Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra statistiky

Diplomová práce

Analýza kybernetické kriminality v ČR a Ústeckém kraji

Bc. Jan Racín

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Jan Racín

Veřejná správa a regionální rozvoj – c.v. Most

Název práce

Analýza kybernetické kriminality v ČR a Ústeckém kraji

Název anglicky

Analysis of cybercrime in the Czech Republic and Ústí nad Labem Region

---

Cíle práce

Diplomová práce si za hlavní cíl klade provedení statistické analýzy vybraných hospodářských a majetkových trestných činů, které nejčastěji spadají do oblasti kybernetické kriminality, kdy bude provedeno zkoumání struktury a vývoje registrovaných skutků mezi lety 2011 až 2023 v České republice a Ústeckém kraji a jejich vzájemné porovnání.

Vedlejšími cíli diplomové práce pak bude zkoumání poměrových tendencí, vývoje objasněnosti a vypočtení indexu kybernetické kriminality pro Českou republiku a Ústecký kraj.

Dalším vedlejším cílem bude vymezení trestných činů, které se dají zařadit do kybernetické kriminality, zjištění jejich vývojových trendů, zhodnocení úrovně a kvality stávající prevence, možných nedostatků, slabin a jejich řešení z hlediska praxe v oboru provedením kvalitativního výzkumu formou rozhovorů.

Metodika

Práce bude rozdělena na teoretickou a praktickou část.

V teoretické části budou s využitím metody rešerše literatury vymezeny základní definice a pojmy z oblasti kybernetické kriminality. Dále budou definovány pojmy škodlivých programů.

V praktické části budou využity metody kvantitativního a kvalititativního výzkumu. Nejprve bude provedena statistická analýza dat za účelem kvantifikace vývoje počtu trestných činů v kyberprostoru v České republice v porovnání s Ústeckým krajem s využitím metod pro analýzu časových řad.

Pro vypracování kvantitativního oddílu praktické části diplomové práce budou použita data z Policejní statistiky a Českého statistického úřadu pro jejichž zpracování bude využito základních charakteristik časových řad.

V kvalitativním oddílu praktické části diplomové práce budou získávána data pomocí dotazování pracovníků z oblasti kyberkriminality. Po provedeném zkoumání budou zjištěná data vyhodnocena.

Doporučený rozsah práce

60-80 stran

Klíčová slova

anonymita uživatele, časová řada, digitální stopa, kvalitativní výzkum, kvantitativní výzkum, kybernetická hygiena, kybernetická kriminalita, škodlivé programy

---

Doporučené zdroje informací

KOLOUCH, Jan. CyberCrime. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7.

KONRÁD, Zdeněk; PORADA, Viktor; STRAUS, Jiří a SUCHÁNEK, Jaroslav. Kriminalistika: kriminalistická taktika a metodiky vyšetřování. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. ISBN 978-80-7380-547-0.

PUŽMANOVÁ, Rita. TCP/IP v kostce. 2., upr. a rozš. vyd. České Budějovice: Kopp, 2009. ISBN 978-80-7232-388-3.

SEDLÁK, Petr a KONEČNÝ, Martin. Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

SMEJKAL, Vladimír. Kybernetická kriminalita. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. ISBN 978-80-7380-849-5.

STREBE, Matthew a PERKINS, Charles. Firewally a proxy-servery: praktický průvodce. Brno: Computer Press, 2003. ISBN 80-7226-983-6.

VÁLKOVÁ, Helena a KUCHTA, Josef. Základy kriminologie a trestní politiky. 2. vyd. Beckovy mezioborové učebnice. V Praze: C.H. Beck, 2012. ISBN 978-80-7400-429-2.

Zároveň další literatura dle pokynů vedoucí DP

Předběžný termín obhajoby

2023/24 LS – PEF

Vedoucí práce

Ing. Zuzana Pacáková, Ph.D.

Garantující pracoviště

Katedra statistiky

Elektronicky schváleno dne 11. 3. 2024

Ing. Tomáš Hlavsa, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 11. 3. 2024

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 24. 03. 2024

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Analýza kybernetické kriminality v ČR a Ústeckém kraji" jsem vypracoval(a) samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 31. 3. 2024 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Zuzaně Pacákové, Ph.D. za odborné vedení, trpělivost, cenné rady a připomínky, které mi pomohly vypracovat mou diplomovou práci.

Analýza kybernetické kriminality v ČR a Ústeckém kraji

Abstrakt

V diplomové práci byla za využití kombinace kvantitativního a kvalitativního výzkumu, posouzena struktura vývoje vybraných hospodářských a majetkových trestných činů, které nejčastěji spadají do oblasti kybernetické kriminality v České republice a Ústeckém kraji. Kvantitativním výzkumem byly zjištěny rostoucí vývojové trendy ve zkoumané oblasti, a to jak v absolutním počtu registrovaných trestných činů, tak v poměrové tendenci, kdy bylo zjištěno, že se zkoumaná trestná činnost přesouvá do kyberprostoru. Provedeným kvalitativním výzkumem byly potvrzeny výsledky statistických analýz a dále byly zjištěny slabiny a problémy v nastavených procesech a zvyklostech ve zkoumané oblasti, kdy na základě zjištěných informací byla stanovena zlepšující doporučení.

Klíčová slova: anonymita uživatele, časová řada, digitální stopa, kvalitativní výzkum, kvantitativní výzkum, kybernetická hygiena, kybernetická kriminalita, škodlivé programy

Analysis of cybercrime in the Czech Republic and Ústí nad Labem Region

Abstract

In the diploma thesis, using a combination of quantitative and qualitative research, the structure of the development of selected economic and property penalties, which most often fall into the field of cybercrime in the Czech Republic and the Ústí nad Labem Region, was assessed. Quantitative research revealed increasing development trends in the researched area, bot in the absolute number of registered criminal acts and in the relative tendency, when it was found that the researched criminal activity is moving into cyberspace. The conducted qualitative research confirmed the results of statistical analyses, and further identified weaknesses and problems in the set processes and practices in the researched area, where improvement recommendations were established based on the information found.

Keywords: user anonymity, time series, digital footprint, qualitative research, quantitative research, cyber hygiene, cyber crime, malicious program

Obsah

1 Úvod **11**

2 Cíl práce a metodika **12**

2.1 Cíl práce 12

2.2 Metodika 12

2.2.1 Časové řady a jejich srovnatelnost 13

2.2.2 Indexní analýza 14

2.2.3 Index kriminality 14

2.2.4 Rozhovory s experty 15

3 Teoretická východiska **16**

3.1 Úvod do problematiky 16

3.1.1 Kriminologie 17

3.1.2 Stav kriminality 17

3.1.3 Charakteristika trestného činu 18

3.1.4 Zdroje informací o kriminalitě 18

3.1.5 Hospodářská kriminalita 19

3.2 Kybernetická kriminalita 20

3.2.1 Anonymita uživatele 21

3.2.2 Digitální stopa 22

3.2.3 Kybernetická hygiena 23

3.3 Škodlivé programy, podvodné metody a jejich charakteristika 23

3.3.1 Ransomware 24

3.3.2 Phishing (Spear Phishing, Vishing a Smishing) 26

3.3.3 Malware 30

3.3.4 Sociální inženýrství 31

3.3.5 Hacking 33

3.3.6 Cracking 34

3.4 Možnosti prevence 35

4 Vlastní práce **37**

4.1 Charakteristika Ústeckého kraje 37

4.2 Rozbor trestných činů spáchaných v letech 2011 až 2020 37

4.2.1 Vývoj počtu registrovaných skutků 38

4.2.2 Poměrové tendence 44

4.2.3 Porovnání objasněnosti 47

4.2.4 Index kriminality 52

4.3 Rozbor trestných činů spáchaných v letech 2021 až 2023 54

4.3.1 Vývoj počtu registrovaných skutků 54

4.3.2 Poměrové tendence 59
4.3.3 Porovnání objasněnosti 61
4.3.4 Index kriminality 65
4.4 Rozhovory s osobami participujícími při řešení kybernetické kriminality 66
4.4.1 Analytik ÚSKPV 66
4.4.2 Zástupce vedoucího okresní OHK 72
4.4.3 Vyšetřovatelka okresní OHK 75
4.4.4 Vedoucí krajského OKK 79
4.4.5 Vyšetřovatel krajské OHK 82
4.4.6 Okresní státní zástupce 86
4.4.7 Sumarizace provedených rozhovorů 92

5 Výsledky a diskuse 94

6 Závěr 99

7 Seznam použitých zdrojů 102

8 Seznam obrázků, tabulek, grafů a zkratek 104
8.1 Seznam obrázků 104
8.2 Seznam tabulek 104
8.3 Seznam grafů 105

1 Úvod

V současné době žijeme v digitálním světě, což přináší klady i zápory. Digitalizace přináší usnadnění spousty procesů, ale zároveň i nová rizika. Kyber prostor nemá hranice a je propojen v celosvětovém měřítku, což vede k větší anonymitě jeho uživatelů.

S každodenním využíváním moderních technologií v běžných oblastech lidských činností, sdílením dat a informací na sociálních sítí, využíváním virtuálního prostoru k převážné většině komunikace, používání elektronických bankovnictví, využívání služeb internetových obchodů a aplikací obchodů kamenných, kde ve všech těchto oblastech o sobě každý z nás poskytuje citlivá data ke své osobě může docházet k jejich zneužití.

Tato škodlivá jednání se projevují převážně v hospodářské a majetkové kriminalitě, která se čím dál více přenáší do digitálního prostoru a označujeme ji jako kyberkriminalitu. Tato kriminalita je páchána za využití internetu a ostatních sítí za pomoci počítačů a mobilních zařízení, které jsou přirozenou součástí lidského života. Přičemž zavádění bezpečnostních opatření nestačí tempu zavádění a zneužívání nových technologií.

Proto je společensky žádoucí se nově nastupujícím fenoménem kyberkriminality zabývat.

2 Cíl práce a metodika

2.1 Cíl práce

Diplomová práce si za hlavní cíl klade provedení statistické analýzy vybraných hospodářských a majetkových trestných činů, které nejčastěji spadají do oblasti kybernetické kriminality, kdy bude provedeno zkoumání struktury a vývoje registrovaných skutků mezi lety 2011 až 2023 v České republice a Ústeckém kraji a jejich vzájemné porovnání.

Vedlejšími cíli diplomové práce pak bude zkoumání poměrových tendencí, vývoje objasněnosti a vypočtení indexu kybernetické kriminality pro Českou republiku a Ústecký kraj.

Dalším vedlejším cílem bude vymezení trestných činů, které se dají zařadit do kybernetické kriminality, zjištění jejich vývojových trendů, zhodnocení úrovně a kvality stávající prevence, možných nedostatků, slabin a jejich řešení z hlediska praxe v oboru provedením kvalitativního výzkumu formou rozhovorů.

2.2 Metodika

Práce bude rozdělena na teoretickou a praktickou část.

V teoretické části budou s využitím metody rešerše literatury vymezeny základní definice a pojmy z oblasti kybernetické kriminality. Dále budou definovány pojmy škodlivých programů.

V praktické části budou využity metody kvantitativního a kvalititativního výzkumu. Nejprve bude provedena statistická analýza dat za účelem kvantifikace vývoje počtu trestných činů v kyberprostoru v České republice v porovnání s Ústeckým krajem s využitím metod pro analýzu časových řad.

Pro vypracování kvantitativního oddílu praktické části diplomové práce budou použita data z Policejní statistiky a Českého statistického úřadu pro jejichž zpracování bude využito základních charakteristik časových řad.

V kvalitativním oddílu praktické části diplomové práce budou získávána data pomocí dotazování pracovníků z oblasti kyberkriminality. Po provedeném zkoumání budou zjištěná data vyhodnocena.

Pro naplnění cílů práce bude kombinován kvantitativní výzkum hodnocení časových řad a kvalitativní výzkum provedení kvalitativního dotazování, rozhovorů s experty.

2.2.1 Časové řady a jejich srovnatelnost

Časové řady jsou sekvence srovnatelných údajů z hlediska jejich věcnosti a prostorového zařazení, kdy tato data jsou z časového hlediska srovnána od minulosti k přítomnosti. Vyhodnocování dat z časových řad za pomoci jednoduchých ukazatelů funguje jako nástroj k jejich interpretaci. Před vyhodnocováním a dalším zpracováváním dat z časové řady musíme posoudit, zdali lze tato data porovnávat. K tomuto posouzení slouží tři hlediska, a to věcné, prostorové a časové. Věcné hledisko posuzuje obsahovou jednotnost zkoumaných dat. Prostorové hledisko odráží srovnávání dat ze stejného zeměpisného regionu. Časové hledisko zkoumaných dat je důležité hlavně u intervalových ukazatelů.[1]

V rámci této diplomové práce budou zkoumány dlouhodobé roční časové řady.

[1] HINDLS, Richard. Statistika pro ekonomy. 8. vyd. Praha: Professional Publishing, 2007. Str.246 – 251. ISBN 978-80—86946-43-6.

2.2.2 Indexní analýza

Základní trendy vývoje časových řad je možné určit skrze základní míru jejich dynamiky, přičemž nejzákladnějším mírou dynamiky je absolutní přírůstek (první diference), tato hodnota představuje časovou změnu v časové hodnotě t oproti časové hodnotě t – 1.[2]

$$\Delta y_t = y_t - y_{t-1}, \qquad t = 2, \ldots, T. \qquad (1)$$

Dalším významným ukazatelem míry dynamiky časových řad je koeficient růstu nebo také tempo růstu, který po vynásobení 100 ukazuje procentuální nárůst v čase t – 1 oproti času t.[3]

$$k_t = y_t / y_{t-1}, \qquad t = 2, \ldots, T. \qquad (2)$$

2.2.3 Index kriminality

Intenzita (úroveň) kriminality, která je dána rozsahem kriminality v přepočtu na počet obyvatel na vymezeném území. Je vyjádřena indexem (koeficientem) kriminality. Údaje o intenzitě kriminality vyjádřené v indexech podávají přesnější přehled o kriminalitě než údaje o jejím rozsahu. Získaný údaj více reflektuje demografické vlivy, ale i zde je nutné počítat s určitým zkreslením, neboť obětí mohl být i cizinec. Primárně však vypovídá především o trestní politice uplatňované na určitém území.[4]

Index = (počet trestných činů / počet obyvatel na vymezeném území) x 100 000 (3)

[2] ARLT, Josef; ARLTOVÁ, Markéta a RUBLÍKOVÁ, Eva. Analýza ekonomických časových řad s příklady. Praha: Vysoká škola ekonomická, 2002. Str. 14. ISBN 80-245-0307-7.
[3] ARLT, Josef; ARLTOVÁ, Markéta a RUBLÍKOVÁ, Eva. Analýza ekonomických časových řad s příklady. Praha: Vysoká škola ekonomická, 2002. Str. 15. ISBN 80-245-0307-7.
[4] *Kriminalita v ČR a EU* [Web]. 2023 [cit. 2024-03-31]. ISSN 080009-23. Dostupné z: https://www.czso.cz/csu/czso/kriminalita-v-cr-a-eu-2012-2022. Str. 5.

2.2.4 Rozhovory s experty

Jednou z metod kvalitativního dotazování, které slouží k získávání informací v empirickém výzkumu je rozhovor s expertem, kdy tento je použit při zkoumání vědomostí a praktických zkušeností odborníků z oboru. Cílem této metody je zjistit zkušenosti a erudice expertů, jejich analýza a využití pro stanovené cíle. Expertům budou nejdříve kladeny obecné dotazy ke zkoumanému tématu, které umožní náhled na dané odvětví, aby byly zjištěny jeho možné aktuální problémy a slabiny v nastavených procesech a zvyklostech, dle praktických zkušeností dotazovaných respondentů. Zjištěné problémy a slabiny budou v další fázi do upřesňujícími dotazy více rozebrány tak, aby byla zjištěna bližší a konkrétnější zájmová data, která budou následně podrobena analýze.[5]

V rámci této diplomové práce budou jako respondeti pro kvalitativní výzkum vybráni experti z oboru napříč celou organizační strukturou policie, a to z okresní, krajské i celorepublikové úrovně a také bude osloven okresní státní zástupce. Zjištěné poznatky budou využity pro identifikaci slabých stránek stávajících postupů a formulaci doporučení k jejich nápravě.

[5] HENDL, Jan. *Kvalitativní výzkum: základní teorie, metody a aplikace*. Čtvrté, přepracované a rozšířené vydání. Praha: Portál, 2016. Str. 193. ISBN 978-80-262-0982-9.

3 Teoretická východiska

3.1 Úvod do problematiky

„Základní charakteristika naší digitální epochy je asi následující: obyvatelé naší planety vlastní 5,2 miliardy mobilů, to je 73% populace, z toho asi 40% jsou smartphony; denně se prodá více mobilů, než se narodí dětí; každou minutou je rozesláno 204 milionů e-mailů, přidáme 2,46 milionů příspěvků na Facebook, vytvoříme a publikujeme 216 tisíc fotek, natočíme a pošleme na síť 72 hodin videa, vznikne 48 tisíc aplikací; denně se v průměru díváme 150krát na svůj mobil; každé dvě minuty je pořízeno tolik digitálních fotografií jako v celém 19. století.“[6]

Růst digitálních technologií postupuje vpřed exponenciálním tempem a zdá se, že nemá v úmyslu zpomalit. V digitálním věku jsou klíčové dovednosti schopnost správně chápat informační a kybernetickou bezpečnost jako nedílnou a související část digitální gramotnosti, do které patří rozpoznání, kdy a proč jsou informace potřebné, jak je správně a bezpečně najít, jak je zhodnotit, využít a komunikovat s nimi v souladu s etickými principy. Termín „počítačová gramotnost“ obsahuje znalosti, schopnosti a dovednosti, které se zaměřují na efektivní a spolehlivé používání výpočetní techniky v každodenním životě.[7]

Veškerá námi poskytnutá data a informace ve virtuálním prostoru mají potenciál významně ovlivnit naše budoucí chování a rozhodování. Každý z nás svá data v kyberprostoru sdílí pomocí komunikačních a informačních technologií, jako jsou různé sociální sítě, mobilní a spotřebitelské aplikace. S tímto procesem je spojen i nárůst kyberkriminality, což představuje trestnou činnost v digitálním prostoru.[8]

Typickým znakem současné doby je propojení moderních počítačových a informačních technologií do všech oblastí lidského života, kdy můžeme říci, že nyní není žádný okruh

[6] SEDLÁK, Petr a KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. Str. 20. ISBN 978-80-7623-068-2.
[7] SEDLÁK, Petr a KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. Str. 19-21. ISBN 978-80-7623-068-2.
[8] SMEJKAL, Vladimír. Kybernetická kriminalita. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. Str. 31-34. ISBN 978-80-7380-849-5.

činností, kde by nedocházelo, ať už v menší, či větší míře, k využívání komunikačních či informačních systémů a zařízení výpočetní techniky.[9]

3.1.1 Kriminologie

Ze slov crimen – zločin a logos – učení definujeme pojem kriminologie jako učení o zločinu. Pokud dále budeme kriminologii brát jako empirickou vědu vycházející z teoretických koncepcí a modelů, které lze prověřit vědeckými metodami – zejména pomocí empirických výzkumů, statistických analýz.

Toto bude prohloubeno ekonomickým pravidlem Gary S. Beckera tedy konceptem racional choice – racionální volby, o člověku jako homo oeconomicus a tím, že svým jednáním se každý snaží o dosažení maximálních užitků a výhod. V kontextu kriminality lez předpokládat, že jednotlivec vědomě posuzuje náklady a zisky spojené spácháním konkrétního trestného činu, a to jaké zisky mu jeho jednání přinese, tak i náklady, které je k tomu třeba investovat. Teprve tehdy, pokud se podle jeho odhadu kriminální akt vyplatí, tak je ochoten ho spáchat. V tomto přístupu hraje klíčovou roli racionální rozhodnutí jednotlivce, které přijímá po pečlivém zvážení všech kladů a záporů porušení společenského právního rámce. Ekonomické posouzení jakéhokoli protiprávního jednání se řídí obecně platnými vzorci lidského chování a ekonomickými principy.[10]

3.1.2 Stav kriminality

Jedním z hlavních prvků studia kriminologie je analýza kriminality jako sociálně patologického fenoménu, a na toto téma se zaměřuje kriminální fenomenologie. Důraz na tuto problematiku není motivován pouze snahou porozumět povaze kriminality v určitém regionu, sledovat její vývoj v průběhu času a zkoumat její strukturu. Zájem spočívá rovněž v možnosti přispět k identifikaci kořenů kriminality. Při analýze dat o rozsahu kriminality je nezbytné brát v úvahu, že tato čísla nemusí zohledňovat demografické vlivy. Při interpretaci těchto údajů může dojít k významnému zkreslení skutečné situace, zejména pokud se

[9] KOLOUCH, Jan. CyberCrime. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2016. Str. 31. ISBN 978-80-88168-15-7.
[10] VÁLKOVÁ, Helena a KUCHTA, Josef. Základy kriminologie a trestní politiky. 2. vyd. Beckovy mezioborové učebnice. V Praze: C.H. Beck, 2012. Str. 110-111. ISBN 978-80-7400-429-2.

porovnává počet trestných činů v různých regionech bez zohlednění jejich obyvatelstva. To může vést k nesprávnému závěru, že region s nejvyšším počtem registrovaných trestných činů je výrazněji postižen kriminalitou, i když je ve skutečnosti oblastí s vysokým počtem obyvatel. Proto je důležité při popisu kriminality brát v úvahu tzv. intenzitu (úroveň) kriminality, která zohledňuje rozsah kriminality v přepočtu na počet obyvatel na daném území, která je vyjádřena indexem (koeficientem) kriminality.[11]

3.1.3 Charakteristika trestného činu

Pokud má kriminalistika vytvářet efektivní metody odhalování, vyšetřování a prevence trestných činů, je nezbytné důkladně studovat charakteristiku samotné trestné činnosti. Trestný čin představuje komplexní sociální jev, jehož analýzou se zabývá několik vědních oborů, včetně kriminologie a trestního práva. Kriminalistická charakteristika trestného činu představuje popis kriminalisticky relevantních vlastností, což znamená takových charakteristik, které ovlivňují proces identifikace stop s podrobností trestného činu. Hlavním cílem kriminalistických metod je umožnit poznání podstaty trestného činu, proto jsou zvláště významné skutkové znaky trestného činu, což platí pro znaky, které jsou promítnuty ve stopách, mají trvalý charakter a jsou specifické.[12]

3.1.4 Zdroje informací o kriminalitě

Zdroje informací o kriminalitě rozdělujeme do dvou skupin, a to na zdroje informací o registrované kriminalitě, kam zařazujeme kriminální statistiky získávané a zpracovávané orgány činnými v trestním řízení a dále na zdroje informací o latentní kriminalitě, jejichž hlavními zdroji jsou výzkumy obětí a pachatelů trestné činnosti.

V této práci budeme vycházet z prvně uvedených zdrojů, tedy statistik orgánů činných v trestním řízení, kdy v České republice jde o policejní statistiky, které jsou shromažďované a zpracovávané Policejním prezidiem ČR a statistiky státních zastupitelství a soudů, které

[11] VÁLKOVÁ, Helena a KUCHTA, Josef. Základy kriminologie a trestní politiky. 2. vyd. Beckovy mezioborové učebnice. V Praze: C.H. Beck, 2012. Str. 1-8. ISBN 978-80-7400-429-2.
[12] VÁLKOVÁ, Helena a KUCHTA, Josef. Základy kriminologie a trestní politiky. 2. vyd. Beckovy mezioborové učebnice. V Praze: C.H. Beck, 2012. Str. 8-12. ISBN 978-80-7400-429-2.

jsou shromažďované a zpracovávané Ministerstvem spravedlnosti. V této práci budou konkrétně využita data z policejních statistik.

Z uvedených zdrojů získáváme nejúplnější a nejpřesnější obraz o rozsahu kriminality prostřednictvím policejní statistiky, neboť poskytuje údaje, které jsou časově nejblíže dni spáchání trestného činu. Policejní statistika obsahuje data o všech zjištěných (policií registrovaných) trestných činech a není při tom brán zřetel na to, jestli byl pachatel identifikován a trestně stíhán. Je důležité rozlišovat údaje o trestných činech a jednotlivých skutcích od údajů o počtu pachatelů, protože jeden pachatel se může dopustit více trestných činů a naopak. Při analýze registrovaných trestných činů se musí zohlednit, že české policejní statistiky evidují počet spáchaných skutků a každý skutek je zaznamenán jako jeden trestný čin. Tento postup se týká zejména případů pokračujících trestných činů, nebo pokud se jedná o jednočinný souběh, kde se eviduje pouze nejzávažnější ze všech skutků. Z jiného pohledu mohou být data z policejních statistik méně relevantní z důvodu toho, že některé skutky mohou být zaznamenány jako trestné činy, i když se během prověřování v trestním řízení vyjde najevo, že se o trestné činy nejedná.[13]

Dalším důležitým zdrojem informací o kriminalitě je informační systém Kriminalisticky sledované události (KSU), což je centrální informační systém kriminalisticky relevantních událostí, jedná se o celostátní databázi, s jejímiž daty umožňuje dále pracovat. Tento systém je určen především pro příslušníky Služby kriminální policie a vyšetřování a patří mezi informační systémy, které postupují data dále do Schengenského informačního systému.[14]

3.1.5 Hospodářská kriminalita

Hlavní podstatou hospodářské kriminality jsou trestné činy v oblasti hospodářství, kterou jsou definovány v Hlavě VI. zvláštní části trestního zákoníku. Část z těchto skutků může být spáchána i během neobchodních činností, jako jsou trestné činy proti měně a daňové trestné činy. Další trestné činy uvedené v Hlavě V. zvláštní části trestního zákoníku, jedná se o trestné činy proti majetku, mají rovněž charakter hospodářské kriminality, pokud jsou

[13] VÁLKOVÁ, Helena a KUCHTA, Josef. Základy kriminologie a trestní politiky. 2. vyd. Beckovy mezioborové učebnice. V Praze: C.H. Beck, 2012. Str. 140-142. ISBN 978-80-7400-429-2.
[14] KONRÁD, Zdeněk; PORADA, Viktor; STRAUS, Jiří a SUCHÁNEK, Jaroslav. *Kriminalistika: kriminalistická taktika a metodiky vyšetřování*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. Str. 156. ISBN 978-80-7380-547-0.

spáchány za příslušných podmínek. Dále mezi hospodářskou kriminalitu spadají i trestné činy v oblasti konkursu a úpadku, zahrnuje i další trestné činy jako teroristický útok, sabotáž, úplatkářské trestné činy, trestné činy obecně nebezpečné, trestné činy proti životnímu prostředí a takzvané počítačové trestné činy – kybernetickou kriminalitu.[15]

3.2 Kybernetická kriminalita

Kybernetickou kriminalitu můžeme definovat jako trestnou činnost, která je páchána za výrazného využití informační a komunikačních technologií, nejčastěji se používají počítače, mobilní telefony a internet, jakožto významného prostředku k jejímu páchání.
Při definování tohoto pojmu musíme brát v potaz velké množství možností zneužívání informačních a komunikačních technologií ke společensky škodlivému jednání, z tohoto důvodu nelze vymezit nějakou obecnou definici.

