Vysoká škola evropských a regionálních studií, z. ú.,
České Budějovice

Bakalářská práce

Počítačová kriminalita jako nový prvek trestné činnosti

Autor práce: Petr Maloň, DiS.
Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Vedoucí práce: RNDr. Růžena Ferebauerová
Katedra: Katedra právních oborů a bezpečnostních studií

2022

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 6, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Petr Maloň, DiS.

Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Počítačová kriminalita jako nový prvek trestné činnosti

Název bakalářské práce v anglickém jazyce: Computer crime as a new element of crime

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, titul): RNDr. Růžena Ferebauerová

Datum zadání bakalářské práce (měsíc, rok): říjen 2021

Cíl bakalářské práce:
Cílem bakalářské práce je teoretické i praktické vymezení problematiky počítačové kriminality, která je velmi rozsáhlá a zahrnuje několik oblastí. Teoretická část práce bude obsahovat popis klíčových prvků kybernetické kriminality. Praktická část bude zpracovaná díky kvantitativně vědecko-výzkumným metodám, kde bude na základě dotazníkového šetření vytvořena analýza situace bankovní počítačové kriminality. V dotazníkovém šetření se zaměříme na praktické zkušenosti oslovených respondentů s kybernetickou kriminalitou v procesu užívání elektronických bankovních nástrojů v prostředí bankovních internetových operací. Součástí praktické části bude také návrh opatření pro zamezení nebo snížení výskytu počítačové kriminality v bankovních operacích.

Student: Petr Maloň, DiS.	5.11.2021 *datum*	*podpis*
Vedoucí práce: RNDr. Růžena Ferebauerová	8.11.2021 *datum*	*podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	6.12.2021 *datum*	*podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	8.12.2021 *datum*	*podpis*
Pověřený rektor: doc. Ing. Jiří Dušek, Ph.D.	14.12.2021 *datum*	*podpis*

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucího a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů

……

Tímto bych chtěl poděkovat vedoucí práce RNDr. Růženě Ferebauerové za pomoc při vyhledávání zdrojů informací, doporučením vhodné literatury a za poskytnuté rady a metodické vedení po celou dobu realizace bakalářské práce. Dále bych chtěl poděkovat svému kamarádovi PhDr. Mgr. Dušanovi Kaláškovi, za odborné konzultace a v neposlední řadě také děkuji své rodině za podporu při mém studiu.

ABSTRAKT

MALOŇ, P. *Počítačová kriminalita jako nový prvek trestné činnosti: bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, The College of European and Regional Studies, 2022. 91 s. Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová

Klíčová slova: Kyberprostor, počítačová kriminalita, kriminalita s platebními kartami, automatizace, internet věcí, cloud a cloudová řešení

Tato bakalářská práce se zaměřuje na velmi aktuální oblast trestné činnosti, která souvisí s rapidním nárůstem vlivu informačních technologií do života většiny občanů a přesahuje hranice států, tedy týká se doslova celosvětové problematiky počítačové kriminality v kyberprostoru. Jedním z mnoha projevů této počítačové kriminality je bankovní počítačová kriminalita, které je věnována nejpodstatnější část této práce. V uceleném kontextu jsou zde rozebrány klíčové prvky, jakými jsou phishing, viry a specifická kriminalita s platebními kartami. Nedílnou součástí této práce je shrnutí stavu počítačové kriminality z hlediska historického vývoje, současné situace a predikce do budoucna, kde je možné předpokládat velmi expanzivní vývoj počítačové kriminality v souvislosti s cloudy a cloudovými řešeními, botizací a automatizací a s fenoménem internetu věcí.

V praktické části této práce je zpracována analýza situace bankovní počítačové kriminality na základě vyhodnoceného dotazníkového šetření od oslovených respondentů. Součástí praktické části je také návrh opatření pro zamezení nebo snížení výskytu počítačové kriminality v bankovních operacích.

ABSTRACT

MALOŇ, P. *Computer Crime as a New Element of Crime: Bachelor Thesis.* České Budějovice: Vysoká škola evropských a regionálních studií, The College of European and Regional Studies, 2022. 91 s. Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová

Keywords: Cyberspace, cybercrime, credit card crime, automation, the Internet of Things, cloud and cloud solutions

This bachelor thesis focuses on a very topical area of crime, which is related to the rapid increase in the influence of information technology in the lives of most citizens and transcends national borders, i.e. it concerns literally the global issue of cybercrime in cyberspace. One of the many manifestations of this cybercrime is banking cybercrime, to which the most substantial part of this thesis is devoted. Key elements such as phishing, viruses and specific credit card crime are discussed in a comprehensive context. An integral part of this work is a summary of the state of cybercrime in terms of historical development, the current situation and predictions for the future, where a very expansive development of cybercrime can be expected in connection with clouds and cloud solutions, botisation and automation and the phenomenon of the Internet of Things.

In the practical part of this thesis, an analysis of the situation of banking cybercrime is prepared based on an evaluated questionnaire survey among the respondents. The practical part also includes the proposal of measures to prevent or reduce the occurrence of cybercrime in banking operations.

OBSAH

ÚVOD

V současné postmoderní společnosti, která je charakterizovaná mnoha změnami ve vývoji celého lidstva, se jako marginální a nový prvek jeví vznik a nárůst nových technologií a s tím související nutnost vzniku nejenom vědních, ale i společenských oborů, které se touto oblastí zabývají, studují ji nebo aplikují přímo v praxi.

Tyto technologie vychází z nutnosti reagovat na náročnější lidské potřeby a zasahují doslova do každodenního života. Nejde jenom o průmyslové technologie, které se využívají jak v těžkém průmyslu báňském a hutním, tak v lehkém průmyslu, ale také ve strojírenství, stavebnictví, automobilovém průmyslu a v neposlední řadě zasahují i do oblasti služeb, obchodu a dopravy. V souvislosti s narůstajícími požadavky na zvyšování produkce, výkonu, efektivity a zároveň snižování nákladů a časového hlediska nutného na zkrácení doby výroby, činnosti nebo dopravy z místa A do místa B, a to co nejrychleji, došlo k přirozené reakci společnosti na tuto novou situaci a vznikla nová technologická potřeba, která vychází především z podstaty organizování a zjednodušení tohoto překotného vývoje a pomocí informací co nejvíce usnadnit a naplnit všechny tyto společenské potřeby.

Z historického hlediska k této změně ve společnosti došlo v období průmyslové revoluce a s nárůstem nových vědních disciplín, které přinášely nové, v mnoha ohledech převratné objevy a do dnešního dne je stále generují, došlo také v dějinách lidstva k rapidnímu nárůstu informací. V takové situaci není vůbec překvapivé, že každých 10 roků vývoje společnosti představuje minimálně dvojnásobný nárůst počtu nových informací, které je nutné ukládat, analyzovat, zpracovávat, archivovat a především využívat v praxi. Není proto ani překvapivé, že s nárůstem informací a technologií vznikl zcela nový vědní, a dnes už můžeme doslova říci, multioborový prvek, který nazýváme obecně pojmem „Informační a komunikační technologie“ - zkráceně ICT.

S průběhem zavádění všech procesů souvisejících se vznikem oboru informačních technologií bylo obrovské nadšení a snaha zjednodušit lidský život a zpočátku se výhody informačních technologií zdály být pouze a výhradně ku prospěchu lidstva v souladu s původními cíli. Postupem času se ovšem, jak to ostatně bývá skoro u každého lidského počinu, začaly objevovat také stinné stránky problematiky informačních technologií, což mělo za následek první snahy o zneužití, jinak velmi prospěšné technologie, a můžeme hovořit o nejprve náhodných kriminálních skutcích a později také o organizovaném

zločinu zaměřeném na počítačovou technologii, potažmo na zneužití informační technologie v globálu.

1 CÍL A METODIKA BAKALÁŘSKÉ PRÁCE

Tato práce se zabývá problematikou počítačové, někdy také uváděno pod pojmem kybernetické, kriminality a zaměřuje se především na velmi diskutovanou oblast zneužívání informačních technologií ve finančním a bankovním sektoru k páchání trestné činnosti.

Cílem této bakalářské práce je teoretické i praktické vymezení oblasti počítačové kriminality, která je velmi rozsáhlá a zahrnuje několik oblastí. Práce má za úkol vytvořit ucelený přehled o problematice počítačové kriminality, který může nejenom odborníkům, ale především laické veřejnosti posloužit jako odrazový můstek v orientování se v této problematice.

Teoretická část práce obsahuje popis klíčových prvků kybernetické kriminality, která byla zpracovaná **kompilační metodou** z odborných zdrojů. Praktická část je pak zpracovaná dle kvantitativně vědecko-výzkumných metod, kde je na základě dotazníkového šetření vytvořena analýza situace bankovní počítačové kriminality. V dotazníkovém šetření se práce zaměřuje na praktické zkušenosti oslovených respondentů s kybernetickou kriminalitou v procesu užívání elektronických bankovních nástrojů v prostředí bankovních internetových operací. Součástí praktické části je také návrh opatření pro zamezení nebo snížení výskytu počítačové kriminality v bankovních operacích.

Samotné použité metody této práce vychází z pravidel **kvantitativních vědecko-výzkumných metod**, které se jeví pro zpracování této práce jako nejvýhodnější alternativa. K průzkumu mezi respondenty byla použita **metoda anonymního dotazníkového šetření a sběru dat** od dotazovaných respondentů. Následná analýza těchto údajů a vyhodnocení dat bylo provedeno pomocí **univariační analýzy**, která ze získaných údajů vytváří ucelený statistický výsledek hodnot dané oblasti, a na to navazující interpretace dílčích a celkových závěrů.

2 POČÍTAČOVÁ KRIMINALITA A JEJÍ OBECNÁ ROVINA

Společně s narůstajícím vlivem elektronických technologií se za několik předcházejících desetiletí projevily nejenom nesporné přínosy, ale také rizika a negativní dopady tohoto technologického nástroje ve společnosti a bylo pouze otázkou času, kdy se tyto negativní prvky projeví ve formě kriminální činnosti.

Počítačovou kriminalitu v obecné rovině popsal ve své publikaci Musil, který ji definuje jako každý nekalý čin spáchaný pomocí počítače.[1]

Vznik a rozšíření tohoto sociálně patologického jevu vyústilo až v potřebu vytvoření specializovaného odvětví, které se zabývá počítačovou kriminalitou ve všech formách a podobách, od individuálních trestných činů pachatelů až po organizovaný celek, který v trestné činnosti počítačové kriminality dokáže napáchat nedozírné ekonomické a společenské následky. Je velmi důležité si uvědomit, jak uvádí kolektiv autorů, Válková a Kuchta, že vzniká a vyvíjí se zcela specifická a doposud neznámá skupina pachatelů trestné činnosti, která má zcela specifické rysy.[2]

Aby společnost dokázala zákonným a legálním způsobem s touto skupinou zločinců bojovat, je nepochybně nutné studovat tuto problematiku počítačové trestné činnosti a vytvářet taková protiopatření, která co nejvíce zamezí počítačové kriminalitě. Obecná hlediska ve formě teoretických poznatků lze pak úspěšně zavádět do praxe a mezi první kroky tohoto procesu patří bezesporu pochopení terminologie, historického vývoje a současných a budoucích trendů.

2.1 Elementární názvosloví počítačové kriminality

Nevýhodou boje s počítačovou kriminalitou je skutečnost, že jde o boj na otevřeném poli informací, nikoliv v doposud běžném prostředí kriminálních zločinů, kde je pachatel doslova „hmatatelný a uchopitelný“. Díky trestné činnosti s informacemi a technologiemi je zapotřebí unifikovat především pojmosloví a terminologii, aby byla

[1]MUSIL, S. *Počítačová kriminalita: nástin problematiky: kompendium názorů specialistů.* 1. vydání. Praha: Institut pro kriminologii a sociální prevenci, 2000, s. 6.
[2]VÁLKOVÁ, H., KUCHTA, J., HULMÁKOVÁ, J. *Základy kriminologie a trestní politiky*. 3. vydání. V Praze: C.H. Beck, 2019, s. 602.

srozumitelná a dokázala všem složkám v boji s počítačovou kriminalitou přinést jednotnost myšlenek a činů.

Z kapacitních důvodů této práce je věnován prostor pouze několika základním pojmům, které hrají stěžejní roli v problematice počítačové kriminality. Vyčerpávajícím seznamem relevantních pojmů se zabýval kolektiv autorů Výkladového slovníku kybernetické bezpečnosti, který byl vydán jak v tištěné, tak v elektronické podobě, pod patronací Národního bezpečnostního úřadu a Národního centra kybernetické bezpečnosti, kde je možné na webových stránkách nalézt online verzi tohoto slovníku.[3]

Počítačový systém

Autoři komentáře k trestnímu zákoníku, Gřivna, Šámal a kolektiv, uvádí, že jde o jakékoli zařízení nebo skupinu navzájem propojených, případně spolu souvisejících zařízení, přičemž alespoň jedno z nich provádí zpracování dat na základě programu automaticky.[4]

Samotný zákon č. 40/2009 Sb., Trestní zákoník, pojem „počítačový systém“ užívá např. v § 182, 230, 231 a 232, ovšem nedefinuje pro účely právní a kriminologické význam tohoto termínu a tím může zkomplikovat pojetí významu tohoto klíčového slova v oblasti počítačové kriminality.

Gřivna naopak specifikuje pojem počítačový systém jako zařízení, které se skládá z technického, tedy hardwarového, programového a softwarového vybavení a slouží k automatickému zpracování digitálních dat.[5]

Podle těchto autorů je pak nutné rozlišovat pojem počítač a počítačový systém. Rozdíl mezi těmito pojmy je v tom, že počítačový systém je rozšířený o síťová zařízení, která ovšem nesplňují parametry počítače.[6]

Oproti tomu Kolouch pod pojmem počítačový systém zahrnuje i samostatná zařízení včetně bankomatu, chytrého mobilu nebo laptopu, včetně možnosti propojení ve vzájemných vazbách, které tvoří počítačovou síť. V tomto duchu pak do této kategorie zařízení a počítačového systému řadí také televizory, ostatní domácí spotřebiče nebo

3 JIRÁSEK, P.; NOVÁK, L.; POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti*: Cyber security glossary. 3. aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2015.
4 GŘIVNA, T. § 230 Neoprávněný přístup k počítačovému systému a nosiči informací. In: ŠÁMAL, P. a kol. *Trestní zákoník II: komentář*. § 140-421. 2. vyd. V Praze: C.H. Beck, 2012, s. 2306.
5 GŘIVNA, T. In: ŠÁMAL, P. a kol. *Trestní zákoník II: komentář*, 2012, op. cit, s. 2306.
6 GŘIVNA, T. § 230 Neoprávněný přístup k počítačovému systému a nosiči informací. In: ŠÁMAL, P. a kol. *Trestní zákoník II: komentář*. § 140-421. 2. vyd. V Praze: C.H. Beck, 2012, s. 2306.

chytré prvky v automobilech, které svojí schopností spouštět aplikace a připojením k internetu vykazují možnosti počítačových systémů.[7]

Internet

Významem internetu se zabývá Smejkal ve své práci s názvem Kybernetická kriminalita a připodobňuje zde internet k vynálezu knihtisku a parního stroje.[8]

Jak uvádí Britz, období, kdy americká vláda podporovala vývoj nových komunikačních systémů pod vlivem hrozby jaderné války, lze považovat za historické období spojené s prvními přípravami na propojený komunikační nástroj, který by v probíhající studené válce mohl nahradit případnou ztrátu klasických komunikačních kanálů. V tomto úseku historie informačních technologií můžeme hovořit o počátcích vzniku internetu.[9]

Pojem internet má několik významových rovin.

Z hlediska technologické roviny jde o počítačovou síť, případně celek sestavený ze vzájemně propojených menších počítačových sítí, uvnitř kterého dochází ke komunikaci, předávání informací a dat, a kde jsou pomocí tzv. TCP/IP protokolů poskytovány mezi jednotlivými prvky sítě různé, specifické služby informačně technologického charakteru.

Věcnou rovinu významu pojmu Internet popisuje Válková a kolektiv jako služby, které internet umožňuje a poskytuje a mezi něž patří například World Wide Web.[10]

Právní a majetkovou rovinou je fakt, že internet jako takový nemá žádného vlastníka, ale jednotlivé dílčí prvky internetu své vlastníky mají a díky existenci těchto dílčích prvků vzniká internet především vzájemnou propojeností a interakcí.

Kyberprostor

Kybernetičtí odborníci Kremling a Parker považují Williama F. Gibsona za autora pojmu „cyberspace“, což v přímém překladu do českého jazyka znamená „kyberprostor“. Tento autor vědecko-fantastických knih a románů, definoval počítačový prostor pro

7 KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016, s. 58.

8 SMEJKAL, V. *Kybernetická kriminalita.* 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, s. 57.

9 BRITZ, M. *Computer forensics and cyber crime: an introduction*. 3. vyd. Boston: Pearson, 2013, s. 39.

10 VÁLKOVÁ, H.; KUCHTA, J., HULMÁKOVÁ, J. *Základy kriminologie a trestní politiky*. 3. vydání. Praha: C.H. Beck, 2019, s. 533.

sdílení virtuálních dat už v roce 1982 a následně ve svém románu Neuromancer, vydaném v roce 1984, už standardně používá pojem kyberprostor. Gibson spojuje kyberprostor do kontextu se systémem virtuální reality, ve které mohou mezi sebou uživatelé počítačových sítí celosvětově kooperovat a podílet se na přenosu informací.[11]

Dle Douchy se o rozsáhlejší zavedení pojmu kyberprostor do obecného povědomí odbornosti a laické veřejnosti zasloužila v roce 1996 nezisková organizace Electronic Frontier Foundation, která hájí občanské svobody v kyberprostoru a tato práva a povinnosti uživatelů kybernetického prostoru oficiálně uveřejnila ve své Deklaraci nezávislosti kyberprostoru.[12]

V české legislativě si pojem kyberprostor našel také svoje místo a to především v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti, kde v ustanovení § 2, písm. a) definuje kyberprostor jako *„digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací“*.

Václavík k pojmu kyberprostor ještě dodává jeho rozložení na tři části, přičemž první část je viditelná, pod obecným označením Surface Web a zahrnující cca. 4 % kyberprostoru, druhá a třetí část je tzv. pod hladinou, nazývají se Deep a Dark Weby – souhrnně DarkNets a tvoří 96 % kyberprostoru, tedy zbývající podíl.[13]

Kybernetický útok

Zajímavým faktem u snahy definovat tento pojem je skutečnost, že i přes existenci velkého množství definic pojmu kybernetický útok, nemá žádná z nich obecně právní podobu.

Kolouch tento pojem definuje ve své práci Cyber Crime jako *„jakékoli protiprávní jednání útočníka v kyberprostoru, které* směruje *proti zájmům jiné osoby“* a dodává k tomuto, že kybernetický trestný čin bude vždy kybernetickým útokem.[14]

[11] KREMLING, J.; SHARP-PARKER, A. M. *Cyberspace, cybersecurity, and cybercrime*. Thousand Oaks: SAGE Publications, 2017, s. 12-13.
[12] DOUCHA, M. *Deklarace nezávislosti Kyberprostoru* [online]. Pirátskélisty.cz, publ. 20. 2. 2016 [cit. 2021-10-13]. Dostupné z WWW: <https://www.piratskelisty.cz/clanek-1476-deklarace-nezavislosti-kyberprostoru>.
[13] VÁCLAVÍK, L. *Většina internetu je skrytá. Co jsou to deep a dark web?* CNEWS.cz [online]. publ. 8. 10. 2018 [cit. 2021-10-14]. Dostupné z WWW: < https://www.cnews.cz/co-je-to-deep-invisible-hluboky-dark-temny-web>.
[14]KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016, s. 55.

Kybernetická kriminalita

Povaha definice pojmu kybernetická kriminalita je v současnosti velmi zkomplikována různorodostí a existencí velkého množství synonym, které popisují stejnou oblast a jsou často používána ve stejném kontextu pod různými názvy jako například: internetová kriminalita, počítačová kriminalita, informační kriminalita aj. Na tuto skutečnost upozorňuje Jirovský a dodává, že fakt nejednotnosti v definování tohoto pojmu způsobuje základní neshody v legislativní formě této problematiky.[15]

Obdobný zmatek v definici přináší také jeden z nejvýznamnějších právních aktů v této problematice, kterým je Úmluva Rady Evropy č. 185 o kybernetické kriminalitě ze dne 23. listopadu 2001.[16]

I když původní znění Úmluvy obsahuje pojem „Cybercrime“, což je v českém překladu kybernetická kriminalita, oficiální překlad Úmluvy uvádí pojem „počítačová kriminalita“.

Z výše uvedeného vyplývá, že překlad kybernetická, ve volném pojetí je možné uvádět také počítačová kriminalita, a pro účely této práce se budeme držet popisu podle překladu z této Úmluvy Rady Evropy.

Specialista na právo informačních technologií, Polčák, se snaží vymezit rozdíly v pojmosloví a popisuje, že v současné době už není tento druh kriminality zaměřen výhradně na počítač nebo více propojených počítačů, ale jde o soubor trestné činnosti v kyberprostoru a jako taková obsahuje například trestné činy proti počítačovým systémům nebo datům, podvody a padělaní související s počítači, trestné činy spočívající v šíření závadného obsahu či trestné činy směřující proti ochraně osobních údajů.[17]

Policie ČR definuje kybernetickou kriminalitu jako trestnou činnost, *„páchanou v prostředí informačních a komunikačních technologií včetně počítačových sítí. Samotná oblast informačních a komunikačních technologií je buď předmětem útoku, nebo je*

[15] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, s. 25.
[16] *Úmluva Rady Evropy č. 185 o kybernetické kriminalitě ze dne 23. listopadu 2001*. In: Council of Europe [Treaty Office]. Official website of the Treaty Office [cit. 2021-10-16]. Dostupné z WWW: <https://www.coe.int/en/web/conventions/>.
[17] POLČÁK, R. a kol. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 541.

páchána trestná činnost za výrazného využití informačních a komunikačních technologií jakožto významného prostředku k jejímu páchaní.“[18]

2.2 Historický vývoj počítačové kriminality

Díky pokroku v technologiích, především v posledních několika desetiletích došlo k nebývalému rozšíření těchto technologických přístrojů do každodenního života lidí a do všech odvětví lidských činností.

Ve snaze po uceleném přehledu historických milníků trestné činnosti a počítačové kriminality se uvádí, že počátky počítačové kriminality lze nalézat v zavádění automatizovaných procesů ve výrobě, v porušování pravidel a právních předpisů v telekomunikaci a také v projevech softwarového pirátství.

