr-2016.pdf.

133. NCKB. 2013. *Bezpečnostní incidenty prosinec 2013.* Brno: GovCERT. https://www.govcert.cz/download/bulletiny/container-nodeid-846/nckb-bulletin-1312.pdf.

134. NCKB. 2015. *Bezpečnostní incidenty leden 2015.* Brno: GovCERT. https://www.govcert.cz/download/bulletiny/container-nodeid-1047/nckb-bulletin-1501.pdf.

135. NCKB. 2016a. *Bezpečnostní incidenty červen 2016.* Brno: GovCERT. https://www.govcert.cz/download/bulletiny/container-nodeid-643/nckb-bulletin-1606.pdf.

136. NCKB. 2016b. *Bezpečnostní incidenty listopad 2016.* https://www.govcert.cz/download/bulletiny/bezpecnost-listopad-2016/NCKB-Bulletin-1611.pdf.

137. Neuberger, Anne. 2021. „Update on the International Counter-Ransomware Initiative.“ *U.S. Department of State,* October 15, 2021. https://www.state.gov/briefings-foreign-press-centers/update-on-the-international-counter-ransomware-initiative.

138. NKÚ. 2020a. „Kybernetická bezpečnost v ČR: Stát má před sebou řadu výzev. Jejich podceňování může mít v budoucnu vážné dopady.“ November 2, 2020. https://www.nku.cz/cz/pro-media/tiskove-zpravy/kyberneticka-bezpecnost-v-cr:-stat-ma-pred-sebou-radu-vyzev--jejich-podcenovani-muze-mit-v-budoucnu-vazne-dopady-id11523/.

139. NKÚ. 2020b. *Kontrolní závěr z kontrolní akce 19/26 Budování kybernetické bezpečnosti České republiky.* https://www.nku.cz/assets/kon-zavery/k19026.pdf.

140. NoMoreRansom. n.d. „O projektu.“ Accessed May 22, 2022. https://www.nomoreransom.org/cs/about-the-project.html.

141. Novinky. 2015. „Vyděračský virus požaduje výkupné v Bitcoinech.“ *Novinky.ct,* January 22, 2015. https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/vyderacsky-virus-pozaduje-vykupne-v-bitcoinech-269973.

142. Novinky. 2016. „Nebezpečný virus se maskuje za fotku na Facebooku. Šíří se i v Česku.“ *Novinky.cz,* November 22, 2016. https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/nebezpecny-virus-se-maskuje-za-fotku-na-facebooku-siri-se-i-v-cesku-40015712.

143. Novinky. 2017. „První ransomware existoval už v roce 1989. Největší neplechu způsobil WannaCry.“ *Novinky.cz,* June 28, 2017. https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/prvni-ransomware-existoval-uz-v-roce-1989-nejvetsi-neplechu-zpusobil-wannacry-40038257.

144. NSZ. 2020. *Zpráva o činnosti státního zastupitelství za rok 2019.* Brrno, June 15, 2020. https://verejnazaloba.cz/wp-content/uploads/2020/06/Zprava-o-cinnosti-SZ-za-rok-2019-textova-cast.pdf.

145. NSZ. 2021. *Zpráva o činnosti státního zastupitelství za rok 2020.* Brno, June 15, 2021. https://verejnazaloba.cz/wp-content/uploads/2021/06/Zpr%C3%A1va_o_%C4%8Dinnosti_SZ_za_rok_2020_textov%C3%A1_%C4%8D%C3%A1st.pdf.

146. Nuce, Jordan, Kennelly, Jeremy, Goody, Kimberly, Moore, Andrew, Rahman, Alyssa, Williams, Matt, McKeague, Brendan, and Jared Wilson. 2021. „Shining a Light on DARKSIDE Ransomware Operations.“ *Mandiant,* May 11, 2021. https://www.mandiant.com/resources/shining-a-light-on-darkside-ransomware-operations.

147. NÚKIB (@petr.vytrzny). n.d.i. Accessed May 22, 2022. https://www.instagram.com/petr.vytrzny/?hl=cs.

148. NÚKIB, AFCEA and MV ČR. 2020. *Minimální bezpečnostní standard.* July 17, 2020. https://www.nukib.cz/download/publikace/podpurne_materialy/2020-07-17_Minimalni-bezpecnostni-standard_v1.0.pdf.

149. NÚKIB, AFCEA and NAKIT. 2020. *Ransomware: Doporučení pro mitigaci, prevenci a reakci.* https://www.nukib.cz/download/publikace/podpurne_materialy/Ransomware%20-%20Doporuceni_pro_mitigaci_prevenci_a_reakci.pdf.

150. NÚKIB. 2018a. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2017.* https://www.nukib.cz/download/publikace/zpravy_o_stavu/zprava-o-stavu-kyberneticke-bezpecnosti-cr-2017.pdf.

151. NÚKIB. 2018b. „Experti z ČR na Africa Endeavor 2018." August 7, 2018. https://www.nukib.cz/cs/infoservis/aktuality/1473-experti-z-cr-na-africa-endeavor-2018/.

152. NÚKIB. 2019a. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2018.* https://www.nukib.cz/download/publikace/zpravy_o_stavu/zprava-o-stavu-kyberneticke-bezpecnosti-cr-2018-cz.pdf.

153. NÚKIB. 2019b. „Zástupci 43 zemí Africké unie čelili cvičným kybernetickým útokům pod dohledem expertů z NÚKIB." August 29, 2019. https://nukib.cz/cs/infoservis/aktuality/1366-zastupci-43-zemi-africke-unie-celili-cvicnym-kybernetickym-utokum-pod-dohledem-expertu-z-nukib/.

154. NÚKIB. 2020a. *Národní strategie kybernetické bezpečnosti České republiky na období let 2021 - 2025.* https://www.nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf.

155. NÚKIB. 2020b. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019.* https://www.nukib.cz/download/publikace/zpravy_o_stavu/NUKIB_ZSKB_2019.pdf.

156. NÚKIB. 2020c. „Festival bezpečného internetu 2020.“ July 17, 2020. https://nukib.cz/cs/infoservis/aktuality/1620-festival-bezpecneho-internetu-2020/.

157. NÚKIB. 2021a. *Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025.* https://www.nukib.cz/download/publikace/strategie_akcni_plany/akcni_plan_2021-2025.pdf.

158. NÚKIB. 2021b. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020.* https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf.

159. NÚKIB. 2021c. *Kybernetické incidenty pohledem NÚKIB Červenec 2021.* https://www.nukib.cz/download/publikace/vyzkum/Kyberneticke_incidenty_2021-07.pdf.

160. NÚKIB. 2021d. *Kybernetické incidenty pohledem NÚKIB Říjen 2021.* https://nukib.cz/download/publikace/vyzkum/Kyberneticke_incidenty_2021-10.pdf.

161. NÚKIB. 2021e. *Kybernetické incidenty pohledem NÚKIB Listopad 2021.* https://www.nukib.cz/download/publikace/vyzkum/kyberneticke_incidenty_listopad_2021.pdf.

162. NÚKIB. 2021f. *Kybernetické incidenty pohledem NÚKIB Prosinec 2021.* https://www.nukib.cz/download/publikace/vyzkum/Kyberneticke_incidenty_prosinec_2021.pdf.

163. NÚKIB. 2021g. *Koncepce rozvoje Národního úřadu pro kybernetickou a informační bezpečnost 2020.* January 11, 2021. https://www.nukib.cz/download/publikace/strategie_akcni_plany/Koncepce_rozvoje_NUKIB.pdf.

164. NÚKIB. 2021h. „Health Czech." Facebook, April 4, 2021. https://www.facebook.com/watch/?v=257153579665158.

165. NÚKIB. 2021i. „Proběhlo cvičení kybernetické bezpečnosti pro strategické firmy obranného průmyslu." May 20, 2021. https://nukib.cz/cs/infoservis/aktuality/1715-probehlo-cviceni-kyberneticke-bezpecnosti-pro-strategicke-firmy-obranneho-prumyslu/.

166. NÚKIB. 2021j. „Dosud největší cvičení ČEPS a NÚKIB prověřilo, jak by energetici zvládli kyberútok." June 7, 2021. https://nukib.cz/cs/infoservis/aktuality/1721-dosud-nejvetsi-cviceni-ceps-a-nukib-proverilo-jak-by-energetici-zvladli-kyberutok/.

167. NÚKIB. 2022a. *Kybernetické incidenty pohledem NÚKIB Leden 2022.* https://www.nukib.cz/download/publikace/vyzkum/2022-01_Kyberneticke_incidenty_leden.pdf.

168. NÚKIB. 2022b. *Kybernetické incidenty pohledem NÚKIB Únor 2022.* https://www.nukib.cz/download/publikace/vyzkum/2022-02_Kyberneticke_incidenty.pdf.

169. NÚKIB. 2022c. *Kybernetické incidenty pohledem NÚKIB Březen 2022.* https://www.nukib.cz/download/publikace/vyzkum/2022-03_Kyberneticke_incidenty.pdf.

170. NÚKIB. 2022d. *Kybernetické incidenty pohledem NÚKIB Duben 2022.* https://www.nukib.cz/download/publikace/vyzkum/2022-04_Kyberneticke_incidenty.pdf.

171. NÚKIB. 2022e. „NÚKIB vyzývá odbornou veřejnost k zasílání návrhů na změny zákona č. 181/2014 Sb., o kybernetické bezpečnosti.“ April 14, 2022. https://www.nukib.cz/cs/infoservis/aktuality/1831-nukib-vyzyva-odbornou-verejnost-k-zasilani-navrhu-na-zmeny-zakona-c-181-2014-sb-o-kyberneticke-bezpecnosti/.

172. NÚKIB. 2022f. „Bankéři a kybernetičtí odborníci se dohodli na spolupráci.“ February 8, 2022. https://nukib.cz/cs/infoservis/aktuality/1802-bankeri-a-kyberneticti-odbornici-se-dohodli-na-spolupraci/.