Do budoucna bude nutno počítačovou kriminalitu a trestné činy páchané v kyberprostoru oficiálně a přesně definovat, kdy díky zvláštní charakteristice tohoto protiprávního jednání bude nutno upravit trestní zákonodárství a stanovit nové postupy při odhalování a prevenci této trestné činnosti.

Pro potřeby trestního řízení se o takové definice pokouší i Policie České republiky, kdy pokynem policejního prezidenta č. 103/2013 je kybernetická kriminalita definována jako *„kriminalita, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí, kdy hlavním objektem útoku je samotná oblast informačních a komunikačních technologií a v nich obsažená data.“*[16]
Dále pokyn policejního prezidenta č. 103/2013 vymezuje ostatní kriminalitu páchanou v kyberprostoru jako *„kriminalitu páchanou za výrazného využití informačních a komunikačních technologií, přičemž hlavním objektem útoku je zejména život, zdraví, majetek, svoboda, lidská důstojnost a mravnost.“*[17]

[15] VÁLKOVÁ, Helena a KUCHTA, Josef. Základy kriminologie a trestní politiky. 2. vyd. Beckovy mezioborové učebnice. V Praze: C.H. Beck, 2012. Str. 417-420. ISBN 978-80-7400-429-2.
[16] Pokyn policejního prezidenta č. 103/2013, o plnění některých úkolů policejních orgánů Policie České republiky v trestním řízení, Str. 3.
[17] Pokyn policejního prezidenta č. 103/2013, o plnění některých úkolů policejních orgánů Policie České republiky v trestním řízení, Str. 3.

3.2.1 Anonymita uživatele

Využitím mechanismu přidělování síťových adres (NAT) dochází k transformaci privátních IP adres v rámci uzavřené vnitřní sítě na společnou veřejnou IP adresu, která je poté využita pro připojení a komunikaci na Internetu. Původně byl NAT zaveden jednak jako bezpečností metoda, tak aby byl koncový uživatel „schovaný za společnou NATovou IP adresou" a dále, aby došlo k umožnění připojení více uživatelů k síti, kvůli nedostatku volných IP adres, dá se tento ochranný prvek také zneužít zastírám identity uživatelů na vnitřní síti.
Využívání principů NAT sice pomáhá utajení datového provozu a ochraňuje vnitřní síť před možnými útočníky z Internetu, protože dochází ke komunikaci z jedné společné IP adresy, tedy se veškerý přenos dat tváří, jako by vycházel z jediného počítače, proto se tohoto mechanismu dá využít také reverzně, při snahách zamaskovat identitu útočníka.[18]

Dochází tedy k maskování identity jednotlivých uživatelů, za jednou hostitelskou adresou, kdy komunikaci do vnější sítě provádí jeden hostitelský počítač, který funguje jako proxy server.

Network Address Translation (NAT) neboli překlad (přidělování) adres se začal využívat hlavně z důvodu uvolnění IP adres pro připojení do globální sítě, protože začaly docházet dostupné adresy protokolu IPv4 (adresa je omezena délkou 32 bitů). NAT měl být řešením zvýšení počtu dostupných adres, než se přejde na novou verzi protokolu IPv6, jehož adresa je dlouhá 128 bitů.[19]

Tedy přidělování síťových adres mechanismem NAT zajišťuje anonymizaci uživatelů služby vnitřní sítě, kdy připojení všech těchto uživatelů zajišťuje navenek jediný počítač, tedy víc uživatelů používá stejnou IP adresu. Tudíž identita uživatelů „vnitřní sítě" za NATem není na první pohled známá a nejde s nimi „zvenčí" komunikovat napřímo.

Další formou anonymizace uživatele je dynamické přidělování (překládání) IP adres, čímž také dochází k ochraně a „maskování" koncového uživatele, kdy po ukončení jedné

[18] STREBE, Matthew a Charles PERKINS. *Firewally a proxy-servery: praktický průvodce*. Brno: Computer Press, 2003. Str. 141. ISBN 80-7226-983-6.
[19] PUŽMANOVÁ, Rita. *TCP/IP v kostce*. 2., upr. a rozš. vyd. České Budějovice: Kopp, 2009. Str. 219. ISBN 978-80-7232-388-3.

komunikace nebo po uplynutí určité doby, je uživateli přidělena nová IP adresa, čímž dochází k zastření komunikační trasy.[20]

Z výše uvedeného tedy vyplývá, že přidělování síťových adres mechanismem NAT a dynamické IP adresy, chrání uživatele „na vnitřní síti" tím způsobem, že nedovolují komunikaci z vnějšku, tedy pokusy o připojení nebo kontakty z vnější sítě. Pokud se ale uživatel sám připojí na nějaký škodlivý obsah nebo si nějaký škodlivý program sám nainstaluje, poté jsou tyto funkce bezúčelné.

3.2.2 Digitální stopa

V současné době digitální stopy začínají být jednou ze složek důkazních prostředků ať už trestných činů z oblasti kybernetické kriminality, tak v oblasti hospodářské nebo majetkové kriminality. Vše je zapříčiněno digitalizací běžného způsobu života, kdy i pachatelé trestné činnosti používají výdobytky dnešní doby a moderní přístroje, jejichž používání za sebou zanechává digitální stopy.

Digitální stopy v kyberprostoru mají zvláštní rysy, proti tradičním stopám se zde většinou jedná o nehmatatelné procesy a operace ve virtuálním prostoru či systému jejichž nalezení, zajištění a případná následná reprodukce vyžaduje určitou míru odborné znalosti a musí se tedy dodržovat určité metody zajišťovaní těchto dat, tak aby byly použitelné při následném vyšetřování.[21]

Užší definici digitální stopy vymezila International Organization of Computer Evidence (IOCE), dnes již neexistující organizace, která za digitální stopu označila „jakoukoliv informaci, uloženou nebo přenášenou v binární formě, která může být předložena soudu jako věcný důkaz". Toto vymezení staví do popředí právě kritérium využitelnosti zajištěných dat v soudním řízení.[22]

---

[20] STREBE, Matthew a Charles PERKINS. *Firewally a proxy-servery: praktický průvodce*. Brno: Computer Press, 2003. Str. 145. ISBN 80-7226-983-6.

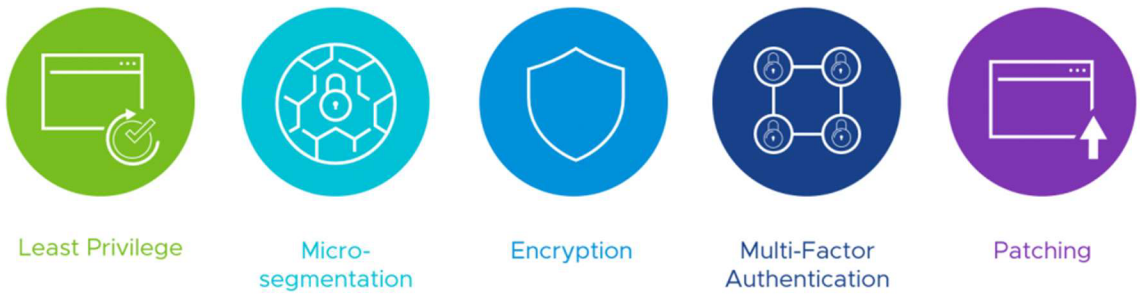
[21] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. Str. 825. ISBN 978-80-7380-849-5.

[22] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. Str. 825. ISBN 978-80-7380-849-5.

3.2.3 Kybernetická hygiena

Koncept kybernetické hygieny můžeme chápat jako pokračování ochranného pohledu na informační a kybernetickou bezpečnost. Tento přístup je postaven na trvalém rozvíjení povědomí o bezpečnosti na všech stupních. Základním předpokladem kybernetické hygieny je analogická koncepce k osobní hygieně s cílem minimalizovat virtuální nebezpečí. Tato doporučení jsou zvláště relevantní ve sférách ochrany perimetru, síťové bezpečnosti, zabezpečení zařízení, bezpečnosti cloudových řešení a ochraně dodavatelského řetězce. Vedle těchto obecných pokynů jsou konkrétnější doporučení směřující k vytváření správných návyků implementována přesněji v rámci pilířů kybernetické hygieny, kdy jde o omezení výjimek, mikrosegmentaci, šifrování, vícefaktorovou autentizaci a pravidelné upgrady softwaru.[23]

Obrázek č. 1: Základní pilíře kybernetické hygieny



Zdroj: VMware[24]

3.3 Škodlivé programy, podvodné metody a jejich charakteristika

Způsoby, jak dochází k neoprávněnému přístupu k počítačovému systému nejsou pouze instalací nebo šířením škodlivých kódů nebo programů jako jsou ransomware nebo malware. Drtivá většina neoprávněných přístupů nebo podvodů je spáchána díky obratnému přesvědčení oběti, která poté prakticky dobrovolně své přístupové údaje. K manipulaci,

[23] SEDLÁK, Petr a KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. Str. 126-131. ISBN 978-80-7623-068-2.
[24] Overcoming the Barriers to Micro-segmentation. Online. In: Network and Security Virtualization. 2019. Dostupné z: https://blogs.vmware.com/networkvirtualization/2019/10/overcoming-barriers-to-micro-segmentation.html/. [cit. 2024-03-31].

někdy i cíleně vybrané oběti dochází za využití podvodných metod, jako jsou různé druhy phisingu, vishingu nebo sociálního inženýrství.

3.3.1 Ransomware

Typickým příkladem neoprávněného přístupu k počítačovému systému a nosiči informací je ransomware. Jedná se o specifický typ škodlivého kódu, který se používá k vydírání uživatelů, jedná se o vyděračský program – software. Některé formy ransomware šifrují soubory na pevném disku, jiné jen zamknou systém a výhružnou zprávou se snaží donutit uživatele k zaplacení nějaké finanční sumy. Po infikování zařízení tento škodlivý program uživateli blokuje k tomuto zařízení přístup nebo na disku šifruje data.

Pro ransomware je příznačné šíření trojským koněm nebo červem vstupujícím do systému například přes stažené soubory nebo skrze chyby v zabezpečení. Ransomware je oblíbený druh malwaru, jedním z důvodů takové obliby ransomware je velice snadná a velká rozšířenost různých jeho kódů na internetu. Tyto různé kódy jejich tvůrci stále vylepšují a upravují, mění i způsoby šifrování, proto se určité druhy ransomwaru mohou objevit i několikrát po sobě. Hlavním cílem útočníků, kteří používají ransomware je rozšířit ho mezi co nejvíce zařízení ke koncovým uživatelům a následně díky němu vydělat, co nejvíce peněz. Proto se hledají i různé alternativní způsoby co největšího šíření.

Ransomware má různé druhy, nejběžnějším druhem je krypto-malware (kryptografický ransomware). Tento druh šifruje soubory a data. Uživatel se po napadení může k zařízení dále přihlašovat, ale jeho soubory nebo data jsou zašifrované. Typickými příklady tohoto druhu jsou WannaCry, AIDS Trojan nebo CryptoLocker.

Druh ransomwaru označovaný jako locker naopak zcela uzamyká napadené zařízení, aby se k němu nedalo přihlásit. Toto dělá například ransomware Petya, který počítač uzamyká zašifrováním hlavní tabulky souborů na pevném disku.

Doxware z napadeného zařízení odesílá možná citlivá data a soubory. Útočník se poté vyhrožováním zveřejnění těchto dat a souborů snaží poškozeného vydírat k zaplacení výkupného. Příkladem lze jmenovat doxware Ransoc.

Dalším druhem ransomwaru je scareware. Jedná se o falešný software, který hlásí, že v napadeném zařízení nalezl nějaký problém a za jeho vyřešení požaduje peníze. Tento software může obrazovku napadeného zařízení zaplňovat vyskakovacími okny nebo různými výstrahami. Také může vyhrožovat uzamknutím napadeného zařízení, pokud nedojde k zaplacení nějaké finanční částky.

V současné době stoupá počet útoků na mobilní zařízení. Ransomware se do mobilních zařízení většinou dostává díky stahování aplikací a programů z jiných zdrojů, než oficiálních stránek obchodů (například pro operační systém Android se jedná o Google Play).

Pokud dojde k infikování zařízením tak samotné odstranění ransomwaru není náročné. Pokud se lze k napadenému zařízení přihlásit, tak se musí restartovat do nouzového režimu a poté se dá malware pomocí antivirového programu najít a smazat.

Pokud ransomware napadené zařízení uzamkne, tak lze aplikovat tři možné způsoby. Za prvé lze přeinstalovat operační systém, za druhé můžeme z externího či spustitelného disku provést antivirovou kontrolu napadeného zařízení nebo za třetí lze pomocí nástrojů na obnovení systému v napadeném zařízení obnovit operační systém do stavu, ve kterém byl před infikování ransomwarem.

Ochranou a prevencí před infikováním různými druhy ransomwaru je pravidelná aktualizace operačního systému, který je v používaném zařízení. Dále se doporučuje nepoužívat staré a nepodporované verze operačních systémů, udržovat používané operační systémy v aktuálních verzích a přecházet na jejich nové a podporované verze.
Aktualizace programů, které jsou nainstalovány v zařízeních uživatelů, zejména pokud se jedná o webové prohlížeče a zásuvné moduly, pravidelná záloha uživatelských dat na externí úložiště a zařízení. Dále je důležité dávat si pozor na pokusy o útoky manipulativního charakteru, při kterých jsou zneužívány různé metody sociálního inženýrství. Neotevírat soubory a odkazy zaslané nebo nalezené na neznámých nebo neprověřených adresách, bezpečnější je nevyžádané nebo podezřelé soubory a maily rovnou smazat.

„V České republice je možné postihnout malware, kterým je i ransomware, dle § 230 (Neoprávněný přístup k počítačovému systému a nosiči informací) trestního zákona. Držení malware, s úmyslem spáchat trestný čin dle § 182 (Porušení tajemství dopravovaných zpráv) či trestný čin dle § 230 trestního zákona, je trestné dle § 231 (Opatření a přechovávání přístupového zařízené a hesla k počítačovému systému a jiných takových dat) trestního zákona.“[25]

V případě ransomware je možné uplatnit i ustanovení § 230 odstavec 3 trestního zákona, kdy útočník páchá tento trestný čin s úmyslem získat sobě nebo jinému neoprávněný prospěch. V úvahu by také mohlo přicházet uplatnění § 175 (Vydírání) trestního zákona, kdy je osoba pohrůžkou jiného těžké újmy (např. i tím, že na ni bude podáno trestní oznámení) nucena k zaplacení dané částky.

3.3.2 Phishing (Spear Phishing, Vishing a Smishing)

Podstavou jednání, které se označuje jako Phishing nebo jeho poddruhy je použití metod Sociálního inženýrství, které si blíže vysvětlíme později, jedná se o podvodná jednání, při kterých se pachatel z obětí snaží vylákat jejich citlivé údaje, jako jsou PINy a údaje kreditních a debetních karet, uživatelská jména a hesla k zpřístupnění účtů internetových bankovnictví nebo se je snaží přimet ke stažení a instalaci dalších škodlivých programů, jako jsou různé nástroje na vzdálenou správu plochy.

Obrázek č. 2: Schéma Phishingu

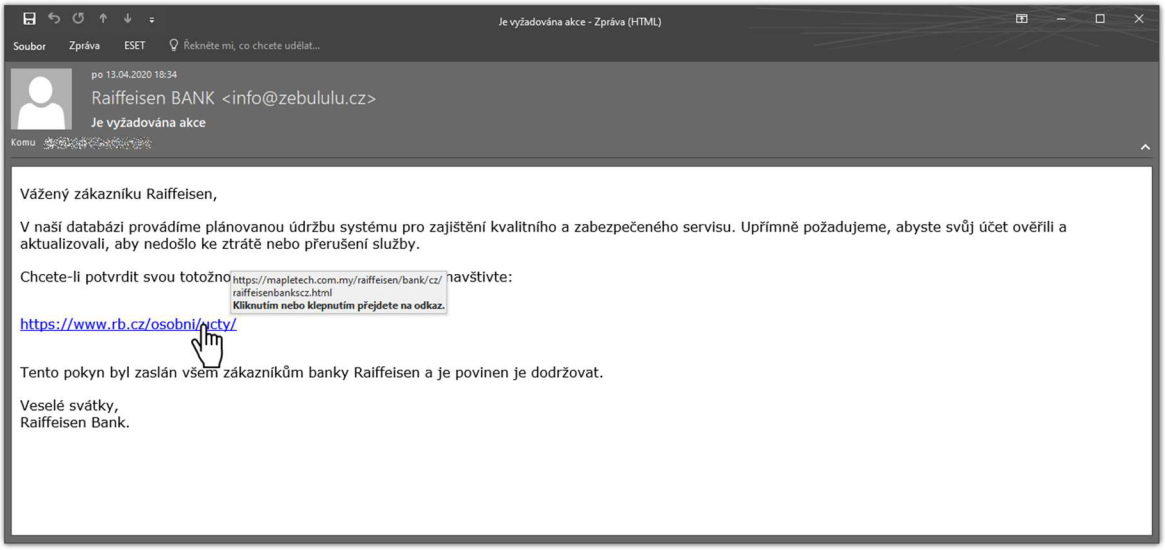
Zdroj: OAKK PČR Ústeckého kraje

[25] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. Str. 221. ISBN 978-80-88168-15-7.

Základní podstatou phishignových útoků je rozesílání podvržených mailových zpráv potenciálním obětem tohoto typu podvodného jednání. Tyto podvodné zprávy se bez detailnějšího zkoumání tváří jako z důvěryhodného zdroje a snaží se využít nepozornosti příjemce takové zprávy a přesvědčit ho, aby tento otevřel podvržený odkaz nebo si stáhnul škodlivou přílohu.[26]

Klasický mailový phishing je, když pachatel rozesílá obětem maily, ve kterých se vydává za někoho jiného, za nějakou důvěryhodnou instituci, jako může být banka, nějaký úřad nebo ministerstvo, či dokonce policie. Cílem takového mailu je stažení škodlivé přílohy nebo prokliknutí odkazu, který oběť přesměruje na podvržené stránky, na kterých se pachatel z obětí snaží vylákat přihlašovací údaje nebo údaje k platebním kartám.

Obrázek č. 3: Mail s viditelným odkazem a reálným skrytým odkazem



Zdroj: OAKK PČR Ústeckého kraje

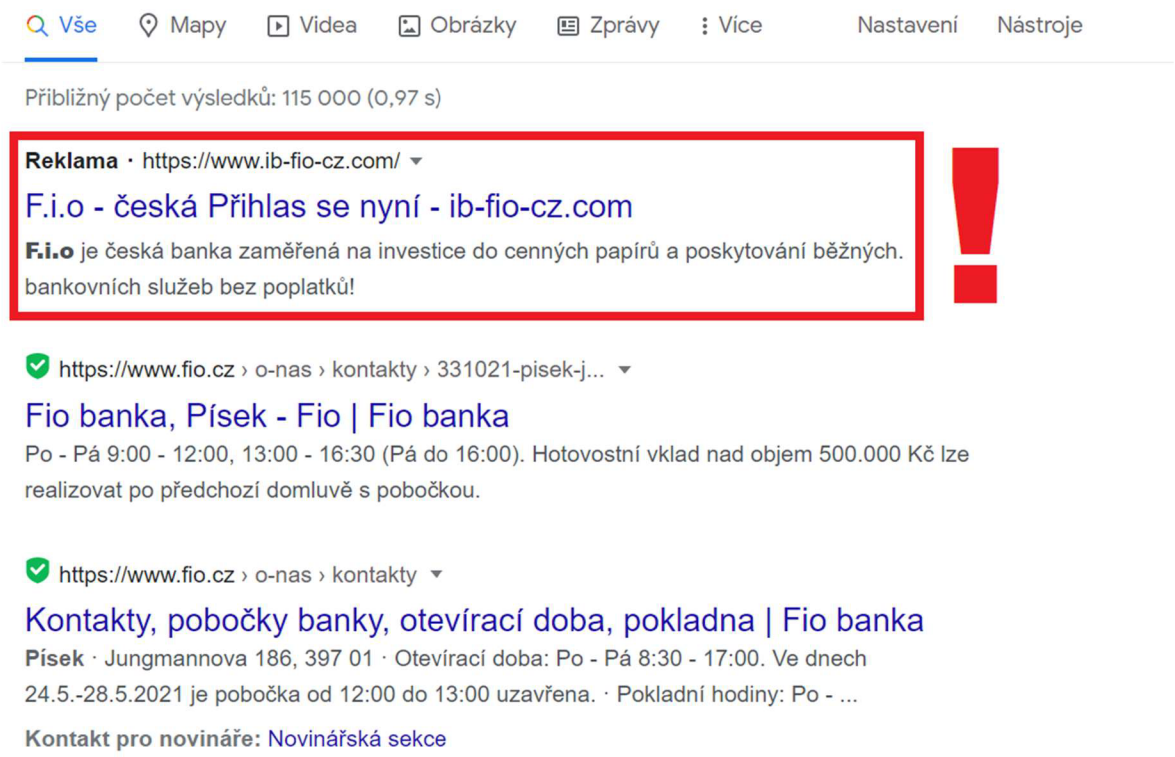
Obecně můžeme jako phishing brát každé škodlivé chování útočníka, které v obětech vytváří pocity důvěry a rozptýlí je natolik, až otupí jejich pozornost vůči možnému nebezpečí nebo podvodu a oběti pak pouze slepě následují jeho pokynů. V takovémto obecném pojetí phishingu také dochází ke zneužití citlivých informací obětí, ale tyto informace z nich nejsou

[26] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. Str. 247. ISBN 978-80-88168-15-7.

vylákávány přímou cestou, útočník tyto informace získává sám právě skrze podvodné zprávy s odkazy nebo přes stažení škodlivého programu do zařízení oběti. Pod tuto definici spadají i různé podvody s dary.[27]

Pachatel nemusí rozesílat pouze mailové zprávy, ale může také rozesílat zprávy s odkazy z falešných profilů na sociálních sítích nebo může takové odkazy „topovat" placenou reklamou.

Obrázek č. 4: Topovaný odkaz s podvodnou reálnou adresou



Zdroj: OAKK PČR Ústeckého kraje

Dle způsobu provedení phishingu ho můžeme dále rozdělovat na poddruhy, kdy mezi nejrozšířenější a nejznámější z nich patří Spear Phishing, Vishing nebo Smishing.

Pokud tedy budeme rozlišovat jednotlivé druhy phishingu a jeho základní formu budeme brát jako hromadně mířený náhodný útok, tak v případě spear phishingu se jedná o specificky mířený útok, který je zamířen proti specifickému cíli, ať už jedinci nebo

[27] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. Str. 246. ISBN 978-80-88168-15-7.

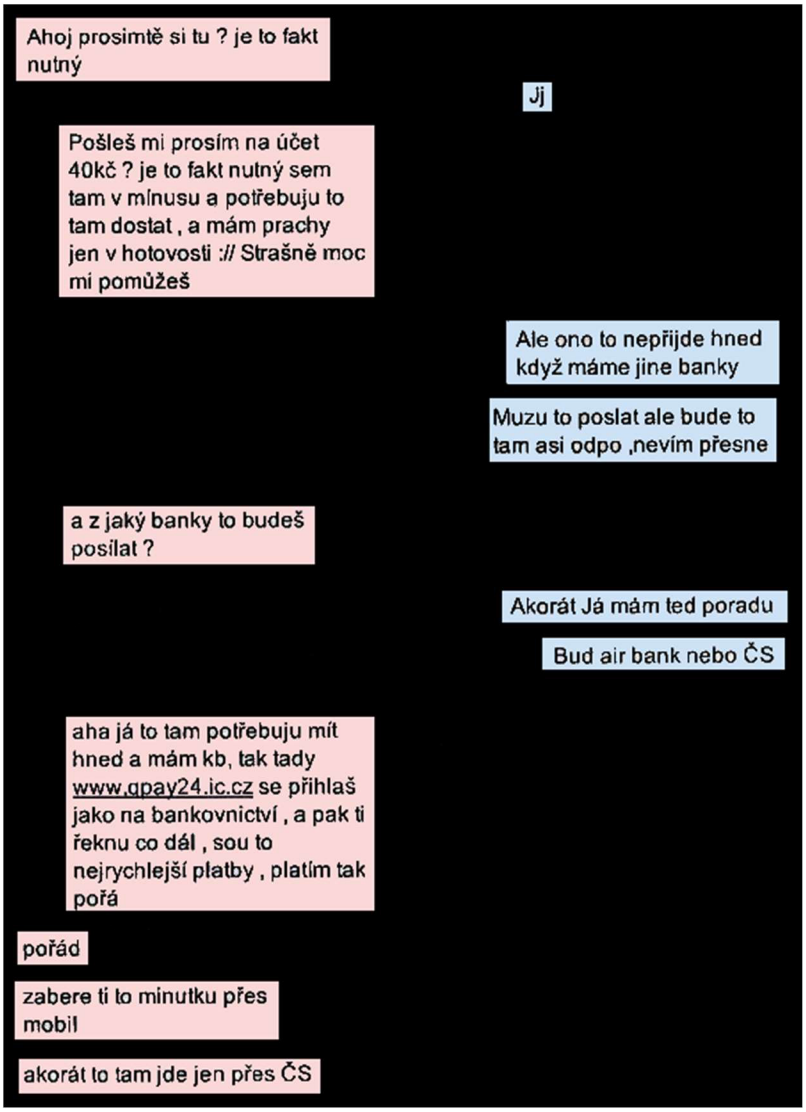
společnosti a tento útok se zaměřuje na jejich specifická data (např. duševní vlastnictví, osobní a finanční údaje, obchodní strategie, utajované informace atd.).