McQuade jde v pátrání po počátcích projevů počítačové kriminality mnohem hlouběji do historie a jako první náznaky praktického zneužití počítače uvádí příklad z roku 1932, kdy se polskému matematikovi Marianu Rejewskemu podařilo prolomit ochranu šifrovacího stroje Enigma. Dalším příkladem, tentokrát už i organizované činnosti, je podle McQuada vznik skupiny studentů z americké Massachusetts Institute of Technology (MIT) v období padesátých roků minulého století, která se zaměřila na překonávání bezpečnostních překážek informačních systémů a tuto činnost provozovala za účelem zábavy.[19]

Podle Britze však masovému nárůstu počítačové kriminality v 80. a 90 letech minulého století předcházelo období 60. a 70. let, kdy byl umožněn rozvoj nejprve počítačů pro vědecké účely, obchodní a výrobní organizace, a následně vzestup prodeje osobních počítačů a tím také rozvoj počítačové gramotnosti koncových uživatelů. V 90. letech minulého století, konkrétně v roce 1989 došlo k zásadnímu zlomu ve vývoji informačních technologií, který nastartoval také zvýšenou aktivitu trestné činnosti v počítačové kriminalitě. Tim Berners-Lee, fyzik z CERNu – Evropská organizace pro jaderný výzkum, v roce 1989 použil pro sdílení informací síťový protokol HTTP – hypertext transfer protokol, čímž umožnil od roku 1993 globální propojení sítě a první

[18] *Kyberkriminalita*. Policie ČR [online]. © 2020 Policie ČR [cit. 2021-10-20]. Dostupné z WWW: <https://www.policie.cz/clanek/kyberkriminalita.aspx>.
[19] McQUADE, S. C. *Encyclopedia of cybercrime*. Westport, Conn.: Greenwood Press, 2009, s. 16-18.

poskytovatelé internetu umožnili celosvětové komunikační propojení a sdílení dat mezi počítači, čímž se otevřela brána do světa počítačové kriminality.[20]

2.3 Současnost počítačové kriminality

Současný stav počítačové kriminality je na lokální úrovni v podstatě neudržitelný, a to z důvodu globalizace informačních technologií a rozšířením těchto technologií do všech oblastí lidského života. Počítače, případně jednotlivé řídící komponenty, se dnes vyskytují ve většině přístrojů a nástrojů, a tendence vývojářů a vývojových skupin ICT je v ještě větším rozšiřování těchto technologií do pracovního i osobního života lidí. Další tendencí je propojení všech těchto zařízení do jedné globální sítě, případně do malých lokálních sítí s prvky umělé inteligence, což se projevuje v různých sadách chytrých zařízení typu mobilní telefon, tablet, čtečka, elektronické hodinky, ale také například ledničky, pračky, sušičky, a to vše je povýšeno do systémů řízení chytré domácnosti, včetně takových činností, jakými je dálkové ovládání domu nebo bytu. Ve své podstatě jakékoliv zařízení, které je schopno připojit se do počítačové sítě, stává se potencionálním nástrojem pro páchání trestné činnosti a rozšiřuje tím množství možných pachatelů nebo obětí počítačové kriminality. Současný stav rozsáhlé trestné činnosti, která je v oblasti počítačové kriminality popisují další kapitoly této práce.

2.4 Budoucnost a prognóza vývoje počítačové kriminality

Prognóza vývoje počítačové kriminality není pozitivní, ovšem díky zaměřenosti různých specializovaných útvarů orgánů činných v trestním řízení, případně skupin prevence je možné hovořit o současné stabilizaci tohoto stavu. Výhled do budoucna je ovšem stále napjatý a souvisí především s neustálou tendencí modernizovat a zavádět nové technologie. Trestná činnost organizovaných skupin je mnohdy umožněna především díky finanční stránce těchto skupin, kdy díky dostatečným finančním prostředkům, které z větší části pocházejí z obdobné trestné činnosti, převyšují možnosti útvarů policie a orgánů zabývajících se kybernetickou bezpečností, pro které jsou náklady na technologie potřebné pro zjištění, detekci, pozorování a následnou eliminaci této trestné činnosti příliš vysoké.

[20] BRITZ, M. *Computer forensics and cyber crime: an introduction*. 3. vyd. Boston: Pearson, 2013, s. 24.

V minulosti se ve větší míře zaměřovala počítačová kriminalita na obohacení se pachatelů, na majetkový prospěch. Díky stále většímu množství útoků na vnitrostátní a mezinárodní úrovni, které se zaměřují na ekonomiku nebo politickou destabilizaci velkých samosprávních nebo správních celků, se dá předpokládat, že boj s počítačovou kriminalitou se rozšíří na globální celosvětovou úroveň.

Bohužel tuto situaci bude podporovat opět sílící tlak po modernizaci a zdokonalování technologií a rozšiřování nových síťových prvků, které mohou ve větší míře usnadnit pachatelům globální útoky proti infrastruktuře celých států.

Jedním z mnoha podobných případů z minulosti, které mohou být modelovou ukázkou, jakých nedozírných následků lze pomocí počítačové kriminalitě dosáhnout, se zabýval Holden, který popisoval případ kybernetického útoku z poloviny roku 2010 v jaderné elektrárně Natanz v Íránu, kdy řídicí systém elektrárny byl útočníky infikován počítačovým červem, který následně poškodil systém kontroly a monitoringu průmyslových procesů této jaderné elektrárny. Obdobné útoky mohou být odkudkoliv v kyberprostoru vedeny na jakékoliv strategicky důležité místo infrastruktury státu.[21]

Lze tedy důvodně předpokládat, že následující oblasti vývoje informačních technologií, jakými jsou botizace, internet věcí, umělá inteligence, automatizace a vývoj nových aplikací a technologií, budou ostře sledovány nejenom organizacemi, které chrání bezpečnost kyberprostoru, ale budou velmi pravděpodobně sledovány především pachateli trestné činnosti počítačové kriminality.

Jedná se o budoucnost vývoje technologií ICT a s tím ruku v ruce potencionální riziko z tohoto vyplývající.

2.4.1 Botizace a automatizace

Automatizace

Podle Groovera je automatizace technologií, která umožňuje realizovat jakékoliv procesy bez zásahu lidského prvku, případně s minimálním zásahem člověka a jeho práce.[22]

[21] HOLDEN, D. *Estonia, six years later* [online]. Publikováno 16. 5. 2013 [cit. 2021-10-26]. Dostupné z: WWW: <http://www.arbornetworks.com/asert/2013/05/estonia-six-years-later/>.
[22] GROOVER, M. P. *Fundamentals of modern manufacturing: materials, processes and systems.* New York: John Wiley, 2001. s. 124

V případě automatizace můžeme hovořit o automatickém řízení procesů, kdy jsou zahrnuty různé řídící systémy pro průmyslová zařízení, jakými jsou například strojní zařízení, kotle a pece pro tepelné zpracování, systémy spínání telefonních sítí, řízení lodní a letecké dopravy a ostatní oblasti řízení, kde není zapotřebí lidského zásahu, případně, kde by tento zásah mohl být zdraví či život ohrožující. Ve skutečnosti se poprvé objevil termín automatizace v průmyslové výrobě již v roce 1947 v souvislosti s Fordovými závody a jeho oddělením automatizace. Dá se bez nadsázky říct, že automatizace zahrnuje od nejjednodušších procesů vyskytujících se u domácích spotřebičů, až po velice sofistikované a složité multioperacionalizované procesy řídících systémů elektráren a obdobných složitých celků.

Botizace

Robotizaci lze chápat jako automatizaci průmyslových procesů pomocí robotů.

Pro vykonávání automatických obchodních procesů v sektoru služeb je používáno tzv. softwarových robotů a takovéto automatizované činnosti, kde procesy vytváří a řídí softwaroví roboti, říkáme botizace.

Boti, tedy, automatizované robotické programy, poskytují obecnou automatizační schopnost v prostředí koncového uživatele i zprostředkovatele a realizátora především k řešení a provádění manuálních a opakovaných úkolů.

Doposud nejčastější využití botů je zaznamenáno v technologických procesech rozpoznávání hlasu a pro komunikace související se získáváním a sběrem dat.

Botizace jako automatizovaný proces souvisí s nově vznikajícím odvětvím vývoje technologií, kde je proces botizace zaměřen především na úplnou náhradu funkce činnosti člověka, a kde díky umělé inteligenci bude docházet k situacím, kdy samotný bot bude rozhodovat, řídit sebe a ostatní procesy, kontrolovat a vyvíjet úpravy vlastního softwarového rozhraní.

Podle údajů z výzkumu společnosti Deloitte, která se v roce 2018 zabývala problematikou umělé inteligence, se tento vývoj v posledních letech zásadním tempem zrychlil a současné schopnosti používané technologie, která byla předmětem výzkumu, napodobují schopnosti způsobu myšlení člověka. *„Vedle tradiční softwarové robotizace, kdy je pro konkrétní úkol napsán specifický program, lze procesy automatizovat pomocí RPA. Jelikož se jedná o práci s informacemi, ať už v číselném nebo textovém formátu, je RPA zaměřeno na rutinní znalostní úkony, které lze vykonávat pomocí souboru pravidel.*

Takovýto software napodobuje chování člověka v rámci již existujícího uživatelského rozhraní. Je schopen číst a zpracovávat data z aplikací, komunikovat s jinými systémy a vykonávat předem definované reakce."[23]

RPA - Robotická Procesní Analýza (Robotic Process Automation) – bude v budoucnu stále rozšířenějším pojmem nejenom v kladném smyslu, ale díky výhodám a předurčenosti využití může být zároveň jedním z nástrojů počítačové kriminality. Už z podstaty činnosti se jedná o nejnovější nástroj k automatizovanému procesu rutinních operací, které za normálních podmínek zabírají čas a jsou opakovaně prováděny stále stejně a beze změn pomocí softwarových robotů s umělou inteligencí.[24]

2.4.2 Internet věcí

Dalším budoucím fenoménem na poli technologií zítřka je Internet věcí, zkráceně IoT - Internet of Things, který je založen na principech interakce a vzájemné provázanosti v komunikaci mezi jednotlivými síťovými prvky, které jsou napojené na architekturu Internetu a zpravidla disponují určitou mírou inteligence. V návaznosti na botizaci a procesy spojené s budoucím vývojem umělé inteligence není překvapující příklad jednoho z prvních prokázaných kybernetických útoků v prostředí IoT, který byl již v roce 2014 popsán ve vědecké publikaci Science X Network a kde došlo pomocí botnetu k cílenému rozesílání stovek tisíc škodlivých e-mailů denně prostřednictvím spotřebních zařízení zapojených do Internetu věcí. Zajímavostí tohoto případu je, že mezi zařízení, která rozesílala tyto škodlivé e-maily, patřily různé chytré domácí spotřebiče včetně chladničky.[25]

Do kategorie věcí ohrožených potencionálním útokem pachatele trestné činnosti počítačové kriminality můžeme také podle Pavlíkové zařadit věci a zařízení denní spotřeby jakými jsou pračky, domácí kina, obojky pro domácí mazlíčky, virtuální brýle, stejně tak sem patří autonomní vozidla a v systému řízení budov různá čidla, alarmy,

[23] DELOITTE. *Automatizace práce v ČR: Proč se (ne)bát robotů* [online]. 2018. Dostupné z WWW: <https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/strategy-operations/Automatizace-prace-v-CR.pdf>.

[24] HLAVÁČEK, V. *Robotická procesní automatizace RPA – Co to je?* In: komix.cz [online]. Publikováno 5. 2. 2021 [cit. 2021-11-12] Dostupné z WWW: <https://www.komix.cz/roboticka-procesni-automatizace-rpa-co-to-je/>.

[25] *Cyberattack traced to hacked refrigerator, researchers report*. Phys.org [online]. Science X Network, publikováno 17. 1. 2014 [cit. 2021-11-08]. Dostupné z WWW: <https://phys.org/news/2014-01-cyberattack-hacked-refrigerator.html>.

senzory, termo-regulace, inteligentní zámky, řízení spotřeby energie a další druhy technologických prvků zapojených do internetu věcí.[26]

Nebezpečí, které v souvislosti s rozšiřováním Internetu věcí hrozí, popisuje Kolouch jako situaci, kdy zatímco tato inteligentní zařízení na jedné straně koncovým uživatelům usnadňují život, na druhé straně je činí zranitelnějšími v trestné činnosti počítačové kriminality.[27]

2.4.3 Cloud a cloudová řešení

S narůstajícím objemem dat roste ekvivalentně k tomu také potřeba ukládat data na datová úložiště, přičemž lokální datová úložiště řeší pouze část otázky jak a kam ukládat data, protože svojí podstatou stacionarity nejsou vždy a plně tato data k dispozici pro svého majitele v pravý okamžik a na tom správném místě.

Tuto situaci může elegantně vyřešit existence datového úložiště, které je svému majiteli k dispozici kdykoliv a kdekoliv. Takovým řešením je Cloud a Cloudové úložiště. Má to samozřejmě jako všechno svoje výhody a také nevýhody. Mezi výhody patří dostupnost, často také menší finanční náročnost. Mezi nevýhody patří nutnost připojení k internetu a v neposlední řadě potencionální riziko hrozby kybernetického útoku.

Situací se současným a budoucím vývojem Coudového řešení se zabývá velká řada IT odborníků a za všechny lze uvést názory tří, Holta, Bosslera a Seigfried Spellarové, kteří vyzdvihují výhody tohoto řešení především v tom, že i přes mechanismus ukládání a sdílení souborů doslova odkudkoliv na světě, přináší toto řešení s sebou také riziko v podobě zvýšeného zájmu pachatelů kybernetické kriminality.[28]

Je velmi pravděpodobné, že kybernetických útoků v rámci cloudového řešení bude v budoucnu pouze přibývat.

[26] PAVLÍKOVÁ, E.. *Smart cities – inteligentní města, která nám usnadní život*. Bydlenivevate.cz [online]. Publikováno 5. 9. 2019 [cit. 2021-11-12]. Dostupné z WWW: <https://bydlenivevate.cz/lifestyle/smart-cities-inteligentni-mesta-ktera-nam-usnadni-zivot>.
[27] KOLOUCH, J. *CyberCrime.* Praha: CZ.NIC, z. s. p. o., 2016. op. cit, s. 184.
[28] HOLT, T. J.; BOSSLER, A. M.; SEIGFRIED-SPELLAR, K. C. *Cybercrime and digital forensics: an introduction*. 2. vydání. London: Routledge, 2018, s. 626.

2.4.4 Vývoj technologií

Další oblast, která bude podle Smejkala potencionálně ohrožena kybernetickými útoky je v souvislosti se současným trendem vývoje informačních systémů, trh s kryptoměnou.[29]

V souvislosti s vývojem technologií se zvýšeným zájmem pachatelů o kybernetické útoky pomocí umělé inteligence zabývá Vimmerová problematikou technologií mobilních sítí a poukazuje na zvýšený tlak pachatelů na napadání páté generace technologií mobilních sítí – 5G. I v telekomunikačních technologiích je skrytá hrozba počítačové kriminality v budoucnu.[30]

Hovoříme-li o budoucnosti vývoje technologií, musíme klást na stejnou úroveň také budoucnost vývoje počítačové kriminality i v oblastech zneužívání kvantových počítačů a fake news, na což primárně poukazuje Javůrek ve svých příspěvcích.[31]

Již nyní se projevují kybernetické útoky na vozidla, což je velmi sledovaná oblast nových technologií a rozšiřuje se také útok na demokracii v podobě ovlivňování voleb. Tento trend bude pravděpodobně narůstat, a vzhledem k velkému vlivu mediální komunikace půjde o počítačovou kriminalitu velkého rozsahu, protože média a sdělovací prostředky patří obecně k silným nástrojům používaným k ovlivňování mas občanů a voličů.[32]

Nedílnou součástí budoucího vývoje počítačové kriminality bude zřejmě také snaha ovlivnit nebo podmanit si kontrolu v problematice civilních a armádních navigačních systémů a dnes už se ani další oblast, kterou je propojení lidského mozku s technologiemi, nevnímá jako nereálná, ale naopak, existují první reálné kroky ze strany vědců z ideologické skupiny kolem Elona Muska, který vytvořil svůj futuristický projekt

[29]SMEJKAL, V. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, s. 787-808.
[30]VIMMEROVÁ, V. *Síť jménem 5G vstoupí do našich životů a změní je. Odpor je marný, ostražitost nutná.* Aktuálně.cz [online]. Publikováno 29. 11. 2019 [cit. 2021-11-15]. Dostupné z WWW: <https://zpravy.aktualne.cz/ekonomika/bezpecnost-site-5g-co-si-sami-neuchranime-je-v-ohrozeni/r~8738a046f73511e9ac60ac1f6b220ee8/>.
[31] JAVŮREK, K. *První kvantový počítač stojí deset milionů dolarů.* E15.cz [online]. CZECH NEWS CENTER a.s., © 2020 [cit. 2021-11-15]. Dostupné z WWW: <http://vtm.e15.cz/prvni-kvantovy-pocitac-stoji-deset-milionu-dolaru>.
[32] *eDemocracy*. Jaknainternet.cz [online]. CZ.NIC, z. s. p. o., © 2020 [cit. 15. 11. 2021]. Dostupné z WWW: <https://www.jaknainternet.cz/page/1664/edemocracy/>.

Neuralink a v nedávné době realizoval první úspěšné propojení mozku prasete s informačními technologiemi.[33]

2.5 Typy počítačové kriminality

Na základě různorodosti pojetí počítačové kriminality, jak tuto oblast vnímá Česká republika a okolní státy Evropy, včetně zbytku světa, lze diferencovat problematiku počítačové nebo, chceme-li využít terminologii mezinárodní, kybernetické kriminality na různé typy podle funkčnosti, legislativního rámce a politického postoje k této sociálně patologické činnosti.

Z hlediska pojetí této práce se zaměříme především na dělení podle charakteru trestně právního a dělení podle komparace kritérií Rady Evropy a České republiky.

2.5.1 Dělení z hlediska trestně právního

McGuire a Dowling dělí kybernetickou kriminalitu na dvě základní kategorie:[34]

- **Cyber-enabled** – jde o kriminalitu s prvky tradičních trestných činů, které jsou usnadňovány pomocí počítačů, sítí nebo jiných ICT technologií např.: krádeže identity, krádeže elektronických informací pro komerční zisk, obchodování s drogami, dětská pornografie a mnoho dalších.
- **Cyber-dependent** – jde o kriminalitu, u které je absence informačních technologií zcela nemožná a trestné činy jsou spáchány výhradně přes počítač, počítačové sítě či ICT např.: šíření virů, malware, hacking a jiné útoky

Další možnosti dělení počítačové kriminality jsou popsány v následujících kapitolách.

[33] *Neuralink Elona Muska: ovládání telefonu a počítače pouhou myšlenkou*. ALZA.cz [online]. Publikováno 8. 10. 2019 [cit. 2021-11-15]. Dostupné z WWW: < https://www.alza.cz/neuralink> - *Musk nás zklamal, říkají kyborgové. Jeho Neuralink dává víc otázek než odpovědí*. Forbes.cz, Darek Šmíd 07. 09. 2020 [cit. 2021-12-07]. Dostupné z WWW: <https://www.forbes.cz/musk-nas-zklamal-rikaji-kyborgove-jeho-neuralink-dava-vic-otazek-nez-odpovedi/>.

[34] McGUIRE, M.; DOWLING, S. *Cyber crime: A review of the evidence*, Research Report 75, Summary of key findings and implications [online]. UK Home Office, 2013, s. 5 [cit. 2021-12-20]. Dostupné z WWW: <https://ncvc.dspacedirect.org/handle/20.500.11990/871>.

2.5.2 Trestné činy proti důvěrnosti uživatelů, integritě a dostupnosti počítačových dat a systémů

Do této kategorii trestných činů můžeme zahrnout následující projevy počítačové kriminality:

Hacking

Jedná se o porušování autorských práv, především pronikání do systémů a svým obsahem patří mezi nejvýraznější v oblasti počítačové kriminality. Základem hackingu je průnik do systému, obejití nebo prolomení ochrany a zabezpečení systému. Hacker je pojmenování útočníka, který svojí činností narušuje systém. Původní hackeři pocházeli z řad programátorů a jejich cílem bylo dostat se do systému, dokázat sobě nebo okolí, že zvládnou probourat ochrannou blokádu systému, případně dalším cílem bylo najít chybu v blokovaném systému a opravit ji a tím dokázat větší kvalitu programátorské práce, než jaká byla od původního autora programu. Postupem času se vyčlenily dvě skupiny hackerů. Zatímco první skupina hackerů nemá v úmyslu jakýmkoliv způsobem škodit a nabourávat jádro systému, druhá skupina hackerů se zaměřuje výhradně na materiální zisk.

Sniffing

Zjednodušeně jde o odchytávání komunikace v počítačové síti. Získané informace jsou pak dále určeny k dalšímu zneužití, a to buď například v hackingu, nebo v tradičních formách trestné činnosti, jakými může být například vydírání, vyhrožování apod. K zachytávání komunikace se využívá poměrně velkého množství softwarových i hardwarových prostředků. Touto cestou lze získat v podstatě veškerý obsah komunikace procházející přes daný uzel sítě, zvláště pokud je nešifrovaná.

Narušování dat

Při nejrůznějších útocích hackerů, či crackerů dochází k protiprávnímu zásahu do dat uživatele, a to velmi často s konkrétním, praktickým cílem, kterým bývá nejčastěji odstranění ochrany programu a následné šíření zdrojového souboru dat nebo celého programu. Mezi časté příklady také patří vandalismus webových stránek, kde dochází k napadení webové stránky a pozměnění jejich obsahu.

Narušování systému

V této kategorii trestných činů počítačové kriminality jsou zahrnuty všechna zvláště závažná narušení nebo přerušení funkčnosti informačního systému nebo

samotného počítače. V konkrétních případech se pak jedná zejména o tzv. DoS útoky, které jsou charakterizovány jako útoky za účelem znepřístupnění služby, počítače nebo celé sítě. Zkratka DoS znamená Denial of Service, což se dá volně přeložit jako „odmítnutí služby“.