173. NÚKIB. 2022g. *Hlášení kybernetického bezpečnostního incidentu.* February 21, 2022. https://www.nukib.cz/download/publikace/podpurne_materialy/2022-02-21_Metodika-hlaseni-incidentu_1.0.pdf.

174. NÚKIB. n.d.a. „O úřadu.“ Accessed May 22, 2022. https://www.nukib.cz/cs/o-nukib/o-uradu/.

175. NÚKIB. n.d.b. „Typy cvičení.“ Accessed May 22, 2022. https://nukib.cz/cs/kyberneticka-bezpecnost/cviceni/typy-cviceni/.

176. NÚKIB. n.d.c. „Návody.“ Accessed May 22, 2022. https://www.nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/navody/.

177. NÚKIB. n.d.d. „Vystavené dokumenty.“ Accessed May 22, 2022. https://www.nukib.cz/cs/uredni-deska/.

178. NÚKIB. n.d.e. „Analýzy a Souhrnné zprávy.“ Accessed May 22, 2022. https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/analyzy/.

179. NÚKIB. n.d.f. „Zprávy o stavu.“ Accessed May 22, 2022. https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/.

180. NÚKIB. n.d.g. „Jsem netvor.“ Accessed May 22, 2022. https://osveta.nukib.cz/netvor-domu#uvod.

181. NÚKIB. n.d.h. „Nabízené kurzy.“ Accessed May 22, 2022. https://osveta.nukib.cz/local/dashboard/.

182. NÚKIB. n.d.j. „Festival bezpečného internetu.“ Accessed May 22, 2022. https://osveta.nukib.cz/enrol/index.php?id=111.

183. Palmer, Danny. 2022. „Ransomware Gangs Are Changing Their Tactics. That Could Prove Very Expensive For Some Victims.“ *ZD Net,* February 7, 2022. https://www.zdnet.com/article/ransomware-gangs-are-changing-their-tactics-that-could-prove-very-expensive-for-some-victims/.

184. Patterson, 2021. „The World’s Top Ransomware Gangs Have Created a Cybercrime Cartel.“ *CBS News,* July 22, 2021. https://www.cbsnews.com/news/ransomware-cybercrime-cartel-wizard-spider-viking-spider-lockbit-twisted-spider/.

185. Patton, Carl V., and David S. Sawicki. 1993. *Basic Methods of Policy Analysis and Planning.* Upper Saddle River: Prentice Hall.

186. Patton, Carl V., Sawicki, David S., and Jennifer J. Clark. 2016. *Basic Methods of Policy Analysis and Planning.* New York: Routledge.

187. PČR. 2016. „Co je organizovaný zločin.“ July 31, 2016. https://www.policie.cz/clanek/co-je-organizovany-zlocin.aspx.

188. Pennings, Paul, Keman, Hans, and Jan Kleinnijenhuis. 2006. *Doing Research in Political Science: An Introduction to Comparative Methods and Statistics.* London: SAGE.

189. Petcu, Alina Georgiana. 2020. „Kolz Ransomware 101: The STOP Djvu Variant to Watch Out For.“ *Heimdal Security,* September 30, 2020. https://heimdalsecurity.com/blog/kolz-ransomware/.

190. Phoha, Vir V. 2002. *Internet Security Dictionary.* New York: Springer.

191. Platy.cz. n.d. „Platy v kategorii: Informační technologie.“ Accessed May 29, 2022. https://www.platy.cz/platy/informacni-technologie.

192. Plecitý, David. 2022. [Interview]. Praha, May 11, 2022. Přepis rozhovoru se nachází v příloze B této práce.

193. Rámcové rozhodnutí Rady 2008/841/SVV ze dne 24. října 2008 o boji proti organizované trestné činnosti.

194. Randáková, Růžena. 2017. „Úspěšný projekt No More Ransom je nově v češtině.“ *Policie České republiky,* July 26, 2017. https://www.policie.cz/clanek/archiv-zpravodajstvi-zpravodajstvi-2017-uspesny-projekt-no-more-ransom-je-nove-v-cestine.aspx.

195. Raybould, Brett. 2022. „A Ransomware Outlook for 2022.“ *InfoSecurity,* February 2, 2022. https://www.infosecurity-magazine.com/blogs/ransomware-outlook-2022/.

196. Reichel, Jiří. 2009. *Kapitoly metodologie sociálních výzkumů.* Praha: Grada.

197. Roddie, Megan. 2021. „LockBit 2.0: Ransomware Attacks Surge After Successful Affiliate Recruitment.“ *Security Intelligence,* September 9, 2021. https://securityintelligence.com/posts/lockbit-ransomware-attacks-surge-affiliate-recruitment/.

198. Romo, Vanessa. 2021. „How A New Team of Feds Hacked The Hackers And Got Colonial Pipeline’s Ransom Back.“ *NPR,* June 8, 2021. https://www.npr.org/2021/06/08/1004223000/how-a-new-team-of-feds-hacked-the-hackers-and-got-colonial-pipelines-bitcoin-bac?t=1653041067947.

199. Rosencrance, Linda. 2021. „Definition: WannaCry Ransomware.“ *TechTarget,* September, 2021. https://www.techtarget.com/searchsecurity/definition/WannaCry-ransomware.

200. Ryan, Matthew. 2021. *Ransomware Revolution: The Rise of a Prodigious Cyber Threat.* Cham: Springer.

201. Sangani, Priyanka. 2018. „Targeted Ransomware Attacks Surge In 2018: Report." *The Economic Times,* November 20, 2018. https://economictimes.indiatimes.com/tech/internet/targeted-ransomware-attacks-surge-in-2018-report/article-show/66709042.cms?from=mdr.

202. Savage, Kevin, Coogan, Peter, and Hon Lau. 2015. *Security Response: The Evolution of Ransomware.* Symantec. https://its.fsu.edu/sites/g/files/imported/storage/images/information-security-and-privacy-office/the-evolution-of-ransomware.pdf.

203. Seals, Tara. 2021. „Ryuk Ransomware: Now with Worming Self-Propagation." *ThreatPost,* March 2, 2021. https://threatpost.com/ryuk-ransomware-worming-self-propagation/164412/.

204. Sedlák, Jan. 2018. „Nemocnici na Rokycansku napadl ransomware, útočníci chtějí bitcoiny." *Lupa.cz,* June 29, 2018. https://www.lupa.cz/aktuality/nemocnici-na-rokycansku-napadl-ransomware-utocnici-chteji-platbu-v-bitcoinech/.

205. Sedlák, Jan. 2020. „Za útok na radnici Prahy 3 opět může ransomware, NÚKIB varuje před další vlnou." *Lupa.cz,* April 8, 2020. https://www.lupa.cz/aktuality/za-utok-na-radnici-prahy-3-opet-muze-ransomware-nukib-varuje-pred-dalsi-vlnou/.

206. Shemesh, Rotem. 2021. „What Is Maze Ransomware and How Does It Work?“ *Datto,* May 18, 2021. https://www.datto.com/blog/what-is-maze-ransomware-and-how-does-it-work.

207. Shepherd, Adam. 2021. „What is NotPetya?“ *ITPro,* October 8, 2021. https://www.itpro.co.uk/malware/34381/what-is-not-petya.

208. Sikora, Vojtěch. 2022. [Interview]. E-mail, May 20, 2022. Přepis rozhovoru se nachází v příloze C této práce.

209. Singer, Peter W., and Allan Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford: Oxford University Press.

210. Sjouwerman, Stu. 2021. „Ransomware Gangs: Who Are They And How To Stop Them.“ *Forbes,* September 27, 2021. https://www.forbes.com/sites/forbestechcouncil/2021/09/27/ransomware-gangs-who-are-they-and-how-to-stop-them/?sh=104795726651.

211. Spring, Tom. 2016. „Meet the Cryptoworm, The Future of Ransomware.“ *ThreatPost,* April 12, 2016. https://threatpost.com/meet-the-cryptoworm-the-future-of-ransomware/117330/.

212. Suchánková, Vlasta. 2014. „POZOR! Hackeři mohou napadnout váš počítač.“ *Policie České republiky,* December 4, 2014. https://www.policie.cz/clanek/pozor-hackeri-mohou-napadnout-vas-pocitac.aspx.

213. Sultana, Jabeen and Abdul Khader Jilani. 2021. „Exploring and Analysing Surface, Deep, Dark Web and Attacks.“ In *Security Incidents & Response Against Cyber Attacks,* edited by Akashdeep Bhardwaj and Varun Sapra, 85-96. Cham: Springer. https://doi.org/10.1007/978-3-030-69174-5.

214. Šafář, Ondřej, and Jan Potůček. 2017a. „WannaCry se České republice vyhnul, aktuálním statistikám napadených zemí vévodí Rusko.“ *Eset,* May 16, 2017. https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/wannacry-se-ceske-republice-vyhnul-aktualnim-statistikam-napadenych-zemi-vevodi-rusko/.

215. Šafář, Ondřej, and Jan Potůček. 2017b. “Svět ohrožuje nová epidemie ransomware, Česko je mezi deseti nejpostiženějšími zeměmi.“ *Eset,* June 27, 2017. https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/svet-ohrozuje-nova-epidemie-ransomware-cesko-je-mezi-deseti-nejpostizenejsimi-zememi/.

216. Šmíd, Tomáš. 2008. „Teoretické vymezení fenoménu organizovaného zločinu.“ *Politologický časopis* 9, no. 3, 270-296. https://www.politologickycasopis.cz/userfiles/file/2008/3/Polcas_2008_3_pp_270-296.pdf.

217. Štrbáková, Marie. 2012. „Napadení počítače virem RANSOMWARE.“ *Policie České republiky,* November 23, 2012. https://www.policie.cz/clanek/napadeni-pocitace-virem-ransomware.aspx.

218. Švéda, Martin. 2022. [Interview]. E-mail, May 23, 2022. Přepis rozhovoru se nachází v příloze F této práce.