V případě vishingu se pak jedná o útok telefonickým hovorem, během kterého pachatel používá techniky sociálního inženýrství za účelem vylákání důvěrných dat z oběti (např. čísla účtů, přihlašovací údaje – jméno a heslo, čísla platebních karet atd.). Pachatelé při těchto útocích často zastírají svoji totožnost a vydávají se za zaměstnance reálných úřadů a společností tak, aby ve svých obětech vzbudili pocit důvěry.

Smishing pracuje na obdobných zásadách, jehož specifikem je využití SMS zpráv. Jeho cílem je vylákání platby nebo důvěrných dat, kdy je oběti zaslán podvržený odkaz skrz, který je tato odkázána na falešné webové stránky, které se mohou tvářit, jako weby státních institucí nebo bank, kam pak oběť zadává své přihlašovací údaje, které jsou následně zneužity nebo dojde ke stažení škodlivého programu.[28]

[28] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. Str. 264-266. ISBN 978-80-88168-15-7.

Obrázek č. 5: SMS konverzace s podvodným odkazem



Zdroj: OAKK PČR Ústeckého kraje

3.3.3 Malware

Pod malicious software, v překladu škodlivý software, zkráceně malware, spadají programy, které mají za úkol nějak poškodit běžný chod počítačových systémů, neoprávněně z těchto systémů čerpat citlivé informace a umožňovat k nim přístup. Na základě svého určení a zaměření jsou pak různé malwary pojmenovány, některé druhy jsou schopny vykonávat více druhů škodlivého jednání, jiné jsou určeny pouze k šíření prostřednictvím přiložených

souborů k mailovým zprávám nebo k těžbě databází a dat z napadených systémů, získáváním kontaktních údajů a dalších adres.[29]

Malware je souhrnné označení pro různé typy škodlivých softwarů mezi které patří trojské koně, ransomware, různé druhy spywaru, počítačové viry a červy.

3.3.4 Sociální inženýrství

Sociální inženýrství je v současné době bráno jako jedna z největších bezpečnostních hrozeb. Je extrémně efektivní, protože útoky jsou přesvědčivé a velmi klamavé. Většina útoků nebo podvodů v kyberprostoru využívá některé z forem sociálního inženýrství. Je to takový typ útoku, kdy pachatel pomocí manipulace zkouší od svých cílů získat citlivé údaje a data nebo se je snaží přesvědčit k nějakému jednání. Pokud útočníci v přípravě sledují digitální stopu svých obětí, pak potenciální útok může být mnohem cílenější, přesnější a tím pádem nebezpečnější a s většími následky.

Sociální inženýrství nebo též sociotechniku nemůžeme ve všech případech brát přímo jako kybernetický útok, je to ale metoda, či způsob, jak docílit a pomoci tomu, aby útok mohl skončit úspěchem. Samotný útok nemusí být realizován přímo jako nějaké podvodné jednání nebo průnik do počítačového systému, může být realizován pouze za účelem zjištění zájmových dat a informací, například hesel, kdy tato data či informace mohou být poskytnuty nebo prodány třetím stranám a až následně použity k nějakému dalšímu kybernetickému útoku.

Při definici sociálního inženýrství můžeme říct, že je jedná o společenské techniky, které jsou zaměřeny na přesvědčování, ovlivňování a manipulaci ostatních, aby se chovali tak, jak je potřeba, aby určité věci dělali nebo nedělali, aby poskytli svá citlivá data. Cílem celého jednání je vytvořit klamné zdání o probíhajících okolnostech, zastřít probíhající podvodné jednání, proto se někdy uvádí, že jde o umění klamu.[30]

[29] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. Str. 204. ISBN 978-80-88168-15-7.
[30] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. Str. 186. ISBN 978-80-88168-15-7.

Idea využití metod sociálního inženýrství spočívá v tom, že se nepoužijí pouze technické způsoby k provedení útoku a zjištění hesla „hrubou silou“, například za využití slovníkové metody nebo testování veškerých kombinací při využití alfanumerických a speciálních znaků. Mnohem jednodušší způsob je, se prostě na heslo oběti zeptat a uvést ji v omyl tak, aby požadované heslo sama útočníkovi sdělila. Nejzranitelnější část zabezpečení každého počítačového systému je vždy mezi klávesnicí a židlí. Všechny počítačové systémy, jejich zabezpečení, prvotní a další nastavení nebo následná údržba jsou závislé na správcích sítí, technicích nebo jejich uživatelích a nejsnazším způsobem, jak se dostat k citlivým a zájmovým informacím z těchto systémů, je právě od jejich uživatelů nebo správců.

Napadení za využití metod sociálního inženýrství využívá tři základní metody, které mohou být dále souběžně použity, kdy nejprve se o vytipované oběti zjišťují informace z veřejně dostupných zdrojů, dále se přejde do fáze, kdy je oběť kontaktována a pod smyšlenou podvodnou legendou se z oběti útočník snaží zjistit i další interní a konkrétnější informace a v poslední fázi dochází k psychologickému útoku.[31]

Metody sociálního inženýrství se využívají při Phishingu, Pharmingu, Spear Phishigu, Vishingu i Smishingu. Důvodem jsou nízké náklady na provedení takových útoků s možností zacílit na velké množství cílů, potenciálních obětí. Útočníci mohou realizovat velké „kampaně“, které mohou být zaměřené, jak na jednotlivce nebo na velké skupiny obyvatel. Prvotním spouštěčem útoku může být spam, nevyžádaná komunikace, při které se její odesílatel často vydává za uznávanou autoritu, jako může být policie, orgán státní správy, bankovní instituce nebo nějaká všeobecně známá společnost.

Nejběžnějšími způsoby využití technik sociálního inženýrství jsou falešné maily nebo weby, hovor po telefonu, prohledávání dat, která byly obětí přesunuta „do koše“, sledování historie webového prohlížeče, sociálních sítí nebo veřejně dostupných údajů obětí, ať už jednotlivců nebo firem, rozesílání marketingových předmětů na různých nosičích, nastrčených ztrát flash disků, na kterých jsou připravené škodlivé programy nebo třeba využívání podvržených webových služeb.[32]

[31] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. Str. 187. ISBN 978-80-88168-15-7.
[32] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. Str. 188. ISBN 978-80-88168-15-7.

Proč tyto formy útoků fungují? Útoky tímto způsobem fungují, protože využívají lidské zranitelnosti a tendenci, že lidé podléhají autoritám.

Útočníci využívají strachu a časového nátlaku, kdy v časové tísni nebo pod vlivem strachu lidé obecně nereagují rozumně a s rozvahou. Většinou, čím více peněz lidé na účtu mají, tím větší strach o ně mají a pak snáze podlehnou strachu a nerozvážným rozhodnutím o ně přijdou.

Dále útočníci mohou využívat reciprocity, kdy lidé většinou oplácejí laskavosti, což může být zneužito při údajné pomoci přátelům, známým nebo rodinným příslušníkům v tísni nebo při příspěvcích do falešných sbírek.

Také je zneužíváno sociální přizpůsobení, že lidé mají tendence dělat věci, které vidí dělat ostatní. Tímto mohou podlehnout falešným doporučením od přátel nebo klamavým recenzím a uveřejněným komentářům.

Lidé se chtějí mít lépe a z určité své podstaty jsou chamtiví, mají pocit vlastní výjimečnosti a nedostatku. Šikovné zacílení „exkluzivní a výhodné“ nabídky ve správný okamžik dokáže potenciální oběť zcela pohltit a zaslepit, kdy tato se nechá zcela přesvědčit o správnosti svého úsudku a poté podlehne podvodnému jednání. Takto podvedených je paradoxně více mezi vzdělanějšími lidmi, kteří mají ve svůj úsudek vyšší důvěru. Principy jako zvýšený zájem nebo nedostatek nějakého produktu či služby fungují nejen v marketingu, ale i při rozličných podvodných jednání.

Dále je zneužíváno důslednosti a závazků, pokud se někdo k něčemu, ústně nebo písemně, zaváže, je pravděpodobné, že takový závazek dodrží i poté, co prvotní nabídka nebo motivace budou změněny nebo zcela odstraněny a lidé budou přesto nadále dodržovat původní dohody.

3.3.5 Hacking

Pokud je uváděn termín hacking, tak panuje všeobecná představa, že se jedná o aktivity, kterými se útočník nabourává do počítačových systémů a zařízení. Takto bylo toto jednání

prezentováno i v médiích a jako hackeři byly označováni všichni pachatelé jejichž útoky směřovali vůči výpočetní technice. Takové definice a vnímaní ze strany společnosti jsou v rozporu s definicemi a vnímáním osob a společenských skupin, které se za hackery sami označují.[33]

„Jednání hackera, spočívající pouze ve využití svých schopností, díky nimž překoná bezpečnostní opatření a získá přístup k počítačovému systému nebo jako části, je možné postihnout podle § 230 odst. 1 (Neoprávněný přístup k počítačovému systému a nosiči informací) TZK. V případě kombinovaných forem útoků, kdy je například užit malware k infikování počítače, je třeba takového jednání pachatele postihnout také dle § 230 odst. 2 (Neoprávněný přístup k počítačovému systému a nosiči informací) TZK. Pokud je cílem útoku získat sobě nebo jinému neoprávněný prospěch, nebo neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat, je možné uplatnit i ustanovení § 230 odst. 3 TZK.“[34]

3.3.6 Cracking

„Pojem cracking je s pojmem hacking spojován, někdy jsou dokonce tyto pojmy veřejností či ve sdělovacích prostředcích nesprávně zaměňovány. Pojem lze do českého jazyka přeložit jako louskání či pukání. Obsahově pojem cracking znamená prolamování nebo obcházení ochranných prvků počítačového systému, programů nebo aplikací, s cílem jejich následného neoprávněného užití. Jednání pachatele, v rámci kterého dochází k prolamovaní ochrany počítačového systému či programu, s úmyslem zisku informací a jejich následném neoprávněném užití naplňuje skutkovou podstatu trestného činu dle § 230 odst. 1 či 2 (Neoprávněný přístup k počítačovému systému a nosiči informací) TZK. Pokud je cílem crackingu získat sobě nebo jinému neoprávněný prospěch je možné uplatnit i ustanovení § 230 odst. 3 TZK.“[35]

[33] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. Str. 269. ISBN 978-80-88168-15-7.
[34] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. Str. 276. ISBN 978-80-88168-15-7.
[35] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. Str. 276. ISBN 978-80-88168-15-7.

3.4 Možnosti prevence

Preventivní působení a osvěta v oblasti kybernetické kriminality a moderních technologií je důležitá a nutná, protože kriminalita páchaná v kyberprostoru nebo za využití moderních technologií není v současné době plně poznaná a nedokážeme pozorovat a popsat veškeré její projevy, díky novým poznatkům a zjištěním proto můžeme také pozorovat vysoký nárůst této trestné činnosti. Preventivní opatření jsou nutná z důvodů vysoké společenské nebezpečnosti kybernetické kriminality a možných následných škod, které mohou vzniknout.

Prevence kybernetické kriminality však nemůže být zaměřena pouze na zlepšování informovanosti potenciálních obětí. Prevence musí být zaměřena i na další oblasti jako jsou způsoby autorizace a přihlašování uživatelů k zařízením a do počítačových sítí a na technická prostředí používaných zařízení. Dalšími možnostmi ochrany může být monitoring datového provozu na sítích, zavedení standardů pro transfery dat a šifrování zdrojových kódů programů nebo samotných přenášených dat a zpráv.

Při předcházení kybernetické kriminality je klíčové pochopení metod, kterými je tato trestná činnost páchána. Důležité je orientovat se v problematice, znát možnosti aktuální výpočetní techniky a moderních technologií jako jsou například různé sociální sítě. Využívat tato moderní média ke zjišťování aktuálních preventivních postupů z jiných zemí a sjednotit právní úpravu a postihy represivního charakteru. Nejúčinnějším preventivním nástrojem je pak přesně zamířená prevence a osvěta, protože u kybernetické kriminality hrozí riziko vážné majetkové újmy.[36]
Výsledkům preventivních opatření také napomáhá zvýšená činnost kontrolních orgánů a včasné hlášení podezřelých situací a chování k jejich dalšímu prověření a ověření správnosti nebo nezávadnosti.

V případě útoků, které využívají metod sociálního inženýrství se jako potenciální oběť můžeme bránit tím, že

- budeme podezíraví,

[36] VÁLKOVÁ, Helena a Josef KUCHTA. *Základy kriminologie a trestní politiky*. 2. vyd. V Praze: C.H. Beck, 2012. Beckovy mezioborové učebnice. Str. 610-611. ISBN 978-80-7400-429-2.

- nebudeme poskytovat a zveřejňovat osobní údaje a přihlašovací údaje ke svému bankovnictví,
- budeme používat selský rozum,
- nebudeme jednat v časové tísni a pokusíme se nenechat zastrašit,
- budeme věnovat neustálou pozornost tomu, na jakém webu se nacházíme,
- pokud s někým ve virtuálním světě komunikujeme, i pokud je to v rámci ověřených a prověřených komunikačních nástrojů, tak budeme brát v potaz, že na druhé straně může sedět osoba s podvrhnutou identitou, která se na nás pokusí zaútočit,
- proto nebudeme nikomu svěřovat citlivé informace o naší osobě, ani intimního charakteru,
- brát v úvahu, že veškerá data, i například fotografie, které sdílíme na svých sociálních sítích, mohou být zneužita k lepšímu zacílení útoku na naši osobu,
- budeme si ověřovat kontaktní a další údaje zaslané protistranou,
- budeme používat přihlašování pomocí vícefaktorové autentizace,
- budeme používat „silná“ hesla, pokud možno pro každou používanou službu jiné,
- budeme používat antivirový program.

4 Vlastní práce

4.1 Charakteristika Ústeckého kraje

Ke dni 12. 12. 2023 měl Ústecký kraj, dle Českého statistického úřadu, 810.224[37] obyvatel a dle statistické ročenky z roku 2022, která byla úřadem zveřejněna, se jedná o pátý nejlidnatější kraj v České republice. Skladba obyvatelstva je ovlivněna historickým vývojem, který v druhé polovině 20. století kladl velký důraz na industrializaci a v kraji byla vytvořena centra těžkého průmyslu, se zaměřením na těžbu nerostných surovin, energetiku a chemický průmysl. Další vývoj a společenské změny vyústily ve vznik několika vyloučených lokalit a ovlivnění důležitých faktorů jako je nezaměstnanost a úroveň dosaženého vzdělání, ovlivňujících kriminalitu a příčiny kriminogenních situací.

Obecná míra nezaměstnanosti v České republice ve 2. čtvrtletí 2023 byla 2,5%[38] a v Ústeckém kraji 4,1%[39]. Ústecký kraj je tedy v tomto ukazateli nad republikovým průměrem.

Z výsledků posledního sčítání obyvatelstva České republiky, které proběhlo v roce 2021 je patrné, že Ústecký kraj je, co se týče podílu osob s vysokoškolským vzděláním i podílu osob bez vzdělání nebo neukončeného základního vzdělání na předposledním místě, před krajem Karlovarským.[40]

4.2 Rozbor trestných činů spáchaných v letech 2011 až 2020

V rámci vlastní práce bude provedena statistická analýza skutků spáchaných na území celé České republiky s porovnáním detailu Ústeckého kraje.

Za hlavní zkoumané kritérium byla zvolna kybernetická kriminalita kdy, jak bylo vysvětleno v teoretické části práce, se tato nejčastěji dotýká kvalifikací trestných činů podvodu podle § 209 trestního zákoníku, neoprávněného přístupu k počítačovému systému a nosiči

[37] https://www.czso.cz/csu/xu/1-xu
[38] https://www.czso.cz/csu/czso/zamestnanost_nezamestnanost_prace
[39] https://www.czso.cz/csu/xu/1-xu
[40] https://scitani.gov.cz/vzdelani

informací podle § 230 trestního zákoníku a neoprávněného opatření, padělání a pozměnění platebního prostředku podle § 234 trestního zákoníku.

Policejní statistika kriminality pracuje s takticko-statistickými kvalifikacemi (TSK), přičemž tyto trestné činy jsou zahrnuty pod TSK 511 a 830 pro podvod, TSK 509 (přičemž TSK 509 se vykazuje až od roku 2021 a bude tedy zahrnuta až v rámci kapitoly 4.3) a 838 pro neoprávněné opatření, padělání a pozměnění platebního prostředku a TSK 865, pod kterým je zahrnut neoprávněný přístup a poškození záznamu v počítačovém systému, opatření a přechovávání přístupového zařízení a hesla tedy souhrnně obsahuje § 230, 231 a 232 trestního zákoníku.

4.2.1 Vývoj počtu registrovaných skutků

Pro další práci a analýzu dat došlo v této první části k sečtení vybraných kritérií v letech 2011 až 2020.
V prvé řadě došlo k sečtení všech registrovaných skutků v rámci celé České republiky.

Tabulka č. 1: Počty vybraných registrovaných skutků v ČR

TSK	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
865	134	178	301	669	707	635	784	893	1092	1287
511	4910	5403	5940	6028	5780	5289	5074	5077	6556	5920
830	4153	4363	4998	4725	4865	4547	3678	3372	2623	2032
509	0	0	0	0	0	0	0	0	0	0
838	8269	7844	8272	7471	7272	6911	6626	6252	7440	5662
Celkem	17466	17788	19511	18893	18624	17382	16162	15594	17711	14901

Zdroj: vlastní zpracování z interní statistiky kriminality PČR

Z dat zpracovaných v první tabulce, z absolutních počtů všech skutků vidíme, že u TSK 865, skutků neoprávněného přístupu a poškození záznamu v počítačovém systému, opatření a přechovávání přístupového zařízení a hesla došlo téměř k desetinásobnému nárůstu. Naproti tomu u trestného činu podvodu, TSK 511 a 830, došlo k mírnému celkovému poklesu o 1111 skutků. Trestný čin neoprávněného opatření, padělání a pozměnění

platebního prostředku, TSK 838 (později i 509) je patrný pokles o 2607 skutků. V celkovém počtu všech vybraných skutků je vidět pokles o 2565 skutků.

Vývojový trend celkového počtu skutků je blíže zpracován v tabulce č. 2, ve které byly vypočteny statistické ukazatele 1. diference a koeficientu růstu. Z výsledků indexní analýzy je mezi lety 2011 – 2013 patrný mírný nárůst o 2% a 10%. V dalších letech, do roku 2018 celkový počet skutků vykazuje sestupnou tendenci, kdy na rok 2019 byl vykázán skokový nárůst o 14% a následně na rok 2020 skokový pokles o 16%.

Tabulka č. 2: Indexní analýza z celkového počtu registrovaných skutků v ČR

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
1. diference		322	1723	-618	-269	-1242	-1220	-568	2117	-2810
koeficient růstu		1,02	1,10	0,97	0,99	0,93	0,93	0,96	1,14	0,84

Zdroj: vlastní zpracování z tabulky č. 1

Ze zvoleného zpracování vybraných registrovaných skutků byly vyčleněny kategorie skutků „spáchané internetem a ostatními sítěmi“. Tato kategorie je pro potřeby této práce dále zpracovávána, jako kyberkriminalita.

Tabulka č. 3: Počty skutků spáchaných internetem a ost. sítěmi v ČR

TSK	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
865	58	102	206	542	578	513	608	696	930	1160
511	720	1039	1419	1745	1851	1841	1900	2053	3413	3368
830	154	166	321	369	540	538	592	690	499	442
509	0	0	0	0	0	0	0	0	0	0
838	28	51	71	103	173	210	234	225	283	328
Celkem	960	1358	2017	2759	3142	3102	3334	3664	5125	5298

Zdroj: vlastní zpracování z interní statistiky kriminality PČR

Z dat uvedených v tabulce č. 3 vyplývá, že u všech kategorií došlo mezi lety 2011 a 2020 k nárůstu počtu spáchaných skutků ze zvolené skupiny kyberkriminality. Pouze mezi lety 2015 a 2016 došlo k poklesu o 40 skutků, což byl pokles o 1%.

Tabulka č. 4: Indexní analýza skutků spáchaných int. a ost. sítěmi v ČR

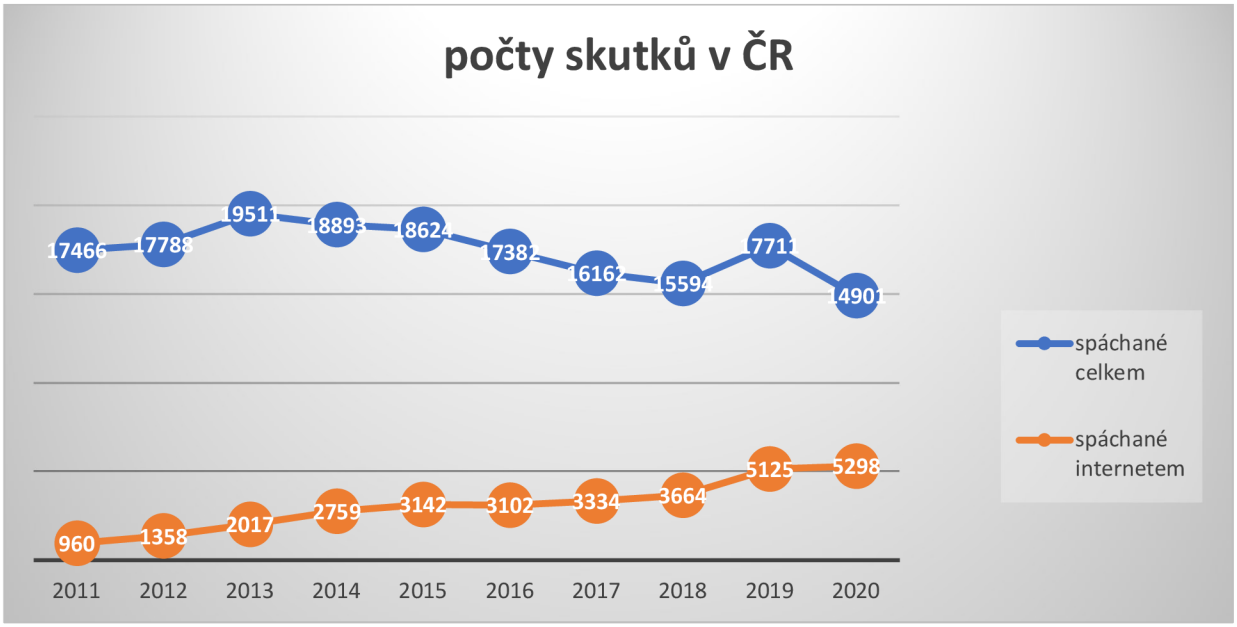
	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
1. diference		398	659	742	383	-40	232	330	1461	173
koeficient růstu		1,41	1,49	1,37	1,14	0,99	1,07	1,10	1,40	1,03

Zdroj: vlastní zpracování z tabulky č. 3

Jednotlivé meziroční změny jsou interpretovány tabulkou č. 4, kde je vidět výše zmíněný pokles mezi lety 2015 a 2016 a dále je vidět, že k největšímu nárůstu v absolutním počtu spáchaných skutků došlo mezi roky 2018 a 2019, kdy došlo k nárůstu o 1461 skutků.

Tabulky č. 1 a č. 3 byly graficky zpracovány do vývojového trendu, který je znázorněný v Grafu č. 1, který přehledně znázorňuje zjištěné výsledky.

Graf č. 1: Vývojový trend počtů vybraných skutků v ČR



Zdroj: vlastní zpracování z interní statistiky kriminality PČR

Z vývojového grafu č. 1 je zřejmá oscilace celkového počtu spáchaných skutků, kdy maxima bylo dosaženo v roce 2013 a minima v roce 2020. Co se týče skutků z oblasti

kyberkriminality, tak je z grafu ve sledovaných letech vidět postupný nárůst, kdy rozdíl mezi roky 2011 a 2020 je více než pětinásobný.

Dále byl vypočten a zpracován detail Ústeckého kraje, přičemž byla použita stejná sledovaná kritéria, aby mohlo dojít k následnému srovnání s celou Českou republikou.

Tabulka č. 5: Počty vybraných registrovaných skutků v ULK

TSK	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
865	11	8	17	34	28	30	60	86	85	64
511	480	505	528	565	501	416	432	359	425	367
830	229	222	262	265	241	290	160	110	122	91
509	0	0	0	0	0	0	0	0	0	0
838	749	661	703	598	540	509	510	457	513	395
Celkem	1469	1396	1510	1462	1310	1245	1162	1012	1145	917

Zdroj: vlastní zpracování z interní statistiky kriminality PČR

Celkové počty vybraných skutků spáchaných v Ústeckém kraji vykazují podobný trend jako celorepublikové výkazy. Ve sledovaném období došlo k celkovému poklesu absolutního počtu spáchaných skutků, kromě kategorie TSK 865, kde ve sledovaném období došlo k téměř šestinásobnému nárůstu.

Tabulka č. 6: Indexní analýza registrovaných skutků v ULK

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
1. diference		-73	114	-48	-152	-65	-83	-150	133	-228
koeficient růstu		0,95	1,08	0,97	0,90	0,95	0,93	0,87	1,13	0,80

Zdroj: vlastní zpracování z tabulky č. 5

Trend vývoje absolutního počtu spáchaných skutků je detailně zpracován v tabulce č. 6, kde kromě nárůstů mezi lety 2012 a 2013 a následně 2018 a 2019 vidíme klesající tendenci, viz. hodnoty koeficientu růstu.

I v případě Ústeckého kraje došlo ke zpracování a vyčlenění skutků zařazených do kategorie kyberkriminality, které byly spáchány internetem a ostatními sítěmi.

Tabulka č. 7: Počty skutků spáchaných internetem a ost. sítěmi v ULK

TSK	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
865	6	5	12	31	24	23	44	56	60	56
511	69	128	164	203	198	146	174	181	215	185
830	11	4	23	77	26	20	23	12	30	26
509	0	0	0	0	0	0	0	0	0	0
838	1	2	5	6	9	11	13	9	20	14
Celkem	87	139	204	317	257	200	254	258	325	281

Zdroj: vlastní zpracování z interní statistiky kriminality PČR

Naproti tomu počty skutků spáchaných internetem a ostatními sítěmi v Ústeckém kraji dle jednotlivých kategorií mají v celkovém počtu stejný zvyšující se trend jako u skutků v České republice. Mezi jednotlivými lety docházelo ke kolísání, kdy maxim bylo dosaženo v letech 2014 a 2019. Celkový počet skutků, ale i tak narostl o 3,2 násobek.