Mezi DoS útoky patří například:

- **Mass mailing list** – zahlcení určité e-mailové schránky, aby byla nepoužitelná. V tomto případě se nejedná přímo o Spam, ale úkolem je zaplnit schránku tak, aby již do této schránky nebylo možné přijímat další zprávy. Jedná se o záplavový útok na e-mailovou schránku a nebezpečí tohoto útoku je veliké s minimálním úspěchem vystopování útočníka.
- **E-mail bombs (E-mail bombing)** – útok, který je velmi podobný mass mailing listu, ovšem v tomto případě se k vytvoření e-mailů využívá programu nikoliv e-mailového účtu a adresy. Útočník pomocí programu sám generuje útoky ve formě e-mailů a ovlivňuje také jejich frekvenci a množství zasílání. V takovém případě nemusí dojít pouze k zaplnění e-mailové schránky ale přímo ke zhroucení poštovního serveru. Velice často je tento typ útoku používaný jako osobní pomsta.
- **Fork bomb** – jde o lokální DoS útok. V tomto případě jde o programy, které pouští do nekonečna samy sebe. Jméno tohoto typu útoku vzniklo díky funkci fork(), která má za úkol spustit běžící program ještě jednou a tím vytvořit další instanci, což se opakovaně děje do nekonečna. Nebezpečí je sice omezeno pouze na lokální použití, ovšem účinnost je stoprocentní. V případě aktivace tohoto útoku například v letovém provozu v navigačním systému, může dojít ke katastrofálním následkům a z tohoto hlediska se jedná o typ trestného činu s naplněním skutkové podstaty obecného ohrožení.

Prolamovače hesel

Programy používané k prolomení ochrany nebo autorizace, která je realizovaná především statickým heslem. Legální využívání na internetu volně dostupných prolamovačů hesel lze využít oprávněnými uživateli, kteří zapomněli heslo k systému nebo jednotlivému dokumentu, stejně tak tohoto způsobu prolomení hesla mohou využít systémoví administrátoři, kteří s jejich pomocí kontrolují, vhodnost či nevhodnost uživatelem zvolených hesel. K nelegálnímu použití se uchylují hackeři za účelem získání protiprávního přístupu nebo dešifrování cizích dat.

Malware

Software nebo jiná data, jejichž cílem je škodit počítači nebo jeho obsahu, případně je jinak zneužít. Může jít také pouze o škodlivý kód se stejným účelem.

Základní druhy malwaru:

- **Viry** – programy, které se umí samy šířit bez vědomí a obvykle proti vůli uživatele počítače.
- **Červi**– umí se také samy šířit, ovšem od virů se liší tím, že ne vždy užívají hostitele.
- **Trojský kůň** – jde o neškodně nebo zajímavě se tvářící program, který ovšem po spuštění aktivuje obvykle vir nebo spyware, který s sebou nese. Nebezpečí tohoto trojského koně je také v tom, že dokáže otevírat porty a tím umožnit nebo usnadnit další hackerský útok.
- **Spyware** – software, který bez vědomí uživatele z počítače odesílá přes Internet důvěrné informace.
- **Adware** – někdy je dokonce se souhlasem uživatele nainstalován jako součást freewaru. Patří většinou mezi neškodný software.
- **Dialer** – jde o malware, který může přesměrovat vytáčené připojení Internetu na jinou, drahou linku, a takto získané prostředky následně čerpá autor dialeru.

Spamming

Jedná se o zasílání nevyžádaných elektronických zpráv, tj. emailů, zpráv instant messagingu apod. V současné době se odhaduje, že podíl spamu na veškeré emailové komunikaci tvoří 75 % z celkového objemu všech e-mailem provozovaných zpráv.

2.5.3 Trestné činy se vztahem k počítači

Jedná se o počítačovou kriminalitu, u které vede pachatel svůj útok pouze proti programovému vybavení počítače nebo uloženým datům. Závažnost útoku může být od nejjednoduššího smazání programového vybavení až po infikování programového vybavení virem s následnou ztrátou programů a dat.

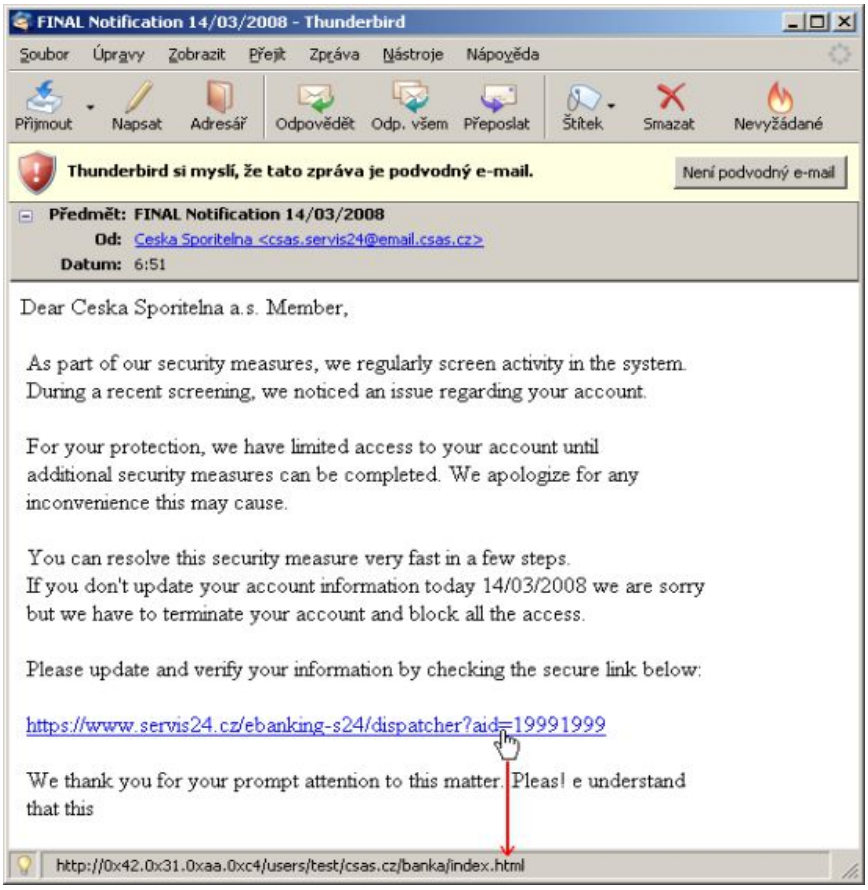
Phishing a Pharming

Phishing, do českého jazyka volně přeloženo jako „rybaření“ je zacíleno na získávání důvěrných a citlivých informací, jakými jsou například hesla, informace o kreditních kartách a jeho účelem je získat přístup s následným obohacením se z cizích zdrojů.

Nejčastější a nejznámější formou jsou podvodné emailové zprávy zasílané do e-mailových schránek nic netušících obětí. V podvodném emailu pak oběť nalezne informaci o tom, že si adresátova banka případně jiná instituce s finančními službami online potřebuje ověřit určité údaje, a proto žádá adresáta o přihlášení na odkazovanou podvrženou stránku, kde adresát vyplní požadované údaje (nejčastěji přihlašovací údaje nebo PIN a číslo karty). Po takovémto přihlášení a uvedení všech údajů má pachatel přístup do účtu oběti a následuje zneužití nebo vykradení tohoto účtu.

Pharming je mnohem nebezpečnější způsob útoku. Pachatel nejprve hackuje DNS server, který je odpovědný za přiřazování doménových jmen IP adresám tak, že odkazuje na podvržené stránky. Oběť tohoto útoku nemá žádné podezření o spáchání podvrhu. Dále následuje stejný postup jako v případě Phishingu, jenom s tím rozdílem, že zde pachatel hacknul DNS server.

Obrázek 1: Příklad Phishingového dopisu[35]



[35] Zdroj : PrtScrn autorovy obrazovky – výukový manuál České spořitelny.

Cyberstalking a kyberšikana

Jedná se o zasílání různých zpráv s pomocí softwarových nástrojů, přičemž frekvence nebo obsah těchto zpráv je nepřiměřený a z hlediska významu anglického slova „stalking“, což znamená pronásledování, se může oběť cítit pod tlakem a manipulována. V případě Cyberstalkingu jde o obdobu fyzického pronásledování, která je virtuálně realizovaná prostřednictvím zpráv v kyberprostoru. Mezi nejčastější oběti Cyberstalkingu lze zařadit celebrity, politiky a veřejně činné osoby, expartnery nebo partnery v mezilidských vztazích, které přestaly fungovat.

V případě kyberšikany jde o obdobnou trestnou činnost jako u Cyberstalkingu s většími projevy šikany a dehonestace osobnosti a realizují se pomocí telefonu, e-mailu, blogu apod. Podoby kyberšikany jsou různé, od zasílání obtěžujících zpráv, urážejících, zesměšňujících nebo výhružných e-mailů a útočných SMS zpráv, nahrávání dehonestujících situací a následné rozesílání ostatním uživatelům internetu.

Škodlivé šíření informací

S ohledem na velký objem informací, které se v kyberprostoru vyskytují, je dnes už velmi složité rozpoznat pravdivé informace od vymyšlených nebo dokonce účelově vytvořených. Mezi nejzajímavější a také svým projevem nejnebezpečnější formu šíření nepravdivých varování patří HOAX, což je nevyžádaná e-mailová, nebo ICQ zpráva, která adresáta varuje před hrozbou nějakého viru, případně prosí o pomoc, nebo informuje o jiném nebezpečí, a také se snaží adresáta pobavit apod. Tato zpráva většinou obsahuje i výzvu k rozeslání hoaxu mezi další adresáty a touto podstatou se také někdy označuje jako řetězový e-mail.

Na tuto formu činnosti HOAXu se specializují některé servery, které pro uživatele zachytávají HOAXy a zveřejňují je jako varování nebo osvětu a vedou si jejich databázi: viz příloha č. I – Vzor HOAXu

2.5.4 Trestné činy se vztahem k obsahu informace

Rozvoj Internetu vedl mimo jiné také k rozvoji jiných forem závažné trestné činnosti a to především v souvislosti s šířením závadného obsahu, což platí zejména pro šíření dětské pornografie a pornografických materiálů obecně.

Obdobně šíření a podpora extremismu je považována v právním měřítku za trestnou činnost a v mnoha případech přesahuje do oblasti hanobení národa, etnické skupiny, rasy a přesvědčení, násilí proti skupině obyvatelů a proti jednotlivci, podporování a propagace hnutí směřujících k potlačování práv a svobod člověka, případně směřující k projevům sympatií k takovým hnutím, a jsou zdokumentovány celosvětově i trestné činy počítačové kriminality související s terorismem.

2.5.5 Trestné činy související s porušováním autorského práva a souvisejících práv

Počítačové pirátství a Warez

Je zajímavé, že valná většina z nás si pod pojmem počítačová kriminalita na prvním místě představí právě počítačové pirátství.

Snahy o zkopírování softwaru nebo počítačové hry bez placení se objevily již v dobách prvních osobních počítačů.

Tato tendence přetrvává doposud, ovšem díky sofistikovanějšímu zabezpečení nebo jiné formě distribuce legálního softwaru se původní kopírování her a softwaru

přesunulo na jiné komodity kyberprostoru. Těmito komoditami jsou hudební, filmové nahrávky. Tuto situaci umožnil opět rozvoj Internetu, kdy vzniká fenomén Warez, což je nelegální šíření dat na FTP serverech a Peer-to-Peer sítích.

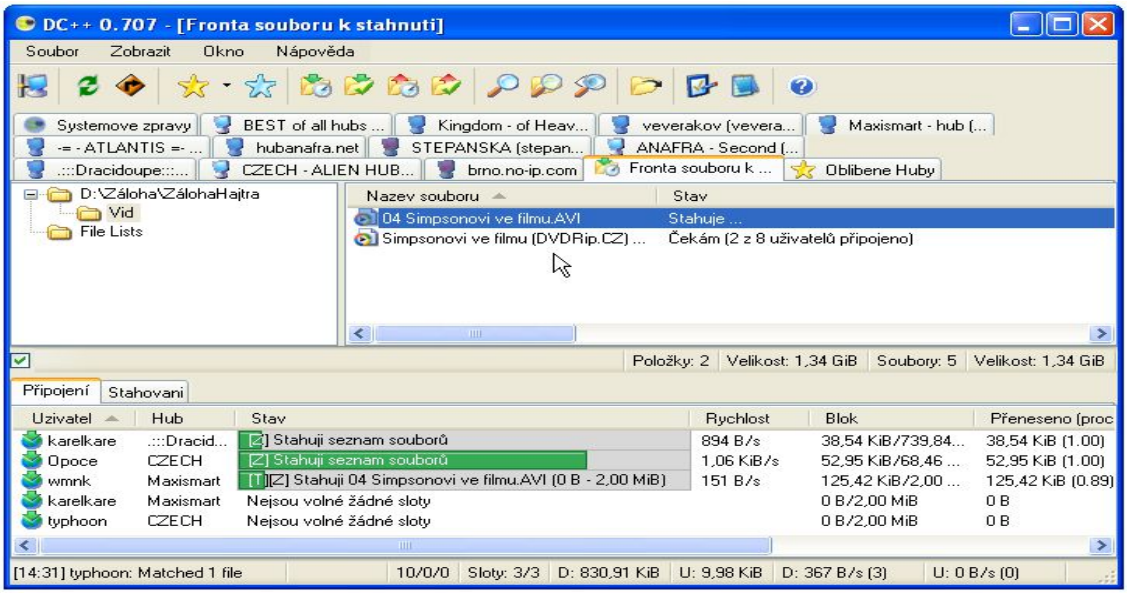
Na rozdíl od motivu počítačových pirátů, který je zaměřený na zisk prostřednictvím nelegálního šíření za úplatu, je motivem Warezových skupin nelegální zpřístupnění softwaru a audio nebo videonahrávek zdarma, přičemž si na financování této činnosti vydělávají v projektech zaměřených na prodej reklamy a často také ve spojení s porno průmyslem.

P2P

Sítě Peer-to-peer, P2P případně označované jako klient-klient jsou svojí strukturou architektury počítačových sítí, ve své podstatě jednoduchým propojením počítačů napřímo, kdy spolu komunikují přímo jednotliví klienti a nevyužívají prostřednictví serveru.

V praxi pak jde o výměnné sítě P2P, ve kterých si může mnoho uživatelů vyměňovat vzájemně data. Velmi známá je dnes už původní verze Napsteru, dalším příkladem je Direct Connect. Výhodou sítí P2P je, že s nárůstem počtu uživatelů zároveň roste celková dostupná přenosová kapacita. Další výhodou, které využívají především pachatelé trestných činů je, že anonymita této výměnné sítě umožňuje nelegální výměnu dat s prakticky nulovou zodpovědností k vlastnictví dat ze strany jednotlivých uživatelů.

Obrázek 2: Příklad P2P programu DC++[36]



[36] Zdroj : PrtScrn autorovy obrazovky – ilustrační příklad.

Cybersquatting

V tomto případě se jedná o výkup marketingově zajímavých nebo oblíbených slov a následnou registraci internetových adres s cílem jejich budoucího prodeje společnostem a vlastníkům ochranných známek, a to s vysokým ziskem. Zdánlivě je tato situace vnímána jako legální a bez znaků trestné činnosti, ovšem narážíme zde na práva duševního vlastnictví a jeho porušování. Na druhé straně existují také aukční servery, které s touto informační komoditou spekulativně obchodují.

2.6 Dělení podle kritérií Rady Evropy

Vzhledem k nutnosti zabývat se počítačovou kriminalitou na mezinárodní úrovni, vznikla jako reakce na tuto situaci Úmluva rady Evropy o počítačové kriminalitě,[37] která byla publikována dne 23. listopadu 2001 a vstoupila v platnost 1. července 2004. Následně ji podepsala také Česká republika dne 9. února 2005.

Smyslem tohoto dokumentu je sjednocení legislativy evropských zemí, za účelem společného boje a součinnosti v problematice počítačové kriminality, ale také z důvodu, že trestná činnost spojená s počítačovou kriminalitou má mezinárodní charakter.

Členění podle Rady Evropy je následující:

Do minimálního seznamu trestných činů jsou zahrnovány:

- počítačové podvody,
- počítačové falzifikace,
- poškozování počítačových dat a programů,
- počítačová sabotáž,
- neoprávněný přístup,
- neoprávněný průnik,
- neoprávněné kopírování autorsky chráněného programu,
- neoprávněné kopírování fotografie.

Do volitelného seznamu trestných činů je zahrnuto:

- změna v datech nebo počítačových programech,
- počítačová špionáž,
- neoprávněné užívání počítače,

[37] *Úmluva Rady Evropy o počítačové kriminalitě*, Budapešť, 23. listopadu 2001, Convention on Cybercrime - ETS no. 185. Dostupné z WWW: <https://www.coe.int/en/web/conventions/>.

- neoprávněné užívání autorsky chráněného programu.

Minimální seznam obsahuje taková jednání, která by měla být jako skutkové podstaty trestných činů zapracována do právních řádů jednotlivých zemí, aby bylo možné vést účinný boj proti počítačové kriminalitě. Ve volitelném seznamu jsou uvedena jednání, která by bylo vhodné kvalifikovat jako trestné činy, avšak není to nezbytné.

3 SPECIFIKA BANKOVNÍ POČÍTAČOVÉ KRIMINALITY

V projevech trestných činů počítačové kriminality jsou velmi specifickým prvkem trestné činy spáchané v oblasti bankovního a finančního sektoru. Charakteristika těchto trestných činů je vždy spojená s konáním pachatele za účelem finančního zisku a s tím také souvisí různé specifické projevy pachatelova konání, ať už jde o kybernetický útok prostřednictvím počítače, kriminalitu s platebními kartami nebo následné fyzické projevy trestné činnosti spojené s krádeží platební karty a získáním PINu ke kartě. Rozdělením jednotlivých možných útoků dosáhneme větší přehlednosti v projevech této počítačové kriminality. Je také vhodné se zaměřit na elementy a charakter pachatelů, ze kterého lze usuzovat na způsoby provedených útoků.

3.1 Charakter pachatele

Z pohledu dělení pachatele trestného činu vůči bance je možné rozdělit tyto pachatele na externí a interní, přičemž poměr interních a externích pachatelů hospodářské kriminality je z dlouhodobého hlediska vyrovnaný.

3.1.1 Externí pachatel

Obrázek 3: Profil externího podvodníka/pachatele[38]

Z výzkumu PricewaterhouseCoopers, který byl zveřejněn v roce 2016, vyplývá, že externí podvody jsou takové, ve kterých nemusí mít pachatel vztah k bance, případně může být současným či bývalým zákazníkem banky, ale může jít také například o externího dodavatele nebo poskytovatele služeb a mezi trestné činy spáchané těmito podvodníky patří šekové podvody, kriminalita s platebními kartami, případně

[38] Zdroj: PwC, ©2016 PricewaterhouseCoopers.

zpronevěra. Nejčastějšími trestnými činy přitom byly podvody související s počítačovou kriminalitou a zneužitím platebních karet.[39]

3.1.2 Interní pachatel

Obrázek 4: Profil interního podvodníka/pachatele[40]

Ze stejného výzkumu společnosti PricewaterhouseCoopers vyplývá, že nejčastějším charakteristickým prvkem pro definici interního pachatele trestné činnosti v bance je interní zaměstnanec, muž s vysokoškolským titulem ve věku mezi 31 až 40 roků a s praxí 3 až 5 roků ve společnosti. Obdobně i zde bylo výzkumem potvrzeno, že nejčastější trestná činnost interního pachatele souvisí s počítačovou kriminalitou a na rozdíl od externího pachatele, který má ztíženou situaci s možnými formami přístupu do bankovního systému, interní pachatel díky tomuto přístupu, dobré znalosti firemního prostředí a pracovních návyků více využívá formu počítačové kriminality.

3.2 Kybernetická kriminalita z hlediska banky nebo finanční instituce

V narůstající atmosféře strachu o kybernetickou bezpečnost jsou v současné době finanční organizace a banky donuceny investovat nemalé finanční prostředky do zabezpečení hardwarového a softwarového vybavení proti cíleným útokům pachatelů trestné činnosti v souvislosti s počítačovou kriminalitou. Kybernetických útoků stále přibývá a tento stav je varovným signálem pro bankovní i nebankovní sektor. V souvislostmi s těmito útoky se nejedná pouze o odcizená data a finanční prostředky, ale sekundární dopady tohoto stavu se mohou projevit také ve ztrátě důvěry zákazníků k bezpečnostnímu systému banky a tím může dojít nejenom ke ztrátě dobrého jména banky, ale také ke ztrátě významných obchodních partnerů a klientů. Jak je z tohoto výčtu patrno, počítačová kriminalita nemá pro banku nebo finanční instituci pouze charakter primární hrozby, ale zasahuje v sekundárním pojetí do mnohem hlubších kořenů stability

[39] SVÍZELOVÁ, S., 2018. *Operační riziko v bankovnictví.* In: MUNI.cz [online] [cit. 2021-12-20]. Dostupné z WWW: <https://is.muni.cz/th/zx42p/Svizelova-DP_5_1__FINAL_.pdf >.
[40] Zdroj: PwC, ©2016 PricewaterhouseCoopers.

této instituce. Banka je v podstatě permanentní potencionální obětí mnoha různých projevů počítačové kriminality, a to jak od těch jednodušších forem kybernetických útoků jakými je například Phishing, až po velmi závažnou trestnou činnost jakou je infikování virem nebo kriminalita s platební kartou.

3.2.1 Phishing

V případě banky nebo finanční instituce je Phishing snahou pachatelů po získání citlivých osobních informací zákazníků, jakými jsou například hesla, údaje o platebních kartách, rodná́ čísla nebo čísla bankovních učtů. Po získání těchto údajů následuje konkrétní trestná činnost spojená se zneužitím takto získaných údajů a zaměřená na nelegální finanční obohacení pachatele na úkor své oběti. Projevy a druhy Phishingu jsme detailně popisovali v kapitole 2.1.2 Trestné činy se vztahem k počítači.

3.2.2 Viry

Problematiku virů jsme popisovali v kapitole 2.1.1 Trestné činy proti důvěrnosti uživatelů, integritě a dostupnosti počítačových dat a systémů, nicméně v bankovnictví se viry projevují specifickým způsobem a autoři těchto virů při tvorbě kladou velký důraz na specifické vlastnosti prostředí, do kterého bude virus infikován. Z tohoto důvodu je vhodné uvést různé typy virů a popsat jejich působení v bankovním sektoru.