219. TechLib. n.d. „Bota." Accessed April 4, 2022. https://tech-lib.eu/definition/boot.html.

220. The BlackBerry Research & Intelligence Team. 2021. „Threat Thursday: STRRat Malware." *BlackBerry ThreatVector Blog,* October 14, 2021. https://blogs.blac-kberry.com/en/2021/10/threat-thursday-strrat-malware.

221. The White House. 2021. „Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021." October 14, 2021. https://www.white-house.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/.

222. TRADOC. 2010. *Cyberspace Operations Concept Capability Plan 2016-2028.* Fort Monroe: United States Army. https://irp.fas.org/doddir/army/pam525-7-8.pdf.

223. Trend Micro. 2017. „Ransomware Recap: Satan Offered as Ransomware as a Service." March 15, 2017. https://www.trend-micro.com/vinfo/es/security/news/cybercrime-and-digital-threats/ransomware-recap-satan-offered-as-ransomware-as-a-service.

224. Uberti, David. 2021. „How the FBI Got Colonial Pipeline's Ransom Money Back." *The Wall Street Journal,* June 11, 2021. https://www.wsj.com/articles/how-the-fbi-got-colonial-pipelines-ransom-money-back-11623403981.

225. UNODC. 2004. *United Nations Convention Against Transnational Organized Crime And the Protocols Thereto.* New York: United Nations. https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf.

226. Úřad vlády ČR. 2018. *Vládní koncepce boje s korupcí.* https://www.vlada.cz/assets/dokumenty/aktuality/Vladni-koncepce-boje-s-korupci-na-leta-2018-az-2022.pdf.

227. Ústavní zákon č. 1/1993 Sb., Ústava České republik

228. Veselý, Arnošt, Drhová, Zuzana, and Marta Nachtmanová. 2005. *Veřejná politika a proces její tvorby. Co je „policy" a jak vzniká.* Praha: UK FSV CESES. https://ceses.cuni.cz/CESES-20-version1-sesit05_08_vesely.pdf.

229. Veselý, Arnošt. 2007. „Veřejná politika." In *Analýza a tvorba veřejných politik: Přístupy, metody a praxe,* edited by Arnošt Veselý and Martin Nekola, 13-42. Praha: SLON.

230. Vigliarolo, Brandon. 2021. „These Industries Were The Most Affected By the Past Year of Ransomware Attacks.“ *TechRepublic,* November 20, 2021. https://www.techrepublic.com/article/these-industries-were-the-most-affected-by-the-past-year-of-ransomware-attacks/.

231. VKR. 2017. „Nebezpečný virus Bad Rabbit se šíří Evropou a už udeřil i v Česku. Tvůrci se inspirovali ve Hře o trůny.“ *Info.cz,* October 25, 2017. https://www.info.cz/zpravodajstvi/svet/nebezpecny-virus-bad-rabbit-se-siri-evropou-a-uz-uderil-i-v-cesku-tvurci-se-inspirovali-ve-hre-o-truny.

232. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

233. Vypořádání připomínek k materiálu s názvem Návrh zákona, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů

234. Winder, Davey. 2021. „$70 Million Demanded As REvil Ransomware Attackers Claim 1 Million Systems Hit.“ *Forbes,* July 5, 2021. https://www.forbes.com/sites/daveywinder/2021/07/05/70-million-demanded-as-revil-ransomware-attackers-claim-1-million-systems-hit/?sh=d3fc38b57c01.

235. Wollmann, Hellmut. 2017. „Policy Evaluation and Evaluation Research.“ In *Handbook of Public Policy Analysis: Theory, Politics, and Methods,* edited by Frank Fischer, Gerald J. Miller and Mara S. Sidney, 393-404 . Boca Raton: CRC Press.

236. Zákon č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních.

237. Zákon č. 141/1961 Sb., zákon o trestním řízení soudním (trestní řád).

238. Zákon č. 151/2010 Sb., o zahraniční rozvojové spolupráci a humanitární pomoci poskytované do zahraničí.

239. Zákon č. 153/1994 Sb., o zpravodajských službách.

240. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

241. Zákon č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky (kompetenční zákon).

242. Zákon č. 234/2014 Sb., o státní službě.

243. Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu.

244. Zákon č. 273/2008 Sb., o Policii České republiky.

245. Zákon č. 361/2003 Sb., o služebním poměru příslušníků bezpečnostních sborů.

246. Zákon č. 370/2017 Sb., o platebním styku

247. Zákon č. 40/2009 Sb., trestní zákoník.

Příloha A Přepis rozhovoru s Expertem č. 1

Tab. 3: Informace o rozhovoru s Expertem č. 1 (vlastní tabulka)

Expert č. 1	
Označení ve zdrojích	Anonymní zdroj č. 1
Pracoviště	NCOZ SKPV
Délka praxe	7 let
Forma rozhovoru	Korespondenční via e-mail
Datum provedení rozhovoru	20. 5. 2022

Jaká je role PČR v boji proti ransomware?

Policie České republiky jedná v dikci ustanovení § 1 a § 2 Trestního řádu. Tedy když je zřejmé, že se jedná o podezření z trestné činnosti (kdy aplikace škodlivého kódu, který způsobí zašifrování systému a pachatel tohoto jednání požaduje za odšifrování tzv. výkupné je jednoznačně jednání, které je protiprávní) jsou orgány činné v trestním řízení povinny věc prověřit, případně konat i v procesu vyšetřování a následně podat návrh na podání obžaloby dozorovému státnímu zástupci.

Disponuje PČR dostatečnými finančními prostředky pro boj proti ransomware (potažmo proti kybernetické kriminalitě obecně)?

V oblasti financování boje proti kybernetické trestné činnosti jsou z minulosti značné rezervy. Nicméně v současné době je plánovaná sanace potřeb policejních jednotek které řeší trestnou činnost v oblasti kybernetické kriminality. Jde zejména např. o pořízení některých speciálních softwarových nástrojů. V rámci objektivity je nutné uvést, že Policie České republiky např. vlastní softwarový nástroj na trasování virtuálních měn, lze

tedy konstatovat, že postupně jsou vyslyšeny žádosti OČTŘ k zajištění alespoň některých nástrojů, které jsou zcela nezbytné k prověřování/vyšetřování trestné činnosti na daném úseku. Nicméně je v tomto úsilí (financovat policejní jednotky tak, aby byly schopné pořizovat speciální software ale i hardware) nutné pokračovat a dávat podklady managementu Policejního prezidia tak, aby zajistilo alespoň část finančních nároků na pořizování patřičného vybavení.

Jakým způsobem usiluje PČR o zajištění adekvátní expertní základny pro boj proti ransomware (potažmo pro boj proti kybernetické kriminalitě obecně)?

Policie České republiky má přednastavenu personální politiku v rámci uplatňování dikce služebního zákona (zák. č 361/2003 Sb.). Může zajistit, že policejní útvary, které mají vůli si zajistit místo IT specialisty, mohou za určitých a přesně daných podmínek dané tabulkové místo obsadit odborníkem z řad tzv. civilního sektoru, tedy nemusí notně být v tu dobu policistou.

Jakým způsobem je zajištěna konkurenceschopnost PČR v této oblasti na trhu práce?

O konkurenceschopnosti se nedá hovořit. Pouze jde o vlastenecké cítění či vnitřní touhu potírat kriminalitu v ČR. Například v rovině finančního odměňování je Policie ČR absolutně nekonkurenceschopná. Dlouhodobě se nedaří nabrat na celorepublikový útvar IT specialistu, který by aspoň trochu splňoval odborností a zároveň neměl požadavek na platové ohodnocení jako v soukromé sféře.

Účastní se PČR cvičení zaměřených na řešení kyberbezpečnostních incidentů spojených s ransomware?

Oblast cvičení k případům Ransomware nebylo realizováno. Pro policejní orgány je to jasné – vždy případ zadokumentovat, zajistit si stopy a věc v trestně právní rovině tzv. rozpracovat. Je možné tzv. procvičit komunikační dovednosti, ale lze se domnívat, že toto je na základě praktických případů relativně zvládnutá věc. Jen je třeba komunikovat s osobou, ve správné úrovni (nejlépe s vedoucí IT oddělení apod.). Nicméně je faktem, že právě toto má koncem května 2022 procvičovat jedna ze státních organizací.

Jakým způsobem spolupracuje PČR v boji proti ransomware (potažmo v boji proti kybernetické kriminalitě obecně) se soukromým sektorem?

Může přibrat znalecká i jiná pracoviště v rámci znaleckého zkoumání (či vypracování odborného vyjádření). Dále je možné spolupracovat ad hoc se společností, která zajišťuje v napadené společnosti konkrétní softwarové nástroje resp. jejich správu a údržbu, které např. zajišťují kybernetickou bezpečnost.

Využívá PČR v boji proti ransomware ustanovení § 18 Zákona o Policii ČR?

Obecně můžeme odpovědět že ano, ale pouze před zahájením úkonů trestního řízení, neboť následně po zahájení úkonů se postupuje dle Trestního řádu. Pro představu, ust. § 18 Zákona o Policii se využívá při dotazu na konkrétní subjekt, zda nemá napadenou počítačovou síť a následně při

kladné odpovědi se již koná pouze podle trestního řádu. Jinak informace pořízené dle zákona o Policii ČR nejsou brány jako důkaz v trestním řízení.

Jakým způsobem se PČR angažuje v oblasti sdílení informací za účelem boje proti ransomware (potažmo v oblasti boje proti kybernetické kriminalitě obecně)?

Sdílení informací je jasně dáno zákonným zmocněním dle Trestního řádu. Policie obecně musí v přípravným řízení informace chránit tak, aby nebyly vyzrazeny a nebyl zmařen účel trestního řízení. Proto sdílení dat je vcelku sledováno a nesmí být nahodilé a neuvážené. Pro dopřesnění - přípravné řízení je neveřejný proces, na rozdíl od řízení před soudem. Nicméně, Policie pracuje s „určitými" informacemi v rámci prevence a taktéž v rámci předcházení trestné činnosti tak, aby bylo bráněno rozvoji kriminální činnosti na území ČR. Nicméně je na tom konkrétním policejním orgánu, jaké informace z trestního řízení uvolní a jaký subjekt bude adresátem sdílení. Lze tedy konstatovat, že sdílení informací z trestního řízení není běžná záležitost.