Tabulka č. 8: Indexní analýza skutků spáchaných int. a ost. sítěmi v ULK

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
1. diference		52	65	113	-60	-57	54	4	67	-44
koeficient růstu		1,60	1,47	1,55	0,81	0,78	1,27	1,02	1,26	0,86

Zdroj: vlastní zpracování z tabulky č. 7

Meziroční rozdíly celkového počtu spáchaných skutků ze zvolené oblasti kyberkriminality v Ústeckém kraji jsou vypočteny v tabulce č. 8, kde vidíme, že mezi jednotlivými roky docházelo ke kolísání. Největšího procentuálního nárůstu bylo dosaženo mezi lety 2011 a 2012, celkového maxima v roce 2019, ze kterého pak došlo k poklesu o 14%.

Následně byly tyto výpočty z tabulek č. 5 a č. 7 také graficky zpracovány do vývojového trendu v Grafu č. 2, který přehledně znázorňuje zjištěné výsledky.

Graf č. 2: Vývojový trend počtů vybraných skutků v ULK

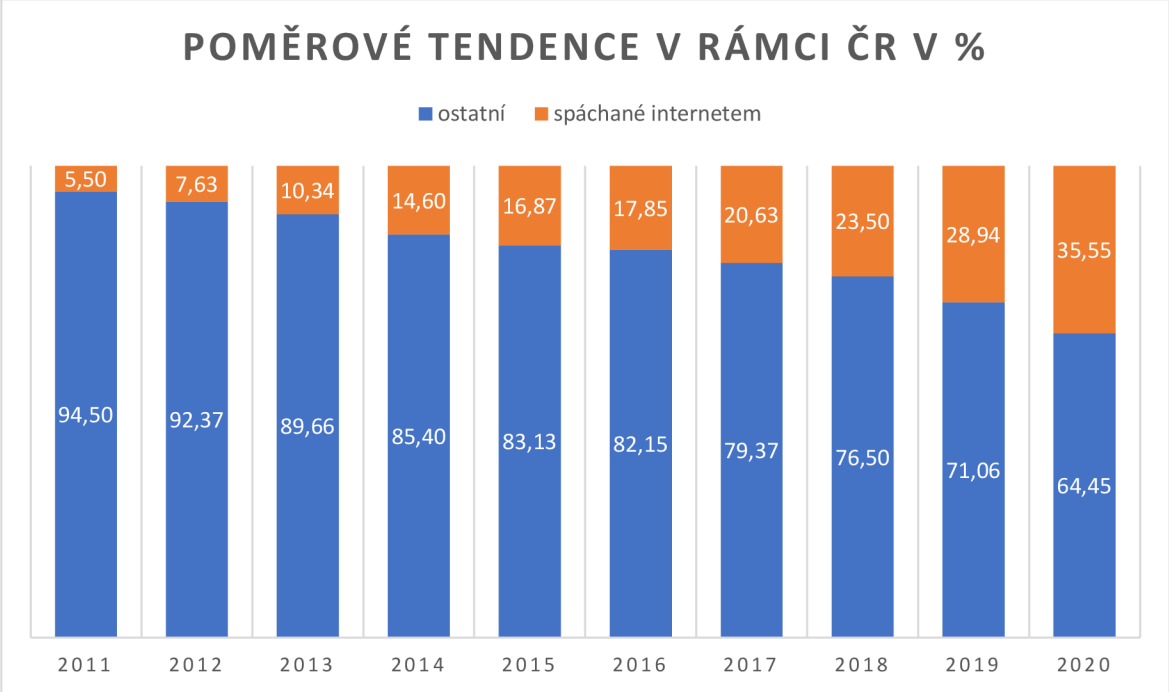
Zdroj: vlastní zpracování z interní statistiky kriminality PČR

Z grafu č. 2 vývojového trendu skutků v Ústeckém kraji vyplývá, že trend celkového počtu vybraných skutků má výrazně klesající tendenci oproti republikovému trendu. U skutků spadajících do oblasti kyberkriminality v Ústeckém kraji je podobný zvyšující se trend jako u republikového vývoje.

4.2.2 Poměrové tendence

Vypočtené výsledky byly zpracovány do poměrové tendence, čímž bylo zjištěno, že se vybrané skutky překlápí do oblasti kyberkriminality, kdy tento trend je znázorněn v grafech č. 3 a 4.

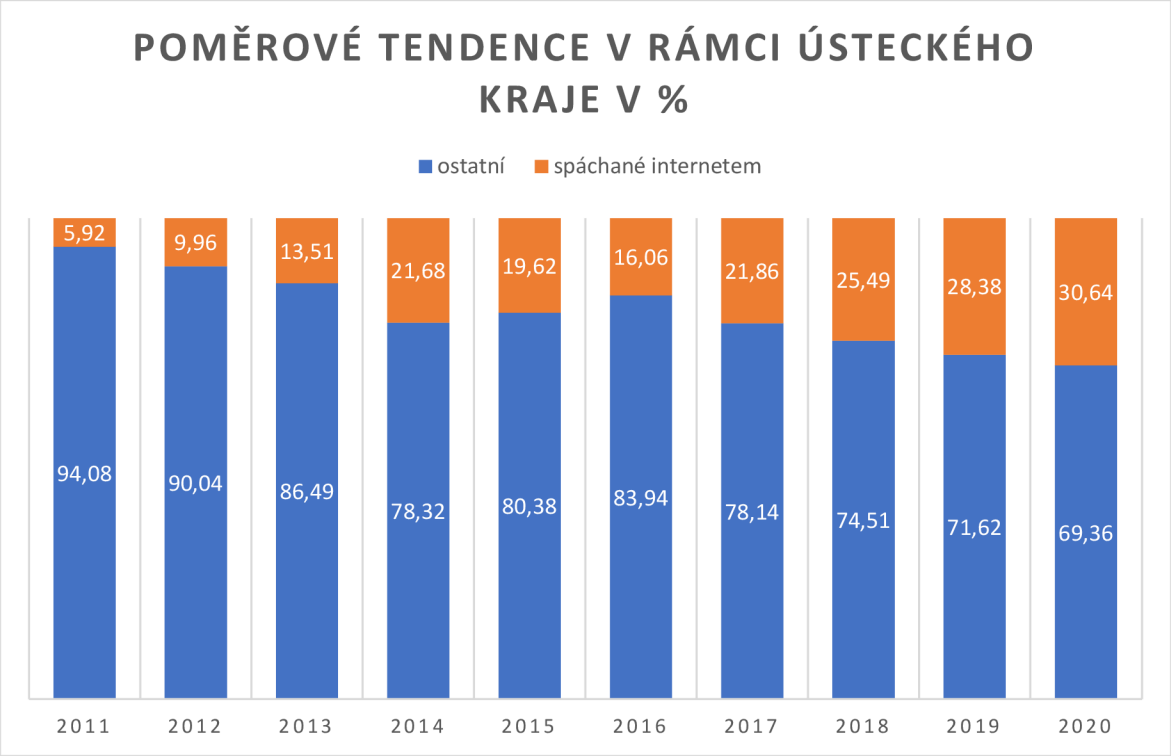
Graf č. 3: Poměrový trend počtů skutků v ČR v %



Zdroj: vlastní zpracování z interní statistiky kriminality PČR

Co se týká poměrových tendencí pro celou Českou republiku, tak vidíme, že v roce 2011 bylo skutků z oblasti kyberkriminality pouze 5,5% z celkového počtu skutků. V dalších letech následoval jejich postupný růst a v roce 2020 již skutky z oblasti kyberkriminality tvořily 35,55% z celkového počtu spáchaných skutků.

Graf č. 4: Poměrový trend počtů skutků v ULK v %

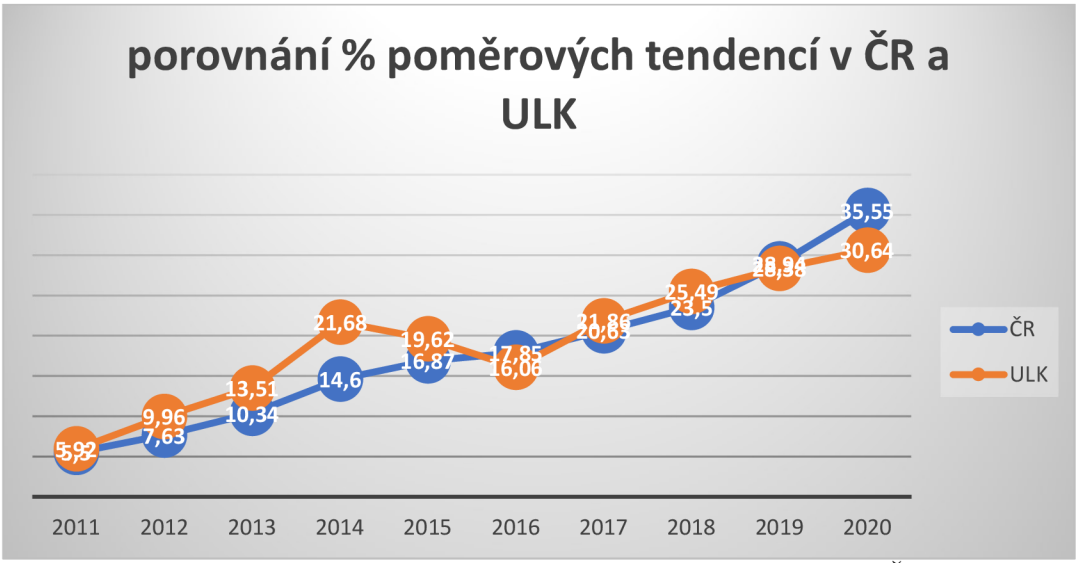


Zdroj: vlastní zpracování z interní statistiky kriminality PČR

Poměrové tendence v Ústeckém kraji také celkově stoupají, v roce 2011 bylo skutků z oblasti kyberkriminality jen 5,92% z celkového počtu skutků, přičemž v roce 2020 byla v oblasti kyberkriminality vypočtena hodnota 30,64% z celkového počtu spáchaných skutků.

Z grafů č. 3 a č. 4 vyplývá, že v Ústeckém kraji i České republice je podobný trend nárůstu skutků zařazených do kyberkriminality, což je znázorněno v grafu č. 5.

Graf č. 5: Porovnání % poměrových tendencí v ČR a ULK



Zdroj: vlastní zpracování z interní statistiky kriminality PČR

4.2.3 Porovnání objasněnosti

Po zjištění a analýze počtu spáchaných skutků bylo předmětem dalšího zkoumání, kolik z nich bylo úspěšně vyřešeno. Za dalším sledované kritérium byla tedy zvolena objasněnost.

V následující tabulce jsou uvedené počty skutků, které byly spáchány internetem a ostatními sítěmi a byly v daných letech objasněny.

Tabulka č. 9: Počty objasněných skutků, které byly spáchány internetem v ČR

TSK	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
865	15	23	44	166	109	124	113	125	123	96
511	348	520	632	731	691	834	781	665	733	680
830	83	84	216	230	331	376	359	409	244	181
509	0	0	0	0	0	0	0	0	0	0
838	10	14	34	18	25	40	45	38	44	43
Celkem	456	641	926	1145	1156	1374	1298	1237	1144	1000

Zdroj: vlastní zpracování z interní statistiky kriminality PČR

V tabulce č. 10 jsou poté vypočteny rozdíly mezi jednotlivými roky, kde vidíme, že docházelo k nárůstu počtu objasněných skutků, jejichž maxima bylo dosaženo v roce 2016 a v následujících letech začalo docházet k jejich poklesu.

Tabulka č. 10: Indexní analýza objasněných kyber skutků v ČR

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
1. diference		185	285	219	11	218	-76	-61	-93	-144
koeficient růstu		1,41	1,44	1,24	1,01	1,19	0,94	0,95	0,92	0,87

Zdroj: vlastní zpracování z tabulky č. 9

Grafické znázornění vypočtených výsledků zobrazuje vývojový trend v oblasti počtu spáchaných a objasněných skutků v grafu č. 6.

Graf č. 6: Počet spáchaných a objasněných skutků v ČR

Zdroj: vlastní zpracování z interní statistiky kriminality PČR

Z grafického znázornění je zřejmé, že trend objasněnosti nekopíruje trend strmého nárůstu počtu spáchaných skutků. Vyjádření % objasněnosti je dále zpracováno v tabulkách č. 13 a 14.

Pokud se podíváme na objasněnost skutků, které spadají do kyberkriminality a byly spáchány v Ústeckém kraji, tak vidíme, že v roce 2014 došlo k výkyvu a maximu, kdy bylo objasněno 198 skutků. V následujících letech měl pak počet objasněných skutků sestupnou tendenci. Jak je zaznamenáno v tabulce č. 11 a znázorněno grafem č. 7.

Tabulka č. 11: Počty objasněných skutků, které byly spáchány internetem v ULK

TSK	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
865	1	1	1	8	7	5	10	9	8	4
511	32	59	67	117	85	62	64	51	49	39
830	10	1	19	73	21	17	19	9	21	21
509	0	0	0	0	0	0	0	0	0	0
838	1	1	3	0	2	2	1	1	5	1
Celkem	44	62	90	198	115	86	94	70	83	65

Zdroj: vlastní zpracování z interní statistiky kriminality PČR

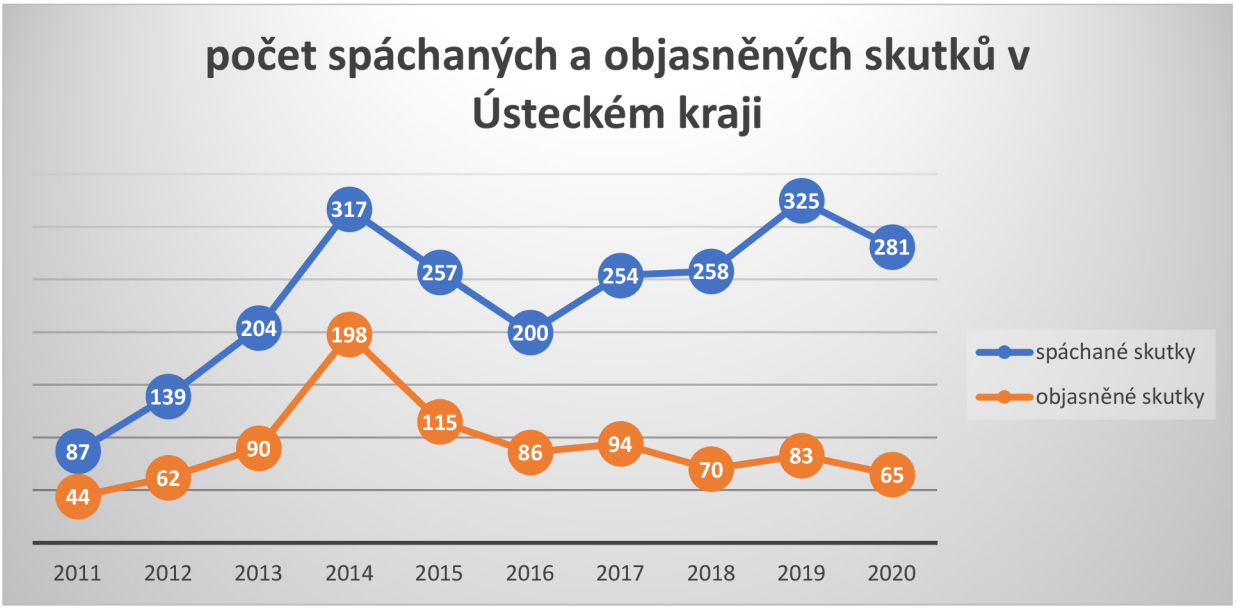
Tabulka č. 12: Indexní analýza objasněných kyber skutků v ULK

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
1. diference		18	28	108	-83	-29	8	-24	13	-18
koeficient růstu		1,41	1,45	2,20	0,58	0,75	1,09	0,74	1,19	0,78

Zdroj: vlastní zpracování z tabulky č. 11

Indexní analýzou v tabulce č. 12 je patrný počáteční strmý nárůst počtu objasněných skutků, kdy v roce 2014 bylo proti roku 2011 objasněno téměř pětinásobek skutků a následný trend počtu objasněných skutků byl již kolísavě klesající.

Graf č. 7: Počet spáchaných a objasněných skutků v ULK



Zdroj: vlastní zpracování z interní statistiky kriminality PČR

Z grafu č. 7 vyplývá, že trend vývoje objasněnosti spáchaných skutků v Ústeckém kraji částečně kopíruje trend vývoje spáchaných skutků.

Výše uvedené výsledy byly dále zpracovány, aby mohlo být provedeno další srovnání České republiky a Ústeckého kraje, kdy byla vypočtena procentuální objasněnost v jednotlivých sledovaných letech.

Tabulka č. 13: Objasněnost v ČR

ČR	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
spácháno	960	1358	2017	2759	3142	3102	3334	3664	5125	5298
objasněno	456	641	926	1145	1156	1374	1298	1237	1144	1000
v %	48%	47%	46%	42%	37%	44%	39%	34%	22%	19%

Zdroj: vlastní zpracování z interní statistiky kriminality PČR

Z tabulky č. 13 je patrné, že objasněnost skutků spadajících do kyberkriminality v České republice v uvedených letech klesla ze 48% na 19%.

Tabulka č. 14: Objasněnost v ULK

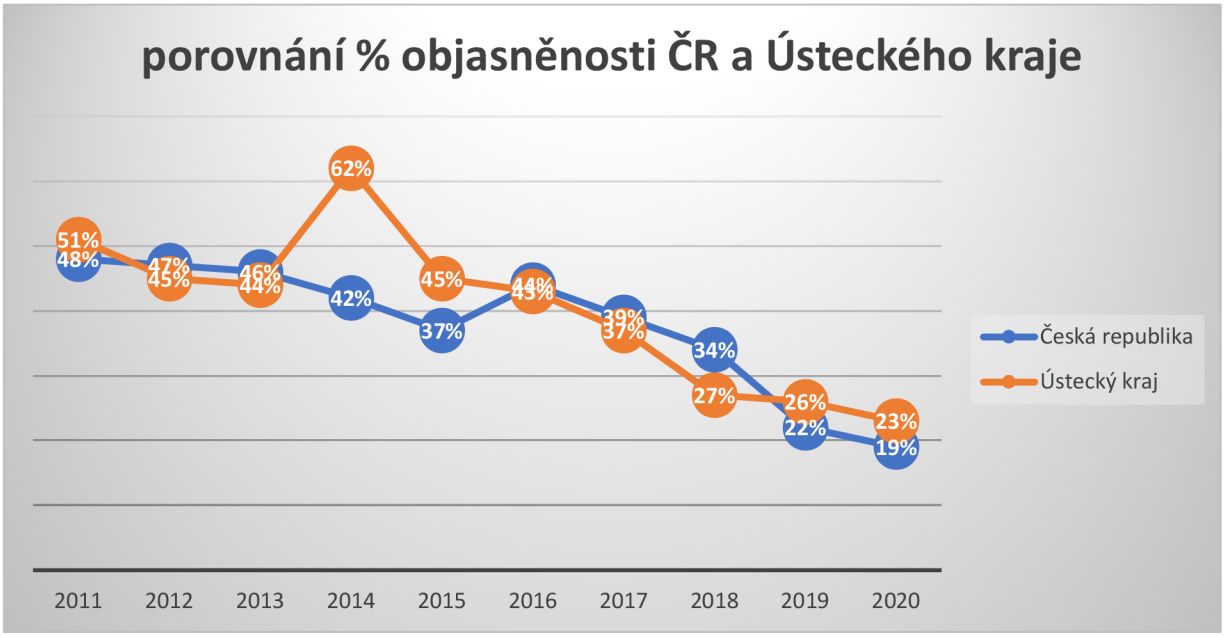
Ústecký kraj	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
spácháno	87	139	204	317	257	200	254	258	325	281
objasněno	44	62	90	198	115	86	94	70	83	65
v %	51%	45%	44%	62%	45%	43%	37%	27%	26%	23%

Zdroj: vlastní zpracování z interní statistiky kriminality PČR

Tabulka č. 14 zpracovává objasněnost v Ústeckém kraji, kdy je vypočten pokles objasněnosti z 51% na 23% ve sledovaném období.

Z výše vypočtených výsledků procentuální objasněnosti bylo provedeno grafické porovnání objasněnosti České republiky a Ústeckého kraje, které je znázorněno grafem č. 8.

Graf č. 8: Porovnání procentuální objasněnosti ČR a ULK



Zdroj: vlastní zpracování z interní statistiky kriminality PČR

Trendy objasněností vykazují podobný vývoj, kromě roku 2014, kdy se v Ústeckém kraji podařilo procentuálně objasnit výrazně více skutků.

4.2.4 Index kriminality

Dalším kritériem ke zkoumání a následnému srovnání byl zvolen Index kriminality, který byl vypočítán jako podíl počtu trestných činů na daném území a počtu obyvatel na daném území x 100 000. Index kriminality nám říká, kolik obyvatel ze 100 000 na daném území bylo dotčeno touto formou kriminality.

K výpočtům byly použity hodnoty počtu obyvatel České republiky a Ústeckého kraje, které byly zjištěny z demografických příruček Českého statistického úřadu, které byly vydány pro sledované roky. Tyto údaje jsou uvedeny v tabulce č. 15, kde jsou také dále uvedeny vypočtené hodnoty Indexu kriminality pro jednotlivé roky, jak pro celou Českou republiku, tak pro Ústecký kraj.

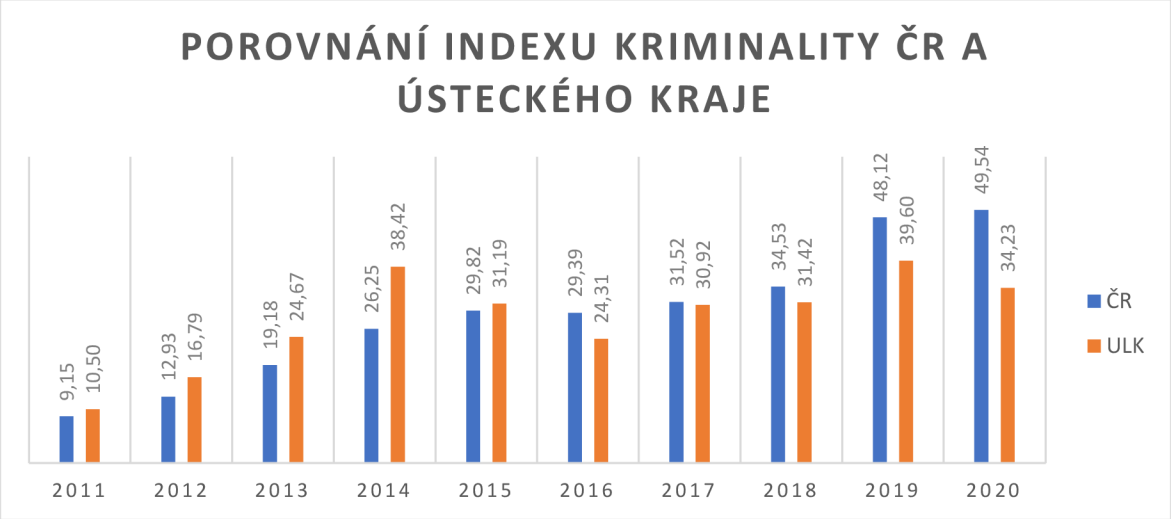
Tabulka č. 15: Počet obyvatel a Index kriminality v ČR a ULK

	Počet obyvatel		Index kriminality	
	v ČR	v ULK	v ČR	v ULK
2011	10 486 731	828 448	9,15	10,5
2012	10 505 445	828 026	12,93	16,79
2013	10 516 125	826 764	19,18	24,67
2014	10 512 419	825 120	26,25	38,42
2015	10 538 275	823 972	29,82	31,19
2016	10 553 843	822 850	29,39	24,31
2017	10 578 820	821 377	31,52	30,92
2018	10 610 055	821 080	34,53	31,42
2019	10 649 800	820 789	48,12	39,6
2020	10 693 939	820 965	49,54	34,23

Zdroj: vlastní zpracování z demografických příruček Českého statistického úřadu

Vypočtené výsledky byly pro názornější porovnání zpracovány také graficky do grafu č. 9.

Graf č. 9: Porovnání indexů kybernetické kriminality ČR a ULK



Zdroj: vlastní zpracování

Porovnání indexů kriminality v České republice a Ústeckém kraji ukazuje, že v letech 2011 až 2015 měl Ústecký kraj vyšší hodnotu indexu kriminality než Česká republika, a naopak v letech 2016 až 2020 měl hodnoty indexu kriminality nižší.

Koncem roku 2020 došlo ke změně legislativy, kterou došlo k úpravě hranice výše škody ke kvalifikování přestupku a trestného činu, kdy byla zvýšena hranice způsobené škody pro kvalifikaci skutku jako trestného činu z 5.000,- Kč na 10.000,- Kč, čímž dochází ke zkreslení výsledků z let před legislativní změnou a následujících. Z tohoto důvodu jsou další roky zpracovávány samostatně v dalším oddílu praktické části této práce.

4.3 Rozbor trestných činů spáchaných v letech 2021 až 2023

Zvýšením hranice výše škody od kdy bude skutek kvalifikován jako trestný čin by se teoreticky mělo promítnout ve snížení celkového počtu registrovaných skutků. Důležité je ale podotknout, že toto se týká trestných činů pro jejichž kvalifikaci je výše škody obligatorním znakem, tedy z našeho výběru skutků se jedná pouze o trestný čin podvodu podle § 209 trestního zákoníku (TSK 511 a 830). Pro kvalifikaci trestných činů neoprávněného opatření, padělání a pozměnění platebního prostředku podle § 234 trestního zákoníku nebo neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 trestního zákoníku není nutné způsobení škody. Způsobení škody při těchto skutcích vede k rozšíření právní kvalifikace o vyšší odstavce.

Od roku 2021 se v policejních statistikách začala nově vykazovat také druhá takticko-statistická kvalifikace pro trestný čin neoprávněného opatření, padělání a pozměnění platebního prostředku podle § 234 trestního zákoníku (TSK 509).

4.3.1 Vývoj počtu registrovaných skutků

Stejně jako v předcházející části, i v této byl zvolený stejný postup, kdy byla sečtena celková četnost zvolených skutků, které byly vybrány jako nejčastěji zatížené kritériem kyberkriminality – spácháním za pomoci internetu a ostatními sítěmi.

Tabulka č. 16: Počty vybraných registrovaných skutků v ČR

TSK	2021	2022	2023
865	1866	2848	1909
511	6789	11658	12634
830	1682	1605	1586
509	6107	11848	12802
838	223	128	115
Celkem	16667	28087	29046

Zdroj: vlastní zpracování z interní statistiky kriminality PČR

Z tabulky č. 16 vidíme, že dochází k celkovému nárůstu počtu vybraných skutků, zejména to platí pro kategorie TSK 511 a 509.