Podle Baráka se nejčastěji jedná o následující:[41]

- **Keylogger** – jedná se o modul, který umožňuje zaznamenávat stisknutí kláves, a odeslat tato zaznamenaná data s kombinacemi stisknutí kláves pachateli. Tímto způsobem se může pachatel dostat k přihlašovacím údajům do systému internetového bankovnictví a pomocí zadání správných údajů do políčka Login a Password získá kontrolu nad bankovním účtem oběti.
- **Network interception** – pomocí tohoto modulu může pachatel zjistit nejrůznější údaje o oběti a to z hlediska chování oběti na internetu, kdy pachatel „odchytí“ chování oběti v síťovém provozu. Takto lze získat například informace o telefonním čísle, zůstatku na účtu nebo osobní údaje oběti.
- **Pořizování snímku obrazovky** – Printscreen modul, který umožňuje pořizovat a odesílat útočníkovi snímky obrazovky.

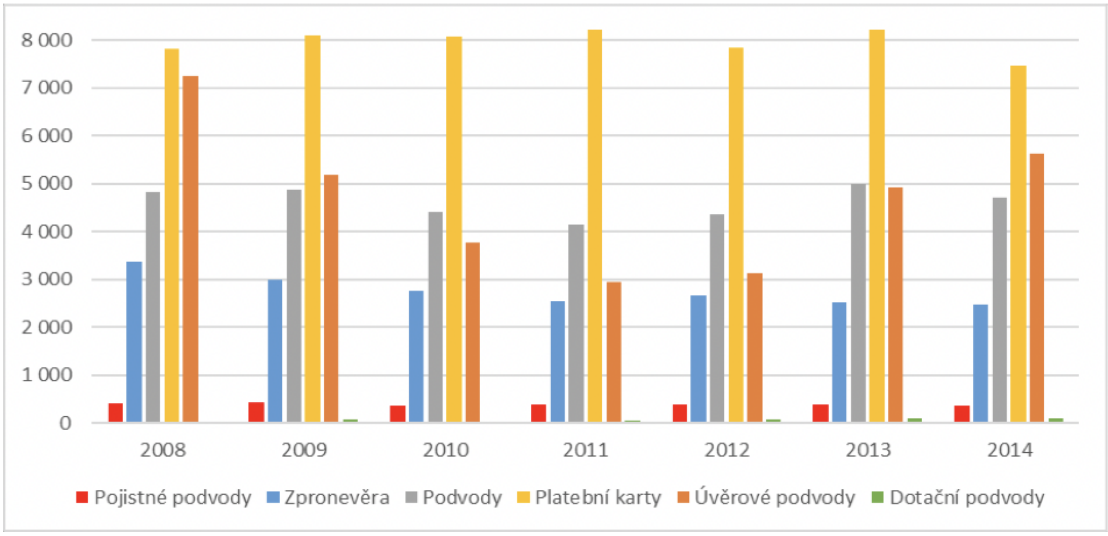
[41] *BARÁK, P., 2015. Podvody páchané v bankách. Brno.* Seminář pro finanční trh.

- **Videozáznam obrazovky** – modul, který umožňuje pořizovat videozáznamy obrazovky a odesílat je útočníkovi.
- **Skrytá VNC sezení** – modul, který umožňuje navázat skrytý vzdálený přístup do počítače, který je spouštěn na jeho monitoru. Útočník tak může libovolně ovládat napadený počítač, aniž by uživatel cokoli poznal.

3.2.3 Kriminalita s platebními kartami

Podle statistik Policie ČR z měření hospodářské kriminality i přes velkou snahu bank o co nejkvalitnější zabezpečení proti trestné činnosti související s manipulací s platebními kartami vyplývá, že v období od roku 2008 do roku 2014 ze sledovaných typů trestné činnosti jsou právě platební karty na prvním místě. Tuto skutečnost znázorňuje graf č. 1 – vývoj jednotlivých druhů trestných činů v bankovním sektoru.

Graf 1: Vývoj jednotlivých druhů trestných činů v bankovním sektoru[42]



[42] Vlastní zdroj na základě dat Policie ČR.

Krádež

V podstatě nejfrekventovanějším a zároveň, z pohledu pachatele trestné činnosti, nejjednodušším způsobem zneužití platební karty je fyzické odcizení jejímu majiteli. Zneužití se pak může odehrát, ať už díky odcizení nebo nálezem ve ztracených peněženkách, ovšem v obou případech se jedná o trestný čin zneužití platební karty.

V případě vícenásobného použití vybírané částky z bankomatu do 500 korun bez nutnosti použití PINu, mají české banky na platebních kartách nastavené tzv. sublimity, které v případě vícenásobného použití takovéto transakce vyžadují po určitém počtu transakcí za sebou odsouhlasení výběru pomocí PINu. V takovém případě, kdy pachatel k odcizené kartě nezná PIN, automaticky se další transakce zablokuje.

Skimming

Jde o techniku nelegálního kopírování dat z platebních karet, které se majitel platební karty jen velmi těžko ubrání. Forma zabezpečení proti tomuto trestnému činu je tedy spíše na straně banky, ovšem i pro ni je to technicky velmi náročné. Pachatelé stále zdokonalují svoje techniky, jak překonat ochranu bankomatů a z tohoto důvodu je opatření na straně banky stále složité. Skimmovací technologie detailně popisuje Součková a z jejího popisu vyplývá, že je složená ze dvou částí. První částí je čtecí zařízení, které útočník umístí v bankomatu do otvoru na kartu a může jím data následně po vložení karty zkopírovat. Druhou částí je miniaturní kamera, kterou umístí do těla bankomatu tak, aby zasahovala svým zorným polem do části bankomatu s klávesnicí, kde majitel bankovní karty v okamžiku vložení karty vkládá svůj PIN. Další možností, která nahrazuje miniaturní kameru, je sofistikovaná podložka, kterou útočník umístí přímo na klávesnici bankomatu a ta následně zaznamenává pořadí a číselnou kombinaci zadávaného PINu.[43]

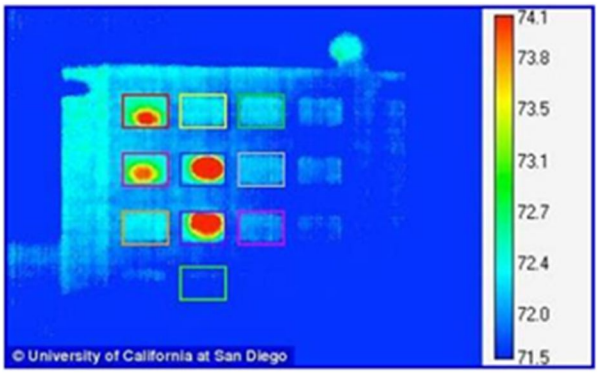
Kromě této technologicky vyspělé podložky může útočník použít také termokameru, která zaznamenává zbytkové teplo z dotyků prstů na klávesnici, přičemž pořadí stisku kláves na klávesnici bankomatu lze zjistit na základě postupného chladnutí míst, kde došlo ke stisku kláves – viz obrázek č. 5 a 6. Získaná data k platební kartě jsou

[43] SOUČKOVÁ, K., 2017. *Přibývá podvodů s platebními kartami. Rizikem jsou univerzální bankomaty*. In: *iRozhlas* [online]. [cit. 2021-12-21]. Dostupné z WWW: <https://www.irozhlas.cz/ekonomika/pribyva-podvodu-s-platebnimi-kartami-rizikem-jsou- univerzalni-bankomaty_1707251034_mos>.

následně pachatelem odeslána do zahraničí, kde jejich spolupachatelé vyrobí padělky a pomocí nich vybírají peníze z účtu oběti.[44]

Obrázek 5: Skimmovací zařízení[45]

Obrázek 6: Sejmutí klávesnice pomocí termokamery[46]



Libanonská smyčka

Jedná se o starší způsob útoku, kdy pomocí jednoduchého zařízení nazývaného libanonská smyčka, které útočník nainstaluje do vkládacího prostoru pro karty v inkriminovaném bankomatu a v okamžiku, kdy majitel platební karty vloží svoji kartu do tohoto otvoru, karta se v libanonské smyčce zachytne a nepropadne dovnitř vstupního prostoru pro kartu. Zároveň nejde platební karta ani vytáhnout. Momentu překvapení využívá útočník, který se pohybuje v blízkosti bankomatu a v situaci, kdy majitel karty neví, jak postupovat dále, nabídne útočník majiteli pomoc a poradí mu, aby opětovně vložil svůj PIN. Poté co majitel odchází vyřešit svoji situaci do banky a kdy útočník po

[44] KALAMÁR Š., PETRÁK, M. *Skimming jako jeden z druhů kybernetické kriminality.* In: Cybersecurity.cz [online]. [cit. 2022-01-05]. Dostupné z WWW: <https://www.cybersecurity.cz/data/skimming.pdf>.
[45] Zdroj: iDnes.cz, 2007.
46 Zdroj: iDnes.cz, 2007.

odchodu majitele vysune kartu i s libanonskou smyčkou, použije útočník vysunutou a v tomto okamžiku již odcizenou platební kartu a pomocí odpozorovaného PINu má přístup k financím na účtu oběti. Tímto postupem a způsobem zneužití platební karty se velmi detailně zabývá Tůma ve svém příspěvku „Dávejte si pozor na platební kartu! Podvodníci jsou stále vynalézavější“ z roku 2013.[47]

I přesto, že nejde o přímé využití počítače, jedná se o formu počítačové kriminality, kdy dochází za pomoci bankomatu a díky vstupnímu zařízení, kterým se zadává do bankovního systému přístupový kód k platební kartě a tím dojde následně ke zpřístupnění financí na účtu klienta, oběti, lze hovořit o počítačové kriminalitě.

Obrázek 7: Libanonská smyčka – zařízení k zadržení platební karty[48]

Cash Trapping

Obdobou výše zmíněné fyzické trestné činnosti s kombinací počítačové trestné činnosti je Cash Trapping, což doslova znamená past na hotovost. Jedná se o nainstalované zařízení do slotu bankomatů v místě pro výdej hotovosti. Toto zařízení je uzpůsobeno tomu, aby zachytilo nebo skrylo část nebo celou sumu z vydávaných papírových bankovek. Jakmile se poškozený od bankomatu vzdálí, pachatel této chvilky využije a skrytou nebo lapenou hotovost si vyzvedne.[49]

[47] TŮMA, O., 2013. *Dávejte si pozor na platební kartu! Podvodníci jsou stále vynalézavější*. In: Peníze.cz [online]. [cit. 2022-01-05]. Dostupné z WWW*:* <https://www.penize.cz/platebni-karty/248343-davejte-si-pozor-na-platebni-kartu!- podvodnici-jsou-stale-vynalezavejsi>.
[48] Zdroj: iDnes.cz, 2007.
[49] KREBS, B., 2012. *Beware Card- and Cash-Trapping at the ATM*. In: Krebs on security [online]. [cit. 2022-01-05]. Dostupné z WWW: <https://krebsonsecurity.com/2012/11/beware-card-and-cash-trapping-at-the-atm/>.

4 PREVENTIVNÍ OPATŘENÍ PROTI POČÍTAČOVÉ KRIMINALITĚ

Jak uvádí Zapletal, jedním z nejdůležitějších prostředků v boji proti počítačové kriminalitě je především proaktivní přístup a plánování preventivních opatření, která by zamezila nebo alespoň zpomalila rostoucí tlak v trestné činnosti počítačové kriminality.

Podle Zapletala je celý proces v komplexní povaze kyberprostoru velmi složitý a nemůže být jednorázový. Je zapotřebí mít na zřeteli, že prevence je mnohem účinnější a ve výsledku i efektivnější z dlouhodobého hlediska než represe.

Prevenci kriminality lze definovat jako cílenou snahu o eliminaci trestné činnosti ještě před zahájením nebo před jejím pokračováním. Pro dosažení kýžených výsledků je nutné nastavit takové podmínky, které budou implementovány do praxe na úrovni právních opatření, organizačních a technických opatření a v neposlední řadě osvětové úrovni.[50]

4.1 Právní opatření

Bez zavádění a vytváření patřičných legislativních opatření, která budou v souladu s vývojem kybernetické kriminality nelze úspěšně dosáhnout snížení této trestné činnosti, a proto právní opatření představují klíčový prvek nutný pro boj proti různým formám kybernetické kriminality v rovině represe a prevence.

Podle Šámala nelze pachatele počítačové trestné činnosti účinně postihovat, pokud budou chybět účinné legislativní nástroje vyplývající z problematiky počítačové kriminality.

Do budoucna je nutné předpokládat, že s narůstající dynamikou vývoje oblasti počítačové kriminality bude nutné stejně tak dynamické přizpůsobení ve změnách zákonů a v zavádění nových legislativních nástrojů. Mezi úskalí v procesu zavádění nových právních opatření pak řadí pomalý legislativní proces. Trestní zákoník v současné době plní jak preventivní, tak represivní funkci, což je činnost, která splňuje jednu ze základních funkcí trestního práva.[51]

[50]ZAPLETAL, J. a kol. *Prevence kriminality. 2*. přepracované vydání. Praha: Policejní akademie ČR, *2005, s. 8.*
[51] ŠÁMAL, P. a kol. *Trestní právo hmotné.* 8. přepracované vydání. Praha: Wolters Kluwer, 2016, s. 35.

4.2 Systémová opatření organizace a institucionalizace

V roce 2010 schválila Vláda České republiky (dále jen „vláda“) usnesení č. 205 o řešení problematiky kybernetické problematiky České republiky.[52]

V rámci tohoto usnesení, bylo v bodu II ustaveno Ministerstvo vnitra ČR gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast.

V bodu III bylo dále Ministerstvu vnitra uloženo:
„1. koordinovat činnost ostatních státních institucí v oblasti zajišťování kybernetické bezpečnosti,
2. koordinovat zastupování České republiky v otázkách kybernetické bezpečnosti na mezinárodních fórech, včetně účasti státních orgánů na činnosti příslušných mezinárodních organizací,
3. do 30. dubna 2010 předložit vládě ke schválení statut meziresortní koordinační rady pro kybernetickou bezpečnost,
4. do 15. prosince 2010 předložit vládě strategii pro oblast kybernetické bezpečnosti,
5. nejpozději k 31. prosinci 2010 zahájit zajišťování provozu vládního pracoviště CSIRT (Computer Security Incident Response Team).“[53]

Na základě usnesení č. 205 bylo téhož roku vládou schváleno usnesení č. 380 o zřízení Meziresortní koordinační rady pro oblast kybernetické bezpečnosti.[54]

Dále Ministerstvo vnitra podepsalo dne 9. prosince 2010 se zájmovým sdružením právnických osob z oblasti doménových jmen na trhu služeb elektronických komunikací CZ.NIC, jakožto správcem domény CZ, Memorandum o Computer Security Incident Response Team České republiky[55] (dále jen „Memorandum“). Memorandem převzalo sdružení CZ.NIC agendu národního CSIRT a zavázalo se k jejímu dalšímu budování a rozvíjení.

Na podzim roku 2011 bylo vládou přijato usnesení č. 781 o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň

[52] ČESKO. VLÁDA *Usnesení Vlády ČR č. 205 ze dne 15. března 2010 o řešení problematiky kybernetické bezpečnosti České republiky*.
[53] ČESKO. VLÁDA *Usnesení Vlády ČR č. 205 ze dne 15. března 2010 o řešení problematiky kybernetické bezpečnosti České republiky*.
[54] ČESKO. VLÁDA *Usnesení Vlády ČR č. 380 ze dne 24. května 2010 o zřízení Meziresortní koordinační rady pro oblast kybernetické bezpečnosti*.
[55] *Memorandum o Computer Security* Incident Response Team České republiky. CZ.NIC [online]. 9. prosince 2010 [cit. 2022-01-10].

národní autoritou pro tuto oblast,[56] který tak v dané oblasti nahradil činnost Ministerstva vnitra ČR. V rámci tohoto usnesení byla rovněž na základě bodu II zřízena Rada pro kybernetickou bezpečnost coby poradní orgán předsedy vlády pro oblast kybernetické bezpečnosti a na základě bodu III mj. schválen vznik Národního centra kybernetické bezpečnosti, jako součásti Národního bezpečnostního úřadu. Jedním z úkolů NBÚ dle bodu IV usnesení bylo „vybudovat do 31. prosince 2015 plně funkční Národní centrum kybernetické bezpečnosti a jako jeho součást vládní koordinační místo pro okamžitou reakci na počítačové incidenty (vládní CERT – Computer Emergency Response Team).“[57]

Národní centrum kybernetické bezpečnosti bylo oficiálně otevřeno v Brně dne 13. května 2014.[58]

V červnu roku 2013 byl vládě předložen návrh zákona o kybernetické bezpečnosti (dále jen „ZoKB“) z „dílny“ NBÚ. Návrh prošel legislativním procesem bez větších obtíží a dne 29. srpna 2014 vstoupil ZoKB v platnost s účinností od 1. ledna 2015.

V souladu s požadavky ZoKB (§ 17 a násl. ZoKB) byl v létě roku 2015 vybrán provozovatel Národního CERT, kterým se stalo sdružení CZ.NIC.[59]

Rozdíl mezi národním a vládním CERT je vymezen v ZoKB (§ 17 a § 20 ZoKB). Nicméně zjednodušeně lze tento rozdíl vnímat tak, že „vládní CERT je určen pro řešení bezpečnostních incidentů v počítačových sítích státní správy, kritické informační infrastruktury a významných informačních systémů dle zákona o kybernetické bezpečnosti. Národní CERT je bezpečnostní tým pro koordinaci řešení ostatních bezpečnostních incidentů v počítačových sítích provozovaných v České republice.“[60]

Na obdobném principu poté fungují i jednotlivé CSIRT týmy, tyto ovšem „vznikají na úrovni jednotlivých organizací, přičemž jde jak o organizace, které

[56] ČESKO. VLÁDA *Usnesení Vlády ČR č. 781 ze dne 19. října 2011 č. 781 o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast*.
[57] ČESKO. VLÁDA *Bod IV odst. 2 písm. c) Usnesení Vlády ČR č. 781 ze dne 19. října 2011*.
[58] *V Brně bylo otevřeno Národní centrum kybernetické bezpečnosti*. Krajský úřad Jihomoravského kraje [online]. Publikováno 13. května 2014.[cit. 2022-01-10]. Dostupné z WWW: <https://www.kr-jihomoravsky.cz/Default.aspx?ID=230019&TypeID=2>.
[59] *NBÚ vybral provozovatele národního CERT (CSIRT.CZ), je jím CZ.NIC*. GovCERT [online]. Publikováno 27. srpna 2015 [cit. 2022-01-10]. Dostupné z WWW: <https://www.nbu.cz/cs/aktualne/820-621-nbu-vybral-provozovatele-narodniho-cert-csirtcz-je-jim-cznic/>.
[60] *NBÚ vybral provozovatele národního CERT (CSIRT.CZ), je jím CZ.NIC*. GovCERT [online]. Publikováno 27. srpna 2015 [cit. 2022-01-10]. Dostupné z WWW: <https://www.nbu.cz/cs/aktualne/820-621-nbu-vybral-provozovatele-narodniho-cert-csirtcz-je-jim-cznic/>.

zprostředkovávají chod internetu (ISP, poskytovatelé služeb a obsahu), tak i o organizace, které prostředí internetu používají ke své hlavní činnosti (např. banky).“[61]

4.3 Technická a technologická opatření

Opatření tohoto typu se odvíjí od budoucího vývoje v oblasti informačních technologií a korespondují s hlavními cíli a myšlenkami národního programu kybernetické bezpečnosti. Je vcelku logické, že tato opatření budou také závislá nejenom na technologických požadavcích, které budou muset splňovat moderní trendy v ICT tak, aby složky prevence a represe udržely takzvaně krok s druhou stranou, přičemž se druhou stranou myslí především představitelé pachatelů trestné činnosti v oblasti počítačové kriminality.

Nesporně důležitou roli v oblasti technického a technologického opatření hraje finanční stránka věci, a proto i zde je nutné v rámci prevence investovat do podpůrných preventivních programů jakými je například Bezpečný internet.

4.4 Osvěta a vzdělávací opatření

Osvětová činnost napříč celému spektru obyvatelstva je snad nejsnadnějším nástrojem pro snížení, případně eliminaci patologických jevů a trestné činnosti počítačové kriminality.

Zvyšování bezpečnostního povědomí a počítačové gramotnosti, zejména u starších lidí, lze dosáhnout kýžených výsledků, zvláště pak, když dojde ke vzájemné interakci zúčastněných stran, přičemž nedílnou součástí tohoto osvětového opatření hraje Policie ČR ve formě pořádání přednášek, workshopů, nebo výukových bloků zaměřených na kybernetickou bezpečnost a prevenci počítačové kriminality.[62]

[61] KROPÁČOVÁ, A. *CERT/CSIRT týmy a jejich role*. ROOT.CZ [online]. Publikováno 6. května 2013. [cit. 2022-01-10]. Dostupné z WWW: <https://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/>.
[62] RANDÁKOVÁ, R. #SayNo! - *Celoevropská kampaň proti zneužívání dětí online*. Policie ČR [online]. Policie ČR, © 2020, publikováno 19. června 2017. [vid. 2022-02-09]. Dostupné na WWW: <https://www.policie.cz/clanek/sayno-celoevropska-kampan-proti-internetovemu-sexualnimu-natlaku-a-vydirani-deti-rekni-ne.aspx>.

5 DOTAZNÍKOVÉ ŠETŘENÍ

Na základě Projektu a zadání bakalářské práce, jejímž cílem je analýza situace bankovní počítačové kriminality proběhly v termínech od 01. 11. 2021 do 21. 03. 2022 činnosti, které vedly k vyhotovení této praktické části bakalářské práce sestávající se z průzkumu problematiky počítačové kriminality.

Procesní kroky připraveného průzkumu byly zrealizovány ve formě dotazníkového šetření, které proběhlo v lokalitě města Brna v osmi subjektech poskytujících bankovní služby pro svoje klienty. V přípravné fázi bylo za účelem spolupráce na tomto průzkumu osloveno 10 bank a bankovních institucí, ovšem spolupráci na tomto projektu odsouhlasilo pouze 8 z těchto 10 subjektů. Jednou z podmínek ze strany spolupracujících bankovních subjektů, které by umožnily realizaci tohoto průzkumu byla podmínka anonymity klientů a identity bankovních subjektů. Vzhledem k této skutečnosti nebudou uváděna žádná jména konkrétních osob a pracovní zařazení, ani názvy bankovních subjektů a celá praktická část bude vedena pouze na úrovni obecného popisu procesů, postupů, analýz údajů od anonymních respondentů a v obecné rovině také návrhů opatření, bez konkrétních identifikací směřovaných k jednotlivým bankovním subjektům.