Bylo by vhodné legislativně upravit povinnost fyzických i právnických osob sdílet informace o kyberbezpečnostních incidentech (např. povinně hlásit ransomwarové útoky či pokusy o ně i nad rámec povinností stanovených Zákonem o kybernetické bezpečnosti)?

Nelze nutit subjekty k něčemu co nechtějí. Pokud se jakýkoliv subjekt rozhodne, že se nebude cítit jako poškozený. Domníváme se, že je to jeho svobodné rozhodnutí a nemělo by se oznámení na něm vynucovat. Jsme v demokratickém státě, a stát by měl hodně zvažovat, jaké povinnosti ukládá svým občanům a např. právnickým osobám. Samozřejmě, bylo by

ideální mít veškerá data ze všech ransomware útoků v jedné databázi, ale musíme dát na misku vah svobodné rozhodování a donucování z úrovně stání moci. Domníváme se, že nynější nastavení dle Zákona o kybernetické bezpečnosti + Zákona o elektronických komunikací je vyvážené s tím, že již teď je zřejmé, že v rámci směrnice NIS II bude okruh povinných subjektů značně rozšířen.

Podílí se PČR na osvětové činnosti zaměřené na prevenci ransomware (potažmo v oblasti základů kyberhygieny)?

Ano, přispíváme do kampaně nomoreransom.org

Umožňuje současná legislativní úprava PČR stíhat ransomwarové útočníky na území ČR?

Ano, jde o porušení ustanovení § 230 odst. 2 Trestního zákona (viz citace) + je zde souběh s kvalifikací trestného činu dle ustanovení § 175 Trestního zákoníku (viz. citace 1 odstavce). S tím, že lze dle požadavku na výkupné kvalifikaci zpřísňovat – např. pro ilustraci odst. 3 písm. c)

Co je největší překážkou stíhání ransomwarových útočníků (v ČR i za hranicemi)?

Využívání anonymizačních prostředků, včetně sítě TOR a platby v kryptoměně, možnost registrace např. domén na smyšlené identity.

Pomohla by kriminalizace placení výkupného ransomwarovým útočníkům v boji proti ransomware?

Nelze kriminalizovat oběť, která je sama v tísni. Pokud by v teorii o tom někdo přemýšlel, měl by tedy stát v případě, že vznikly oběti milionové škody a oběť měla vůli zaplatit statisíce (a milionové škody tím

odstranit) nahradit i budoucí škodu (reparace). Je to oblast, kterou by stát měl ponechat na vůli jedince, který se musí sám svobodně rozhodnout jak bude dále konat – zda zaplatí. Nicméně, samozřejmě pokud se bude platit výkupné ve větším množství případů je zřejmé, že u pachatelů poroste s jídlem chuť a budou to mít jako vynikající byznys model s tím, že se bude aplikace ransomware zvyšovat co do počtu. Nicméně trestání oběti, jenž je pod obrovským tlakem a má vůli si zachránit vlastní podnikání (tedy živobytí) se nám jeví jako zbytečné, kdy navíc tam z našeho pohledu není zcela jasně vyhraněna škodlivost tohoto jednání (placení výkupného).

Jakým způsobem funguje spolupráce mezi PČR a dalšími státními institucemi v boji proti ransomware?

Různě, jde o včasné ohlašování těchto případů a schopnost předat resp. umožnit Policii ČR zajistit kvalitní stopy (elektronické důkazy).

Jakým způsobem funguje spolupráce mezi PČR a NÚKIB v oblasti boje proti ransomware?

Považujeme spolupráci za dobrou.

Jakým způsobem funguje spolupráce mezi PČR a FAÚ v oblasti boje proti ransomware (zejména v oblasti praní špinavých peněz skrze virtuální aktiva)?

Velmi dobře, nicméně FAÚ koná dle zákona a jejich oprávnění. Spočívá v nahlášení podezřelých transakcí, tedy nemůže hlásit logicky transakce ve virtuální měně.

Jakým způsobem funguje spolupráce PČR s dalšími institucemi věnujícími se boji proti kybernetické kriminalitě na mezinárodní úrovni?

Dobře, spolupracuje se na preventivních programech, vzdělávání, + je tam aktivita agentury EUROPOL, CEPOL apod. Dále se do této problematiky zapojuje Interpol, který zprostředkovává přednášky například z akademické sféry ze zahraničí.

Existují specifické iniciativy či příklady této spolupráce?

Toto není vhodné podrobně rozepisovat.

Příloha B Přepis rozhovoru s Expertem č. 2

Tab. 4: Informace o rozhovoru s Expertem č. 2 (vlastní tabulka)

Expert č. 2	
Označení ve zdrojích	Plecitý, David
Pracoviště	FAÚ – Analytické oddělení 042
Délka praxe	28 let
Forma rozhovoru	Osobní, Praha
Datum provedení rozhovoru	11. 5. 2022

Angažuje se FAÚ v boji proti ransomware?

Zprostředkovaným způsobem ano. FAÚ se zabývá tématem legalizace výnosů z trestné činnosti a financování terorismu a s tím souvisejícími zdrojovými trestnými činy. To znamená ten ransomware bych opravdu podsadil pod kybernetické trestné činy. V případech, že mi tady legalizaci podobného typu zachytíme. Obecně jak to funguje – naše vyhledávací činnost je zákonem přenesená na zákonem povinné osoby, které si v praxi nejlépe můžeme představit jako banky, spořitelní a úvěrová družstva, a mnoho dalších, mimo jiné také osoby poskytující služby spojené s virtuálními aktivy. Ty nám reportují tzv. podezřelé obchody. My z nich to nějakým způsobem čerpáme. To je jedna taková důležitá a podstatná část informací, se kterými my pracujeme, a které máme i analyzovat a dělat z nich nějaký výstup, v tomto případě by nejrelevantnějším výstupem bylo podání trestního oznámení anebo o schůdek níž poskytnutí informace významné pro činnost – a teď např. Policii ČR nebo zpravodajské služby, která se tím zabývá atp. A tou druhou částí je právě úzká spolupráce s těmi adresáty, o kterých jsem mluvil. To znamená, že za určitých podmínek FAÚ

spolupracuje se svými adresáty v rámci součinnosti v reakci na jejich dožádání, nejčastěji s orgány činnými v trestním řízení. Takže ano, působíme v boji proti ransomware, ale nějakou odvozenou formou. Přímo na tom hlavním meritu věci se nepodílíme, spíše získáváme informace o tocích, které by případně s tou legalizací výnosů z ransomware nějakým způsobem souvisely.

Je současná legislativní úprava praní špinavých peněz skrze virtuální aktiva adekvátní?

Já myslím, že ano. Počítám, že ona stejně ještě není ukončená. V oblasti evropské legislativy je to čím dál názornější a větší téma. ČR měla drobnější výhodu, že předběhla tzv. pátou AML směrnici ve vztahu ke kryptoměnám, tedy virtuálním aktivům, kdy začala působit svoji vlastní novelou od 1. 1. 2017. Takže my jsme vlastně s osobami, které by poskytovaly služby spojené s virtuálními aktivy spolupracovali už jakoby nad rámec těch požadavků, které přišli jakoby později. Takže jsme měli jakoby drobný náskok. A myslím, že ta legislativa je postavená dobře a hlavně se bude neustále vyvíjet. Zase tady platí ten starý axiom, že technologický vývoj bude daleko dynamičtější, než bude jakákoli legislativní akce jej podchytit a nějakým způsobem regulovat. Ale myslím si, že pro podmínky ČR mi přijde to penzum vlastně povinností a práv, které se s tím ve vztahu k našemu zákonu pojí s virtuálními aktivy dostatečné.

Nehodnotím už oblast kapitalizace virtuálních aktiv ve vztahu k finančním úřadům. Či věčný filozofický boj, jestli se virtuálními aktivy má nebo nemá zabývat Česká národní banka jako hlavní regulátor bankovního trhu v ČR. Je to měna, není to měna, a ty podobné věci. Ve vztahu k legalizaci myslím, že tak jak je to zatím postaveno, tak je dobře. A za nutné bych považoval říct, že jedna záležitost je legislativní vymezení, a druhá

fungování těch jednotlivých subjektů a jejich vzdělávání v té problematice, nebo vůbec pochopení jejich hlavní role. Tam jsou sice trvale nějaké nedostatky, ale řekl bych, že postupně se do daří odstraňovat.

Jsou národní kapacity ČR (např. personální základna) pro boj proti praní špinavých peněz skrze virtuální aktiva dostačující?

To rozhodně ne. Chápejte to tak, že s ohledem na rozsah pracovníků FAÚ a tu plejádu informací a témat, kterým se věnujeme, tak to v tomhle pohledu samozřejmě dostatečné není. Ten výčet, respektive legalizace prostřednictvím virtuálních aktiv, je jenom určitou částí. Virtuální aktiva chápejme jenom jako určitou jednu metodu, kterou k té legalizaci dochází. Za současného stavu nám bude stačit, aby pracovníci analytického odboru měli alespoň základní povědomí o oblasti virtuálních aktiv a aby se v odboru našli jeden/dva specialisté, kteří budou mít tu povědomost poměrně hlubší a budou schopni držet krok s aktuálními trendy, aby mohli reagovat na aktuální projevy trestné činnosti a možnosti legalizace tak, jak je bankovní sektor, případně osoby virtuálníci jakoby oznamují.