Tabulka č. 17: Indexní analýza registrovaných skutků v ČR

	2021	2022	2023
1. diference		11420	959
koeficient růstu		1,69	1,03

Zdroj: vlastní zpracování z tabulky č. 17

Z indexní analýzy, která je zpracována v tabulce č. 18 vidíme mezi lety 2021 a 2022 skokový nárůst celkového počtu skutků o 69% a v dalším roce se zvýšením o další 3%.

Z celkového počtu vybraných skutků byly opět vyčleněny skutky, které byly spáchány za pomoci internetu a ostatními sítěmi, které jsme označili jako kyberkriminalitu.

Tabulka č. 18: Počty skutků spáchaných internetem a ostatními sítěmi v ČR

TSK	2021	2022	2023
865	1682	2575	1687
511	4087	7727	8495
830	381	407	359
509	500	4283	5515
838	28	35	44
Celkem	6678	15027	16100

Zdroj: vlastní zpracování z interní statistiky kriminality PČR

V tabulce č. 18 je zpracováno výše zmíněné vyčlenění. Z uvedených dat vidíme nárůst počtu skutků, kde mezi roky 2021 a 2022 je také patrný skokový nárůst.

Tabulka č. 19: Indexní analýza skutků spáchaných int. a ost. sítěmi v ČR

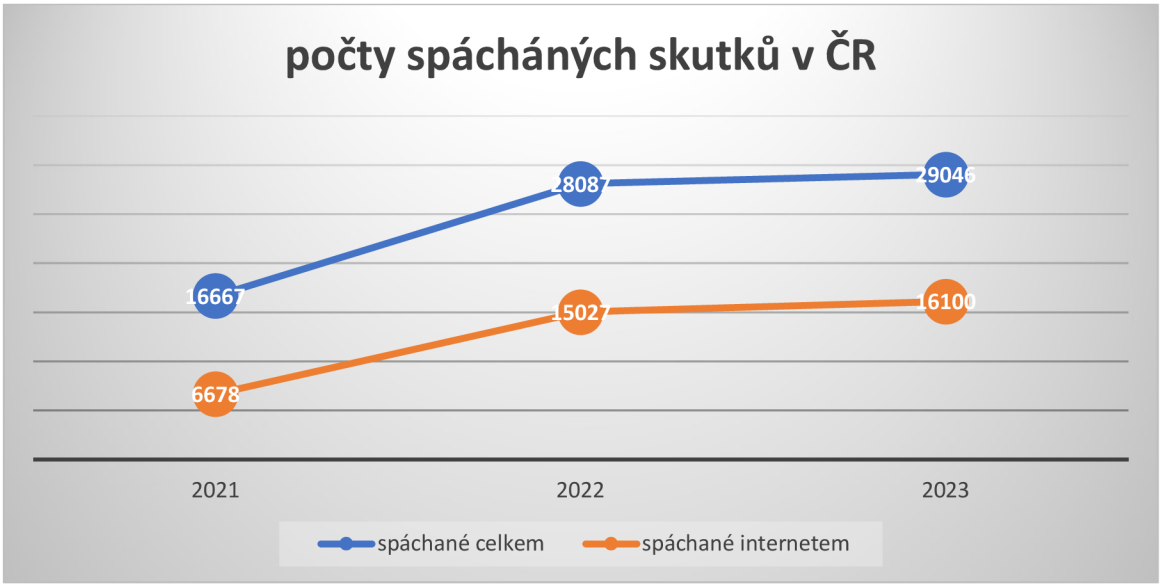
	2021	2022	2023
1. diference		8349	1073
koeficient růstu		2,25	1,07

Zdroj: vlastní zpracování z tabulky č. 19

Zpracovanou indexní analýzou vidíme, že mezi lety 2021 a 2022 nárůst činil 125% a v dalším roce 7%.

Data zpracovaná v tabulkách č. 16 a 18 byly dále zpracovány do grafické podoby, které znázorňuje graf č. 10, ve kterém vidíme onen skokový nárůst mezi lety 2021 a 2022 a další růst v roce 2023. Dále je z grafu patrný stejný růstový trend, jak u celkového počtu skutků, tak u skutků spáchaných za pomoci internetu. Nárůst u celkového počtu skutků je způsobený nárůstem počtu skutků spáchaných za využití internetu.

Graf č. 10: Vývojový trend počtů skutků v České republice



Zdroj: vlastní zpracování z interní statistiky kriminality PČR

Dále byl zpracován detail Ústeckého kraje, opět za využití stejných sledovaných kritérií, kdy byly sečteny všechny zkoumané trestné činy.

Tabulka č. 20: Počty vybraných registrovaných skutků v ULK

TSK	2021	2022	2023
865	108	192	119
511	472	852	932
830	103	95	92
509	430	668	901
838	4	4	6
Celkem	1117	1811	2050

Zdroj: vlastní zpracování z interní statistiky kriminality PČR

Tabulka č. 21: Indexní analýza registrovaných skutků v ULK

	2021	2022	2023
1. diference		694	239
koeficient růstu		1,62	1,13

Zdroj: vlastní zpracování z tabulky č. 20

Z indexní analýzy počtu všech skutků v Ústeckém kraji také vidíme mezi lety 2021 a 2022 nárůst, který činil 62% a v dalším roce 2023 o 13%.

Tabulka č. 22: Počty skutků spáchaných internetem a ostatními sítěmi v ULK

TSK	2021	2022	2023
865	98	188	114
511	278	647	685
830	28	8	16
509	32	189	401
838	0	0	0
Celkem	436	1032	1216

Zdroj: vlastní zpracování z interní statistiky kriminality PČR

I v Ústeckém kraji u vyčleněných skutků spáchaných za pomoci internetu a ostatními sítěmi je vidět jejich nárůst.

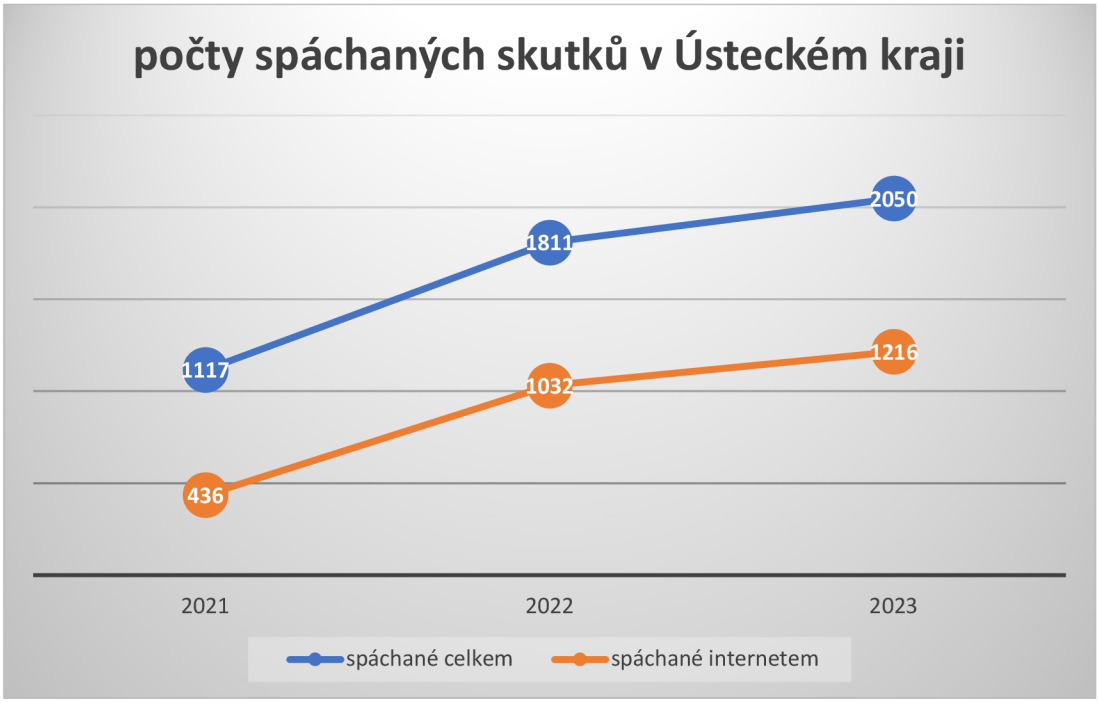
Tabulka č. 23: Indexní analýza skutků spáchaných int. a ost. sítěmi v ULK

	2021	2022	2023
1. diference		596	184
koeficient růstu		2,37	1,18

Zdroj: vlastní zpracování z tabulky č. 22

Provedenou indexní analýzou vidíme, že tento nárůst byl mezi lety 2021 a 2022 o 137% a v dalším roce o 18%.

Graf č. 11: Vývojový trend počtů skutků v ULK



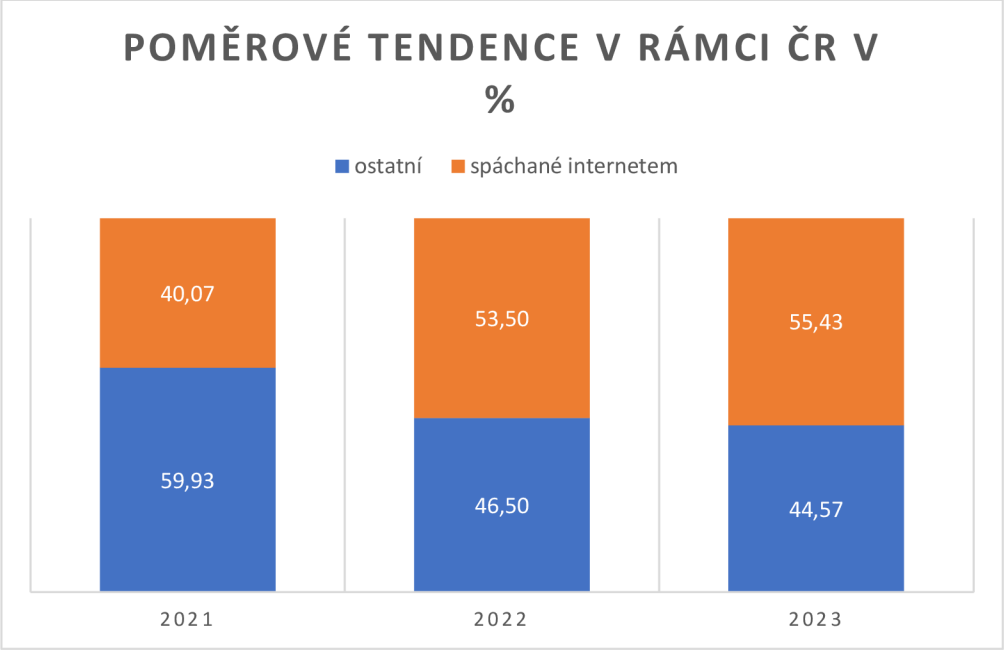
Zdroj: vlastní zpracování z interní statistiky kriminality PČR

Data zpracovaná pro Ústecký kraj jsou znázorněná v grafu č. 11, kde je opět patrný stejný růstový trend jako v případě výsledků celé České republiky.

4.3.2 Poměrové tendence

Pro roky 2021–2023 byly také zpracovány poměrové tendence, ze kterých je patrný další nárůst kyberkriminality na celkovém počtu skutků. K tomuto byly vypracovány grafy č. 12 a 13.

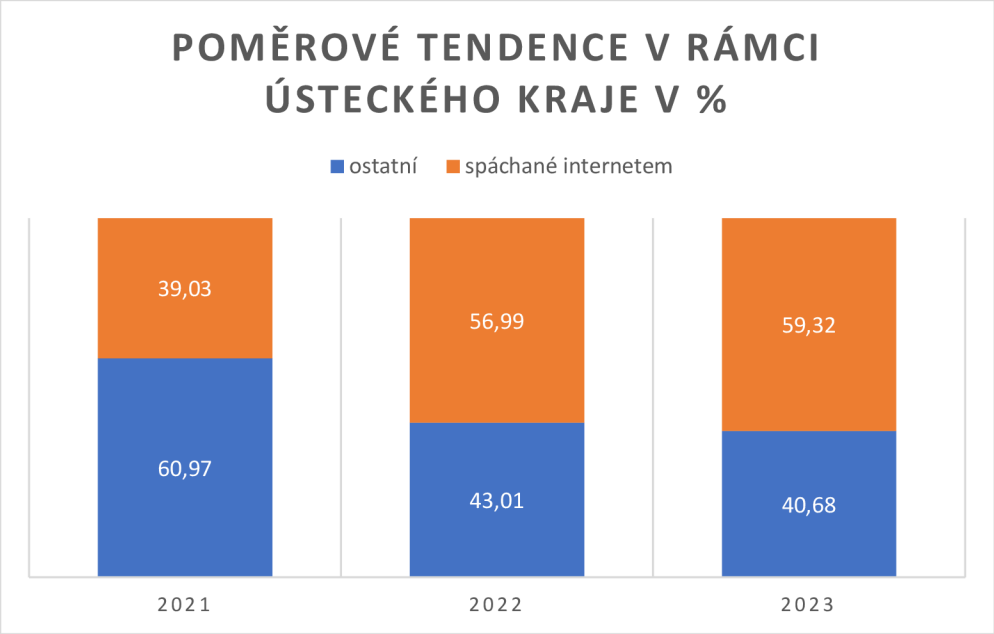
Graf č. 12: Poměrový trend počtů skutků v ČR v %



Zdroj: vlastní zpracování z interní statistiky kriminality PČR

Graf č. 12 znázorňuje situaci v České republice, kde celkový počet vybraných skutků zařazených do kyberkriminality v roce 2021 dosahoval 40,07% a poté dále narůstal, kdy v roce 2022 již činil 53,5% a v roce 2023 55,43%. Tedy v posledních dvou zkoumaných letech již byla většina vybrané trestné činnosti spáchána za pomoci internetu.

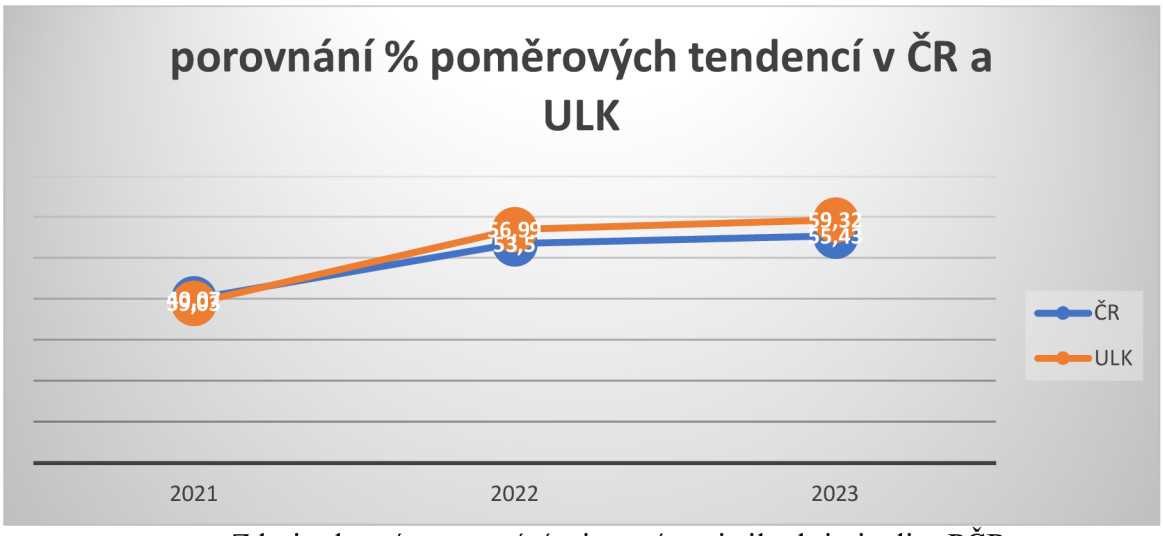
Graf č. 13: Poměrový trend počtů skutků v ULK v %



Zdroj: vlastní zpracování z interní statistiky kriminality PČR

Z grafu č. 13 je patrné, že to samé platí i pro Ústecký kraj, kde je poměr mezi spáchanými skutky ještě markantnější. Vzájemné srovnání poměrových trendů je zpracováno v grafu č. 14, čímž vidíme, že poměry jsou téměř stejné.

Graf č. 14: Porovnání poměrových tendencí v ČR a ULK



Zdroj: vlastní zpracování z interní statistiky kriminality PČR

4.3.3 Porovnání objasněnosti

V následující části je zpracována objasněnost skutků spáchaných za pomocí internetu pro roky 2021–2023. V první části je zpracována objasněnost celé České republiky a ve druhé je zpracována objasněnost v Ústeckém kraji.

Tabulka č. 24: Počty objasněných skutků, které byly spáchány internetem v ČR

TSK	2021	2022	2023
865	119	93	81
511	516	568	676
830	151	121	113
509	36	106	138
838	2	10	9
Celkem	824	898	1017

Zdroj: vlastní zpracování z interní statistiky kriminality PČR

Tabulka č. 24 zpracovává absolutní počty objasněných skutků v rámci všech vybraných trestných činů.

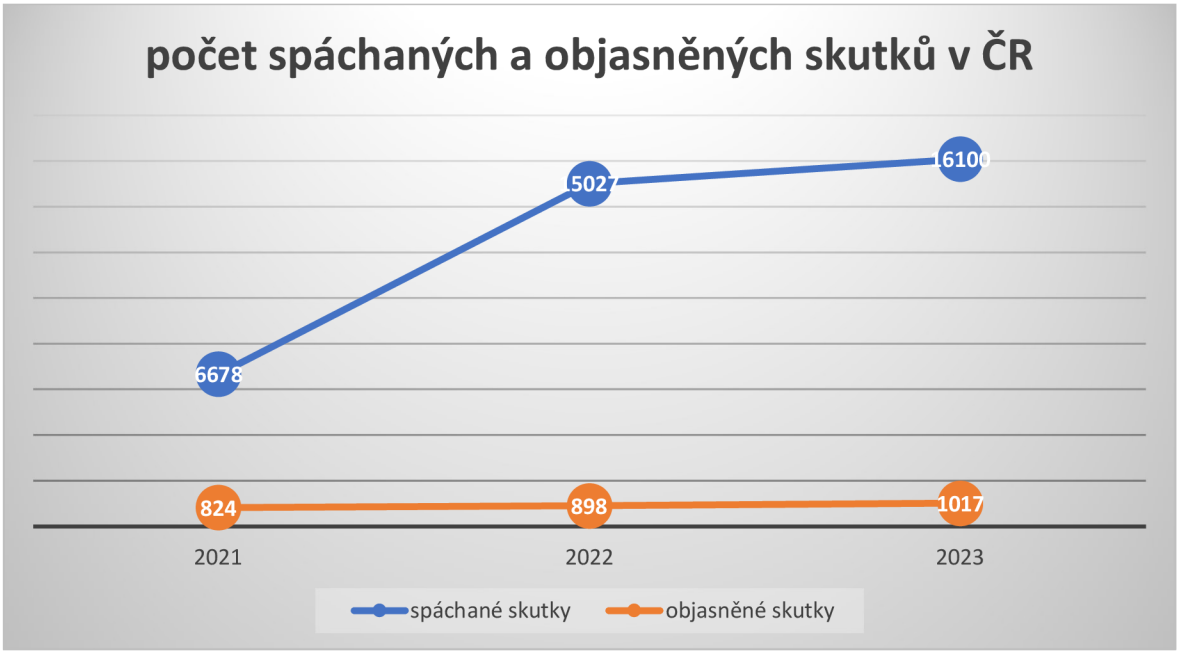
Tabulka č. 25: Indexní analýza objasněných kyber skutků v ČR

	2021	2022	2023
1. diference		74	119
koeficient růstu		1,09	1,13

Zdroj: vlastní zpracování z tabulky č. 24

Z provedené indexní analýzy vidíme, že počet objasněných skutků meziročně stoupá, kdy mezi lety 2021 a 2022 byl jejich nárůst o 9% a mezi lety 2022 a 2023 byl jejich nárůst o 13%.

Graf č. 15: Počet spáchaných a objasněných skutků v ČR



Zdroj: vlastní zpracování z interní statistiky kriminality PČR

Grafem č. 15 je znázorněn velký nárůst počtu spáchaných skutků, který ale nekoresponduje s menším růstem počtu objasněných skutků.

Dále je zkoumána objasněnost skutků zařazených do kyberkriminality, a které byly spáchány v Ústeckém kraji.

Tabulka č. 26: Počty objasněných skutků, které byly spáchány internetem v ULK

TSK	2021	2022	2023
865	9	1	7
511	34	61	68
830	17	4	2
509	4	8	16
838	0	0	0
Celkem	64	74	93

Zdroj: vlastní zpracování z interní statistiky kriminality PČR

V absolutních počtech vidíme, že dochází k nárůstu počtu objasněných skutků, hlavně v kategoriích TSK 511 a 509.

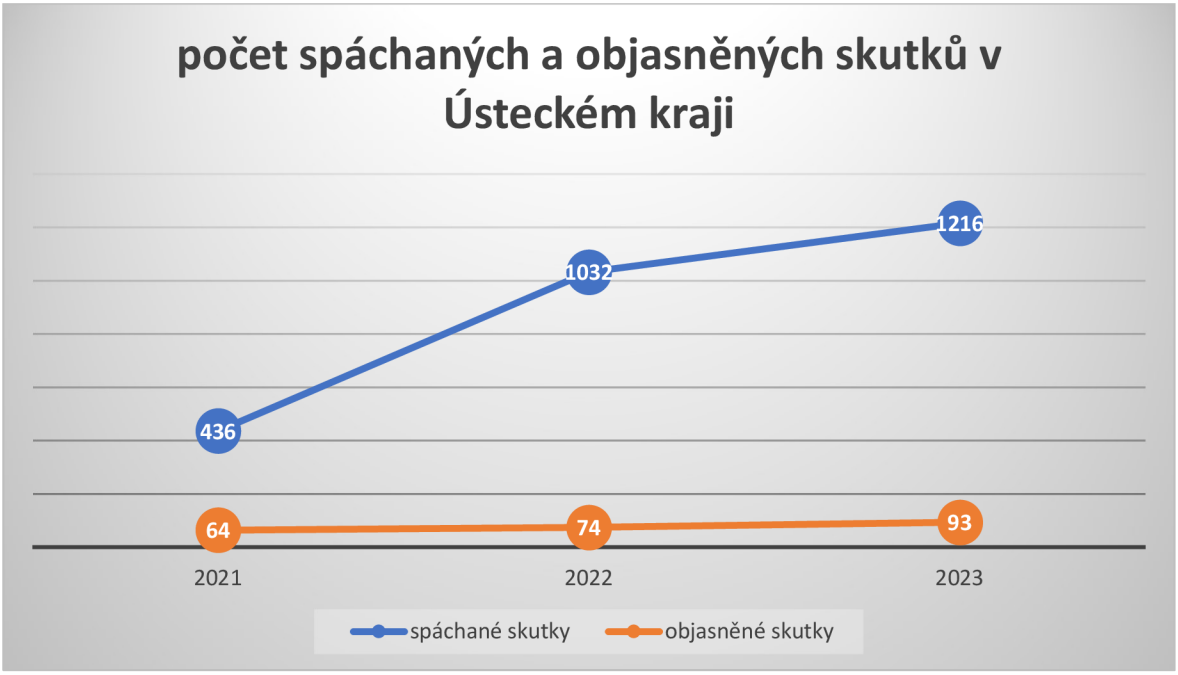
Tabulka č. 27: Indexní analýza objasněných kyber skutků v ULK

	2021	2022	2023
1. diference		10	19
koeficient růstu		1,16	1,26

Zdroj: vlastní zpracování z tabulky č. 27

Z indexní analýzy vidíme, že nárůst objasněných skutků byl mezi roky 2021 a 2022 o 16% a mezi roky 2022 a 2023 o 26%.

Graf č. 16: Počet spáchaných a objasněných skutků v ULK



Zdroj: vlastní zpracování z interní statistiky kriminality PČR

Grafickým znázorněným zjištěných výsledků vidíme, že v Ústeckém kraji jsou stejné růstové trendy jako v České republice.

Dále byla vypočtena procentuální objasněnost v jednotlivých sledovaných letech, jak pro celou Českou republiku v tabulce č. 28, tak pro Ústecký kraj v tabulce č. 29.

Tabulka č. 28: Objasněnost v ČR

ČR	2021	2022	2023
spácháno	6678	15027	16100
objasněno	824	898	1017
v %	12%	6%	6%

Zdroj: vlastní zpracování z interní statistiky kriminality PČR

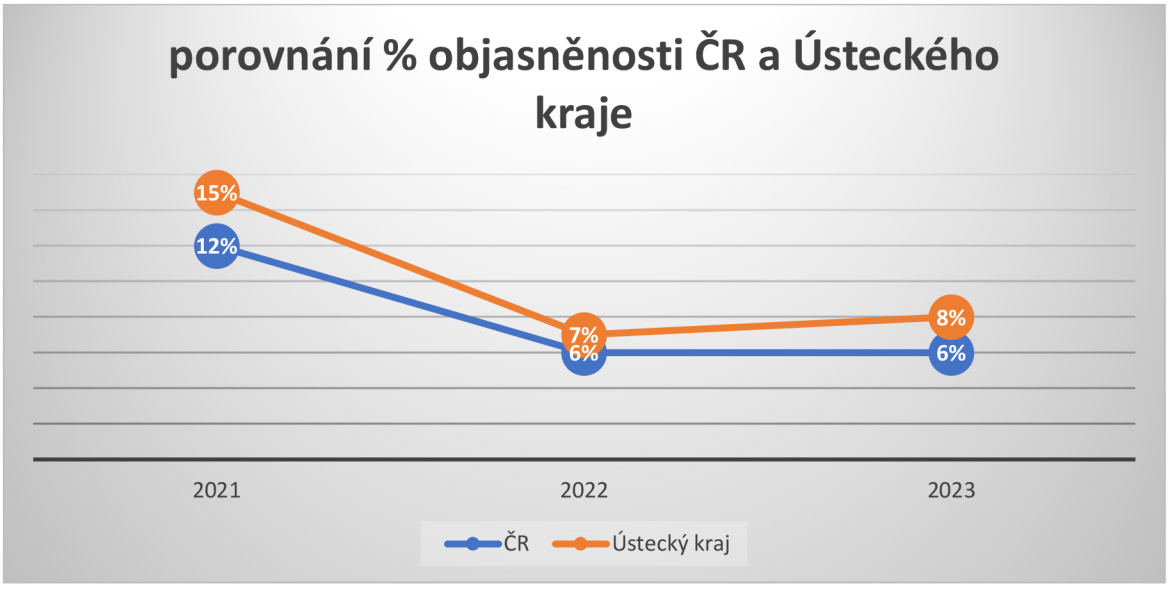
Tabulka č. 29: Objasněnost v ULK

Ústecký kraj	2021	2022	2023
spácháno	436	1032	1216
objasněno	64	74	93
v %	15%	7%	8%

Zdroj: vlastní zpracování z interní statistiky kriminality PČR

Z obou výše uvedených tabulek je vidět klesající tendence objasněnosti, jak v České republice, tak v Ústeckém kraji, kdy obě tempa poklesu spolu zhruba korespondují, což je znázorněno i v grafu č. 17.