6 METODOLOGIE PRŮZKUMU

Za účelem dosažitelnosti předem stanoveného cíle této bakalářské práce bylo velmi důležité stanovit metodu, která by co nejvhodnějším způsobem odpovídala splnění tohoto cíle, nebo se alespoň co nejvíce přibližovala potenciálním výstupům, které by mohly stanovené cíle obsahově doplňovat.

V rámci posuzovaných metod a technik výzkumné části práce bylo nutné zvolit a použít metodologii průzkumu jako efektivní nástroj pro získání, analýzu a následné vyhodnocení informací, potřebných pro sestavení alespoň dílčích závěrů ke stanovenému cíli práce.

Posouzením výhod a nevýhod vědeckovýzkumných metod, které lze rozdělit na kvalitativní a kvantitativní, přičemž kvalitativní metody posuzují především formální data uváděná ve zdrojích teoretických a interpretují tato data z pohledu zkoumaných subjektů, kdy dochází k určité zakřivenosti indukce díky přejímání perspektivy, kterou vnímá samotný výzkumník subjektivně, zatímco metody kvantitativní vyhodnocují soubor získaných údajů z pohledu striktně racionalizovaného se zaměřením na matematickou a statistickou analýzu těchto dat získaných od samotných dotazovaných subjektů, které na zkoumanou problematiku odpovídají bez zkreslování perspektivy a ovlivňování z vnějšího prostředí. V případě vlastních odpovědí nejsou dotazované subjekty manipulováni a na danou problematiku odpovídají více, či méně pod vlivem vlastních zkušeností a znalostí.

Výhodou kvantitativních výzkumných metod je možnost validace a testování zkoumaných subjektů a získaných dat, následná interpretace těchto dat na základě analýzy, se zaměřením na zkoumání většího počtu respondentů s poměrně rychlým a specificky zaměřeným sběrem dat.

Další výhodou kvalitativních metod je především jejich zaměřenost na zkoumání dané problematiky v teoretické rovině a v obecné šíři.

Vzhledem k tomu, že cílem této práce je posoudit stav problematiky kybernetické kriminality v současné populaci zkoumaných subjektů, což u kvalitativních výzkumných metod lze pouze v omezené míře, použité metody této práce vychází z pravidel kvantitativních vědeckovýzkumných metod.

Z pohledu technického řešení kvantitativních metod průzkumu respondentů se jeví jako nejschůdnějším a nejrelevantnějším nástrojem metoda dotazníková, která umožňuje v poměrně krátkém časovém úseku a s minimálním personálním obsazením, získat velké množství dat od většího počtu dotazovaných.

Hlavním kritériem volby vhodného nástroje byl tedy požadavek na rychlost, vysoký počet oslovených respondentů, vysoký poměr získaných údajů k relevantnosti a validitě ve vztahu k užitné hodnotě, s ohledem na stanovený cíl této práce.

Tato kritéria splňuje dotazníkové šetření a sběr údajů od dotazovaných respondentů, následná analýza těchto údajů, vyhodnocení pomocí univariční analýzy, která ze získaných údajů vytváří ucelený statistický výsledek hodnot dané oblasti, a na to navazující interpretace dílčích a celkových závěrů.

6.1 Fáze průzkumu

Průzkum, který je marginální součástí praktické části této bakalářské práce, bylo zapotřebí ve vztahu ke stanovenému cíli této práce, předem naplánovat a před samotnou realizací sestavit procesní kroky, které lze rozdělit do následujících fází, přičemž každá fáze tohoto průzkumu je dále rozšířená o popisnou část, ve které jsou popsané jednotlivé postupy používané v každé fázi tohoto průzkumu.

V průzkumu se jedná o tyto čtyři základní fáze:

- **Přípravná fáze** – stanovení cíle, metod, harmonogramu, technik a plán proveditelnosti průzkumu.
- **Realizační fáze** – tisk dotazníků, komunikace se spolupracujícími subjekty, distribuce dotazníků, sběr dat, redistribuce odevzdaných dotazníků.
- **Analytická a vyhodnocovací fáze** – zpracování a vyhodnocení získaných údajů z dotazníkového šetření.
- **Interpretační fáze** – stanovení závěrů na základě analýzy a vyhodnocení a následné publikování těchto údajů.

6.1.1 Přípravná fáze

V každém, tedy i v tomto průzkumu je pro konečný úspěch nejdůležitější fáze přípravná, která v sobě zahrnuje následující procesní kroky:

- Stanovení cílů průzkumu.
- Výběr vědeckovýzkumné metody průzkumu.
- Výběr vhodného nástroje pro splnění cíle průzkumu.
- Sestavení harmonogramu a časového plánu procesních kroků průzkumu.
- Analýza faktorů ovlivňujících proces průzkumu.
- Analýza postupů a vyhodnocení použitých nástrojů.

Stanovení cílů průzkumu:

Z charakteru teoretické části této práce vyplývá, že stěžejním tématem průzkumu je problematika počítačové, kybernetické kriminality, trestná činnost a její dopady na občany, uživatele internetu, a jako hlavní bod zkoumání je zde stanoven průzkum specifické oblasti této trestné činnosti, kterou je bankovní počítačová kriminalita.

Cílem průzkumu je zaměřit se na získání co největšího množství údajů v krátkém časovém úseku od velkého počtu respondentů, přičemž hlavním nástrojem sběru dat bude dotazníkové šetření, následná analýza a vyhodnocení s interpretací získaných údajů. Hlavní obsahové zaměření otázek v dotazníku je cíleno na praktické zkušenosti oslovených respondentů a jejich znalost kybernetické kriminality ve specifických oblastech používání elektronických bankovních nástrojů a dalších procesů ve spojení s bankovními operacemi těchto oslovených respondentů, majitelů bankovních účtů a ostatních bankovních produktů.

Nedílnou součástí stanoveného cíle průzkumu je také sestavení návrhu opatření pro zamezení nebo snížení výskytu počítačové kriminality, která se může objevovat u majitelů bankovních produktů v souvislosti s nedostatky a znalostmi prostředí bankovních operací.

Výběr vědeckovýzkumné metody průzkumu:

Pro úspěšné dosažení stanoveného cíle této bakalářské práce a jejího průzkumu není vhodné použití kvalitativní metody průzkumu, a z tohoto důvodu se jako nejvýhodnější alternativa jeví forma kvantitativní metody sběru a analýzy dat. Výhody

a nevýhody jednotlivých druhů vědeckovýzkumných metod jsou popsány v kapitole 6. Metodologie průzkumu, této bakalářské práce.

Výběr vhodného nástroje pro splnění cíle průzkumu.

Pro účely tohoto průzkumu se jako nejvhodnější nástroj jeví použití kvantitativního metodického nástroje dotazníkového šetření, což umožňuje pomocí 15 otázek v dotazníku získat ucelený soubor dat se stejným zaměřením a specifickou sadou otázek odpovídající formě a předpokládanému cíli průzkumu. Tato zaměřenost na specifické projevy bankovní počítačové kriminality vyžaduje, aby byl samotný průzkum realizovaný ve specifickém prostředí, z čehož vyplývá, že průzkum probíhal v prostorách bankovních institucí ve formě fyzicky dostupného dotazníku, který respondenti na základě dobrovolnosti vyplňovali na sběrném místě, případně si jej mohli odnést a později odevzdat do předem připravené sběrné nádoby. Aby u respondentů nedocházelo k obavám a pocitu ztráty identity, celý dotazníkový průzkum probíhal na principech dobrovolnosti, anonymity a zainteresovanosti, přičemž byla touto cestou zajištěna eliminace možnosti zneužití poskytovaných údajů a respondenti nebyli vystaveni žádnému nátlaku nebo manipulaci, která by předcházela nebo provázela dotazníkové šetření.

Sestavení harmonogramu a časového plánu procesních kroků průzkumu:

Jednou z hlavních částí přípravné fáze průzkumu byla část plánování procesních kroků a vymezení těchto postupů v časové ose průzkumu.

Výsledkem plánování procesů průzkumu je plán stanovených termínů a činností, které se v průzkumu realizovaly v následujícím časovém období:

1. **01. 11. – 31. 12. 2021:** sběr a sestavování informací o problematice počítačové kriminality a bankovních elektronických operacích, bankovní počítačové kriminalitě a dalších souvislostech, vyplývajících z obsahu teoretické části této bakalářské práce. Následné vyhodnocení získaných informací, a komparace informací s tříděním relevantních informací, potřebných pro další procesní kroky na sebe navazujících v přípravné fázi projektu.
2. **01. 01. – 16. 01. 2022**: sestavení dotazníku na základě principů kvantitativně vědeckovýzkumných metod a pravidel tvorby dotazníkového šetření. Grafická úprava dotazníku, tisk, sestavení listinné podoby dotazníku,

příprava pro distribuci. Výroba sběrných nádob pro odevzdání vyplněných dotazníků.

3. **17. 01. – 20. 01. 2022:** oslovení představitelů bankovních institucí v lokalitě město Brno a představení plánovaného průzkumu dané problematiky bankovní počítačové kriminality. V rámci oslovení došlo také k žádosti o možnost realizace tohoto průzkumu v prostorách těchto bankovních institucí. Z 10 různých oslovených bankovních institucí v Brně souhlasilo 8 oslovených bankovních institucí s realizací tohoto dotazníkového šetření. Všechny instituce trvaly na podmínce anonymity na straně klienta i na jejich straně, z tohoto důvodu nebude v této práci uveden název žádné banky ani bankovní instituce, která se na dotazníkovém šetření podílela.
4. **21. 01. 2022:** doručení dotazníků a sběrné nádoby do předem vyčleněných prostor v klientské zóně u těch bank a bankovních institucí, které souhlasily s realizací dotazníkového průzkumu.
5. **24. 01. – 28. 02. 2022:** realizace fáze sběru vyplněných dotazníků do zapečetěných sběrných nádob v prostorách bank a bankovních institucí.
6. **01. 03. 2022:** ukončení fáze sběru dat a redistribuce zapečetěných sběrných nádob do místa, kde došlo k otevření a výběru odevzdaných dotazníků. Následná vizuální kontrola a přetřídění vhozených dotazníků od jiných dokladů a předmětů, které byly do zapečetěných sběrných nádob vhozeny.
7. **01. 03. – 20. 03. 2022:** zpracování agendy vstupních dat získaných z odevzdaných dotazníků, analýza údajů, elektronické zpracování informací, matematické zpracování získaných údajů, zpracování grafické a tabulkové podoby získaných a vyhodnocených dat, interpretace výsledků v písemné podobě praktické části bakalářské práce, závěr a návrhy opatření, která vyplývají ze získaných údajů respondentů.
8. **21. 03. 2022:** zakončení procesních kroků praktické části průzkumu.

Analýza faktorů ovlivňujících proces průzkumu:

Stěžejními faktory průzkumu byly procesní znaky, které pro úspěšnost splnění cíle této práce hrají velmi významnou roli. Jedná se o podmínky zpracování průzkumu z hlediska:

Reliability – jde o faktor, který z pohledu statistiky udává spolehlivost odpovědí respondentů a je závislý na psychologických vlastnostech a lidském chování jednotlivých respondentů.

Validity – neboli pravdivosti odpovědí ze strany respondentů, přičemž míra validity je individuálním měřítkem ochoty odpovídat pravdivě a může být také ovlivněna nedostatkem znalostí dané problematiky. Tuto znalost mohou mít respondenti různou. Snaha vytvořit co nejvíce srozumitelnou a jednoduchou skladbu otázek s eliminací odborné terminologie, může míru validity zvýšit a při sestavování dotazníku byl na tuto skutečnost kladen obzvláště velký důraz.

Vědeckého přístupu – jde o faktor, který je požadovaný z důvodu přesahu teoretického základu této bakalářské práce do praktického využití a z pohledu vědeckého procesu mohou být výsledky průzkumu využity v další implementaci do různých odborných a vědeckých oborů, ať již z kriminalistiky, psychologie, nebo bankovnictví a informačních technologií.

Analýza postupů a vyhodnocení použitých nástrojů:

Účelově nejdůležitějším krokem v přípravné a následně v realizační fázi průzkumu je analýza, tedy rozbor, získaných dat a vyhodnocení těchto dat z hlediska statistického a kvantitativního. V návaznosti na to se jako jeden z nejdostupnějších nástrojů pro analýzu jeví aplikace MS Excel, ve které proběhla kompletní analytická část údajů a vyhodnocení ve formě tabulek a grafů, které slouží k volné interpretaci výsledků průzkumu.

6.1.2 Realizační fáze

Poté, co v přípravné fázi proběhly procesní kroky nutné pro zahájení druhé fáze průzkumu, fáze realizace, bylo nutné zahájit postupy, které by korespondovaly s plánovanými procesními kroky této druhé fáze průzkumu.

Realizace tohoto průzkumu byla velmi náročná především z důvodu nedostatku personálních zdrojů a v praxi celá realizační fáze proběhla tak, že všechny činnosti a procesní kroky jsem realizoval zcela sám.

Postupoval jsem podle plánů a postupů, které jsou uvedeny v harmonogramu a časovém plánu procesních kroků průzkumu v popisu přípravné fáze. Díky předem

stanovenému plánu postupu se podařilo ke dni 21. 03. 2022 zrealizovat plán průzkumu dotazníkovou metodou.

6.1.3 Analytická a vyhodnocovací fáze

Pro účely vyhodnocení získaných údajů byla v průzkumu použitá metoda univariační analýzy, která spočívá ve vyhodnocení údajů dodaných respondenty v rovině racionálních výpočtů pomocí matematických součtů odpovědí jednotlivých respondentů u jednotlivých otázek a následně se tyto součty v kontextu s porovnáním procentuálního vztahu k celku, popřípadě ke skupině odpovídajících vyhodnocuje a interpretuje každá otázka samostatně. Univariační analýza nepředpokládá vztahové záležitosti k ostatním proměnným tak, jak je tomu například u jiné metody, bivariační analýzy. Z důvodu přehlednosti a jednoduchosti a také z důvodu nedostatku prostoru pro detailnější rozbor získaných údajů odpovídá tato metoda charakteru cíle této bakalářské práce.

6.1.4 Interpretační fáze

Výstupy a stanovení závěrů na základě analýzy a vyhodnocení a následné publikování těchto údajů jsou nedílnou součástí praktické části této bakalářské práce a svým přesahem zasahují do praxe v oblasti bankovnictví, kriminalistiky a informačních technologií. Výstupy z tohoto průzkumu lze také interpretovat na poli výsledků práce z hlediska sociologie a psychologie osobnosti.

6.2 Dotazníkové šetření

Anonymní dotazníkové šetření z oblasti počítačové kriminality probíhalo v podobě dotazníku, který obsahuje 15 otázek zaměřených na danou problematiku a je specificky zacílený na klientelu bank a bankovních institucí, které poskytují produkty a služby, zahrnující potenciální riziko hrozby vzniku některého z projevů počítačové kriminality.

Součástí této bakalářské práce je v příloze doložený vzor používaného dotazníku – příloha č. II – „Dotazníkové šetření z oblasti počítačové kriminality“.

Průběh dotazníkového šetření byl předem plánovaný a jeho samotná realizace korespondovala s časovým a organizačním harmonogramem procesních kroků, které byly v přípravné fázi zdokumentovány.

Popis dotazníkového šetření

Zadavatel:	Dotazníkové šetření proběhlo na základě Projektu a zadání BP pod vedením RNDr. Růženy Ferebauerové
Průzkum provedl:	Petr Maloň, DiS.
Průzkum vyhodnotil:	Petr Maloň, DiS.
Místo konání dotazníkového šetření:	8 subjektů-banky a bankovní instituce v lokalitě města Brna
Termín stavby dotazníku:	01. 01. – 16. 01. 2022
Termín tisku dotazníků:	01. 01. – 16. 01. 2022
Termín distribuce dotazníků:	21. 01. 2022
Termín realizace sběru dat:	24. 01. – 28. 02. 2022
Termín ukončení sběru dat:	01. 03. 2022
Zpracování, analýzy a vyhodnocení dat:	01. 03. – 20. 03. 2022
Ukončení projektu – dotazníkové šetření:	21. 03. 2022
Metoda průzkumu:	kvantitativní průzkum
Nástroj průzkumu:	dotazníkové šetření (15 otázek)
Výstup a vyhodnocení:	kvantitativní metoda zpracování získaných údajů, analýza a vyhodnocení
Celkový počet vystavených dotazníků:	2000
Celkový počet vyplněných:	1426
Referenční vzorek respondentů:	674 žen, 728 mužů, 24 neuvedlo

7 INTERPRETACE VÝSLEDKŮ PRŮZKUMU

Výsledky analýzy získaných dat od respondentů lze interpretovat různými způsoby, přičemž pro účely této bakalářské práce se jeví nejvhodnější způsob popisný a informativní, ve kterém jsou interpretovány získané údaje ve formě univariační analýzy a souhrnu statistických údajů s krátkou prezentací výskytu nejčastějších, případně nejvyšších hodnot z naměřeného celku nebo z části celku odpovědí respondentů.

Každá otázka je zde reprezentována v tabulkovém vyjádření číselných údajů a pro lepší orientaci je nedílnou součástí interpretačních pravidel použitá podoba ztvárněná v grafu, přičemž každá otázka má svoji popisnou část.

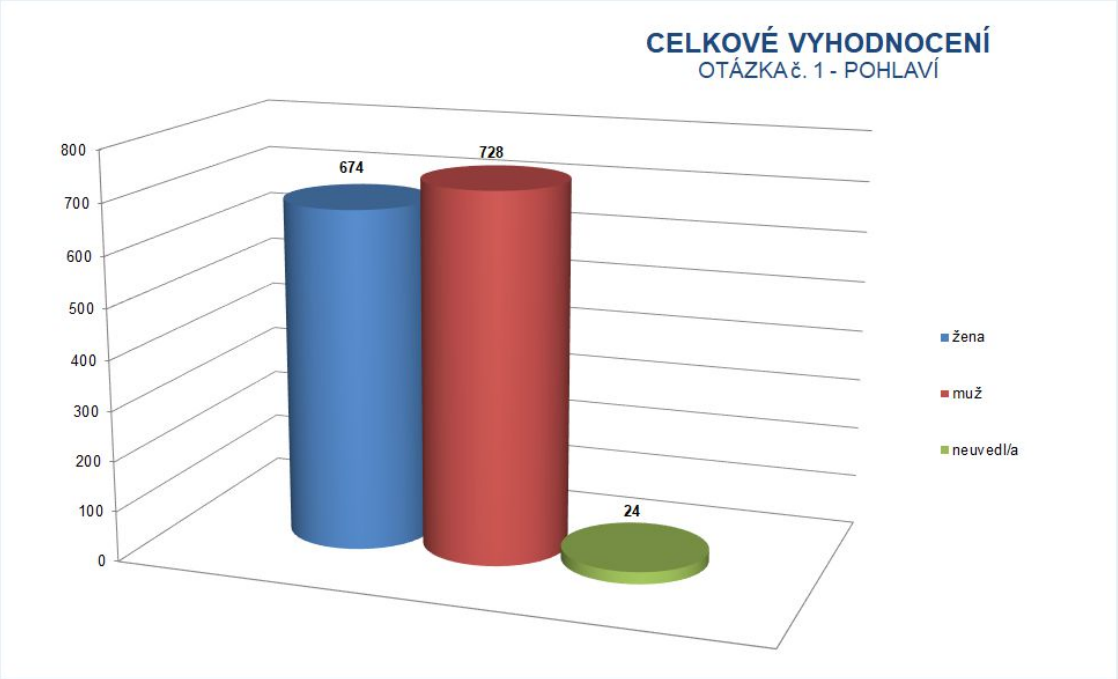
Otázka č. 1 – POHLAVÍ

Z celkového počtu respondentů, kteří se dobrovolně zúčastnili anonymního dotazníkového šetření odpovídalo 51 % mužů a 47 % žen. Jedná se o vyvážený poměr, přičemž 2 % respondentů svoje pohlaví neuvedlo.

Tabulka 1 - POHLAVÍ[63]

DOTAZNÍKOVÉ ŠETŘENÍ Z OBLASTI POČÍTAČOVÉ KRIMINALITY				
1.	Pohlaví		POČET ODPOVĚDÍ	% z 1426
	a)	žena	674	47
	b)	muž	728	51
	c)	neuvedl/a	24	2
			1426	100

Graf 2 - POHLAVÍ[64]



[63] Vlastní zdroj

[64] Vlastní zdroj

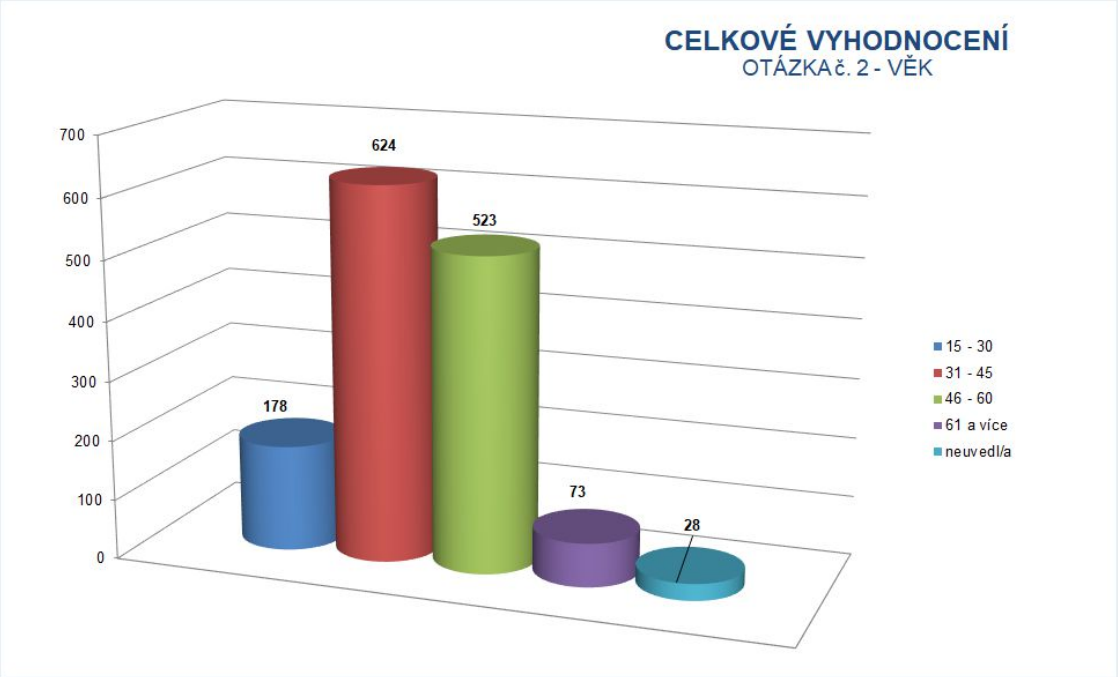
Otázka č. 2 – VĚK

Z dostupných výsledků vyplývá, že největší zájem o vyplnění dotazníků byl v kategorii 31-45 let, a druhou nejpočetnější věkovou skupinu tvořili respondenti ve věku mezi 46-60 lety. Oproti tomu nejmenší zájem projevili respondenti ve věku 61 a více a 2 % respondentů svůj věk neuvedlo.