Na druhou stranu, obecně bych řekl, že ČR a to s ohledem na obecné pojetí law enforcement má výrazný deficit v obecné kybernetické kriminalitě. Táhne se to již celou řadu let, zde si dovolím opravdu odbočku – začalo se o tom hovořit již já nevím před kolika mnoha lety, když si vzpomenete již za tehdejšího policejního prezidenta Tuhého se navykládala strašná spousta věcí, jak vzniknou samostatné útvary a samostatný útvar do dneška nevzniknul. Jestli to půjde dobře, třeba se dočkáme jeho vzniku v současném roce. Ale to je přesně ono, není to uchyceno pořádně. Vidíte rozvoj kybernetické kriminality jak jde mílovými kroky dopředu – covidová doba tomu jenom a jenom pomohla, že se opravdu část trestné činnosti přesunula vyloženě do kybernetické domény. Takže ano, kdybych měl o pár

odborníků na toto téma víc, tak samozřejmě jsme na tom jakoby dobře. Ale nemyslím si, že by to bylo v nějaké situaci, že bychom zrovna s tímhle pohledem žehrali na nějaký personální nedostatek. Spíše podchyceno v rámci celé ČR a osob, které se tomu věnují, čím víc specialistů v tomhle ohledu bude, a tihle ti specialisté budou jako „někdo" vycházet ze škol a budou se věnovat aplikované praxi, tak to bude jenom dobře.

Pokud to chápu dobře, tak v současnosti máte dostatek lidí, ale do budoucna by bylo lepší, kdyby jich bylo víc, protože předpokládáte, že se bude řešit víc věcí?

Vždycky je dobře, když je na to těch lidí jakoby víc. Na konci Vám dám statistiku vývoje, které bude prezentována na našich stránkách a bude i v naší výroční zprávě, takže to budete mít jakoby s předstihem. Tam uvidíte vlastně ten nárůst toho tématu té legalizace. Ale zase, z našeho pohledu FAÚ zůstává na hranici FIAT měny a virtuálních aktiv. My nepostupujeme za tu část, kde došlo ke směně. A nějakým způsobem výrazným neprovádíme trasování v blockchainu nebo podobné věci. To je záležitost orgánů činných v trestním řízení, případně jiných orgánů. Našim hlavním tématem je ten přechod mezi FIAT měnou a virtuální měnou. Tam řekněme, že jsme silní. Když už se dostáváme dál, i když jsme v určitých momentech schopní provést v souladu se zákonem, tak jak provádíme blokaci finančních prostředků, tak jsme schopní za určitých podmínek provést i blokaci virtuálních aktiv. Ale zase, tohle zvládne jenom pár lidí.

Ale při té plejádě specializací, které by tady měli analytici zvládnout, tak ty virtuální měny jsou jakoby jen částí z nich, přitom těch částí tady napočítám třeba 20-25, tak ta dimenze je jakoby dostatečná. Na druhou stranu, kdyby se na nové vypsané výběrové řízení v budoucnu hlásil uchazeč, který o tématu virtuálních aktiv bude mít už nějaké povědomí, nebo

aspoň bude k tomu náchylný – ono se to hodně váže na to, zda jste kvalitní uživatel výpočetní techniky a zajímáte se o to téma, tak už vám pak nedělá problém naskočit na tu specializaci. Ale stejně tak, jako tady tomu někteří kolegové rozumí opravdu jenom na té základní úrovni, tak najdeme také kolegy, kteří na základní úrovni rozumí třeba daňové problematice. Protože to není jejich šálek kávy a nezabývají se tím. Takže ano, celkově kdybych to měl zodpovědět, tak řekněme, že současně kapacity by asi byly dostačující.

Považujete finanční zajištění činnosti FAÚ v boji proti ransomware za adekvátní?

Na takto položenou otázku je odpověď složitější, a netroufnu si hodnotit, zda je zajištění činnosti FAÚ s ohledem na vykonávanou státní službu adekvátní. Lze však připomenout, že pro vykonávané činnosti na FAÚ není zcela jednoduché na pracovním trhu získat odpovídající odborníky, navíc s předpokládanou předchozí praxí v bezpečnostních sborech, finanční správě či veřejné správě s odpovídajícím vzděláním, které je většinou právního či příbuzného směru. Žádoucí se také jeví připomínka toho, že zvláště analytici FAÚ v rámci své činnosti mnohdy pracují s milionovými až miliardovými hodnotami, které jsou následně v ideálním případě odčerpány majiteli, typicky pocházejícím např z prostředí organizovaného zločinu. Tedy, ve finančním zajištění činností je nepochybně vhodné počítat také s možnými bezpečnostními ohroženími personálu FAÚ, či eliminací hrozeb, které může pro zaměstnance vytvářet např. korupční nabídka těchto osob. I z těchto důvodu by bylo možné na pracovníky FAÚ pohlížet jako na specialisty svého druhu v úzce ohraničeném odvětví státní služby v oboru Ekonomická ochrana státu, a finanční ohodnocení jejich práce tomuto faktu

průběžně přizpůsobovat ve vztahu i k jiným ohrožení a omezení, které aktuální doba přináší.

Spolupracuje FAÚ s poskytovateli služeb spojených s virtuálními aktivy i nad rámec Zákona o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu (např. konkrétně v oblasti boje proti ransomware)?

Těžká otázka zase položená nad rámec. Náš vztah je v tomto pohledu opravdu výrazně dán zákonem. To znamená, že ty osoby, které poskytují služby spojené s virtuálními aktivy se od roku 2017 staly povinnými osobami, a s implementací 5. směrnici vlastně s povinnými osobami ještě s nějakými zásadnějšími povinnostmi. Možná nad rámec zákona bych vnímal, že poté co to téma začalo být aktuální, tak se zjistilo, že si tyto osoby vlastně některých svých práv a zejména pak povinností ve vztahu k AML zákonu nejsou vědomy, případně neví, jak si je nějakým způsobem vysvětlit. Takže v těch letech před covidem, kdy bylo umožněno setkávání face to face, tak FAÚ provedl několik tzv. odborných diskuzí. Tam právě byla co možná nejširší účast osob poskytujících služeb s virtuálními aktivy, v té době to zejména byly začínající a působící směnárny, občas provozovatelé bitcoinmatů a podobných služeb, zástupci právních kanceláří. Bylo to doplněno výkladem zákona a těch konkrétních povinnostech od nás, snažili se tam dostat lidé z práce – policie, celníci, aby diskuze bylo co nejširší, k tomu také zástupci bankovního sektoru. V našich podmínkách virtuálník bez bankovního účtu není možný, takže to spolu úzce souvisí, aby k sobě tyto dva segmenty našly cestu. Těch debat bylo asi 5 nebo 6 v nějakém čtvrtletním či pololetním působení. To bych označil za práci nad rámec. To nám zákon rozhodně neukládá a byla to z naší strany podaná ruka oběma těm sektorům – bankovnímu sektoru a virtuálníkům. Fungovalo to jakoby

spojovací článek. Potom to hlavně díky covidu přešlo, ale i z druhé strany jsme byli nuceni, že tato podpora jednomu segmentu povinných osob už nám přijde jakoby výrazně dostatečná na tu edukaci. Neberu však v potaz konkrétní individuální dotazy, které s sebou normálně přináší praxe. Ale v tomto směru už nám tato velká edukace přišla dostatečná a v současné době už se tato setkání v takto velkém duchu neplánují. Ta komunikace na obě dvě strany však probíhá do současné doby. Hlavně se poměrně stabilizovat trh. V letech 2018 a 2019 bylo směnáren virtuálních aktiv poměrně více, než jich je teď. Situaci si sedla a zhruba se pokryly potřeby ČR.

Nemyslíte si tedy, že je třeba tuto spolupráci dále rozvíjet i jiným směrem.

Spolupráce tak, jak je teď nastavená, je třeba rozvíjet. Ale nemyslím si, že je potřeba dělat nějaké velké projekty jako byl např. tento. Já jsem zastáncem denní praxe, takže pokud budeme všichni ruku v ruce postupovat s tím, co ta denní praxe normálně přináší, tak to bude dostatečné. Zjednodušeně bych řekl, že virtuálníci vědí, co FAÚ chce, a FAÚ ví, jaké jsou možnosti virtuálníků. A o této situaci je dále seznámen i bankovní sektor, kdy to je nejčastější výtka virtuálníků, že s nimi bankovní sektor nechce spolupracovat a vnímá je jakoby riziko – to je časté téma. Do tohoto tématu FAÚ nijak nevstupuje. To je přímý vztah banky a klienta, takže dvou samostatných subjektů, které k sobě nějakým způsobem mohou, ale nemusí najít cestu. FAÚ tady nemůže být od toho, aby bankám říkal „vy jim prostě musíte vést účty," nebo na druhou stranu „vy jim ty účty neveďte, protože virtuální měna je nějaké zlo." FAÚ se od začátku snaží, aby byl odborným zprostředkovatelem a odbornou osobou, kde se ty názory budou střetávat, ale pořád je to ve vztahu k tomu, aby došlo k naplnění AML zákona a všech procedur, které s tím souvisí.

Jakým způsobem funguje spolupráce FAÚ s dalšími státními institucemi, např. PČR v oblasti boje proti ransomware?

To je docela problém i pro účely diplomové práce, protože nejsem schopen zaběhnout do detailů. To je vnitřní záležitostí FAÚ a PČR a mnoho je kryto povinností mlčenlivosti.

Zeptala bych se tedy konkrétně, zda dobře funguje komunikace a sdílení informací, tedy zda jsou komunikační kanály dobře zavedené a adekvátně umožňují spolupráci?

Pověřené orgány, které se ransomware převážně zabývají, pracují s úrovní skupin či oddělení internetové kriminality a analytických oddělení krajských ředitelství policie plus NCOZ jako specializovaného orgánu, tak tam podle mě v komunikaci není žádný větší problém. Několikrát za rok se konaly, a bude to nejspíš opět aktualizováno, odborné debaty, školení, kde i my jsme účastní a o současných aspektech spolupráce neustále probíhá nějaká debata. Myslím, že ty kanály jsou nastaveny velmi dobře. I specializovaný orgán, jako NCOZ, pokud se děje něco, co si vyžaduje aktivní zásah a jde o urgentní spolupráci, tak bych řekl a nechci to přehnat, že ten kanál v odůvodněných případech funguje v podstatě 24/7. Ten telefon já zapnutý mám, ale stane se to třeba 2x za ten rok, že vám někdo zavolá, že je takto akutně potřeba něco řešit. Tady zase narážím na naše možnosti ve vztahu k bankovnímu sektoru. My jsme totiž výrazně vázáni na ten bankovní sektor. Ale myslím si, že spolupráce FAÚ s dalšími státními institucemi je v tomhle bezproblémová.