Graf č. 17: Porovnání procentuální objasněnosti ČR a ULK



Zdroj: vlastní zpracování z interní statistiky kriminality PČR

4.3.4 Index kriminality

Pro roky 2021 a 2022 byly k výpočtům použity hodnoty počtu obyvatel České republiky a Ústeckého kraje, které byly zjištěny z demografických příruček Českého statistického úřadu. Pro rok 2023 byly použity aktuální hodnoty zveřejněné na webových stránkách Českého statistického úřadu pro 3. čtvrtletí roku 2023. Zjištěné údaje jsou uvedené v tabulce č. 30, kde je v přepočtu na 100 000 obyvatel vypočten indexy kriminality v České republice a Ústeckém kraji pro jednotlivé zkoumané roky.

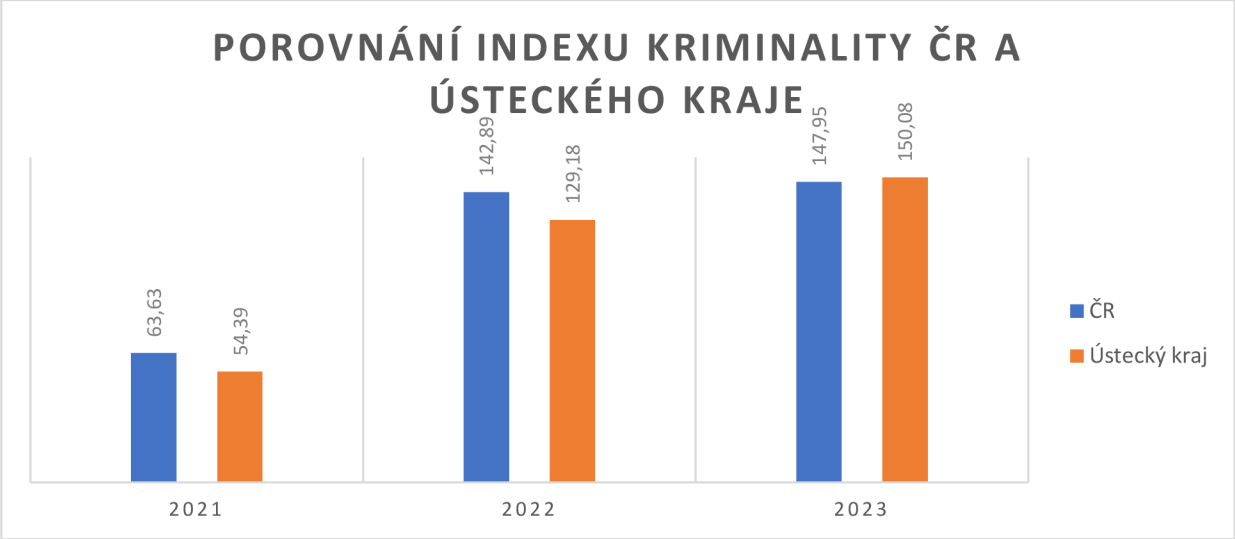
Tabulka č. 30: Počet obyvatel a Index kybernetické kriminality v ČR a ULK

	Počet obyvatel		Index kriminality	
	v ČR	v ULK	v ČR	v ULK
2021	10 494 836	801 586	63,63	54,39
2022	10 516 707	798 898	142,89	129,18
2023	10 882 235	810 224	147,95	150,08

Zdroj: vlastní zpracování z demografických příruček Českého statistického úřadu

V grafu č. 18 je vidět, že v prvních dvou letech 2021 a 2022 byl index kriminality vyšší pro Českou republiku a v roce 2023 pak pro Ústecký kraj.

Graf č. 18: Porovnání indexů kybernetické kriminality ČR a ULK



Zdroj: vlastní zpracování

4.4 Rozhovory s osobami participujícími při řešení kybernetické kriminality

4.4.1 Analytik ÚSKPV

1) Jaká je Vaše pracovní / služební pozice?

Odpověď: V současné době jsem zařazen jako analytik / vrchní komisař na Policejním prezidiu České republiky, Úřadu služby kriminální policie a vyšetřování, Odboru centrální analytiky, Oddělení operativních a taktických analýz. Dříve od roku 2018 do 2022 jako analytik se specializací na kybernetickou kriminalitu / komisař na Krajském ředitelství Ústeckého kraje, Územního odboru Most, Oddělení analytiky a kybernetické kriminality. V rámci své funkce s odborným školením IT kriminalistického specialisty pro provádění kriminalisticko-technických úkonů při zajišťování výpočetní techniky a digitálních dat na místě jejich nálezu.

2) Jak Vaše pracovní / služební pozice zasahuje do procesu odhalování a vyšetřování trestné činnosti páchané v kyberprostoru?

Odpověď: Z pozice analytika provádím analýzy případů v informačních systémech Policie České republiky s čímž souvisí propojování případů trestné činnosti páchané v kyberprostoru a jejich začleňování do takzvaných sérií na základě společných atributů. K určitým případům využívám také Open Source Intelligence (OSINT), kdy jde o získávání informací z otevřených zdrojů sítě Internet. Může se tak jednat např. o hledání záznamů o událostech, osobách, subjektech a vzájemných vztazích, nebo zjišťování digitálních stop definované entity.

3) Jak dlouho se věnujete problematice trestné činnosti páchané v kyberprostoru?

Odpověď: Necelých šest let.

4) Zhodnoťte z Vašeho pohledu vývojový trend trestné činnosti páchané v kyberprostoru?

Odpověď: Vývojový trend je již několik let veden v policejních statistikách, kde lze jednoznačně pozorovat stoupající trend.

5) Které trestné činy jsou dle Vašich zkušeností nejčastěji páchané v souvislosti s kyberprostorem?

Odpověď: Hospodářské trestné činy, a to především podvody, kdy se pachatelé snaží získat finanční prospěch. Velkým problémem jsou však také mravnostní trestné činy související s dětskou pornografií.

6) Jaká je z Vašeho pohledu situace v Ústeckém kraji / okrese Most? Zhodnoťte skladbu trestné činnost páchané v kyberprostoru v Ústeckém kraji / okrese Most? Jaká je podle Vás zatíženost Ústeckého kraje / okresu Most?

Odpověď: Z hlediska svého současného zařazení nejsem schopen na tuto otázku adekvátně odpovědět.

7) Jaká jsou podle Vás v současné době největší úskalí při řešení dané problematiky? Jsou problematické oblasti legislativy a jurisdikce, odborné úrovně pracovníků zabývajících se danou problematikou nebo při odhalování a dokazování a zavedených postupech?

Odpověď: Hlavním problémem je anonymizace pachatelů v síti internet, kteří využívají především službu VPN neboli „Virtual Private Network“. Virtuální privátní síť, je technologie, která umožňuje vytvořit bezpečné a šifrované spojení mezi vaším zařízením a internetem. To znamená, že všechna data, která posíláte a přijímáte přes tuto síť, jsou chráněna před neoprávněným přístupem a špionáží. VPN funguje tak, že vaše internetová data procházejí serverem VPN, který vám poskytuje novou IP adresu, a tím skrývá vaši skutečnou polohu a identitu. S touto službou je spojena legislativa, která se řídí jurisdikcí země, kde má sídlo společnost poskytující tuto službu. Nejčastěji to jsou země, které nemají povinnost uchovávat informace o uživatelích, kterým službu poskytují a tím pádem neposkytují informace orgánům činným v trestním řízení. Takovým státem je například Panama a s tím spojena společnost NordVPN. Za využití této služby pak pachatelé mohou využívat další služby jako je Spoofing, neboli, že u příchozího hovoru vidíte známé telefonní číslo, ve skutečnosti ale volá někdo cizí a pouze se maskuje za někoho jiného. Pachatelé dokážou napodobit jakékoliv telefonní číslo a z něj vám zavolat, tedy třeba i číslo banky. U těchto služeb může být také problém krátká doba uchovávání informací, možnost pachatelů platit za služby tzv. kryptoměnou, a dále nemusí docházet ani k ověřování identit uživatelů těchto služeb.

Dále odborná znalost pracovníků zabývajících se danou problematikou, která je potřebná při odhalování a dokazování není vždy dostatečná a je třeba vytvářet metodiku postupů a možnosti proškolení pro tyto pracovníky.

8) Co považujete za nedostačující v oblasti legislativy a jurisdikce?

Odpověď: Jak jsem již uvedl v případě společnosti NordVPN, tato má sídlo v jurisdikci státu Panama, která nemá v legislativě uvedenu povinnost uchovávat informace o svých uživatelích. Další problém v legislativě může být doba uchovávání potřebných informací, která liší stát od státu.

9) Co považujete za nedostačující v oblasti odborné úrovně pracovníků, kteří se zabývají danou problematikou?

Odpověď: Zde vidím zatím nedostačující zajištění potřebných školení, kdy navíc daná problematika se časem vyvíjí a je tak navíc potřeba školení aktualizovat. S tímto je potřeba vytvářet a aktualizovat metodické postupy především při odhalování a následném dokazování.

10) Co považujete za nedostačující v oblasti odhalování, dokazování a zavedených postupech?

Odpověď: Nedostačující je jistě potřebná legislativa, která odhalování komplikuje. Problém je také ve vývoji celé situace páchané trestné činnosti v kyberprostoru, kdy pachatelé využívají nové služby a nástroje, prostřednictvím čehož trestnou činnost páchají. Pachatelé jsou stále sofistikovanější, a je třeba potřeba na to reagovat aktualizací metodických postupů.

11) Vidíte problémy v nějakých dalších oblastech?

Odpověď: Ne.

12) Popište z Vašeho pohledu proces vyžadování informací od dotazovaných subjektů. Vidíte v tomto procesu nějaké slabiny?

Odpověď: Proces vyžadování informací se liší subjekt od subjektu, kdy ne vždy je spolupráce bezproblémová, rychlá a efektivní. Především spolupráce se zahraničními subjekty není vždy ideální a kolikrát je bez odpovědi. Policie ČR se však snaží dohodnout a najít cestu ke spolupráci se zahraničními subjekty prostřednictvím mezinárodní policejní

nebo justiční spolupráce. V mezinárodní spolupráci se podařilo například vytvořit komunikační kanál „Kodex“ (URL: https://app.kodex.us) pro vymáhání práva, kam se zapojila řada velkých zahraničních subjektů jako je např. Binance, Coinbase, Discord, Badoo, MoonPay a dalších, kdy se jedná o portál vládních žádostí pro vymáhání práva s rychlou a efektivní spoluprací k získávání informací od uvedených subjektů.

13) Jak hodnotíte lhůty, po které dožadované subjekty uchovávají potřebná data?

Odpověď: Lhůty pro uchovávání dat se u zahraničních subjektů také kolikrát velmi liší pro konkrétní data a danou zemi, kdy tyto lhůty jsou nastaveny zákony dané země. Například Česká republika má zákonem č. 127/2005 Sb. Zákon o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), stanoveno v § 97 odst. 3, že právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna uchovávat po dobu 6 měsíců provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování jejích veřejných komunikačních sítí a při poskytovávání jejích veřejně dostupných služeb elektronických komunikací.

14) Jak hodnotíte současnou úroveň prevence, preventivních opatření a osvěty problematiky trestné činnosti páchané v kyberprostoru? Zhodnoťte důležitost faktoru předcházení této trestné činnosti.

Odpověď: Co se týče prevence a osvěty problematiky k trestné činnosti páchané v kyberprostoru, Policie ČR se snaží spolupracovat s médii a společnostmi, jako je např. CZ.NIC, který je správcem české domény CZ.

V rámci projektu Safer Internet Centrum (SIC), jehož garantem je sdružení CZ.NIC, byla s Policií České republiky uzavřena deklarace o spolupráci při provozu linky STOPonline.cz. Vzájemná spolupráce funguje od roku 2019 a společným zájmem je ochrana dětí a mládeže před trestnou činností s cílem minimalizovat výskyt dětské pornografie, kybergroomingu nebo nepatřičné dětské nahoty na Internetu na území České republiky.

Účelem deklarace je především prohloubení spolupráce mezi Policií České republiky, operátory linky STOPonline.cz a širokou veřejností, aby docházelo k efektivnímu

shromažďování informací o aktivních odkazech na zjištěný nezákonný obsah a následnému řešení příslušnými orgány.

Za loňský rok bylo policii předáno k dalšímu prošetření 254 incidentů, které byly nahlášeny prostřednictvím formuláře horké linky STOPonline.cz. Operátoři linky nyní budou spolupracovat s kolegy z Úřadu služby kriminální policie a vyšetřování, který spadá pod Policejní prezídium České republiky. V minulosti tuto agendu vykonávala Národní centrála proti organizovanému zločinu služby kriminální policie a vyšetřování.

Celé znění deklarace o spolupráci je dostupné na stránkách sdružení, více informací o samotné lince STOPonline.cz je pak k dispozici na stránkách www.stoponline.cz, kde se také v případě potřeby nachází formulář pro hlášení nezákonného obsahu na Internetu.

15) Jaká máte doporučení v oblasti prevence a předcházení trestné činnosti páchané v kyberprostoru?

Odpověď: Doporučit lze především vyšší medializace případů, nabízení přednášek a školení pro veřejnost, školy apod. Dále je potřeba zapojování mobilních operátorů, bankovních institucí a dalších společností, které jsou pachateli využívány, aby tyto subjekty aktivně vytvářeli zabezpečení proti tomuto jednání a dále o tom informovali své zákazníky. Z mého pohledu se toto již velmi zlepšilo a třeba v tom pokračovat. Konkrétně u mobilních operátorů jde o informovanost o zneužívání M-Plateb, využívání Spoofingu. U bankovních institucí a společností poskytující například automaty na směnu kryptoměny jde o informovanost o podvodných investicích nejčastěji do kryptoměn, falešných bankéřích a reverzních inzertních podvodech, při kterých se podvodník staví do role falešného zájemce o koupi nabízeného zboží.

16) Jaký očekáváte vývoj s problematikou a trestnou činností, která je páchaná v souvislosti s kyberprostorem?

Odpověď: Vývoj bude mít stále narůstající tendenci, a to především díky vývoji technologií, stále větší sofistikovaností pachatelů, kteří velmi dobře využívají sociální inženýrství. Velký problém v současné době nastává také s příchodem a využíváním umělé inteligence, díky které pachatelé vytváří Deepfake videa či obrázky. Deepfake je označení pro realistickou úpravu videa. Upravuje se především tvář zobrazených osob, mimika obličeje a řeč

jednotlivých aktérů videa. Jedinci pak vykonávají činnosti, které ve skutečnosti nedělají a říkají slova, která ve skutečnosti nikdy nepronesli. Tyto videa již lze zaznamenat ve větší míře u reklam do podvodných investic.

4.4.2 Zástupce vedoucího okresní OHK

1) Jaká je Vaše pracovní / služební pozice?

Odpověď: Moje pracovní pozice je zástupce vedoucího oddělení.

2) Jak Vaše pracovní / služební pozice zasahuje do procesu odhalování a vyšetřování trestné činnosti páchané v kyberprostoru?

Odpověď: Z mé strany dávány pokyny podřízeným policistům k úkonům, které mají provádět v rámci vyšetřování, respektive prověřování této trestné činnosti, tedy zcela zásadně.

3) Jak dlouho se věnujete problematice trestné činnosti páchané v kyberprostoru?

Odpověď: Cca od roku 2006.

4) Zhodnoťte z Vašeho pohledu vývojový trend trestné činnosti páchané v kyberprostoru?

Odpověď: Dle mého názoru kriminalita páchaná v kyberprostoru stále narůstá, a taktéž si myslím, že klasická kriminalita z „ulice“ se přesouvá právě do tohoto prostoru. Stává se taktéž více anonymní díky vývoji programů a výpočetní techniky.

5) Které trestné činy jsou dle Vašich zkušeností nejčastěji páchané v souvislosti s kyberprostorem?

Odpověď: Nejčastěji trestný čin podvodu, neoprávněného držení, padělání a pozměnění platebního prostředku.

6) Jaká je z Vašeho pohledu situace v Ústeckém kraji / okrese Most? Zhodnoťte skladbu trestné činnost páchané v kyberprostoru v Ústeckém kraji / okrese Most? Jaká je podle Vás zatíženost Ústeckého kraje / okresu Most?

Odpověď: Domnívám se, že v Ústeckém kraji je zvýšená s ohledem i na celkovou trestnou činnost v Ústeckém kraji. Z toho vyplývá i vyšší zatíženost Územního odboru Most.

7) Jaká jsou podle Vás v současné době největší úskalí při řešení dané problematiky? Jsou problematické oblasti legislativy a jurisdikce, odborné úrovně pracovníků zabývajících se danou problematikou nebo při odhalování a dokazování a zavedených postupech?

Odpověď: Největším úskalím dle mého názoru je legislativa, a příp. složité (zdlouhavé) postupy při odhalování, resp. vyšetřování této trestné činnosti. Dalším, asi největším úskalím je, že tato trestná činnost má v současné době tendenci mezinárodního přesahu, tj. její objasnění je buď dosti ztížené, někdy až nemožné. K odborné úrovni pracovníků mimo náš útvar se nedokážu vyjádřit, za náš útvar je odborná vybavenost na střední úrovni (bráno s pohledu na celkové množství policistů, kteří se jí zabývají).

8) Co považujete za nedostačující v oblasti legislativy a jurisdikce?

Odpověď: Faktická nemožnost vyžadovat údaje od zahraničních subjektů, zdlouhavé řízení a cesta k informacím, pokud je vyžádat lze.

9) Co považujete za nedostačující v oblasti odborné úrovně pracovníků, kteří se zabývají danou problematikou?

Odpověď: Z hlediska našeho útvaru jde o to, že se podřízení nezabývají jedním druhem trestné činnosti, okolnosti, resp. trestná činnost páchaná v kyberprostoru se stále mění a rozvíjí, tudíž nelze ihned informačně reagovat na každý případ, jelikož se nezabýváme pouze tímto jedním druhem trestné činnosti.

10) Co považujete za nedostačující v oblasti odhalování, dokazování a zavedených postupech?

Odpověď: Problémem je nesjednocení postupů jednotlivých policejních orgánů, i když v poslední době se to zlepšuje.

11) Vidíte problémy v nějakých dalších oblastech?

Odpověď: Nedokážu posoudit.

12) Popište z Vašeho pohledu proces vyžadování informací od dotazovaných subjektů. Vidíte v tomto procesu nějaké slabiny?

Odpověď: Některé subjekty si doslova „diktují“ podmínky, za kterých vydávají informace, policie nemá silné právní zastoupení, které byl „podrželo“ jednotlivého zpracovatele, resp. útvar, ani se na toto právní zastoupení není možné obrátit (alespoň mi není známo kam). Za druhé vymahatelnost informací u zahraničních subjektů, např. pod pohrůžkou uložení pořádkové pokuty, je téměř nulová.

13) Jak hodnotíte lhůty, po které dožadované subjekty uchovávají potřebná data?

Odpověď: S těmi, co spolupracují jsou lhůty přiměřené.

14) Jak hodnotíte současnou úroveň prevence, preventivních opatření a osvěty problematiky trestné činnosti páchané v kyberprostoru? Zhodnoťte důležitost faktoru předcházení této trestné činnosti.

Odpověď: Troufám si říct, že prevence je nedostatečná. Konkrétně, domnívám se, že ze strany Policie České republiky jsou preventivní programy prováděny zřejmě v nejvyšší možné míře, ale pouze v rámci jejích programů. Prevence by měla být více ve sdělovacích prostředcích, nicméně na toto není žádná právní úprava, která by složkám moci umožňovala vstupovat do médií podle potřeby. Pokud by byla, mohlo by být prevence více.

15) Jaká máte doporučení v oblasti prevence a předcházení trestné činnosti páchané v kyberprostoru?

Odpověď: Doporučil bych před používáním výpočetní techniky projít nějakým kurzem bezpečnosti v kyberprostoru, přizpůsobený věku uživatele. Dalším problémem jsou kryptoměny, prostřednictvím kterých odcházejí výnosy z trestné činnosti a nemožnost jejich regulace, resp. anonymita příjemců. Zde by bylo vhodné nějaké zákonné opatření.

16) Jaký očekáváte vývoj s problematikou a trestnou činností, která je páchaná v souvislosti s kyberprostorem?

Odpověď: Pokud nedojde ke vzniku zákonů regulujících trh s kryptoměnami, respektive určujících zjištění příjemce kryptoměn atd., bude dále tato trestná činnost růst.

4.4.3 Vyšetřovatelka okresní OHK

1) Jaká je Vaše pracovní / služební pozice?

Odpověď: Jsem na pozici vyšetřovatele na oddělení hospodářské kriminality, Územní odbor Most.

2) Jak Vaše pracovní / služební pozice zasahuje do procesu odhalování a vyšetřování trestné činnosti páchané v kyberprostoru?

Odpověď: Vzhledem k tomu, že na našem územním odboru není vytvořena skupina kybernetické kriminality, zpracovává kybernetickou kriminalitu naše oddělení, a to v obou procesních stupních. Tedy vedle hospodářské kriminality a stanovené majetkové kriminality běžně zpracováváme a kybernetickou kriminalitu.

3) Jak dlouho se věnujete problematice trestné činnosti páchané v kyberprostoru?

Odpověď: Od nástupu na oddělení hospodářské kriminality v roce 2020 zpracovávám mimo jiné i trestnou činnost spáchanou v kyberprostoru, a to související s trestnými činy neoprávněný přístup k počítačovému systému a nosiči informací dle § 230 trestního zákoníku a podvod dle § 209 trestního zákoníku.

4) Zhodnoťte z Vašeho pohledu vývojový trend trestné činnosti páchané v kyberprostoru?

Odpověď: V letech 2010 až 2020 to byly jen jednoduché podvody na inzertních portálech, kdy pachatel byl občan České republiky a relativně snadno odhalitelný (IP adresa a telefonní číslo vedlo přímo k němu), jednalo se spíše o majetkovou trestnou činnost páchanou na internetu. Od roku 2020 začali sofistikované podvody – oběti jsou nalákáni např. na investice známých osobností a společností s příslibem rychlé návratnosti a vysokého zisku nebo vztah na dálku např. lékař v JEMENU/AFGÁNSTANU, tyto oběti dají pachateli vzdálený přístup ke svým zařízením a postupně pak od nich vylákají finanční prostředky, jedná se o dlouhodobí kontakt trvající i jeden rok, oběti jsou jako „dojné krávy“, další typ podvodů jsou oproti tomu velice rychlé, během pár minut nemá oběť na účtu žádné finanční prostředky typicky přihlášení oběti do internetového bankovnictví na stránku napodobující portál banky (phishingovou stránku), inzertní portály s odkazy na phishingové stránky nebo zadání údajů z platební karty na odkazy zaslané pachatelem a mnoho dalších. Pachatele

nelze dohledat ani přes IP adresu, telefonní čísla či odchozí platby, tyto většinou směřují do zahraničí.

5) Které trestné činy jsou dle Vašich zkušeností nejčastěji páchané v souvislosti s kyberprostorem?

Odpověď: Z trestných činů bych uvedla podvod dle § 209 trestního zákoníku, neoprávněný přístup k počítačovému systému a nosiči informací dle § 230 trestního zákoníku a neoprávněné opatření, padělání a pozměnění platebního prostředku dle § 234 trestního zákoníku.

6) Jaká je z Vašeho pohledu situace v Ústeckém kraji / okrese Most? Zhodnoťte skladbu trestné činnost páchané v kyberprostoru v Ústeckém kraji / okrese Most? Jaká je podle Vás zatíženost Ústeckého kraje / okresu Most?

Odpověď: Myslím, že stejná jako na jiných Územních odborech vzhledem k tomu, že je páchána v kyberprostoru nemá konkrétní lokalitu. Jinou situaci vidím ve výstupech – legalizacích, to je jednoznačně nejzatíženější naše hlavní město a Brno.

7) Jaká jsou podle Vás v současné době největší úskalí při řešení dané problematiky? Jsou problematické oblasti legislativy a jurisdikce, odborné úrovně pracovníků zabývajících se danou problematikou nebo při odhalování a dokazování a zavedených postupech?

Odpověď: Čas. Čas je jednoznačně proti nám. Tím, že je nutné žádat státního zástupce na postup dle §8 odst. 2 trestního řádu (bankovní tajemství), nutnost příkazu soudu dle § 88a (telekomunikační provoz - IP adresy a telefony), odpověď bank s velkou časovou prodlevou, krátkodobé uložení dat telekomunikačních společností. To bych v oblasti legislativy a jurisdikce změnila a dala větší pravomoc policii. Pokud se týká odborné úrovně pracovníků, tak nemyslím si, že policista musí být odborník na danou problematiku, ale musí umět správně rozlišit a aplikovat postup, který takový odborník vytvořil.

8) Co považujete za nedostačující v oblasti legislativy a jurisdikce?

Odpověď: Krátké lhůty pro uchování dat. Malá pravomoc policie, a hlavně úskalí mezinárodní spolupráce zejména cestou státního zastupitelství, kdy odpověď ze zahraničí trvá řádově několik měsíců i let. Zahraniční společnosti (např. facebook, whatsapp) v každé

zemi by v rámci internetového prostředí měli mít styčnou osobu pro danou zemi, která zaručí okamžité získání dat a i adekvátní opatření.

9) Co považujete za nedostačující v oblasti odborné úrovně pracovníků, kteří se zabývají danou problematikou?

Odpověď: Nedostatek pracovníků, které jsou skutečně odborníky v oblasti kyberkriminality nikoli běžnými uživateli počítače.

10) Co považujete za nedostačující v oblasti odhalování, dokazování a zavedených postupech?

Odpověď: Na našem oddělení rozhodně to, že musíme být univerzální, bez konkrétní specializace, učíme se zkušenostmi.