Tabulka 2- VĚK[65]

DOTAZNÍKOVÉ ŠETŘENÍ Z OBLASTI POČÍTAČOVÉ KRIMINALITY				
2.	**Věk**		**POČET ODPOVĚDÍ**	**% z 1426**
	a)	15 - 30	178	12
	b)	31 - 45	624	44
	c)	46 - 60	523	37
	d)	61 a více	73	5
	f)	**neuvedl/a**	28	2
			1426	**100**

Graf 3 - VĚK[66]



[65] Vlastní zdroj

[66] Vlastní zdroj

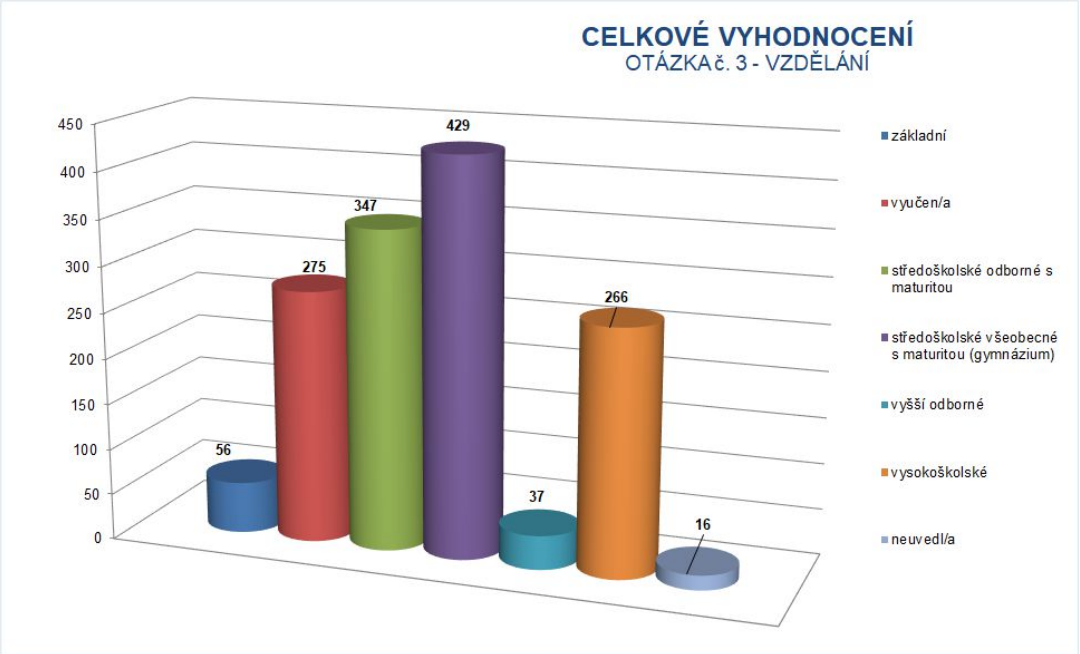
Otázka č. 3 – VZDĚLÁNÍ

Z celkového počtu respondentů, kteří se průzkumu zúčastnili byl největší počet středoškoláků s maturitou se všeobecným zaměřením gymnaziálně vzdělaných, což činilo 30 % z celku, na druhém místě projevili o průzkum zájem respondenti s odborným vzděláním s maturitou, což bylo 24 % a o třetí místo s procentuálním vyjádřením 19 % se podělili respondenti s vyučením a vysokoškolským vzděláním. Z výsledků početního zastoupení respondentů v této otázce je patrné, která vzdělanostní skupina má nejčastěji zájem o zkoumanou problematiku.

Tabulka 3 - VZDĚLÁNÍ[67]

DOTAZNÍKOVÉ ŠETŘENÍ Z OBLASTI POČÍTAČOVÉ KRIMINALITY				
3.	**Vzdělání**		**POČET ODPOVĚDÍ**	**% z 1426**
	a)	základní	56	4
	b)	vyučen/a	275	19
	c)	středoškolské odborné s maturitou	347	24
	d)	středoškolské všeobecné s maturitou (gymnázium)	429	30
	e)	vyšší odborné	37	3
	f)	vysokoškolské	266	19
	g)	**neuvedl/a**	16	1
			1426	**100**

Graf 4 - VZDĚLÁNÍ[68]



[67] Vlastní zdroj

[68] Vlastní zdroj

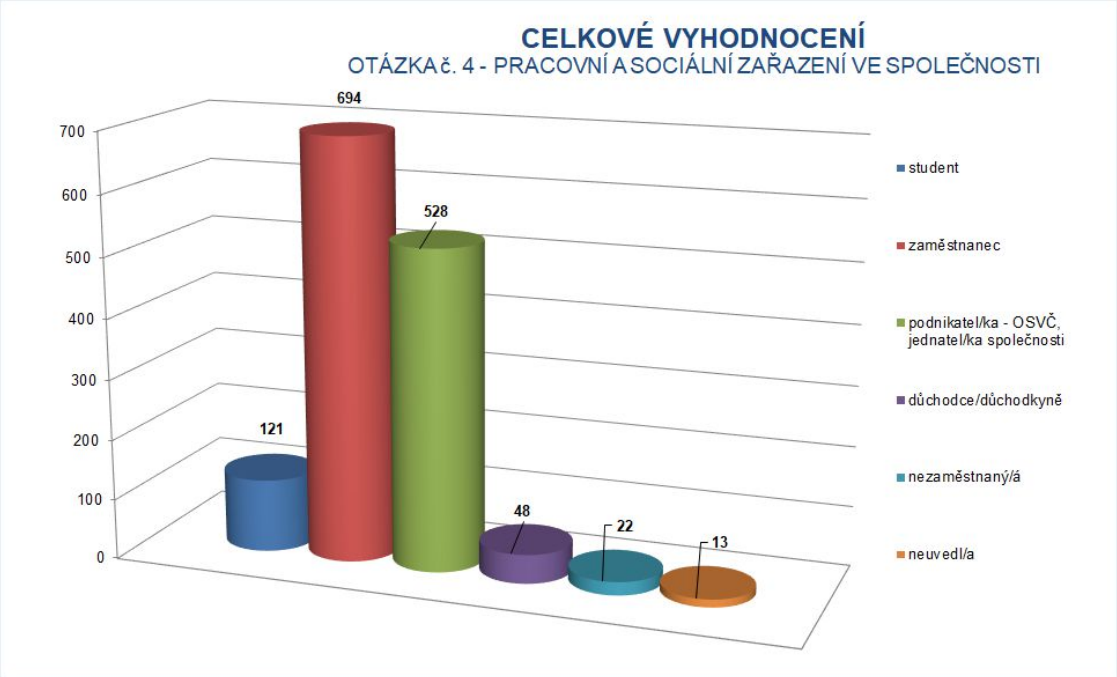
Otázka č. 4 – PRACOVNÍ A SOCIÁLNÍ ZAŘAZENÍ VE SPOLEČNOSTI

Skoro polovinu respondentů průzkumu tvoří se 49 % zaměstnanci, na druhém místě se průzkumu zúčastnili respondenti z kategorie podnikatel/ka, OSVČ, jednatel/ka společnosti ve 37 % a třetí pozici respondentů obsadili studenti s 8 % početnosti.

Tabulka 4 - PRACOVNÍ A SOCIÁLNÍ ZAŘAZENÍ VE SPOLEČNOSTI[69]

DOTAZNÍKOVÉ ŠETŘENÍ Z OBLASTI POČÍTAČOVÉ KRIMINALITY				
4.	**Pracovní a sociální zařazení ve společnosti**		**POČET ODPOVĚDÍ**	**% z 1426**
	a)	student	121	8
	b)	zaměstnanec	694	49
	c)	podnikatel/ka - OSVČ, jednatel/ka společnosti	528	37
	d)	důchodce/důchodkyně	48	3
	e)	nezaměstnaný/á	22	2
	f)	**neuvedl/a**	13	1
			1426	**100**

Graf 5 - PRACOVNÍ A SOCIÁLNÍ ZAŘAZENÍ VE SPOLEČNOSTI[70]



[69] Vlastní zdroj

[70] Vlastní zdroj

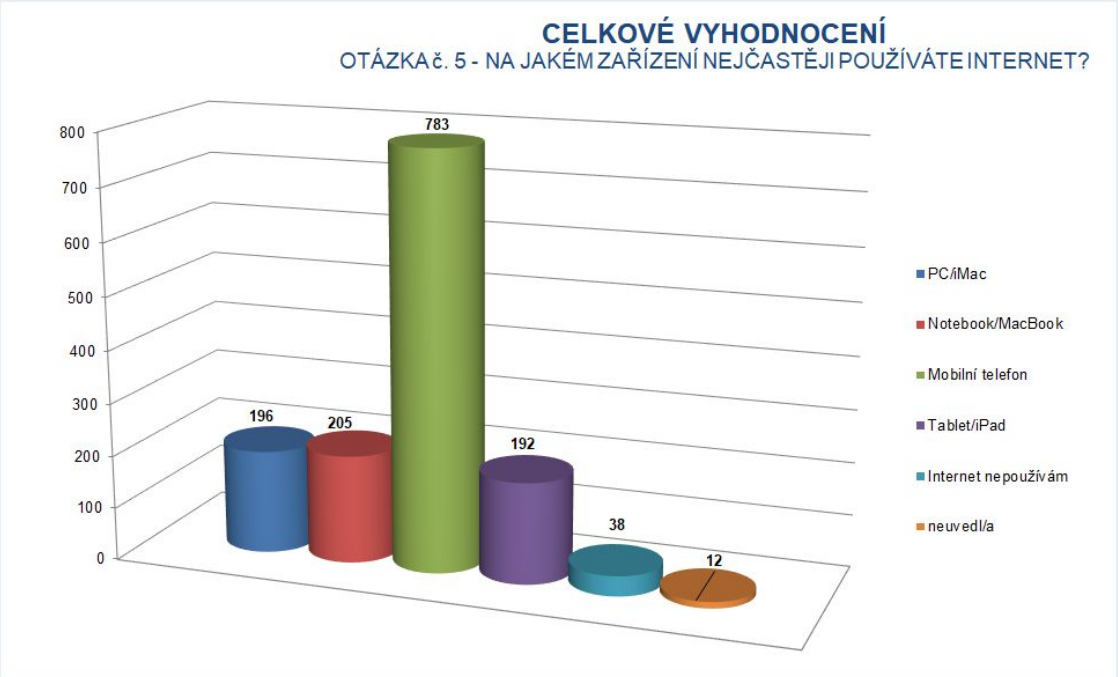
Otázka č. 5 – Na jakém zařízení nejčastěji používáte internet?

Pro práci s internetem používá 55 % respondentů nejčastěji mobil, o druhé nejčastější používání se dělí se 14 % uživatelé PC/iMac s uživateli Notebook/MacBook a třetím nejčastějším zařízením používaným pro práci s internetem je ve 13 % Tablet/iPad.

Tabulka 5 - Na jakém zařízení nejčastěji používáte internet?[71]

DOTAZNÍKOVÉ ŠETŘENÍ Z OBLASTI POČÍTAČOVÉ KRIMINALITY				
5.	**Na jakém zařízení nejčastěji používáte internet?**		**POČET ODPOVĚDÍ**	**% z 1426**
	a)	PC/iMac	196	14
	b)	Notebook/MacBook	205	14
	c)	Mobilní telefon	783	55
	d)	Tablet/iPad	192	13
	e)	Internet nepoužívám	38	3
	f)	**neuvedl/a**	12	1
			1426	**100**

Graf 6 - Na jakém zařízení nejčastěji používáte internet?[72]



[71] Vlastní zdroj

[72] Vlastní zdroj

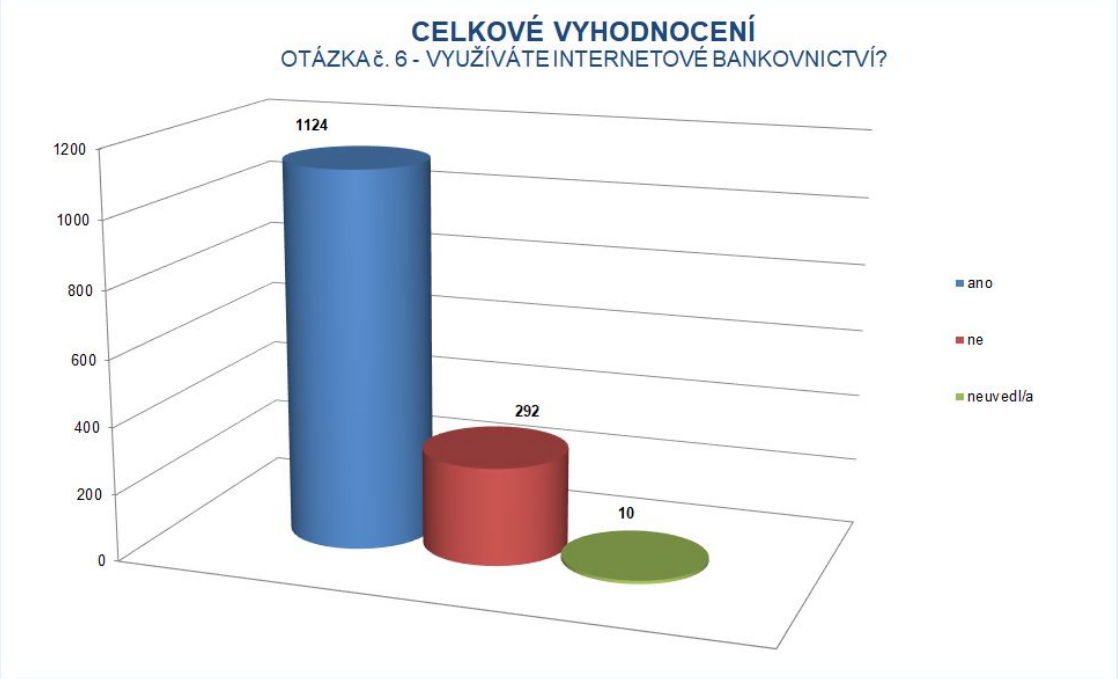
Otázka č. 6 – Využíváte internetové bankovnictví (dále jen „IB“)?

Majoritní počet respondentů s procentuálním zastoupením 79 % na otázku využívání internetového bankovnictví odpovědělo kladně. 20 % odpovědělo záporně a nepodstatné 1 % neuvedlo žádnou odpověď. Mezi respondenty tedy dominují uživatelé internetového bankovnictví, což potvrzuje zájem respondentů o problematiku bankovní počítačové kriminality v souvislosti s používáním bankovních finančních produktů a služeb.

Tabulka 6 - Využíváte internetové bankovnictví (dále jen „IB“)?[73]

DOTAZNÍKOVÉ ŠETŘENÍ Z OBLASTI POČÍTAČOVÉ KRIMINALITY				
6.	**Využíváte internetové bankovnictví (dále jen „IB“)?**		**POČET ODPOVĚDÍ**	**% z 1426**
	a)	ano	1124	79
	b)	ne	292	20
	c)	**neuvedl/a**	10	1
			1426	**100**

Graf 7 - Využíváte internetové bankovnictví (dále jen „IB“)?[74]



[73] Vlastní zdroj

[74] Vlastní zdroj

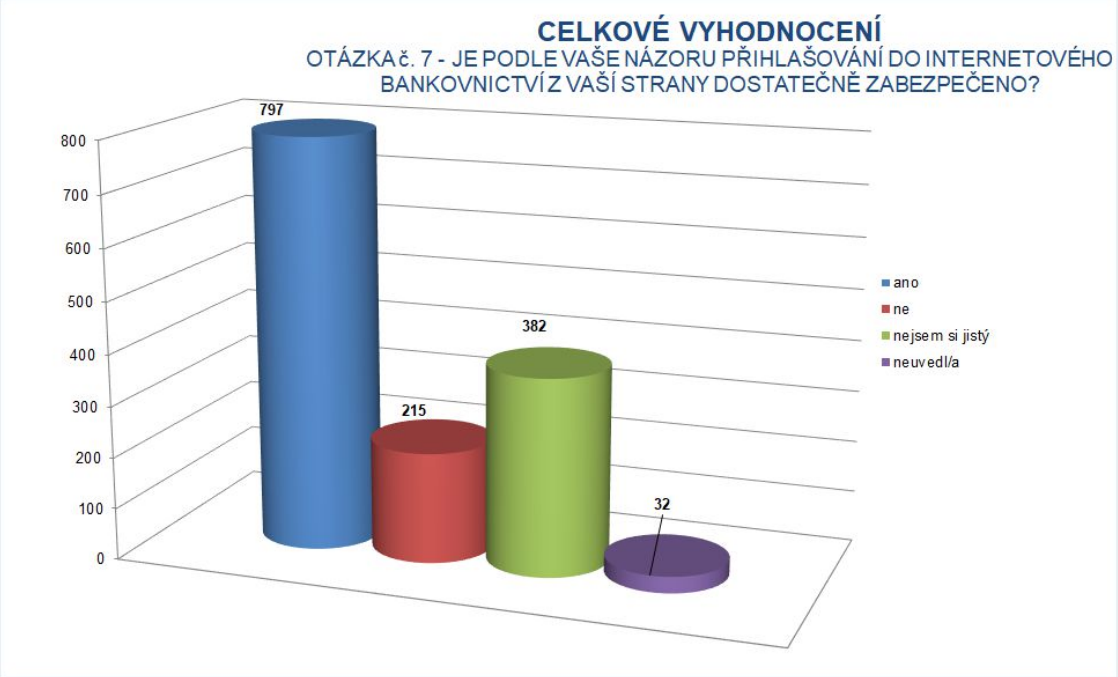
Otázka č. 7 – Je podle Vaše názoru přihlašování do Internetového bankovnictví z Vaší strany dostatečně zabezpečeno?

56 % respondentů se domnívá, že jejich přihlašování do internetového bankovnictví je dostatečně zabezpečeno a 15 % respondentů je přesvědčeno o tom, že naopak není. Skoro jedna třetina, 27 % respondentů si v oblasti zabezpečení IB nejsou jistí.

Tabulka 7 - Je podle Vaše názoru přihlašování do Internetového bankovnictví z Vaší strany dostatečně zabezpečeno?[75]

DOTAZNÍKOVÉ ŠETŘENÍ Z OBLASTI POČÍTAČOVÉ KRIMINALITY				
7.	**Je podle Vaše názoru přihlašování do Internetového bankovnictví z Vaší strany dostatečně zabezpečeno?**		**POČET ODPOVĚDÍ**	**% z 1426**
	a)	ano	797	56
	b)	ne	215	15
	c)	nejsem si jistý	382	27
	e)	**neuvedl/a**	32	2
			1426	**100**

Graf 8 - Je podle Vaše názoru přihlašování do Internetového bankovnictví z Vaší strany dostatečně zabezpečeno?[76]



[75] Vlastní zdroj

[76] Vlastní zdroj

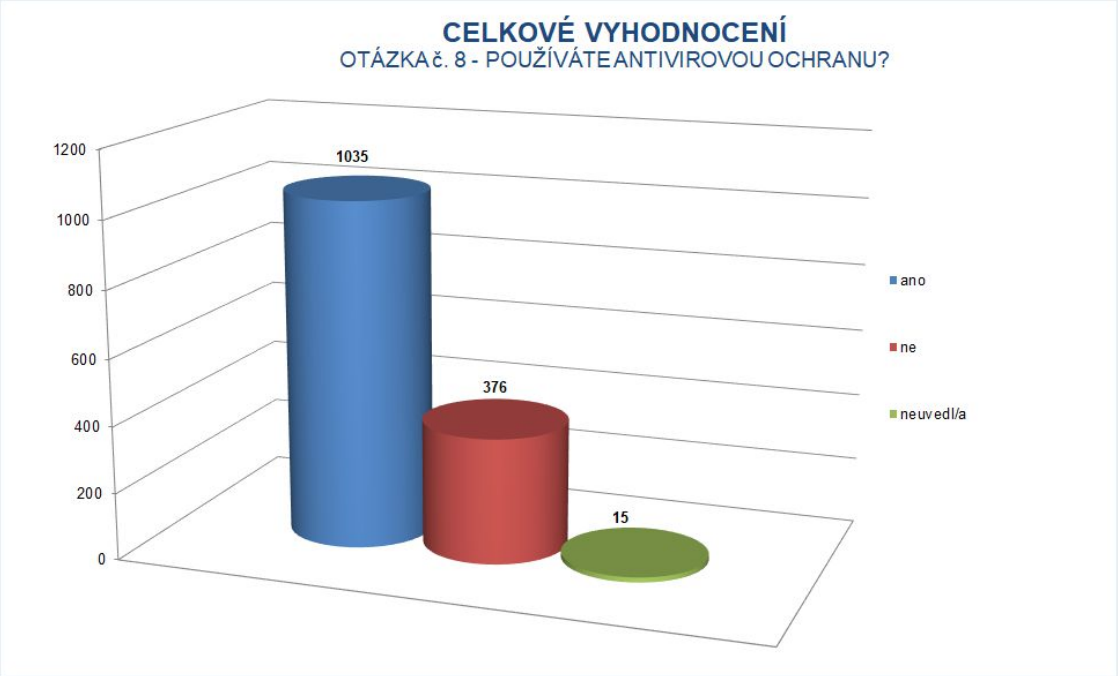
Otázka č. 8 – Používáte antivirovou ochranu?

Skoro ¾ respondentů, a to 73 % dotazovaných uvádí, že používají antivirovou ochranu. Statisticky nepodstatné 1 % respondentů se k problematice antivirové ochrany vůbec nevyjádřilo a 26 % respondentů nepoužívá žádnou antivirovou ochranu.