Jakým způsobem funguje spolupráce FAÚ s dalšími státními institucemi, např. NÚKIB v oblasti boje proti ransomware?

S NÚKIB tam jsme ve vztahu spíše legislativním v rámci té problematiky, případně v rámci odborných meziresortních skupin, které probíhají např. na Ministerstvu vnitra, kde je zvláštní skupina právě na Dark Web a kryptoměny. Tam se to jednou za čas sejde a probírají se nějaké věci. Takže tam jsme jakoby v kontaktu. S NÚKIB jsme nikdy neměly náznaky spolupráce, které by byly jak negativního, tak pozitivního. Prostě o sobě víme, ale ta témata jsou přeci jenom jakoby jiná. My jsme naše možnosti prezentovali tam, kde to bylo třeba – např. Národní centrum kybernetických operací. Vědí o nás, my víme o nich, nějaká forma spolupráce tam funguje, nebudu už konkrétní.

Vedla z NÚKIB směrem k FAÚ např. nějaká osvětová činnost zaměřená na základy kyberhygieny, případně pak konkrétně na problematiku ransomware?

Možná, ale spíše v oblasti kybernetické bezpečnosti obecně. Přímo na ransomware myslím, že nic neproběhlo. Nevím o tom. Spíše to byly záležitosti obecně bezpečného chování v kyberprostoru pro pracovníky. Pokud jsou naši pracovníci IT bližším způsobem školeni v zabezpečení našeho provozu i směrem k ransomware, tak nevím. Předpokládal bych, že to je záležitost zcela běžná. Náš systém není ani v minulosti nebyl zcela běžný, na rozdíl od jiných státních internetových nebo elektronických systémů třeba ministerstva. V tomhle my jsme byli vždy poměrně specifičtí. Speciální školení o ransomware si ale od NÚKIB nevybavuji.

Jakým způsobem funguje spolupráce FAÚ se zahraničními finančními zpravodajskými jednotkami (případně jinými zahraničními orgány) v oblasti boje proti praní špinavých peněz skrze virtuální aktiva (případně i konkrétně v oblasti boje proti ransomware)?

Probíhá. Zahraniční spolupráce je téma samo o sobě. Ve vztahu k problematice virtuálních aktiv probíhá základní spolupráce dvěma směry. Myslím, že jsme příjemci – ten počet kanálů se poměrně rozšířil, od několika zpravodajských jednotek a vesměs jsou to jednotky, kde je příslušný nějaký větší poskytovatel virtuálních aktiv či větší kryptoměnová burza. Od nich nějaké věci chodí, tam dochází k nějaké větší analýze, ale právě proto.

My tady vlastně nikoho většího tohoto typu nemáme. My máme podchyceny osoby, které jsou pro nás, což je pro vaši informaci podle živnostenského rejstříku, kde se měly tyto subjekty evidovat, tak tam jich je okolo 2500. Takže přibližně 2500 směnáren, ale neodpovídá to. Tam si každý zapsal živnost, co kdyby byla v budoucnu potřeba, takže si troufnu odhadnout, že těch reálných subjektů poskytujících služby spojené s virtuální měnou je tady v republice kolem 40. Tohle zjištění vychází z toho, co my zjistíme naší běžnou činností. Odhadoval bych, že tady je asi 10 až 15 hlavních hráčů na trhu, tedy směnáren a poskytovatelů institucionálního charakteru. Vedle toho tady ale zase máte ohromnou spoustu řekněme fyzických osob, které samy působí v rámci nákupu a prodeje virtuálních aktiv nějakými peer-to-peer směnami. Je to v tom bankovních sektoru vidět.

Výměna zahraničních informací probíhá. Je to ale postaveno poměrně jinak. Podle mě nám se chodí velké množství dat zpracovaných pouze základní formou, čemu se ale nedivím, pokud rozebírají nějakou velkou burzu a těch dat je tam spousta. Posílají nám to, co má příznak ČR, ať už občan či adresa apod. Na druhou stranu naše zahraniční jednotky odesílají informace zpracovanější. Takže hlavní rozdíl je, že ze zahraniční obdržíme

informaci v podstatě na vstupu a my odesíláme informaci na výstupu – už zpracovanou s nějakým příběhem a s nějakým výsledkem, tedy obohacenou vnitřní analýzou a zesumírováním toho výsledku.

Pomohlo by tedy vaší činnosti, kdyby zahraniční partneři posílali více zpracované informace?

Je to spíše otázka na kolik jsou tyto informace využitelné. U nás zůstávají v informačním systému, ale o tyto informace se dělíme také s dalšími adresáty ryze příslušnými. To znamená např. s orgány činnými v trestním řízení a popravdě řečeno, nemám úplně zpětnou vazbu v rámci toho objemu, na kolik jsou ty informace tam jakoby využitelné. My pokud jsme orgánem činným osloveni, tak už víme, že se jde na něco konkrétního a tam cítíte, že se jde jakoby na přímo. To, že oni některé informace využijí nelze vyloučit. Informace o virtuálních aktivech, která jsou využívána v darkwebu k nakupování nelegálních komodit, ale nevíte, o co jde konkrétního, tak je dost možné, že to práci policie, případně zpravodajských služeb nepomůže teď, ale třeba za 3 roky. Tohle je tedy poměrně dostatečné. Když se vrátím zpět, a řekli bychom „tak nám všichni posílejte informace o virtuálních aktivech," tak by nás tady muselo sedět 500 a ne ten počet, který nás tady sedí.

Jaká jsou největší úskalí boje proti praní špinavých peněz skrze virtuální aktiva v ČR (případně i obecně)?

No, to se mě ptejte. Aniž bych odhlédl k nějaké výrazné hranici, co se může objevit v budoucnu, tak současný problém při našem monitoringu prokázané legalizace prostřednictvím virtuálních aktiv, tak za posledního půl či třičtvrtě roku to není úplně problém institucionalizovaných obchodníků. Ti své povinnosti mají a provádí identifikaci klienta a kontrolu těch

věcí. Máte tam alespoň základní přehled o tom, co se tam děje alespoň na území ČR.

Samozřejmě, pokud budu zločinec tady a budu posílat peníze do zahraničí, respektive zahraničnímu poskytovateli, tak vznikl velký nárust legalizace prostřednictvím těch peer-to-peer obchodů fyzických osob. Tam já jsem osobně přesvědčen, podle těch lidí, kteří tam obchodují, a které my pak vidíme a jsou nám reportování v rámci bankovního sektoru, jsou to jak tuzemští občané tak cizinci, a teď po uprchlické vlně ten počet těch cizinců ještě jakoby narůstá. Z určité části ti lidé opravdu netuší, že jde o peníze z trestné činnosti. U určité části jsem přesvědčen, že jakoby tuší, že ty peníze jsou z trestné činnosti, ale říkají „heleďte já vlastně nic, já jakoby jenom prodávám a všechno musí udělat poskytovatel služby, včetně identifikace a kontroly klienta." A pak je tady značná část osob, které nejen tuší, ale vědí, že to tak je a jsou součástí legalizačních skupin a je to jen vhodně použitá legenda.

Takže třeba tohle je úskalí, na které se prakticky za současných zákonných mantinelů nedá dosáhnout. Je ale otázka filozofické či zákonné úvahy, jestli opravdu dát do zákona něco takového, co by postihovalo i ty fyzické osoby a blížilo se to Číně, kde ta kontrola té společnosti je v tomto vztahu v podstatě 100%. Já bych z těch virtuálních aktiv nedělal nějakého strašáka. Bude to věc, se kterou se budeme muset naučit žít. Zejména pak tradiční bankovní sektor. A i z pohledu legalizačních nástrojů obecně se nejedná o top legalizační nástroj, byť jeho význam roste.

To ale souvisí s tou predikativní trestnou činností, která je páchána na internetu a tudíž k tomu zhodnocení dochází přes internet. To významně souvisí i s obecným povědomím občanů ČR o tom, jak to funguje. Souvisí to s tou zdrojovou trestnou činností. Inflace jde nahoru, neustále do vás někdo tlačí jak máte investovat a nenechávat si věci pod polštářem. Neustále se

mluví o tom, jak jsou kryptoměny skvělý nástroj pro zhodnocení úspor. Začínají do toho investovat lidi, kteří o tom neví v podstatě nic, kterým někdo zavolá „investujte s námi do kryptoměn" a oni hned „jasně" a už se to posílá. Je to takové téma, kterému část občanů vůbec nerozumí a neví, co si pod tím představit. Kdyby někdo řekl „pojďte, nakoupíme zlato," tak už jsou schopni si představit, jak jim někdo přiveze cihlu zlata, ale to, jak budou mít uloženy svoje aktiva v nějaké adrese někde v blockchainu, tak to už nedomyslí.

Takže úskalí vychází ze současných modelů a zůstane to tady s námi. Internet s námi zůstane, protože už je nedílnou součástí životů a virtuální aktiva se k tomu budou blížit a jde o to, do jaké hloubky. Ale to už je zase úvaha spíše filozofického náhledu na téma kryptoměn jako takových. Boj proti praní špinavých peněz, ještě mě napadá ten finanční rozměr pro ČR – posouzení virtuálních aktiv z pohledu finanční správy a daňových důvodů. To bude velké téma, do kterého se zatím nikomu nechtělo. Souvisí to ale i s decentralizací a jakousi pseudo-anonymitou virtuálních aktiv. Není to ale zcela anonymní, jak si někteří lidé myslí. Z pohledu legalizace výnosů z trestné činnosti je ten nástroj virtuální aktivum už je i v podmínkách ČR pevně usazen.