11) Vidíte problémy v nějakých dalších oblastech?

Odpověď: V oblasti bankovnictví zejména platby obchodníkům přes platební brány do zahraničí.

12) Popište z Vašeho pohledu proces vyžadování informací od dotazovaných subjektů. Vidíte v tomto procesu nějaké slabiny?

Odpověď: Jako slabinu vidím např. u IP adres, kdy poskytovatel poskytuje adresu společnosti, která je dále poskytuje zákazníkům, tedy nutnost dalších příkazů soudů. V případě vyžadování informací u bank, pak pokud pachatel přeposílá záměrně peníze přes x subjektů nutnost ke každému z nich žádat státního zástupce.

13) Jak hodnotíte lhůty, po které dožadované subjekty uchovávají potřebná data?

Odpověď: Nedostatečné zejména u mobilních operátorů.

14) Jak hodnotíte současnou úroveň prevence, preventivních opatření a osvěty problematiky trestné činnosti páchané v kyberprostoru? Zhodnoťte důležitost faktoru předcházení této trestné činnosti.

Odpověď: Každý den je zobrazován nějaký článek s varováním před těmito podvody. Každá banka, inzertní portály a větší obchodníci např. Alza, mají varování před těmito útoky. Prevence je dostatečná. Oběti většinou uvádí, že si toho všimli až když už i jim to přišlo podezřelé, ačkoli jsou tyto články zobrazovány tři roky.

15) Jaká máte doporučení v oblasti prevence a předcházení trestné činnosti páchané v kyberprostoru?

Odpověď: Používat zdravý rozum.

16) Jaký očekáváte vývoj s problematikou a trestnou činností, která je páchaná v souvislosti s kyberprostorem?

Odpověď: Nápad se bude nadále zvyšovat. Pachatelé jsou stále před námi.

4.4.4 Vedoucí krajského OKK

1) Jaká je Vaše pracovní / služební pozice?

Odpověď: Vedoucí oddělení kybernetické kriminality KŘP.

2) Jak Vaše pracovní / služební pozice zasahuje do procesu odhalování a vyšetřování trestné činnosti páchané v kyberprostoru?

Odpověď: Mám řídící a kontrolní pravomoc. Vydávám pokyny do tr. spisů, kontroluji plány prověřování a vyšetřování, seznamuji podřízené s novými postupy, legislativou a metodikami republikových útvarů.

3) Jak dlouho se věnujete problematice trestné činnosti páchané v kyberprostoru?

Odpověď: 7 let.

4) Zhodnoťte z Vašeho pohledu vývojový trend trestné činnosti páchané v kyberprostoru?

Odpověď: Nápad v kyberprostoru dramaticky roste. Porovnám-li rok 2022 a 2021, jde o 100% nárůst. Predikuji podobný vývoj i v následujících letech. Tato skutečnost souvisí s rozvojem digitálních technologií, internetu a obecně přesunem lidské činnosti do virtuálního prostředí.

5) Které trestné činy jsou dle Vašich zkušeností nejčastěji páchané v souvislosti s kyberprostorem?

Odpověď: § 209, 234, 230, 192 TZ.

6) Jaká je z Vašeho pohledu situace v Ústeckém kraji / okrese Most? Zhodnoťte skladbu trestné činnost páchané v kyberprostoru v Ústeckém kraji / okrese Most? Jaká je podle Vás zatíženost Ústeckého kraje / okresu Most?

Odpověď: V Ústeckém kraji je od počátku roku do 30.5. 2023 evidováno celkem 682 skutků evidovaných jako kyber. ÚO Most má spíše menší nápad o proto jiným ÚO (78 skutků). Věc může i ovlivňovat špatná kvalifikace § 234 u přestupkových škod.

Skladba spisů – v celém kraji je obdobná – vede § 209, dále souběh 209+234, následně § 230 a mravnostní delikty §192. Při hodnocení statistiky PČR je důležité si uvědomit následující

věci: Eviduje skutky, nikoliv trestné činy. Pokud je tedy souběh 209+234+230 – statistika vykáže jen jeden skutek a jeden nejzávažnější §. V rámci ETŘ lze dohledat sledované IT události, kde lze vidět i souběhy.

7) Jaká jsou podle Vás v současné době největší úskalí při řešení dané problematiky? Jsou problematické oblasti legislativy a jurisdikce, odborné úrovně pracovníků zabývajících se danou problematikou nebo při odhalování a dokazování a zavedených postupech?

Odpověď: Chybějící vzdělání a kvalifikace policistů. Výrazně rychlejší technologický vývoj oproti vývoji právní ochraně v rámci tr. práva a mezinárodního práva. Vyložené nepružná a obtížně realizovatelná spolupráce v rámci mezinárodní justiční spolupráci.

8) Co považujete za nedostačující v oblasti legislativy a jurisdikce?

Odpověď: Zákonná povinnost všem velkým hráčům (META, GOOGLE, MICROSOFT apod.) evidovat a poskytovat data všem OČTŘ v zemích, kde jsou jejich služby poskytovány.

Minimálně v rámci EU pevná lhůta pro zpracování odpovědi právní pomoci a v rámci ČR pevná lhůta pro SZ k vyřízení podnětu o právní pomoc.

9) Co považujete za nedostačující v oblasti odborné úrovně pracovníků, kteří se zabývají danou problematikou?

Odpověď: Chybí znalosti o možnosti trasování kryptoměn, možnosti přímé policejní spolupráce, využití styčných důstojníků, možnosti přímého vyžadování informací od zahraničních subjektů, analytické myšlení.

10) Co považujete za nedostačující v oblasti odhalování, dokazování a zavedených postupech?

Odpověď: Chybí jasná a jednoduchá koncepce prověřování sériových tr. činů, rychlé a jasné určování místní příslušnosti. Nevymahatelnost mezinárodního práva.

11) Vidíte problémy v nějakých dalších oblastech?

Odpověď: Chybí povinné celoživotní vzdělávání policistů, SZ a soudců.

12) Popište z Vašeho pohledu proces vyžadování informací od dotazovaných subjektů. Vidíte v tomto procesu nějaké slabiny?

Odpověď: Příliš obecný dotaz.

13) Jak hodnotíte lhůty, po které dožadované subjekty uchovávají potřebná data?

Odpověď: Data rentention 6 měsíců v ČR pořádku. V SRN 7 dní na dynamické IP je příliš málo.

14) Jak hodnotíte současnou úroveň prevence, preventivních opatření a osvěty problematiky trestné činnosti páchané v kyberprostoru? Zhodnoťte důležitost faktoru předcházení této trestné činnosti.

Odpověď: Důležitost je vysoká, prevence na prvním místě. V ČR na dobré úrovni. Bohužel lidé jsou „slepí".

15) Jaká máte doporučení v oblasti prevence a předcházení trestné činnosti páchané v kyberprostoru?

Odpověď: Prevence jako součást základního a středního vzdělání, využití soc. sítí stát. organizací, zapojení medií, vložení skryté prevence v rámci televizních pořadů. Význam má jedině masová a opakované prevence.

16) Jaký očekáváte vývoj s problematikou a trestnou činností, která je páchaná v souvislosti s kyberprostorem?

Odpověď: Poroste. S vývojem AI přijdou nové trendy.

4.4.5 Vyšetřovatel krajské OHK

1) Jaká je Vaše pracovní / služební pozice?

Odpověď: Vrchní komisař na Odboru SKPV OHK Ústí nad Labem.

2) Jak Vaše pracovní / služební pozice zasahuje do procesu odhalování a vyšetřování trestné činnosti páchané v kyberprostoru?

Odpověď: Vzhledem ke skutečnosti, že trendem kriminálního jednání je obecně „postupný přesun do kyberprostoru" a zejména hospodářská kriminalita je zaměřena na odhalování specifických forem protiprávního jednání, navázaného na kyberprostor, a také skutečnosti, že se o tuto oblast dlouhodobě zajímám, jsou mi přidělovány trestní spisy, související s touto problematikou.

3) Jak dlouho se věnujete problematice trestné činnosti páchané v kyberprostoru?

Odpověď: Po celou dobu působení u SKPV (cca 7 let), kam jsem byl původně „verbován" se zaměřením výhradně na tuto problematiku.

4) Zhodnoťte z Vašeho pohledu vývojový trend trestné činnosti páchané v kyberprostoru?

Odpověď: Vývoj je zřejmý. Velké množství hospodářské kriminality se přesouvá do kyberprostoru, protože je pro pachatele snadněji dostupný a skýtá anonymitu.

5) Které trestné činy jsou dle Vašich zkušeností nejčastěji páchané v souvislosti s kyberprostorem?

Odpověď: Ryzí kyberkriminalita (např. prolamování počítačových systémů) byla systemizací přesunuta do specializovaných útvarů (OAaKK). Z pohledu hospodářské kriminality se tak jedná převážně o podvodná jednání za využití kyberprostoru.

6) Jaká je z Vašeho pohledu situace v Ústeckém kraji / okrese Most? Zhodnoťte skladbu trestné činnost páchané v kyberprostoru v Ústeckém kraji / okrese Most? Jaká je podle Vás zatíženost Ústeckého kraje / okresu Most?

Odpověď: Ústecký kraj se obecně vymyká celorepublikovému průměru a odpovídá složení kriminality v jiných částech republiky se stejným demografickým složením. Neznám podrobné statistiky, nicméně poškození při tomto typu trestné činnosti, pocházejí z oblasti sociálně slabých se základním, maximálně středoškolským jednáním. To znamená čím více takových jedinců, tím vyšší míra takových poškozených. Ústecký kraj (zahrnujíc veškerá města v severních Čechách) je na tom tedy podobně jako např. Moravskoslezský kraj.

7) Jaká jsou podle Vás v současné době největší úskalí při řešení dané problematiky? Jsou problematické oblasti legislativy a jurisdikce, odborné úrovně pracovníků zabývajících se danou problematikou nebo při odhalování a dokazování a zavedených postupech?

Odpověď: Legislativní systém ČR není vůbec špatný a skýtá dostupné prostředky k potírání kyberkriminality, jako problém vidím však „mezinárodní legislativu", jelikož kyberprostor hranice nemá a informace jsou dostupné převážně v zahraničí. Na tento fakt je navázána i odborná úroveň zmiňovaných pracovníků kyberkriminalitou se zabývajících. Útvar (PČR) jako celek v této oblasti dá se říct „zaspal" a disponuje minimálním množstvím erudovaných osob. Na úrovni okresů i krajů, pokud pomineme OAaKK (ale i zde nejsou dostatečně proškoleni pracovníci) jsou spíše policisté, kteří neví, jak informaci získat, co znamená a jak jí dále užít. To je způsobeno neochotou učit se nové věci a postupy. Typickým příkladem je přijetí oznámení, získání základních informací od poškozených a následný dotaz k analytikovi k lustraci zjištěných atributů, za účelem postoupení věci jinam bez dalších opatření (místo alespoň prvotních nápadů na postup, konzultací atp.).

8) Co považujete za nedostačující v oblasti legislativy a jurisdikce?

Odpověď: Jak jsem uvedl, v ČR problém zásadně nevidím. Spíše na mezinárodní spolupráci, která je zkostnatělá, nepružná a nevyvíjí se dostatečně rychle. Za zásadní považuji získání informace v přijatelném čase (nikoli v řádu měsíců).

9) Co považujete za nedostačující v oblasti odborné úrovně pracovníků, kteří se zabývají danou problematikou?

Odpověď: Nezájem rozvíjet se, získávat nové poznatky. To může být způsobeno velkým počtem prověřovaných věcí, nedostatečným finančním ohodnocením. Ač některé útvary nabízejí různá školení, cílem přihlášených účastníků není vzdělat se, ale „ulejt se“ ze svých současných pracovních povinností. To je způsobenou nedostatečnou pobídkou.

10) Co považujete za nedostačující v oblasti odhalování, dokazování a zavedených postupech?

Odpověď: Odbornost pracovníků, viz výše.

11) Vidíte problémy v nějakých dalších oblastech?

Odpověď: Již jsem zmínil, personální stav obecně u PČR, ale u této problematiky dvojnásob.

12) Popište z Vašeho pohledu proces vyžadování informací od dotazovaných subjektů. Vidíte v tomto procesu nějaké slabiny?

Odpověď: Již popisováno výše. V ČR lze informace nějakým způsobem získat poměrně rychle. V zahraničí obtížně a mnohdy velmi pomalu.

13) Jak hodnotíte lhůty, po které dožadované subjekty uchovávají potřebná data?

Odpověď: Dostačující v ČR, v zahraničí nejsem schopen hodnotit konkrétně, ale obecně převážně dostačující.

14) Jak hodnotíte současnou úroveň prevence, preventivních opatření a osvěty problematiky trestné činnosti páchané v kyberprostoru? Zhodnoťte důležitost faktoru předcházení této trestné činnosti.

Odpověď: Zcela zásadní oblast, ve které je ČR a PČR pozadu. Nedostatečná prevence a osvěta, posílení týmů, zaměřených hlavně na sociální sítě, kde podvodníci „loví“ je největším problémem (vedle odbornosti a nedostatku pracovníků) a řadil bych ho na první místo.

15) Jaká máte doporučení v oblasti prevence a předcházení trestné činnosti páchané v kyberprostoru?

Odpověď: Více se zaměřit na sociální sítě. Ve vztahu ke starší generaci primárně např. na Meta (Facebook), ale i na TikTok, Instagram pro mladší generace. Více kampaní i ve sdělovacích prostředcích (TV), obrazová kampaň je nejúčinnější, texty nejsou ochotni ohrožené skupiny obyvatel číst.

16) Jaký očekáváte vývoj s problematikou a trestnou činností, která je páchaná v souvislosti s kyberprostorem?

Odpověď: Vývoj půjde ruku v ruce s informovaností. Osobně očekávám mírný úpadek (méně takové trestné činnosti) s optimistickým výhledem k prevenci. Z pohledu pachatelů očekávám vývoj exponenciální, pokud už pachatel získá oběť, půjde ho velmi těžce odhalit (spoofing, VPN, protonmail, IPv6, AI…), jelikož kyberprostor se vyvíjí mnohem rychleji než prostředky k jeho ochraně (umělá inteligence bude v budoucnu velký problém – při možnosti změnit vše k obrazu pachatele, již dnes „darknet“ disponuje softwarem, který umí změnit např. data na dokladu, bez jakéhokoliv zásahu člověka – ten pouze zadá parametry).

4.4.6 Okresní státní zástupce

1) Jaká je Vaše pracovní / služební pozice?

Odpověď: Státní zástupce.

2) Jak Vaše pracovní / služební pozice zasahuje do procesu odhalování a vyšetřování trestné činnosti páchané v kyberprostoru?

Odpověď: Dozor nad zákonností přípravného řízení, konzultace spisů, sepis obžaloby a zastupování státu v řízení před soudem.

3) Jak dlouho se věnujete problematice trestné činnosti páchané v kyberprostoru?

Odpověď: Zhruba rok a čtvrt.

4) Zhodnoťte z Vašeho pohledu vývojový trend trestné činnosti páchané v kyberprostoru?

Odpověď: Z mého pohledu je internet využíván primárně jako prostředek k páchání trestné činnosti v tom smyslu, že pachatelé prostřednictvím internetu a nástrojů phishingu, spear phishingu, romance scamu nebo reverzních inzertních podvodů apod. Pachatelé se tedy – alespoň podle mé zkušenosti – minimálně zaměřují na „hard core" internetovou kriminalitu ve smyslu hackingu, ransomware atd.

Co se týče trendu, ačkoli by se s ohledem na frekvenci varování ve sdělovacích prostředcích a jinde (prakticky všude) dalo předpokládat, že poškození budou pozornější, ale zatím to vypadá, že opak je pravdou a podíl kriminality páchané v kyberprostoru roste, a s ohledem na technologický vývoj lze předpokládat, že poroste (při poněkud odvážnějším pohledu do budoucna lze očekávat zneužití kyberprostoru k páchání sofistikovanější kriminality např. za pomoci tzv. rozšířené reality a umělé inteligence, které umožní pachatelům násobně masovější a cílenější útoky, popř. umožní nápodobou hlasů a podoby snadnější uvádění poškozených v omyl).

5) Které trestné činy jsou dle Vašich zkušeností nejčastěji páchané v souvislosti s kyberprostorem?

Odpověď: Zdaleka nejčastěji se v praxi setkávám s (řazeno od nejčastějších po nejméně časté)

- podvody dle § 209 tr. zákoníku,
- neoprávněným opatřením, padělám a pozměněním platebního prostředku dle § 234 tr. zákoníku,
- neoprávněným přístupem k počítačovému systému a neoprávněnému zásahu do počítačového systému nebo nosiče informací dle § 230 tr. zákoníku,
- porušením autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 tr. zákoníku
- porušením tajemství listin a jiných dokumentů uchovávaných v soukromí dle § 183 tr. zákoníku,
- sexuálním nátlakem dle § 186 tr. zákoníku.

6) Jaká je z Vašeho pohledu situace v Ústeckém kraji / okrese Most? Zhodnoťte skladbu trestné činnost páchané v kyberprostoru v Ústeckém kraji / okrese Most? Jaká je podle Vás zatíženost Ústeckého kraje / okresu Most?

Odpověď: Dle mých zkušeností dalece převažují první dva trestné činy uvedené v odpovědi na otázku č. 5, v poslední době se k nim přidává také třetí uvedený.

K zatíženosti nejsem schopen se vyjádřit, protože nemám data pro porovnání z ostatních okresů nebo krajů. Subjektivní dojem mám nicméně takový, že do značné míry kopíruje obecnou zatíženost zdejšího okresu kriminalitou a je tedy vyšší, než v okresech/krajích jiných.

7) Jaká jsou podle Vás v současné době největší úskalí při řešení dané problematiky? Jsou problematické oblasti legislativy a jurisdikce, odborné úrovně pracovníků zabývajících se danou problematikou nebo při odhalování a dokazování a zavedených postupech?

Odpověď: Domnívám se, že největším problémem je technologická (hardwarová i softwarová) vybavenost jak v rámci resortu Ministerstva vnitra, tak v rámci resortu Ministerstva spravedlnosti, zejm. absence dostatečných cloudových úložišť, technická

vybavenost např. Blue-ray mechanikami, softwarová nevybavenost nástroji na trasování kryptoměn, které by umožnily identifikovat kryptoměnové směnárny.

Do určité míry je problematická také zdlouhavost postupů při dožádání nezbytných informací od společností sídlících v zahraničí. Jednodušší je situace v rámci Evropské unie, ačkoli přístup, rychlost a ochota jednotlivých států se výrazně liší, mnohem složitější je situace mezinárodní spolupráce u mimounijních zemí, typicky s USA, kde však mají sídla největší technologické společnosti a jejichž data by mohla být největším přínosem. Doba, kterou si nicméně vyžádá vyřízení žádosti o mezinárodní právní pomoc, znemožňuje efektivní boj s trestnou činností v kyberprostoru, kde k ní dochází rychleji než kdekoli jinde.

Na okraj – často to totiž s trestnou činností v kyberprostoru souvisí, i když se jí to napřímo netýká. Problematickým vidím také přístup a spolupráci bank, zejména ohledně zajišťování finančních prostředků, které je třeba provést rychle a řádově v rámci desítek minut. To, že banky plošně přijímají datové zprávy pouze o půlnoci znamená prakticky nemožnost zajistit výnos z trestné činnosti na bankovním účtu v tentýž den, o víkendu nemluvě.

8) Co považujete za nedostačující v oblasti legislativy a jurisdikce?
Odpověď: Viz výše – zejména zdlouhavý postup s vyžádáním informací ze zahraničí.

Ve vnitrostátním právu pak v tom, že zejména trestní řád z roku 1961 nemůže z logiky věci koncepčně umožňovat efektivní boj s trestnou činností páchanou v kyberprostoru, nedává policejnímu orgánu ani státnímu zastupitelství dostatek nástrojů a jednotlivé zásahy, které vedou ke zlepšení legislativní připravenosti jsou spíše vynuceny mezinárodními nebo unijními závazky, než že by se jednalo o promyšlenou novelu, která by např. reagovala na existenci cloudových úložišť, legislativně zakotvila možnost předávání elektronických důkazů z ciziny, umožnila jejich provádění v řízení před soudy apod.

Jako zcela zásadní nedostatek např. vidím nedostatečné vyjasnění (ke kterému dochází až metodou pokus-omyl a judikaturou) v oblasti možnosti prolamování zabezpečení mobilních telefonů – zda je možné nutit obviněného k tomu, aby přitiskl prst na telefon, popř. na něj

jen telefon namířit, aby se odemkl, zda je možné se pokoušet prolomit zabezpečení mobilního telefonu technickými prostředky a jaké povolení/souhlasy jsou k tomu potřeba.

9) Co považujete za nedostačující v oblasti odborné úrovně pracovníků, kteří se zabývají danou problematikou?

Odpověď: Mohu usuzovat pouze ze svého pohledu – ocenil bych, kdybych mohl svou odbornou úroveň prohloubit zejména ohledně pochopení fungování přístupových bodů, VPN, proxy adres a možnostech, jaké v tomto ohledu v současné době jako resorty máme. Věc nesouvisející s odbornou úrovní, která by však, z mého pohledu, stála za větší pozornost, je pak tzv. OSINT, tedy open source intelligence, zjišťování informací o pachatelích, popř. jejich zázemí ze sociálních sítí a veřejně dostupných informací. To sice nesouvisí s kyberkriminalitou jako takovou, ale jedná se o informace dostupné na internetu, které by mohly být využity nejen při objasňování kriminality páchané mimo kyberprostor, ale také pro zjišťování informací o poměrech pachatelů.

10) Co považujete za nedostačující v oblasti odhalování, dokazování a zavedených postupech?

Odpověď: Zejména výše zmíněnou softwarovou výbavu pro trasování kryptoměn(ových směnáren).

Myslím, že by bylo dobré prohloubit spolupráci na ose policejní orgán – státní zastupitelství – poskytovatelé připojení k internetu, popř. správci domén. Z praxe kolegů ze zahraničí jsem zjistil, že není v rámci trestního řízení problém např. s vytvořením falešných webových stránek za účelem vylákání pachatele, popř. spolupráce s poskytovateli připojení k internetu v reálném čase ohledně zjištění informací zjistitelných z přístupových bodů připojení k internetu, což dopomohlo odhalit síť pachatelů organizované trestné činnosti.

Jako určitý nedostatek vnímám také to, že nedochází k pokusům za pomoci sociálního inženýrství (což je tedy hrozný překlad, social engineering) prolomit např. přístupové údaje k účtům vyšetřovaných/prověřovaných pachatelů (e-mailovým, na sociálních sítích apod.), byť třeba se souhlasem státního zástupce nebo soudce. Totéž platí pro vydané telefony bez přístupových údajů.

Do budoucna si také dokážu představit větší zaměření na „offline věci“ související s online problematikou, typicky domovní prohlídka a v rámci ní hledání seedu ke kryptoměnové peněžence apod.

11) Vidíte problémy v nějakých dalších oblastech?

Odpověď: Popsané výše – hlavně souvislost nedostatečného legislativního rámce pro prolamování zabezpečení mobilních telefonů a účtů obviněných.

12) Popište z Vašeho pohledu proces vyžadování informací od dotazovaných subjektů. Vidíte v tomto procesu nějaké slabiny?

Odpověď: Není mi úplně jasné, na jaké dotazované subjekty otázka míří. K zahraničním subjektům viz výše.

Vyžadování informací o proběhlém telekomunikačním provozu je podle mého zbytečně zatíženo nutností žádat o povolení soud, a to zejména s ohledem na jeho frekvenci. Chápu omezení a nutnost povolení soudu pro odposlech nebo sledování komunikace v reálném čase, ale domnívám se, že na proběhlá telekomunikační data (typicky provoz na IP adresách) by postačil příkaz/souhlas státního zástupce.

Z mého pohledu zajímavou, a ne úplně prošlapanou problematikou je vyžadování informací od obviněných, např. výše zmíněného hesla. Nevidím příkrý rozpor se zásadou zákazu nucení k sebeobviňování – sdělením přístupového kódu do telefonu nedochází k sebeobvinění, k tomu by došlo až vydáním důkazu, který je uvnitř… ale to je spíše teoretickou otázkou.

13) Jak hodnotíte lhůty, po které dožadované subjekty uchovávají potřebná data?

Odpověď: Domnívám se, že je dostatečná, ale je třeba od počátku vyjasnit, jaká data budou třeba. Ustanovení § 7b pak dává dostatečné záruky pro to, aby byla data uchována, i když nejsou přímo vyžádána, v praxi ale nevidím moc časté využití tohoto příkazu (alespoň v písemné formě).

14) Jak hodnotíte současnou úroveň prevence, preventivních opatření a osvěty problematiky trestné činnosti páchané v kyberprostoru? Zhodnoťte důležitost faktoru předcházení této trestné činnosti.

Odpověď: Z mého pohledu je prevence v případě kyberkriminality alfou a omegou. S ohledem na rychlost veškerých procesů v kyberprostoru je často nemožné výnos z trestného činu zachytit už v okamžiku, kdy poškozený věc přijde nahlásit.

Domnívám se, že osvěta je dostatečná, nejen ze strany policejního orgánu, ale také ze strany soukromých subjektů. Často ovšem nezbývá než pouze lakonicky poznamenat: „Komu není rady, tomu není pomoci". Někteří se poučí prostě až v okamžiku, kdy – nejčastěji o peníze – reálně přijdou.

Nezanedbatelnou preventivní funkci pak shledávám v tom, že budou před soud stavěny a odsuzovány osoby legalizátorů, ač původně taky poškozených. Dopad takových odsouzení na okolí snad bude do budoucna dostatečně odstrašující proto, aby si veřejnost dávala větší pozor.

15) Jaká máte doporučení v oblasti prevence a předcházení trestné činnosti páchané v kyberprostoru?

Odpověď: Viz odpověď na otázku 14.

16) Jaký očekáváte vývoj s problematikou a trestnou činností, která je páchaná v souvislosti s kyberprostorem?

Odpověď: Očekávám její nárůst, odkazuji na odpověď na otázku č. 4 ohledně trendu vývoje.

4.4.7 Sumarizace provedených rozhovorů

Provedený kvalitativní výzkum, odpovědi všech respondentů byly sumarizovány do tabulky č. 31.