Tabulka 8 - Používáte antivirovou ochranu?[77]

DOTAZNÍKOVÉ ŠETŘENÍ Z OBLASTI POČÍTAČOVÉ KRIMINALITY				
8.	Používáte antivirovou ochranu?		POČET ODPOVĚDÍ	% z 1426
	a)	ano	1035	73
	b)	ne	376	26
	c)	neuvedl/a	15	1
			1426	100

Graf 9 - Používáte antivirovou ochranu?[78]



Otázka č. 9 – Pokud používáte antivirovou ochranu, na jakém zařízení ji máte nainstalovanou? (Máte možnost výběru více odpovědí).

Na tuto otázku mohli respondenti odpovídat výběrem více odpovědí, z čehož vyplývá, že celkový počet odpovědí byl větší, než počet respondentů. Získané údaje popisují situaci využití antivirové ochrany u respondentů z hlediska technického zařízení, o kterém se domnívají, že je nutné ho takto chránit. Na prvním místě uvádí s největším

[77] Vlastní zdroj

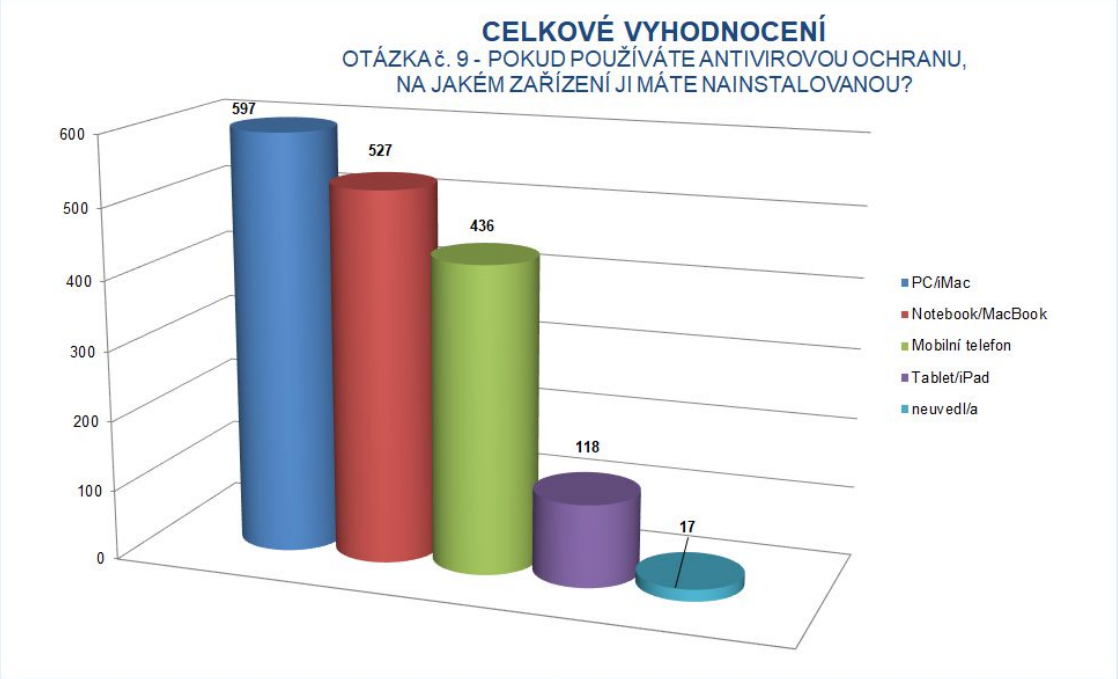
[78] Vlastní zdroj

počtem odpovědí nutnost ochrany PC/iMac, což může být způsobeno obecnou povahou a povědomím o možném napadení počítačovým virem u tohoto typu počítačového zařízení. Druhé technické zařízení v pořadí použitelnosti je respondenty uváděno Notebook/MacBook, což může z hlediska podobnosti technického zařízení odpovídat předchozí volbě u PC/iMac zařízení. Třetím typem zařízení, u kterého respondenti používají antivirovou ochranu jsou mobily, které jsou v otázce č. 5 – Na jakém zařízení nejčastěji používáte internet, uváděny jako nejpoužívanější technická zařízení, která respondenti pro přístup k internetu využívají.

Tabulka 9 - Pokud používáte antivirovou ochranu, na jakém zařízení ji máte nainstalovanou?[79]

DOTAZNÍKOVÉ ŠETŘENÍ Z OBLASTI POČÍTAČOVÉ KRIMINALITY			
9.	Pokud používáte antivirovou ochranu, na jakém zařízení ji máte nainstalovanou? (Máte možnost výběru více odpovědí)		POČET ODPOVĚDÍ
	a)	PC/iMac	597
	b)	Notebook/MacBook	527
	c)	Mobilní telefon	436
	d)	Tablet/iPad	118
	f)	neuvedl/a	17
			1695

Graf 10 - Pokud používáte antivirovou ochranu, na jakém zařízení ji máte nainstalovanou?[80]



[79] Vlastní zdroj

[80] Vlastní zdroj

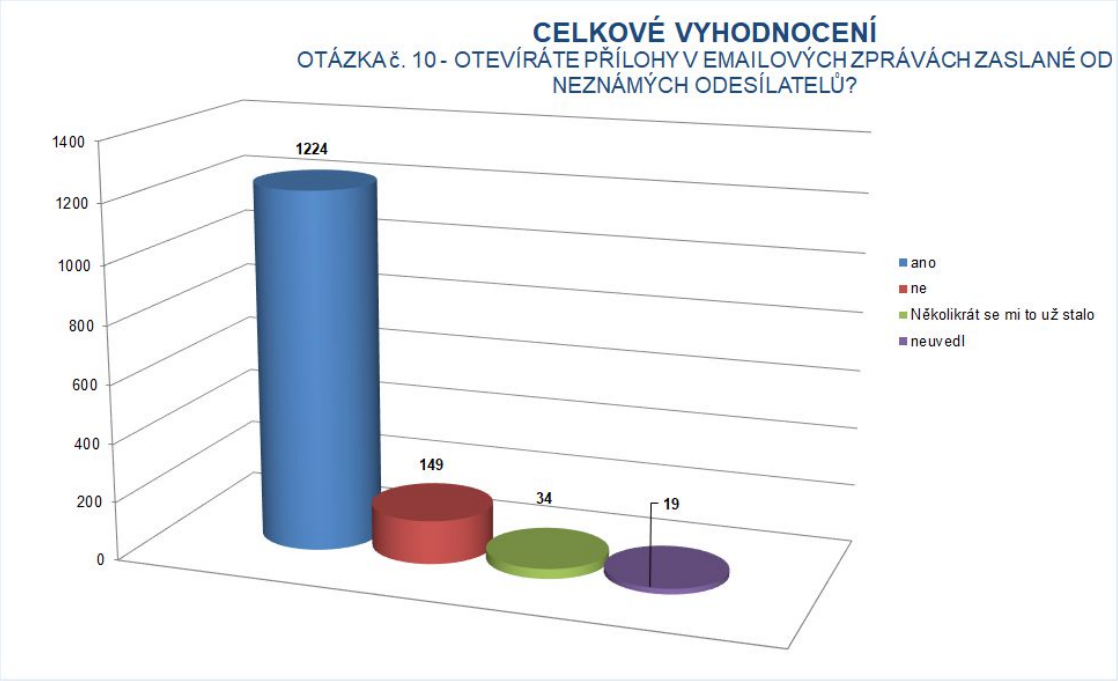
Otázka č. 10 – Otevíráte přílohy v emailových zprávách zaslané od neznámých odesílatelů?

Převládající odpovědí u 86 % respondentů je kladná odpověď. Pouze 10 % respondentů uvádí, že neotevírají přílohy v e-mailových zprávách zaslané od neznámých odesílatelů.

Tabulka 10 - Otevíráte přílohy v emailových zprávách zaslané od neznámých odesílatelů?[81]

DOTAZNÍKOVÉ ŠETŘENÍ Z OBLASTI POČÍTAČOVÉ KRIMINALITY				
10.	**Otevíráte přílohy v emailových zprávách zaslané od neznámých odesílatelů?**		POČET ODPOVĚDÍ	% z 1426
	a)	ano	1224	86
	b)	ne	149	10
	c)	Několikrát se mi to už stalo	34	2
	g)	**neuvedl**	19	1
			1426	**100**

Graf 11 - Otevíráte přílohy v emailových zprávách zaslané od neznámých odesílatelů?[82]



[81] Vlastní zdroj

[82] Vlastní zdroj

Otázka č. 11 – Označte křížkem, pokud jste se někdy stal/a obětí některé z níže uvedených situací? (Máte možnost výběru více odpovědí).

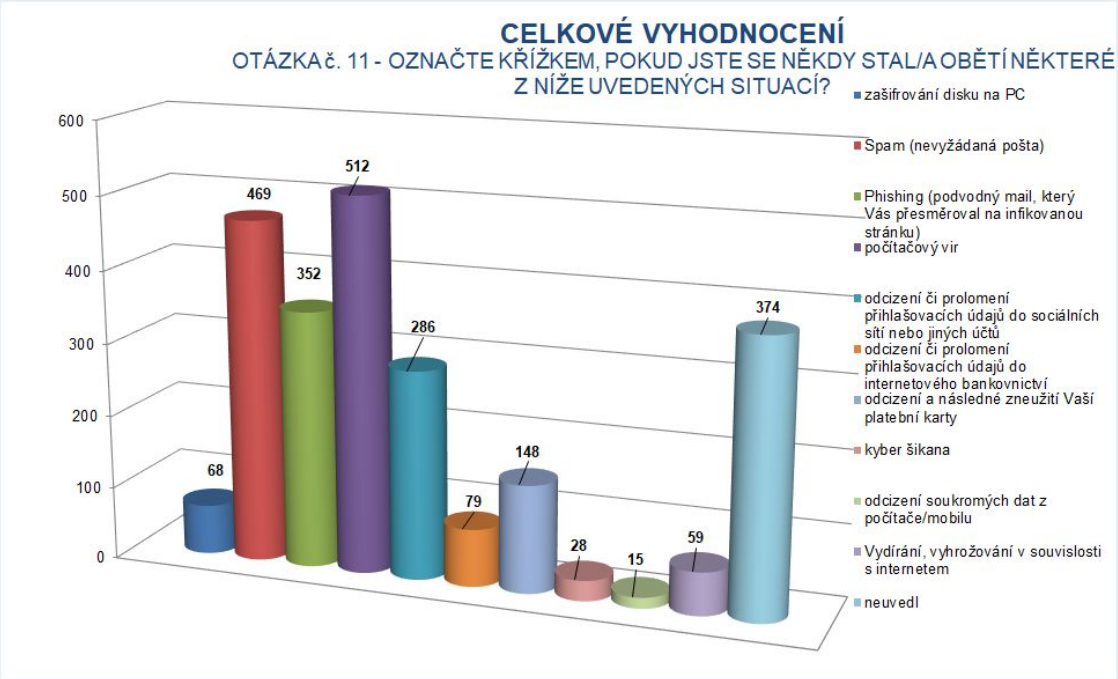
V pořadí nejčastějšího výskytu některých z předkládaných negativních situací, které se mohou při práci s internetem a elektronickými datovými nástroji, případně v bankovnictví vyskytovat, je na prvním místě respondenty uváděna zkušenost s počítačovými viry, na druhém místě se objevuje zkušenost se SPAMy a na třetím místě zkušenost s Phishingem. I přesto, že zaregistrovaný počet odpovědí NEUVEDL/A je na třetím místě větší než počet odpovědí zkušenost s Phishingem, není možné tuto prázdnou odpověď zařadit a kategorizovat do pořadí odpovědí. Další zkušeností v pořadí je odcizení či prolomení přihlašovacích údajů do internetového bankovnictví a odcizení a následné zneužití platební karty. Nejméně uváděná zkušenost je odcizení soukromých dat z počítače/mobilu. Tato skutečnost může znamenat mnohé, nelze dedukovat bez doplňujících informací od respondentů, kteří odpovídali na tuto otázku.

Tabulka 11 - Označte křížkem, pokud jste se někdy stal/a obětí některé z níže uvedených situací?[83]

DOTAZNÍKOVÉ ŠETŘENÍ Z OBLASTI POČÍTAČOVÉ KRIMINALITY			
11.	**Označte křížkem, pokud jste se někdy stal/a obětí některé z níže uvedených situací? (Máte možnost výběru více odpovědí)**		**POČET ODPOVĚDÍ**
	a)	zašifrování disku na PC	68
	b)	Spam (nevyžádaná pošta)	469
	c)	Phishing (podvodný mail, který Vás přesměroval na infikovanou stránku)	352
	d)	počítačový vir	512
	e)	odcizení či prolomení přihlašovacích údajů do sociálních sítí nebo jiných účtů	286
	f)	odcizení či prolomení přihlašovacích údajů do internetového bankovnictví	79
	g)	odcizení a následné zneužití Vaší platební karty	148
	h)	kyber šikana	28
	i)	odcizení soukromých dat z počítače/mobilu	15
	j)	Vydírání, vyhrožování v souvislosti s internetem	59
	e)	**neuvedl**	374
			2390

[83] Vlastní zdroj

Graf 12 - Označte křížkem, pokud jste se někdy stal/a obětí některé z níže uvedených situací?[84]



Otázka č. 12 – Byla Vám někdy kyber útokem způsobena nějaká finanční škoda?

Pouze 10 % respondentů odpovědělo kladně, přičemž 27 % respondentů se k otázce nevyjádřilo. 63 % respondentů odpovědělo záporně. Počet respondentů, kteří se k této otázce nevyjádřili je zarážející a dá se z toho důvodně odvozovat, že v ochotě odpovídat je vedly osobní pohnutky různého založení, související s jejich reliabilitou tohoto průzkumu.

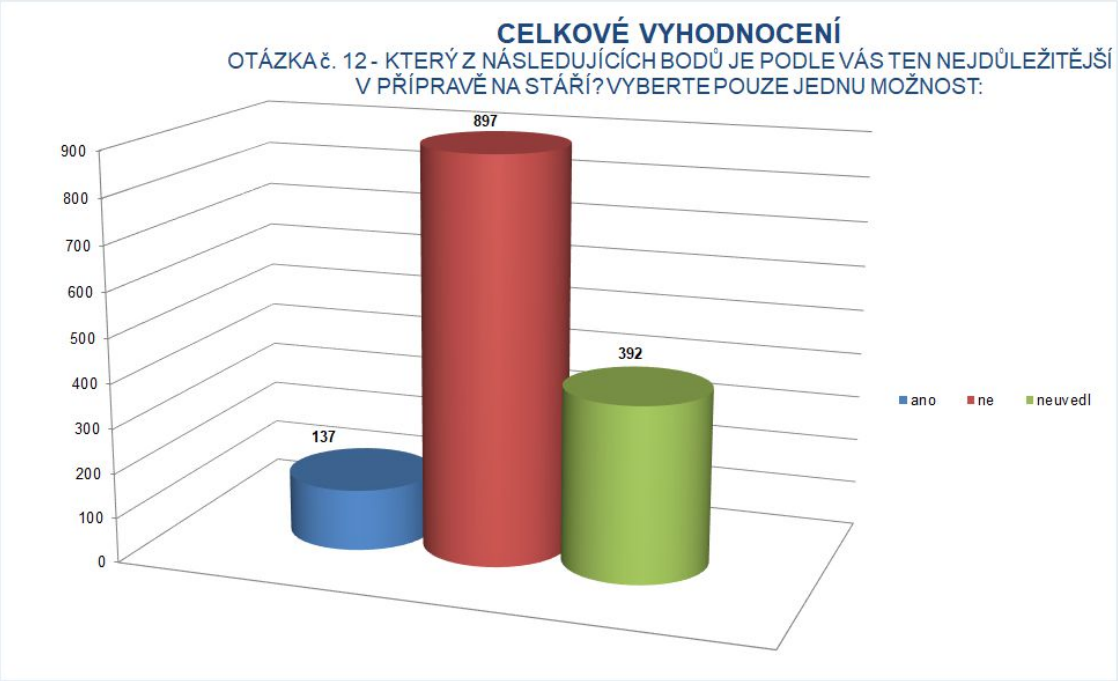
Tabulka 12 - Byla Vám někdy kyber útokem způsobena nějaká finanční škoda?[85]

DOTAZNÍKOVÉ ŠETŘENÍ Z OBLASTI POČÍTAČOVÉ KRIMINALITY				
12.	**Byla Vám někdy kyber útokem způsobena nějaká finanční škoda?**		POČET ODPOVĚDÍ	% z 1426
	a)	ano	137	10
	b)	ne	897	63
	g)	**neuvedl**	392	27
			1426	**100**

[84] Vlastní zdroj

[85] Vlastní zdroj

Graf 13 - Byla Vám někdy kyber útokem způsobena nějaká finanční škoda?[86]



Otázka č. 13 – Pokud jste uvedl/a, že Vám díky kyber útoku vznikla nějaká finanční škoda, vyberte z možností, v jakém rozmezí korun se tato škoda pohybovala:

Z předcházející otázky, která se týkala zkušenosti respondentů se situací, kdy jim byla díky kyber útoku způsobena nějaká finanční škoda vyplývá, že 10 % všech respondentů, což činí 137 kladných odpovědí na tuto otázku, budeme posuzovat v této otázce č. 13 jako celek 100 % sledovaných respondentů s kladnou odpovědí. Jejich odpovědi pak v této otázce č. 13 budeme kategorizovat a posuzovat četnost odpovědí v jednotlivých kategoriích. 55 % respondentů uvedlo, že jim byla způsobena finanční škoda do 10.000 Kč, na druhém místě v četnosti výskytu finanční škody byla zaznamenána v 17 % odpovědích z kategorie více než 10.000 Kč a méně než 50.000 Kč, a jeden respondent ze 137, což reprezentuje 1 % z celkových 137 kladných odpovědí uvedl, že mu byla způsobena finanční škoda více než 1.000.000 Kč. Zajímavé je, že i přesto, že 137 respondentů v otázce způsobené finanční škody způsobené kyber útokem odpovídalo kladně, v otázce konkrétního rozmezí způsobené škody odmítlo kategorizovat tuto škodu 20 % respondentů. Opět zde uvedené vysoké číslo neochoty odpovídat na tuto otázku může znamenat jisté osobní zábrany pravdivého vyjádření se, čímž je reliabilita a validita údajů mírně zkreslena a vypovídající hodnota tohoto okruhu otázek může být z hlediska celkového výsledku průzkumu ovlivněna psychologií

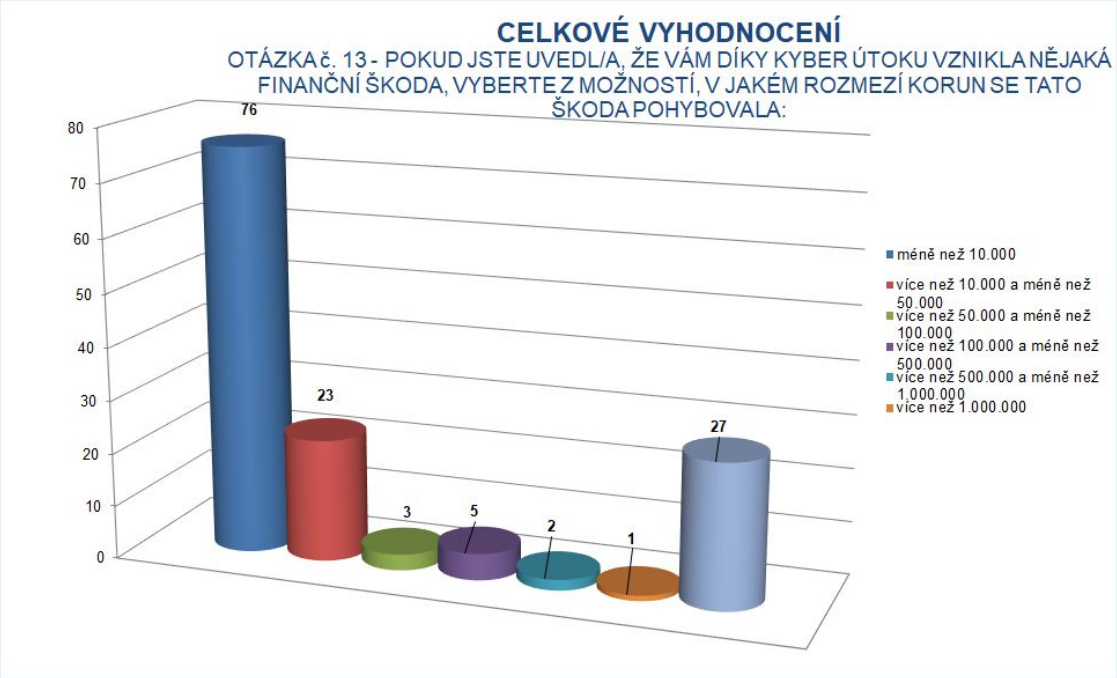
[86] Vlastní zdroj

a jednáním respondentů, kteří cítí, že tato otázka je pro ně těžce posuzovanou oblastí osobního rozhodovacího procesu.

Tabulka 13 - Pokud jste uvedl/a, že Vám díky kyber útoku vznikla nějaká finanční škoda, vyberte z možností, v jakém rozmezí korun se tato škoda pohybovala.[87]

DOTAZNÍKOVÉ ŠETŘENÍ Z OBLASTI POČÍTAČOVÉ KRIMINALITY				
13.	**Pokud jste uvedl/a, že Vám díky kyber útoku vznikla nějaká finanční škoda, vyberte z možností, v jakém rozmezí korun se tato škoda pohybovala:**		**POČET ODPOVĚDÍ**	**% ze 137**
	a)	méně než 10.000	76	55
	b)	více než 10.000 a méně než 50.000	23	17
	c)	více než 50.000 a méně než 100.000	3	2
	d)	více než 100.000 a méně než 500.000	5	4
	e)	více než 500.000 a méně než 1.000.000	2	1
	f)	více než 1.000.000	1	1
	g)	**neuvedl**	27	20
			137	**100**

Graf 14 - Pokud jste uvedl/a, že Vám díky kyber útoku vznikla nějaká finanční škoda, vyberte z možností, v jakém rozmezí korun se tato škoda pohybovala:[88]



[87] Vlastní zdroj

[88] Vlastní zdroj

Otázka č. 14 – Pokud Vám byla kyber útokem způsobena nějaká finanční škoda, řešil/a jste tuto skutečnost s Vaší bankovní institucí?