Příloha C Přepis rozhovoru s Expertem č. 3

Tab. 5: Informace o rozhovoru s Expertem č. 3 (vlastní tabulka)

Expert č. 3	
Označení ve zdrojích	Sikora, Vojtěch
Pracoviště	NÚKIB – Oddělení reaktivní
Délka praxe	4 roky
Forma rozhovoru	Korespondenčně via e-mail
Datum provedení rozhovoru	20. 5. 2022

Jakým způsobem prosazuje NÚKIB dodržování základních technických kyberbezpečnostních opatření?

Dodržování pro regulované subjekty (Významné informační systémy, Kritická informační infrastruktura a Poskytovatelé základních služeb) je povinné ze zákona. Jednotlivé požadavky pak definuje Vyhláška o kybernetické bezpečnosti. Jejich dodržování může NÚKIB prosazovat v rámci kontrolní činnosti. Pro neregulované subjekty, které se aktivně chtějí starat o svou bezpečnost vydal NÚKIB „Minimální bezpečnostní standard."

Jsou současné technické požadavky stanovené Vyhláškou o kybernetické bezpečnosti adekvátní?

Ano, technické požadavky jsou dle mého názoru adekvátní pro regulované subjekty. Technické požadavky bohužel nebudou vždy vyhovovat všem, proto NÚKIB vyzývá odbornou veřejnost k připomínkám do nového zákona a vyhlášky.

Jakým způsobem funguje spolupráce s povinnými subjekty dle Zákona o kybernetické bezpečnosti (případně i se subjekty mimo něj) při řešení kyberbezpečnostních incidentů obecně, případně konkrétně těch spojených s ransomware?

Ze zákona mají subjekty povinnost incident nahlásit a Vládní CERT tyto údaje vyhodnocuje. Dál dle zákona poskytuje těmto subjektům během incidentu součinnost. Prakticky při ransomware incidentu Vládní CERT zjišťuje typ ransomware a nabídne subjektu pomoc při zajišťování dat pro následnou analýzu. K těmto krokům má Vládní CERT metodické materiály. Pokud subjekt požádá o pomoc na místě a NÚKIB vyhodnotí, že závažnost incidentu tomu odpovídá, může vyslat rapid response tým složený z analytiků a odborníků dle domluvy.

Jakým způsobem funguje spolupráce s dalšími státními institucemi (jmenovitě PČR a FAÚ) při řešení kyberbezpečnostních incidentů obecně, případně konkrétně těch spojených s ransomware?

NÚKIB má povinnost PČR oznamovat všechny trestné činy, kterých si je vědom. S FAÚ Vládní CERT nemá nastavenou spolupráci na pracovní úrovni.

Bylo by vhodné legislativně ukotvit zásadu neplacení výkupného ransomwarovým útočníkům?

Dle některých výkladů je již toto v legislativě ČR zajištěno např. porušení péče řádného hospodáře, porušení povinnosti o Zákona o majetku ČR, regulace hospodářské soutěže. Platící osoba může být stíhána za trestný čin zpronevěry, legalizace výnosu z trestné činnosti, zneužití pravomoci úřední osoby, porušeni povinnosti při správě cizího majetku. Pokud by platící uzavřel jakoukoli smlouvu s třetí stranou, která by platbu provedla,

tato smlouva by byla s nejvyšší pravděpodobností považována za absolutně neplatnou.

Bylo by žádoucí rozšířit povinnost sdílet informace (např. nahlašovat kyberbezpečnostní incidenty) i na subjekty, které v současnosti nejsou upraveny Zákonem o kybernetické bezpečnosti?

Dle mého názoru ne. Hlásit incidenty můžou neregulované subjekty dobrovolně jak Vládnímu CERT, tak Národnímu CSIRT. Vymahatelnost by také byla naprosto nereálná.

Jakým způsobem ČR usiluje o eliminaci ransomwarových útočišť?

NÚKIB předává informace OČTŘ. Tuto problematiku řeší OČTŘ mezinárodně.

Jakým způsobem ČR pomáhá dalším státům s bojem proti ransomware (případně se zajišťováním kybernetické bezpečnosti) na jejich území?

V různých pracovních skupinách na evropské i světové úrovni funguje výměna informací, jak kontextuálních, tak technických. Velmi často výměna těchto dat probíhá automatizovaně.

Příloha D Přepis rozhovoru s Expertem č. 4

Tab. 6: Informace o rozhovoru s Expertem č. 4 (vlastní tabulka)

Expert č. 4	
Označení ve zdrojích	Anonymní zdroj č. 2
Pracoviště	NÚKIB – Oddělení vzdělávání
Délka praxe	-
Forma rozhovoru	Korespondenčně via e-mail
Datum provedení rozhovoru	10. 5. 2022

Jakým způsobem se NÚKIB věnuje základům kyberhygieny v rámci své osvětové činnosti?

NÚKIB se věnuje základům kyberhygieny v rámci své činnosti ve dvou rovinách. První z nich je podpora vzdělávacích akcí a aktivit organizací, které se věnují vzdělávání v této oblasti. Takto například podpořil projekt Datová Lhota od MFF Univerzity Karlovy, České televize a CZ.NIC revidováním a připomínkováním materiálů. V současné době se NÚKIB podílí na tvorbě metodik k projektu Kyberpohádek, které připravuje Centrum kybernetické bezpečnosti. Jsme také součástí řady vzdělávacích konferencí, workshopů nebo webinářů.

Kromě toho tvoříme také vlastní vzdělávací aktivity. Snažíme se, aby byly dostupné bez ohledu na čas nebo region, proto se nám velmi osvědčila forma e-learningu. Snažíme se, aby nabídka kurzů pokryla co nejširší spektrum témat z kybernetické bezpečnosti, a to již od úrovně mateřských škol. Mám-li uvést konkrétní příklady, pak jedním z kurzů, který se komplexně věnuje kybernetické hygieně je kurz Jsem netvor, tvor, který žije na netu. Je dostupný ve verzi pro základní i střední školy. Druhým z kurzů, který stojí za to vyzdvihnout, je kurz Dávej kyber! Kurz základů kybernetické

bezpečnosti. Přestože je primárně určen zaměstnancům ve veřejné správě, díky možnosti projít si jej i bez registrace se může vzdělávat prakticky kdokoliv, kdo zavítá na vzdělávací stránky osveta.nukib.cz. Kromě e-learningu se tématům kyberhygieny věnujeme také prostřednictvím komiksového Instagramu @petr.vytrzny. Kromě pravidelných příspěvků z oblasti digitálních technologií a kybernetické bezpečnosti, se pomocí tohoto účtu snažíme upozorňovat na osvětové kampaně jako například Safer Internet Day nebo European Cyber Security Month.

Kyberhygiena je také jedním z témat, na které jsou zaměřené vybrané akce Festivalu bezpečného internetu. Festival bezpečného internetu, který si lze představit jako sérii vzdělávacích akcí a aktivit na poli kybernetické bezpečnosti, je vlastně ukázkou propojení obou rovin. NÚKIB, který Festival koordinuje jednak nabízí své vzdělávací aktivity a kampaně, a zároveň dává prostor ostatním organizacím podílet se na něm, třeba zapojením vlastní akce.

Na koho jsou osvětové aktivity týkající se problematiky kyberhygieny zaměřeny?

Národní strategie kybernetické bezpečnosti České republiky na období let 2021 – 2025 identifikuje zvyšování digitální hygieny jako jeden z předpokladů vybudování tzv. odolné společnosti 4.0. Současně definuje nutnost osvojování návyků pro bezpečný pohyb na internetu a používání digitálních technologií už od mateřských škol, stejně jako nutnost začlenit problematiku kybernetické bezpečnosti do všech úrovní vzdělávacího systému, a to napříč obory. Z toho vyplývá potřeba nejen vzdělávat žáky na všech úrovních vzdělávacího systému, ale také vzdělávání těch, kteří vzdělávají – tedy pedagogů, metodiků prevence, metodiků ICT nebo třeba knihovníků. Další velkou cílovou skupinou jsou zaměstnanci veřejné správy,

zejména v sektorech jako energetika, doprava, bankovnictví, infrastruktura finančních trhů, vodní hospodářství, digitální infrastruktura, chemický průmysl, a zdravotnictví, případně dalších entit dle zákona o kybernetické bezpečnosti a směrnice NIS. Kromě těchto cílových skupin nezapomínáme také na ty, kteří jsou z hlediska kybernetické bezpečnosti zranitelnou skupinou – senioři.

Je v rámci osvětových aktivit přímo zmíněna problematika ransomware?

Primárním cílem kurzů je naučit lidi a organizace chovat se takovým způsobem, aby zašifrování dat a dalším nepříjemným situacím na svých zařízeních předcházeli. Nicméně jmenovitě je problematika ransomware zmíněna v kurzech Jsem netvor, tvor, který žije na netu a Dávej kyber! Kurzu základů kybernetické bezpečnosti. Téma ransomware se také určitě objeví na vzdělávacím Instagramu v letošní kampani u příležitosti Evropského měsíce kybernetické bezpečnosti, kde je jedním ze dvou hlavních témat.

Na koho jsou osvětové aktivity týkající se problematiky ransomware zaměřeny?

V našich e-learningových kurzech jsou zaměřeny na jejich cílovou skupinu – tedy primárně děti a dospívající, a u kurzu Dávej kyber na zaměstnance veřejné správy a dalších entit dle zákona o kybernetické bezpečnosti a směrnice NIS. Co se týče vzdělávacího Instagramu, sledujícími jsou jak dospívající, tak dospělí lidé z řad široké veřejnosti.

Příloha E Přepis rozhovoru s Expertem č. 5

Tab. 7: Informace o rozhovoru s Expertem č. 5 (vlastní tabulka)

Expert č. 5	
Označení ve zdrojích	Anonymní zdroj č. 3
Pracoviště	NÚKIB
Délka praxe	15 měsíců
Forma rozhovoru	Korespondenčně via e-mail
Datum provedení rozhovoru	10. 5. 2022

Jakým způsobem usiluje NÚKIB o zajištění adekvátní expertní základny státní správy v oblasti kyberbezpečnosti?