Tabulka č. 31: Sumarizace odpovědí respondentů

číslo otázky	Vyhodnocení odpovědí respondentů					
	Analytik ÚSKPV	**ZVO OHK**	**Vyšetřovatelka OHK**	**Vedoucí krajské OKK**	**Vyšetřovatel krajské OKK**	**Okresní státní zástupce**
1	republiková úr.	okresní úr.	okresní úr.	krajská úr.	krajská úr.	státní zastupitelství
2	analýza	vedení	vyšetřování	vedení	vyšetřování	dozor
3	6 let	18 let	4 roky	7 let	7 let	2 roky
4	stoupající	stoupající	stoupající	stoupající	stoupající	stoupající
5	hospodářské a mravnostní	hospodářské	hospodářské	hospodářské a mravnostní	hospodářské	hospodářské a mravnostní
6	vysoká	zvýšená	průměrná	nižší	vyšší	vyšší
7	legislativa	legislativa	čas	odborná úroveň	mezinárodní legislativa	technologická vybavenost
8	mezinárodní spolupráce	zdlouhavé spolupráce	lhůty a pravomoce	vymahatelnost a lhůty odpovědí	mezinárodní spolupráce	zdlouhavé spolupráce
9	nedostatek odborných školení	nespecializace na danou problematiku	nedostatek odborných pracovníků	chybějící znalosti o možnostech a spolupráci	nezájem rozvíjet se	nedostatek odborných školení
10	legislativa	nejednotné postupy	nespecializace na danou problematiku	nejednotné postupy a vymahatelnost	odbornost pracovníků	softwarová výbava
11	ne	ne	platby do zahraničí	vzdělávání v problematice	personální stav	legislativní
12	efektivita a rychlost	spolupráce a vymahatelnost	efektivita	-	efektivita a rychlost	zbytečná zatíženost
13	velké rozdíly	přiměřené	nedostatečné	velké rozdíly	dostatečné	dostatečné
14	dostatečná	nedostatečná	dostatečná	dostatečná	nedostatečná	dostatečná
15	vyšší medializace	odborné kurzy	používat zdravý rozum	rozšíření	rozšíření	-
16	růst	růst	růst	růst	mírný pokles	růst

Zdroj: vlastní zpracování provedených rozhovorů

Soupis otázek:

1) Jaká je Vaše pracovní / služební pozice?

2) Jak Vaše pracovní / služební pozice zasahuje do procesu odhalování a vyšetřování trestné činnosti páchané v kyberprostoru?

3) Jak dlouho se věnujete problematice trestné činnosti páchané v kyberprostoru?

4) Zhodnoťte z Vašeho pohledu vývojový trend trestné činnosti páchané v kyberprostoru?

5) Které trestné činy jsou dle Vašich zkušeností nejčastěji páchané v souvislosti s kyberprostorem?

6) Jaká je z Vašeho pohledu situace v Ústeckém kraji / okrese Most? Zhodnoťte skladbu trestné činnost páchané v kyberprostoru v Ústeckém kraji / okrese Most? Jaká je podle Vás zatíženost Ústeckého kraje / okresu Most?

7) Jaká jsou podle Vás v současné době největší úskalí při řešení dané problematiky? Jsou problematické oblasti legislativy a jurisdikce, odborné úrovně pracovníků zabývajících se danou problematikou nebo při odhalování a dokazování a zavedených postupech?

8) Co považujete za nedostačující v oblasti legislativy a jurisdikce?

9) Co považujete za nedostačující v oblasti odborné úrovně pracovníků, kteří se zabývají danou problematikou?

10) Co považujete za nedostačující v oblasti odhalování, dokazování a zavedených postupech?

11) Vidíte problémy v nějakých dalších oblastech?

12) Popište z Vašeho pohledu proces vyžadování informací od dotazovaných subjektů. Vidíte v tomto procesu nějaké slabiny?

13) Jak hodnotíte lhůty, po které dožadované subjekty uchovávají potřebná data?

14) Jak hodnotíte současnou úroveň prevence, preventivních opatření a osvěty problematiky trestné činnosti páchané v kyberprostoru? Zhodnoťte důležitost faktoru předcházení této trestné činnosti.

15) Jaká máte doporučení v oblasti prevence a předcházení trestné činnosti páchané v kyberprostoru?

16) Jaký očekáváte vývoj s problematikou a trestnou činností, která je páchaná v souvislosti s kyberprostorem?

5 Výsledky a diskuse

Kvantitativním výzkumem, provedenou analýzou bylo zjištěno, že trend vývoje celkového počtu vybraných skutků v České republice se mezi lety 2011 až 2020 pohyboval v rozmezí od 14.901 (v roce 2020) do 19.511 (v roce 2013) registrovaných skutků, kdy celkové počty vybraných skutků jsou mírně kolísavé, dá se říct, že jsou na stejné úrovni, bez významného trendu růstu nebo poklesu. Naproti tomu vývojový trend podmnožiny skutků, které byly spáchané internetem a ostatními sítěmi (kyberkriminalita) od roku 2011 (960 skutků) do roku 2020 (5.298 skutků) vykazoval trvalý mírný nárůst, až na 5,5násobek počáteční hodnoty.

Analogickou statistickou analýzou dat Ústeckého kraje byl u celkového počtu vybraných skutků zjištěn klesající trend, kdy z počáteční hodnoty 1.469 skutků v roce 2011 a maxima o hodnotě 1.510 v roce 2013, byl v roce 2020 celkový počet spáchaných skutků pouze 917. Vývojový trend podmnožiny skutků kyberkriminality měl, stejně jako v případě celé České republiky, tendenci mírného růstu. Z počátečního počtu 87 spáchaných skutků v roce 2011 a 325 skutků v roce 2019, což bylo maximum zkoumaného období, bylo na konci zkoumaného období v roce 2020 evidováno 281 spáchaných skutků, což byl 3,2násobek počáteční hodnoty.

Ve druhém zkoumaném období, v letech 2021 až 2023 se celkový počet vybraných skutků v České republice dále zvyšoval, v roce 2021 bylo registrováno 16.667 skutků a v roce 2023 29.046 skutků, což v rozmezí tří let představuje 1,7násobný nárůst. Počet skutků spáchaných internetem a ostatními sítěmi vykázal také růst, když v roce 2021 bylo registrováno 6.678 skutků a v roce 2023 byl počet registrovaných skutků 16.100. Tento růst byl tedy 2,4násobný.

V Ústeckém kraji měl celkový počet vybraných registrovaných skutků, v období 2021 až 2023, také rostoucí tendenci. V roce 2021 bylo registrováno 1.117 skutků a v roce 2023 bylo registrováno 2.050 skutků, což činí 1,8násobný nárůst. Podmnožina kyberkriminality pro Ústecký kraj v roce 2021 registrovala 436 skutků a v roce 2023 registrovala 1.216 skutků, což byl téměř 2,8násobný nárůst.

Růstové trendy celkového počtu vybraných registrovaných skutků v druhém zkoumaném období vykazují prakticky stejné hodnoty, jak v České republice, tak i v Ústeckém kraji. Totéž můžeme říci i o tempu růstu podmnožiny kyberkriminality. Když ale porovnáme trendy růstu celkového počtu registrovaných skutků a růst podmnožiny kyberkriminality, tak vidíme, že počet skutků registrovaných jako kyberkriminalita roste rychleji než celkový počet.

Dalším provedeným zkoumáním poměrových tendencí podmnožiny kyberkriminality, jejího procentuálního podílu na celkovém počtu vybraných skutků, bylo zjištěno, že v rámci České republiky byl na začátku posuzovaného období v roce 2011 podíl podmnožiny kyberkriminality na celkovém počtu vybraných skutků pouze 5,5% a na jeho konci v roce 2020 již podíl kyberkriminality činil 35,55%.

Zpracováním dat pro Ústecký kraj byl pro rok 2011 vypočten poměr 5,92% skutků spáchaných internetem a ostatními sítěmi na celkovém počtu vybraných registrovaných skutků a v roce 2020 tento poměr činil 30,64%.

Oba zjištěné výsledky vykazují zhruba stejný trend stoupajícího vývoje.

Ve druhém zkoumaném období, pro celou Českou republiku, v roce 2021 již poměr kyberkriminality činil 40,07% a v roce 2023 to bylo 55,43%.

V Ústeckém kraji byl v roce 2021 poměr kyberkriminality 39,03% a v roce 2023 dokonce 59,32%.

I ve druhém zkoumaném období vykazuje Česká republika, i Ústecký kraji obdobný růstový trend.

Dalším předmětem zkoumání bylo porovnání objasněnosti skutků spáchaných internetem a ostatními sítěmi. Tímto zkoumáním bylo zjištěno, že v prvním zkoumaném období let 2011 až 2020, byl pro celou Českou republiku v prvních 6 letech (2011–2016) zjištěn růst počtu objasněných skutků, poté se počet objasněných skutků ustálil a se zrychleným

nárůstem počtu spáchaných skutků v letech 2019 a 2020 začal počet objasněných skutků mírně klesat.

Z dat pro Ústecký kraj byl zjištěn skokový nárůst počtu spáchaných i objasněných skutků v roce 2014 a následně u počtu spáchaných skutků došlo ke stagnaci a pouze mírnému kolísání jejich počtu a u počtu objasněných skutků ke stálému mírnému poklesu.

Procentuální hodnoty objasněnosti kybernetické kriminality pro Českou republiku i Ústecký kraj se na počátku prvního zkoumaného období v roce 2011 pohybovaly okolo 50% a na jeho konci v roce 2020 okolo 20%, přičemž měly zhruba stejný klesající trend.

Ve druhém zkoumaném období let 2021 až 2023, byl v České republice zaznamenán mírně rostoucí absolutní počet objasněných skutků, kdy v roce 2021 bylo objasněno 824 skutků a v roce 2023 bylo objasněno 1.017 skutků.

V Ústeckém kraji bylo ve stejném období v roce 2021 objasněno 64 skutků a v roce 2023 bylo objasněno 93 skutků.

Přepočet procentuální hodnoty objasněnosti pro Českou republiku v roce 2021 byl 12% a v roce 2023 byl 6%.

Obdobný klesající trend v tomto kritériu vykazuje i Ústecký kraj, který v roce 2021 dosáhl objasněnosti 15% a v roce 2023 byla objasněnost 8%.

Posledním předmětem zkoumání byl index kriminality, z jehož vypočtených výsledků lze konstatovat kolik obyvatel České republiky a Ústeckého kraje, v přepočtu na 100.000 obyvatel bylo kybernetickou kriminalitou postiženo.

Zatímco v prvním zkoumaném období, do roku 2015 vykazoval vyšší hodnoty indexu kriminality Ústecký kraj a byl tedy, co se týká kybernetické kriminality nebezpečnější a více jeho obyvatel bylo tímto druhem kriminality postiženo, tak v dalších letech začala vyšší hodnoty indexu kriminality vykazovat Česká republika. Z vypočteného indexu bylo

stanoveno, že v roce 2020 bylo ve zvoleném přepočtu kyberkriminalitou v České republice postiženo 49,54 obyvatelů a v Ústeckém kraji pouze 34,23 obyvatele.

V druhém zkoumaném období, pak v prvních dvou letech, 2021 a 2022, vykázala vyšší hodnoty indexu kriminality Česká republika, přičemž v roce 2023 byla pro Českou republiku vypočtena hodnota indexu 147,95 a pro Ústecký kraj to bylo 150,08, tedy v roce 2023 vykázal vyšší hodnotu kybernetické kriminality Ústecký kraj.

Z provedeného kvalitativního výzkumu je patrné, že všichni oslovení respondenti, napříč všemi organizačními úrovněmi se shodli, že vývojový trend trestné činnosti páchané v kyberprostoru má stoupající tendenci a také, že nejčastěji páchané trestné činy v souvislosti jsou ty hospodářské, přičemž polovina oslovených respondentů uváděla i trestné činy mravnostní. Co se týče současné situace zatíženosti Ústeckého kraje, potažmo okresu Most, tak se většina respondentů shodla na spíše vyšší zatíženosti.

Největší úskalí při řešení zkoumané problematiky byla určena v legislativní oblasti se zaměřením na mezinárodní spolupráci, její zdlouhavost a vymahatelnost a vymahatelnost odpovědí.

V oblasti odborné úrovně pracovníků zabývajících se zkoumanou problematikou byl identifikován nedostatek odborných školení, tím pádem chybějící znalosti určených pracovníků, což může být dáno nespecializováním se na danou problematiku a také nezájmem pracovníků o další odborný rozvoj.

Tato zjištění o nedostatečnosti legislativy, odbornosti pracovníků a zavedených postupech se pak promítají do odpovědí respondentů při identifikaci nedostatků při odhalování a dokazování zkoumané trestné činnosti.

Lhůty, po které se uchovávají data s vypovídající informační hodnotou, dotazovaní respondenti hodnotili spíše jako dostatečné, přičemž slabiny při vyžadování těchto informací byly určeny v jejich efektivitě a rychlosti.

Oblast prevence byla většinou dotazovaných hodnocena jako dostatečná, ale shoda panovala v jejím dalším rozšíření, vyšší medializaci a odborných kurzech cílených na ohrožené skupiny.

Většina dotazovaných respondentů v dané problematice a trestné činnosti v kyberprostoru očekává rostoucí vývoj.

6 Závěr

Hlavním cílem diplomové práce bylo stanovení skutků, které nejčastěji spadají do oblasti kybernetické kriminality a provedení jejich statistické analýzy, zaznamenat strukturu a vývoj vybrané části registrované kriminality v České republice a provedení jejího srovnání s Ústeckým krajem v letech 2011 až 2020 a 2021 až 2023.

Vedlejšími cíli bylo zkoumání poměrových tendencí a vývoje objasněnosti kybernetické kriminality a dále vypočtení indexu kybernetické kriminality pro Českou republiku a Ústecký kraj.

Bylo provedeno zkoumání v oblasti vybraných hospodářských a majetkových trestných činů, které z největší části zahrnují podmnožinu skutků, které jsou zařazovány do oblasti kyberkriminality, tzn. skutky spáchané internetem a ostatními sítěmi.

Provedená statistická analýza vycházela z dat Policejní statistky a z dat Českého statistického úřadu. Sesbíraná data byla matematicky zpracována a vypočtené výsledky vyhodnoceny. Dále bylo využito základních charakteristik časových řad, a to 1. diference a koeficientu růstu, kterými byly popsány meziroční změny.

Vybraná skupina zkoumaných registrovaných trestných činů, jak v České republice, tak i v Ústeckém kraji, má stoupající charakter. Přičemž z provedeného zkoumání bylo zjištěno, že příčinou nárůstu celkového počtu skutků je nárůst počtu skutků zařazených do podmnožiny kyberkriminality.

Práce byla rozdělena na dvě zkoumaná období z důvodu legislativní změny z konce roku 2020, kterou byla zvýšena hranice výše škody pro kvalifikaci trestného činu, kdy tato hranice byla zvýšena z 5.000,- Kč na 10.000,- Kč, tedy tato změna mohla přinést snížení počtu trestných činů, což provedeným zkoumáním nebylo potvrzeno. Jedním z důvodů tohoto vývoje je, že z vybraných zkoumaných trestných činů je výše škody obligatorním znakem pouze při kvalifikaci trestného činu podvodu a dále, že tempo růstu kybernetické kriminality je rychlejší než tempo růstu ostatní vybrané trestné činnosti.

Dále bylo zkoumáním zjištěno, že v absolutních číslech počet objasněných skutků nepatrně roste, přičemž procentuální vyjádření objasněnosti kybernetické kriminality rapidně klesá, což také ukazuje na vysoké tempo růstu této kriminality. Tato zjištění platí, jak pro Českou republiku, tak pro Ústecký kraj.

Uvedená zjištění evokují otázku, zdali je toto důsledek naplnění výkonové kapacity pracovníků zabývajících se tímto druhem kriminality.

Provedenými rozhovory byl potvrzen výběr trestných činů, které byly podrobeny bližšímu zkoumání z hlediska kybernetické kriminality. Dále se všichni dotazovaní shodli na rostoucí predikci vývojového trendu v budoucím období. Jako zásadní k řešení problematiky kyberkriminality určili nutnost zvyšování odbornosti interesovaných pracovníků, kteří se těmito skutky zabývají a provádění preventivních opatření, které by mohly zpomalit tempo nárůstu registrovaných skutků.

Na základě provedeného kvalitativního výzkumu lze pro zkoumanou problematiku jako klíčové určit oblasti legislativy, odborné úrovně a prevence a stanovit v nich doporučení.

V oblasti legislativy je jasné, že trestní řád z roku 1961 nemůže plně reflektovat současné potřeby postupů k tomuto zcela novému druhu trestné činnosti a je potřeba provedení jeho „celkové aktualizace“, ne pouze ve formě dílčích novelizací, které by odpovídalo aktuální situaci. Stejně tak zrychlení a zefektivnění mezinárodních spoluprací, zavedení jednotných postupů a možností při vyžadování klíčových informací a ukotvení vymahatelnosti a sankcí, při nedodržení takových postupů. Pro úspěšné řešení tohoto druhu kriminality je potřeba mít na paměti, že nemůže stačit pouze kvalitní tuzemská nebo evropská legislativní úprava, jelikož „kyberprostor nezná hranic“, bylo by, minimálně v základních oprávněních a postupech, potřeba zavést celosvětovou legislativní standardy a zajistit jejich vymahatelnost.

Z výsledků provedených rozhovorů také vyplynula potřeba odborného vzdělávání pracovníků zabývajících se zkoumanou problematikou v souvislosti s vývojem a novými možnostmi, které poskytuje moderní technika tak, aby tito pracovníci byli schopni držet krok

s aktuálními trendy. Vyšší odbornost pracovníků by mohla vést k jejich vyšší produktivitě, a tudíž vyššímu počtu objasněných skutků.

S oblastí odborné úrovně související by mohlo být zřízení specializovaných útvarů a oddělení napříč celou organizační strukturou, kde by byli zařazeni pracovníci se zájmem o tuto problematiku, a tím pádem také se zájmem o prohlubování svých odborných znalostí, které by poté mohly být adekvátně využity při objasňování dané trestné činnosti. K 1. 1. 2023 byla založena Národní centrála proti terorismu, extremismu a kybernetické kriminalitě, jedná se o útvar s celostátní působností. Na nižších úrovních řešení kybernetické kriminality zůstává mnohdy na základních článcích a útvarech.

Dalším důležitým prvkem majícím vliv na kybernetickou kriminalitu byla stanovena prevence. Někteří z respondentů ji považovali za adekvátní, další by ji prohloubili a začlenili ji jako součást vzdělání, ale všichni se shodli, že má zásadní vliv na možné snížení rostoucího vývojového trendu.

V oblasti prevence bude zapotřebí hlubší „osvěta“ u ohrožených skupin. Z praxe se většinou jedná o skupiny, které kyberprostor a jeho možné nástrahy teprve objevují. Může se jednat, jak o starší věkové kategorie, kterých se dotýkají spíše hospodářské a majetkové delikty, tak o mladší kategorie, na které je cílena trestná činnost spíše mravnostního charakteru. Tím ale nechci v žádném případě tyto dvě skupiny nikterak stigmatizovat. Kybernetickou kriminalitou jsou postiženy všechny věkové kategorie, i lidé v produktivním věku, napříč všemi úrovněmi vzdělání, proto bude zapotřebí i rozšíření obecné medializace, aby lidé více přemýšleli a „používali zdravý rozum“.

Informovanost nejvíce ohrožených skupin může být rozšířena zařazením edukativních pořadů a reportáží do veřejnoprávních médií a denního tisku, což by cílilo na střední a starší generaci, přičemž nejstarší generace může být oslovena i přednáškami a besedami v domovech důchodců a klubech seniorů. Základy kybenetické bezpečnosti mohou být vyučovány jak na univerzitách 3. věku, tak na základních školách. Na mladší generace poté zacílit skrze přednášky a besedy na školách anebo prostřednictvím sociálních sítí.

7 Seznam použitých zdrojů

ARLT, Josef; ARLTOVÁ, Markéta a RUBLÍKOVÁ, Eva. Analýza ekonomických časových řad s příklady. Praha: Vysoká škola ekonomická, 2002. ISBN 80-245-0307-7.

HENDL, Jan. Kvalitativní výzkum: základní teorie, metody a aplikace. Čtvrté, přepracované a rozšířené vydání. Praha: Portál, 2016. ISBN 978-80-262-0982-9.

HINDLS, Richard. Statistika pro ekonomy. 8. vyd. Praha: Professional Publishing, 2007. ISBN 978-80—86946-43-6.

KOLOUCH, Jan. CyberCrime. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7.

KONRÁD, Zdeněk; PORADA, Viktor; STRAUS, Jiří a SUCHÁNEK, Jaroslav. Kriminalistika: kriminalistická taktika a metodiky vyšetřování. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. ISBN 978-80-7380-547-0.

PUŽMANOVÁ, Rita. TCP/IP v kostce. 2., upr. a rozš. vyd. České Budějovice: Kopp, 2009. ISBN 978-80-7232-388-3.

SEDLÁK, Petr a KONEČNÝ, Martin. Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

SMEJKAL, Vladimír. Kybernetická kriminalita. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. ISBN 978-80-7380-849-5.

STREBE, Matthew a Charles PERKINS. Firewally a proxy-servery: praktický průvodce. Brno: Computer Press, 2003. ISBN 80-7226-983-6.

VÁLKOVÁ, Helena a KUCHTA, Josef. Základy kriminologie a trestní politiky. 2. vyd. Beckovy mezioborové učebnice. V Praze: C.H. Beck, 2012. ISBN 978-80-7400-429-2.

Legislativní dokumenty

Pokyn policejního prezidenta č. 103/2013, o plnění některých úkolů policejních orgánů Policie České republiky v trestním řízení.

Internetové zdroje

Kriminalita v ČR a EU [Web]. 2023 [cit. 2024-03-31]. ISSN 080009-23. Dostupné z: https://www.czso.cz/csu/czso/kriminalita-v-cr-a-eu-2012-2022.

Overcoming the Barriers to Micro-segmentation. Online. In: Network and Security Virtualization. 2019. Dostupné z: https://blogs.vmware.com/networkvirtualization/2019/10/overcoming-barriers-to-micro-segmentation.html/. [cit. 2024-03-31].

8 Seznam obrázků, tabulek, grafů a zkratek

8.1 Seznam obrázků

Obrázek č. 1: Základní pilíře kybernetické hygieny 23
Obrázek č. 2: Schéma Phishingu 26
Obrázek č. 3: Mail s viditelným odkazem a reálným skrytým odkazem 27
Obrázek č. 4: Topovaný odkaz s podvodnou reálnou adresou 28
Obrázek č. 5: SMS konverzace s podvodným odkazem 30

8.2 Seznam tabulek

Tabulka č. 1: Počty vybraných registrovaných skutků v ČR 38
Tabulka č. 2: Indexní analýza z celkového počtu registrovaných skutků v ČR 39
Tabulka č. 3: Počty skutků spáchaných internetem a ost. sítěmi v ČR 39
Tabulka č. 4: Indexní analýza skutků spáchaných int. a ost. sítěmi v ČR 40
Tabulka č. 5: Počty vybraných registrovaných skutků v ULK 41
Tabulka č. 6: Indexní analýza registrovaných skutků v ULK 41
Tabulka č. 7: Počty skutků spáchaných internetem a ost. sítěmi v ULK 42
Tabulka č. 8: Indexní analýza skutků spáchaných int. a ost. sítěmi v ULK 42
Tabulka č. 9: Počty objasněných skutků, které byly spáchány internetem v ČR 47
Tabulka č. 10: Indexní analýza objasněných kyber skutků v ČR 47
Tabulka č. 11: Počty objasněných skutků, které byly spáchány internetem v ULK 49
Tabulka č. 12: Indexní analýza objasněných kyber skutků v ULK 49
Tabulka č. 13: Objasněnost v ČR 50
Tabulka č. 14: Objasněnost v ULK 51
Tabulka č. 15: Počet obyvatel a Index kriminality v ČR a ULK 52
Tabulka č. 16: Počty vybraných registrovaných skutků v ČR 54
Tabulka č. 17: Indexní analýza registrovaných skutků v ČR 55
Tabulka č. 18: Počty skutků spáchaných internetem a ostatními sítěmi v ČR 55
Tabulka č. 19: Indexní analýza skutků spáchaných int. a ost. sítěmi v ČR 55
Tabulka č. 20: Počty vybraných registrovaných skutků v ULK 56
Tabulka č. 21: Indexní analýza registrovaných skutků v ULK 57
Tabulka č. 22: Počty skutků spáchaných internetem a ostatními sítěmi v ULK 57

Tabulka č. 23: Indexní analýza skutků spáchaných int. a ost. sítěmi v ULK 57
Tabulka č. 24: Počty objasněných skutků, které byly spáchány internetem v ČR 61
Tabulka č. 25: Indexní analýza objasněných kyber skutků v ČR 61
Tabulka č. 26: Počty objasněných skutků, které byly spáchány internetem v ULK 62
Tabulka č. 27: Indexní analýza objasněných kyber skutků v ULK 63
Tabulka č. 28: Objasněnost v ČR 64
Tabulka č. 29: Objasněnost v ULK 64
Tabulka č. 30: Počet obyvatel a Index kybernetické kriminality v ČR a ULK 65
Tabulka č. 31: Sumarizace odpovědí respondentů 92

8.3 Seznam grafů

Graf č. 1: Vývojový trend počtů vybraných skutků v ČR 40
Graf č. 2: Vývojový trend počtů vybraných skutků v ULK 43
Graf č. 3: Poměrový trend počtů skutků v ČR v % 44
Graf č. 4: Poměrový trend počtů skutků v ULK v % 45
Graf č. 5: Porovnání % poměrových tendencí v ČR a ULK 46
Graf č. 6: Počet spáchaných a objasněných skutků v ČR 48
Graf č. 7: Počet spáchaných a objasněných skutků v ULK 50
Graf č. 8: Porovnání procentuální objasněnosti ČR a ULK 51
Graf č. 9: Porovnání indexů kybernetické kriminality ČR a ULK 53
Graf č. 10: Vývojový trend počtů skutků v České republice 56
Graf č. 11: Vývojový trend počtů skutků v ULK 58
Graf č. 12: Poměrový trend počtů skutků v ČR v % 59
Graf č. 13: Poměrový trend počtů skutků v ULK v % 60
Graf č. 14: Porovnání poměrových tendencí v ČR a ULK 60
Graf č. 15: Počet spáchaných a objasněných skutků v ČR 62
Graf č. 16: Počet spáchaných a objasněných skutků v ULK 63
Graf č. 17: Porovnání procentuální objasněnosti ČR a ULK 64
Graf č. 18: Porovnání indexů kybernetické kriminality ČR a ULK 65