Změnou patřičné legislativy. Tvorbou a připomínkováním národních strategických dokumentů, které se touto oblastí zaobírají. Podílením se na změnách vzdělávacích programů středních a vyšších odborných škol a spoluprací s vysokými školami. Osvětovou aktivitou na všech úrovních (vláda, parlament, ministerstva, profesní spolky, odborné konference, soutěže atd.)

Poznámka 1: Role NÚKIB vychází ze Zákona o kybernetické bezpečnosti a NÚKIB se musí řídit i Kompetenčním zákonem. Role v přípravě expertní základny veřejné správy jsou rozděleny mezi MV ČR, MPSV ČR, MŠMT ČR a NÚKIB.

Poznámka 2: Nutno vnímat i rozdělení zaměstnanců veřejné správy. Státní zaměstnanci (Zákon o státní službě, zaměstnanci samospráv (jejich vlastní zákon a ostatní).

Co vnímáte jako slabé stránky zajišťování adekvátní expertní základny státní správy v oblasti kyberbezpečnosti?

Nejednotné vedení a roztříštěnost pravomocí mezi jednotlivá ministerstva a ostatní ÚSO. Neflexibilitu ÚSO při řešení problému. Neflexibilitu VŠ a malou profesní orientaci studijních oborů. Omezené využívání SŠ, VOŠ a kurzů pro přípravu odborníků KB. Nedostatek financí na vzdělávání a odměňování specialistů KB. Neoddělení ICT a KB.

Jakým způsobem je usilováno o zajištění konkurenceschopnosti státní správy na trhu práce v oblasti kyberbezpečnosti?

Není.

Pomohlo by v úsilí o zajištění konkurenceschopnosti státní správy jasné definování kroků k tomu vedoucích v Akčním plánu Národní strategie kybernetické bezpečnosti?

Ne, nepomohlo. Muselo by se začít přerozdělením kompetencí mezi ÚSO (jedna hlava) a dedikováním odpovídajícího množství finančních a materiálních zdrojů. Dále by muselo dojít ke změně myšlení.

Pomohlo by vytvoření specifické normy pro odměňování expertů v oblasti kyberbezpečnosti zajistit větší konkurenceschopnost státní správy?

Ano, pomohlo. Částečně. To je startovní bod. Musí se ovšem měnit i organizační kultura, vybavení a prostředí, ve kterém se specialisté KB pohybují.

Příloha F Přepis rozhovoru s Expertem č. 6

Tab. 8: Informace o rozhovoru s Expertem č. 6 (vlastní tabulka)

Expert č. 6	
Označení ve zdrojích	Švéda, Martin
Pracoviště	NÚKIB – Oddělení regulace soukromého sektoru
Délka praxe	6 let
Forma rozhovoru	Korespondenčně via e-mail
Datum provedení rozhovoru	23. 5. 2022

Jakým způsobem spolupracuje NÚKIB se subjekty ze soukromého sektoru mimo Zákon o kybernetické bezpečnosti?

Spolupráce se soukromým sektorem může být velmi široký pojem. Mezi nejběžnější spolupráce patří společná jednání, přednášky a workshopy, kde NÚKIB adresátům zákona vysvětluje problematiku a snaží se řešit jejich praktické problémy, ale to jsou subjekty spadající pod zákon. S tím však souvisí zcela běžné zodpovídání dotazů a to často i ze strany neregulovaných subjektů. Pokud je to smysluplné, snaží se NÚKIB také přizvat odbornou veřejnost k vytváření legislativy – aktuálně např. zde: Národní úřad pro kybernetickou a informační bezpečnost - NÚKIB vyzývá odbornou veřejnost k zasílání návrhů na změny zákona č. 181/2014 Sb., o kybernetické bezpečnosti (nukib.cz), ale bylo tomu obdobně i v minulosti. Odborná veřejnost se podílí na přípravě některých podpůrných materiálů. S celou řadou soukromých společností má NÚKIB také uzavřena memoranda o spolupráci (např. Národní úřad pro kybernetickou a informační bezpečnost - Bankéři a kybernetičtí odborníci se dohodli na spolupráci - nukib.cz).

Je v současnosti legislativně adekvátně ukotvena povinnost sdílet informace (např. nahlašovat kyberbezpečnostní incidenty) ze strany povinných subjektů dle Zákona o kybernetické bezpečnosti?

Česká republika jde historicky cestou toho, že povinný subjekt má hlásit vše, co naplní definici kybernetického bezpečnostního incidentu. V takovém případě může příslušný CERT situaci analyzovat a rozhodnout o nejlepším možném řešení. To je sice nejlepší možná teoretická situace, ale v praxi má několik zásadních problémů. Především je problém v šíři toho, co je kybernetický bezpečnostní incident – NÚKIB na to v nedávné době vydal obecnou metodiku.

V druhé řadě je pak problémem to, že pokud mají subjekty hlásit vše co takto obecnou definici naplní, nehlásí nic nebo jen velmi omezenou množinu incidentů (při stovkách povinných subjektů se nezdá příliš pravděpodobné, že by se odehrálo průměrně 14 kybernetických bezpečnostních incidentů za měsíc – viz Národní úřad pro kybernetickou a informační bezpečnost - Kybernetické incidenty pohledem NÚKIB: březen 2022 - nukib.cz).

Evropská směrnice NIS a některé členské státy požadují hlášení jen významných incidentů (resp. incidentů s významným dopadem). Tento přístup má zase ten problém, že významnost incidentu je zpravidla možno stanovit až po jeho úplném vyřešení – a tedy je na začátku těžko zodpověditelná otázka, zda to co se děje je skutečně incident s významným dopadem. Diskuze na volbu prvního nebo druhého přístupu není uzavřena a obě mají své obhájce. Dostatečnost našeho aktuálního zhodnocení potom není možné ještě zhodnotit, ale toto téma by mohlo být zajímavou výzkumnou otázkou pro nějakou z akademických prací.

Bylo by žádoucí rozšířit povinnost sdílet informace (např. o kyberbezpečnostních incidentech) i na subjekty, které v současnosti nejsou upraveny Zákonem o kybernetické bezpečnosti?

Zákon aktuálně stojí na principu minimalizace státního donucení, tedy zjednodušeně reguluje a ukládá povinnosti jen těm, u kterých je to nezbytné. Z tohoto pohledu ukládat povinnost neregulovaným osobám je v rozporu s tímto principem. Kdybychom od tohoto principu odhlédli, je otázkou proč vynucovat hlášení incidentů, ale už ne další povinnosti a tedy proč vlastně neudělat z neregulovaných osob regulované.

Hlášení incidentu není také nic, co by se jen tak v organizaci zjevilo – předchází mu vnitřní procesy v organizaci, které stanoví (ať už písemně nebo pouze prakticky) jak vůbec poznat co to je incident, kdo se tím má zabývat, co se má dělat a podobně. Toto vše už je velký překryv s bezpečnostními opatřeními, tedy s podstatou regulace zákona o kybernetické bezpečnosti. Když k tomu zvážíme, že dle zákona o kybernetické bezpečnosti je možné hlásit jakékoliv incidenty dobrovolně i pokud nejste regulovanou osobu, je pak odpověď spíše ne – nezdá se žádoucí rozšířit povinnost na neregulované subjekty, spíše je v této věci možno otevřít diskuzi, zda by neměla být množina povinných osob větší.

Je spektrum subjektů, u kterých jsou dle současné legislativy vyžadována základní technická kyberbezpečnostní opatření adekvátní?

Tato otázka má opět více množin. Historicky se však ukazuje, že dosavadní regulace má stále své mezery. Chybným nastavením kritérií podle nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, nebyly například dlouhou dobu v rámci regulace kybernetické bezpečnosti vůbec zahrnuty nemocnice. K nápravě tohoto stavu došlo v roce 2017 s přijetím vyhlášky č. 437/2017 Sb., o kritériích pro určení

provozovatele základní služby, nicméně během pandemie COVID-19 se ukázalo, že ani tato regulace neodpovídala představám a došlo k jejímu opětovnému rozšíření. Je možné, že tato situace se bude opakovat, nicméně NÚKIB se snaží tyto neregulované ale důležité oblasti průběžně odhalovat a odstraňovat. Problémem je však také fakt, že oblast bezpečnostní prevence trpí tou nevýhodou, že vůle k jejímu komplexnímu řešení je vždy o několik řádu menší, než když problém nastane a toto rozšiřování se tak NÚKIBu daří prosazovat jen omezeně.

Příloha G Přepis rozhovoru s Expertem č. 7

Tab. 9: Informace o rozhovoru s Expertem č. 7 (vlastní tabulka)

Expert č. 7	
Označení ve zdrojích	Anonymní zdroj č. 4
Pracoviště	NÚKIB – Oddělení cvičení
Délka praxe	6 let
Forma rozhovoru	Korespondenčně via e-mail
Datum provedení rozhovoru	25. 5. 2022

Věnuje se NÚKIB budování odolnosti státu či dalších subjektů vůči hrozbě ransomware prostřednictvím cvičení?

Problematiku ransomware zahrnujeme do mnoha našich cvičení, a to především těch netechnických, table-top cvičení. Příkladem může být sektorové cvičení Health Czech, cvičení pro platformu pro spolupráci státu a strategických firem obranného průmyslu, cvičení pro ČEPS apod. Problematika ransomware se dá rovněž využít pro workshopy mířící na kontinuitu činností.

Pro koho jsou tato cvičení organizována?

Cvičení provádíme pro široké spektrum subjektů, a to těch spadajících pod ZKB, ale i pro partnerské instituce.

Jak často jsou tato cvičení organizována?

Nelze říci, jak často provádíme cvičení, která se zaměřují konkrétně na hrozbu ransomware. Pro ilustraci – v roce 2021 jsme zorganizovali a/nebo se zúčastnili 14 cvičení kybernetické bezpečnosti. Do tohoto jsou zahrnuta úplně všechna, nejen ten ransom.

Jakou formou jsou tato cvičení organizována?

Nejčastější formou jsou netechnická, table-top cvičení, kdy účastníci řeší situace představené fiktivním scénářem a navrhují jejich řešení.