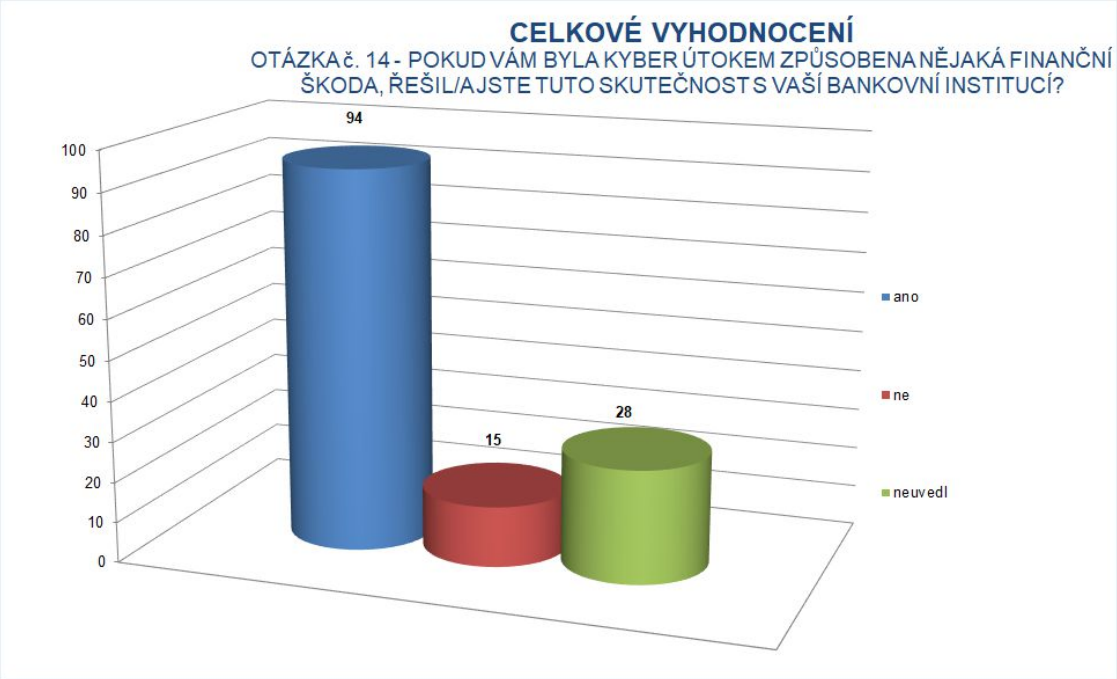
V této otázce byly opět posuzovány pouze ty dotazníky, v nichž respondenti odpovídali kladně v otázce č. 12, kde je průzkum vyzýval k odpovědi, zda jim byla někdy díky kyber útoku způsobena finanční škoda. Ostatní dotazníky nebyly do této analýzy a okruhu otázek týkajících se způsobené škody a následných procesů spojených s řešením této finanční škody, zahrnuty. Z procentuálního vyjádření vyplývá, že 69 % respondentů řešilo skutečnost vzniku finanční škody přímo s bankovní institucí, oproti tomu pouze 11 % respondentů uvedlo, že tuto situaci s bankovní institucí neřešili. Zarážející je poměrně vysoké procento 20 % respondentů, kteří se k této otázce nevyjádřili, i přesto, že vznik finanční škody v otázce č. 12 uvedli. Důvodovou možností se zde jeví stejný motiv neuvést svoje následné kroky poté, co jim vznikla finanční škoda v průzkumu, který by je mohl určitým způsobem vnitřně a osobně diskreditovat.

Tabulka 14 - Pokud Vám byla kyber útokem způsobena nějaká finanční škoda, řešil/a jste tuto skutečnost s Vaší bankovní institucí?[89]

DOTAZNÍKOVÉ ŠETŘENÍ Z OBLASTI POČÍTAČOVÉ KRIMINALITY				
14.	Pokud Vám byla kyber útokem způsobena nějaká finanční škoda, řešil/a jste tuto skutečnost s Vaší bankovní institucí?		POČET ODPOVĚDÍ	% ze 137
	a)	ano	94	69
	b)	ne	15	11
	c)	neuvedl	28	20
			137	100

[89] Vlastní zdroj

Graf 15 - Pokud Vám byla kyber útokem způsobena nějaká finanční škoda, řešil/a jste tuto skutečnost s Vaší bankovní institucí?[90]



Otázka č. 15 – Pokud Vám byla kyber útokem způsobena nějaká finanční škoda, řešil/a jste tuto skutečnost s orgány činnými v trestním řízení?

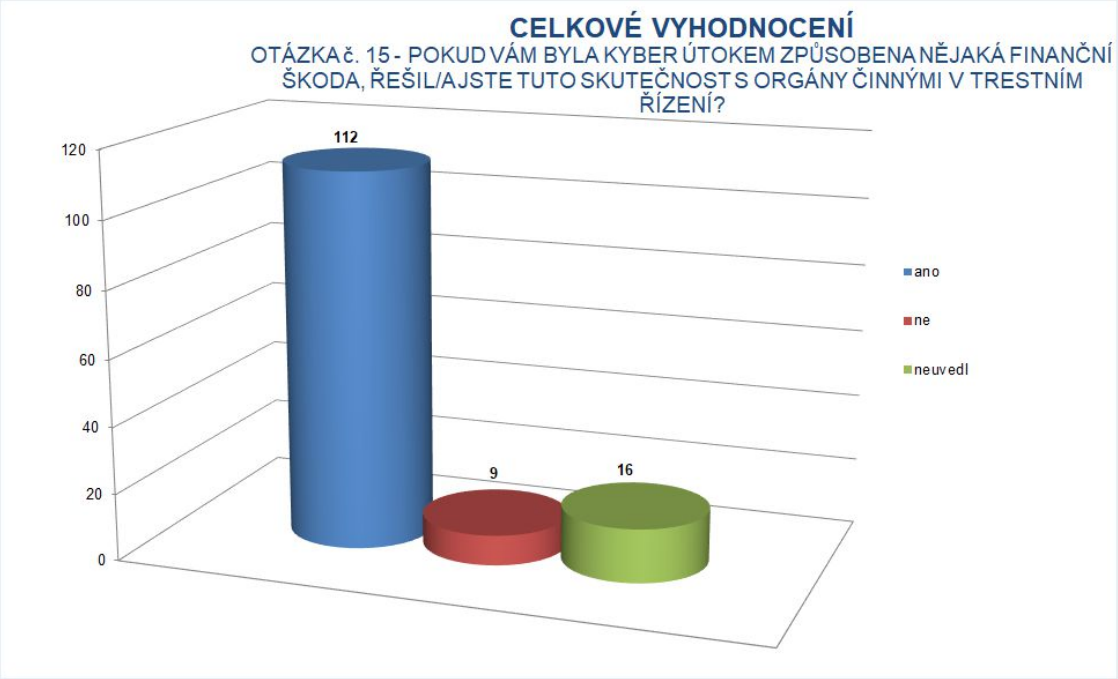
Výsledky vyhodnocení poslední otázky, která se zabývá počítačovou bankovní kriminalitou a zaměřuje se na kyber útok s následným vznikem finanční škody jsou zajímavým popisem odrazu většinové reakce uživatelů bankovních produktů a služeb. V situaci, kdy respondentům vznikla finanční škoda, a respondenti tuto situaci uvedli v otázce č. 12, projevuje se v této otázce č. 15 většinové chování respondentů, které vyhodnoceno znamená, že 82 % respondentů se v takovéto situaci obrací pro řešení na orgány činné v trestním řízení. Pouze 7 % respondentů odpovídalo záporně a jen 12 % respondentů se k této otázce nevyjádřilo, což je menší množství respondentů tzv. nulových, bez ochoty odpovídat, než je tomu u otázky č. 14. Jednoduchou dedukcí výsledků lze konstatovat, že valná většina respondentů, kterým vznikla finanční škoda se více obrací na orgány činné v trestním řízení než na bankovní instituci, což je známkou neznalosti postupů, neboť součinnost orgánů činných v trestním řízení s bankovní institucí je v obdobných případech nutná.

[90] Vlastní zdroj

Tabulka 15 - Pokud Vám byla kyber útokem způsobena nějaká finanční škoda, řešil/a jste tuto skutečnost s orgány činnými v trestním řízení?[91]

DOTAZNÍKOVÉ ŠETŘENÍ Z OBLASTI POČÍTAČOVÉ KRIMINALITY				
15.	Pokud Vám byla kyber útokem způsobena nějaká finanční škoda, řešil/a jste tuto skutečnost s orgány činnými v trestním řízení?		POČET ODPOVĚDÍ	% ze 137
	a)	ano	112	82
	b)	ne	9	7
	c)	neuvedl	16	12
			137	100

Graf 16 - Pokud Vám byla kyber útokem způsobena nějaká finanční škoda, řešil/a jste tuto skutečnost s orgány činnými v trestním řízení?[92]



7.1 Shrnutí výsledků průzkumu a dotazníkového šetření

Z výsledků průzkumu můžeme usuzovat, že zájem o problematiku počítačové bankovní kriminality je mezi respondenty poměrně vysoký. Z připravených 2000 dotazníků v osmi bankovních institucích, bylo odevzdáno v průběhu 35 dnů trvání dotazníkového sběru dat 1426 vyplněných dotazníků, což je 71 % odevzdaných dotazníků.

V oblasti genderové došlo neplánovaně k velmi vyváženému stavu respondentů, přičemž se do průzkumu zcela náhodně zapojilo 51 % mužů a 47 % žen. Z tohoto celku

[91] Vlastní zdroj

[92] Vlastní zdroj

byla nejpočetnější skupina respondentů ve věkové kategorii 31-45 roků a druhou nejpočetnější skupinu tvořili respondenti ve věku 46-60, tedy pracovně aktivní jedinci.

V kategorii vzdělání se zúčastnilo nejvíce, 30 % respondentů se středoškolským všeobecným vzděláním s maturitou z gymnázia, dále 24 % středoškolsky vzdělaných respondentů s odbornou maturitou a shodně po 19 % respondenti s vysokoškolským vzděláním a s vyučením.

Z pohledu pracovní a sociální kategorie respondentů byla nejpočetnější skupina zjištěna ve 49 % s pozicí zaměstnanec, na druhém místě s účastí 37 % respondentů z kategorie podnikatel/ka-OSVČ, jednatel/ka společnosti a s 8 % student.

Z interpretace výsledků dotazníkového šetření vyplývá, že 55 % respondentů, kteří se aktivně, dobrovolně a anonymně zapojili do tohoto průzkumu využívá k přístupu do internetu mobilní telefon, a dále pak dalších dohromady 28 % respondentů se připojuje do internetu na zařízeních typu PC/iMac, notebook/MacBook, což jsou identicky podobná zařízení se stejným účelem a funkcemi, pouze v jiném provedení.

V kontextu s hlavním cílem průzkumu a této bakalářské práce, který je zaměřený na počítačovou bankovní kriminalitu, odpovědělo 79 % respondentů, že využívá internetové bankovnictví a 56 % respondentů je se zabezpečením přístupu do internetového bankovnictví spokojeno, přičemž 73 % respondentů na svém technickém zařízení, díky kterému se do internetu přihlašují, používá antivirovou ochranu.

Z hlediska uživatelského povědomí o nebezpečí otevírání příloh v e-mailu, které jsou zaslány neznámým odesílatelem uvádí 86 % respondentů, že tyto přílohy neotevírají.

Podstatnou součástí a zároveň jedním z nejdůležitějších bodů stanoveného cíle tohoto průzkumu je otázka počítačové kriminality a kyber útoků, včetně vzniku finančních škod v bankovních operacích. Na osobní zkušenost s různými situacemi z výše jmenovaného resortu trestných činů odpovídali respondenti s možností více výběrů, a proto vyhodnocení není procentuální, nýbrž číselné v pořadí největší četnosti. Na prvním místě ve výskytu a osobní zkušenosti setkání s počítačovou trestnou činností dominovala zkušenost respondentů s výskytem počítačového viru s počtem 512 odpovědí, dále s počtem 469 odpovědí je to osobní zkušenost s výskytem Spamu a s 352 označenými možnostmi na třetím místě s výskytem Phishingu. Ostatní případy jsou také velmi důležitým ukazatelem zkušeností respondentů, nicméně pro účely tohoto shrnutí jsou zde uvedeny pouze první tři výskyty podle pořadí.

V otázce vzniklé finanční škody, která byla respondentům způsobena kyber útokem odpovědělo kladně 10 % respondentů a v následujících otázkách dotazníkového šetření byly vyhodnocovány pouze tyto dotazníky respondentů, a to především kvůli charakterové a obsahové povaze otázek č. 13, 14 a 15, které dokumentovaly a vyhodnocovaly odpovědi respondentů s kladným vyjádřením se k osobní zkušeností se vznikem finanční škody. Z tohoto důvodu a v návaznosti na interpretaci jednotlivých otázek lze konstatovat, že bylo u 10 % respondentů, kteří reprezentují vzorek 137 dotazníků detailně rozpracováno vyhodnocení otázek vzniku trestné činnosti díky kyber útoku, včetně získaných údajů o výši finanční škody, která jim byla způsobena.

Nejpočetnější skupina, 55 % respondentů, uvedla, že jim vznikla díky kyber útoku finanční škoda ve výši méně než 10.000 Kč, druhou skupinou je v 17 % výskytu skupina respondentů se vzniklou škodou ve výši více než 10.000 Kč a méně než 50.000 Kč. Zajímavostí je výskyt odpovědi jednoho respondenta, který je v celkovém počtu 137 odpovědí statisticky vyjádřen 1 % respondentů a který uvedl, že mu byla způsobena finanční škoda více než 1.000.000 Kč. Detailnějším vyhodnocením anonymního dotazníku tohoto jediného respondenta lze dojít k závěru, že jeho odpověď je velmi pravděpodobně zavádějící, vzhledem ke skutečnosti, že respondent v kategorii otázek 1 až 4, což jsou sociodemografické otázky, které mají za úkol zařadit skupinu respondentů do jednotlivých kategorií pohlaví, věku, vzdělání a pracovního a společenského zařazení, jedná se o nezaměstnaného muže se základním vzděláním ve věku 61 a více. Na relevantnost údajů by bylo zapotřebí detailnější informovanost a konkrétní informace od tohoto konkrétního respondenta, což by ovšem nebylo proveditelné vzhledem k charakteru a průběhu tohoto dotazníkového šetření.

Jednou z posledních zkoumaných oblastí problematiky počítačové bankovní kriminality byla oblast chování oběti, která má osobní zkušenost s kyber útokem a následnou finanční škodou. Otázka 14 a 15 se zaměřila na reakce obětí a zde uvedlo 69 % respondentů, kteří v otázce č. 12 hlasovali kladně, že tuto situaci řešili s bankovní institucí, přičemž ze stejné skupiny respondentů, kterých bylo 137, uvedlo až 82 % respondentů, že vzniklou finanční škodu řešilo s orgány činnými v trestním řízení.

Z průzkumu tedy vyplývá, že respondenti se v případě vzniku kyber útoku s výskytem finanční škody obracejí prvoliniově na orgány činné v trestním řízení a teprve ve druholiniovém řešení se obracejí na bankovní instituci, u které mají vedené bankovní služby a ve kterých tato škoda vznikla.

Při plánování a realizaci tohoto průzkumu bylo osloveno vedení deseti bankovních institucí z lokality města Brna, přičemž vedení dvou bankovních institucí svoji spolupráci na průzkumu k této bakalářské práci rezolutně odmítlo a dotazníkové šetření mohlo být realizováno ve zbývajících osmi bankovních institucích za podmínek, které si vedení všech těchto bankovních institucí nezávisle na sobě stanovilo a to za podmínek absolutní anonymity údajů o jménech a názvech bankovních institucí, kde průzkum k mé praktické části probíhal.

Z výše uvedených údajů, především z výsledků vyhodnocení otázky č. 14, může vyplývat možný důvod, pro podmínku anonymity ze strany vedení bankovních institucí.

7.2 Doporučení a návrhy opatření v souvislosti s výsledky průzkumu

Problematika počítačové trestné činnosti a bankovní kriminality je rozsáhlou oblastí teoretických i praktických znalostí a zkušeností a je nezbytně nutné, zvláště v moderním způsobu životního stylu, který je doslova závislý na využívání informačních technologií, nalézat nové cesty, jak zabránit ve vzniku jednotlivých nebo i hromadných trestných činů. Neustálý vývoj informačních technologií s sebou nese nutnost dalšího rozvoje a přizpůsobování se trendům nejenom technologií, ale také trendům kriminálních projevů ve společnosti. Dekriminalizace počítačové trestné činnosti je závislá na dobré znalosti teorie, prostředí, procesů, které jsou v trestné činnosti používané a také je nezbytně nutné reagovat na tuto skutečnost především těmito směry:

1. Neustálým zdokonalováním se v oblasti vývoje informačních technologií.
2. Soustavným sledováním vývoje trestné činnosti v oblasti počítačové kriminality.
3. Hledáním nových příležitostí pro spolupráci s potenciálně zajímavými lidmi z oblasti informačních technologií – např. sledováním studentských soutěží, jak v prostředí středoškolském, tak ve vysokoškolském prostředí, kde lze čerpat zdroje informační a personální.
4. Rekrutovat personální zdroje z řad specialistů na informační technologie.
5. Spolupracovat a intenzivně vyhledávat možnosti součinnosti s bankovními institucemi a ostatními společnostmi, které se zabývají ochranou dat, kybernetickou bezpečností a umělou inteligencí, která je zvláště v poslední době na vzestupu i v oblasti výskytu trestné činnosti v souvislosti s informačními technologiemi a řídícími bankovními systémy.

6. Pro uživatele informačních technologií, internetového bankovnictví a dalších informačních služeb vytvářet informační portály, které jsou propojené s řídícími orgány činnými v trestním řízení a budou obsahovat důležité informační zdroje pro řešení, ale také pro prevenci v problematice počítačové kriminality.
7. Realizovat všeobecnou osvětu o problematice počítačové kriminality.

Opatření a navazující doporučení lze v průběhu implementace výše uvedených procesních kroků uzpůsobovat a rozšiřovat. Pro účely této bakalářské práce jsou opatření a návrhy řešení uvedeny pouze v obecné rovině, ale vycházejí z výsledků dotazníkového šetření a reálných odpovědí respondentů.

ZÁVĚR

Problematika počítačové kriminality a nových prvků trestné činnosti je v současné postmoderní společnosti velmi aktuální a je zapotřebí se jí zabývat nejenom teoreticky, ale je existenčně důležité využívat praktických zkušeností za účelem eliminace rostoucího výskytu těchto kriminálních jevů ve společnosti.

Z pohledu orgánů činných v trestním řízení je boj s počítačovou kriminalitou nelehkým úkolem a jakákoliv činnost vedoucí k jejímu potlačení je důležitým pomocníkem v tomto boji.

Tato bakalářská práce vychází z dlouhodobého studia teoretických zdrojů z oblasti počítačové kriminality a ve své praktické části se zaměřuje na jednu z oblastí, kterou je bankovní počítačová kriminalita a její vliv na účastníky, oběti.

Teoretická část této práce v sobě zahrnuje terminologii a názvosloví počítačové kriminality, historický vývoj a komparaci se současnými trendy v počítačové kriminalitě, v návaznosti na predikci budoucnosti ve spojení s nastupujícími technologickými novinkami, jakými jsou botizace, automatizace, internet věcí, cloudová řešení, umělá inteligence a vývojová řešení informačních technologií. V teoretické rovině jsou zde vymezeny typy počítačové kriminality a její dělení z hlediska trestně právního a také z pohledu Rady Evropy.

Nedílnou součástí teoretické části práce je, z důvodu návaznosti na praktickou část, vymezení specifik bankovní počítačové kriminality, včetně teoretických závěrů preventivních opatření.

Na teoretickou část této práce navazuje její praktická část, která koresponduje s předem stanoveným cílem a zaměřuje se na zjištění, analýzu, vyhodnocení, interpretaci a následná doporučení v situacích, které respondenti na základě dotazníku popisují z pohledu konkrétních zkušeností účastníků procesu bankovních operací, popřípadě z pohledu oběti kyber útoku, které vznikla finanční škoda nebo jiná újma.

Na základě průzkumu a dotazníkového šetření z oblasti počítačové kriminality a realizace tohoto průzkumu, následného sběru dat, analýzy, vyhodnocení kvantitativní metodou s účastí univariační analýzy a interpretovaných výstupů z tohoto průzkumu lze konstatovat, že se oblast počítačové kriminality v bankovním sektoru a z hlediska uživatelského prostředí respondentů, kteří se jako klienti bankovních institucí vyjadřovali

k jednotlivým otázkám, jeví jako vysoce exponovanou oblastí výskytu nového druhu trestné činnosti.

Cílem této práce bylo zmapovat problematiku počítačové kriminality jako nového fenoménu trestné činnosti s rozšířením do oblasti bankovní počítačové kriminality.

Vzhledem k rozsahu a obsahu této práce se domnívám, že cíl této bakalářské práce byl splněn a z důvodu vysoké důležitosti a aktuálnosti získaných údajů z teoretické a praktické části této práce, v kontextu s prováděným průzkumem, který probíhal v období leden až březen 2022, doporučuji stejný nebo podobný průzkum opakovat v časovém horizontu druhého pololetí roku 2022, aby bylo možné komparovat nově získané údaje s údaji uvedenými v této bakalářské práci.

SEZNAM POUŽITÝCH ZDROJŮ

Literární zdroje

1. **BRITZ, M**. *Computer forensics and cyber crime: an introduction.* 3rd ed. Upper Saddle River, N.J.: Pearson Prentice Hall, 2013, s. 386. ISBN 978-0132677714.
2. **GROOVER, M. P**. *Fundamentals of modern manufacturing: materials, processes and systems*. New York: John Wiley, 2001. s. 1088. ISBN 978-0-471-36680-5.
3. **GŘIVNA, T.** § 230 Neoprávněný přístup k počítačovému systému a nosiči informací. In: **ŠÁMAL, P. a kol**. *Trestní zákoník II: komentář*. § 140-421. 2. vyd. V Praze: C. H. Beck, 2012, s. 3632. ISBN 978-80-7400-428-5.
4. **HOLT, T. J.; BOSSLER, A. M.; SEIGFRIED-SPELLAR, K. C**. *Cybercrime and digital forensics: an introduction*. 2. vydání. London: Routledge, 2018, s. 738. ISBN 978-1138238732.
5. **JIRÁSEK, P., NOVÁK, L., POŽÁR, J.** *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. s. 240. ISBN 978-80-7251-436-6.
6. **JIROVSKÝ, V.** *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. s. 284. ISBN 978-80-247-1561-2.
7. **KOLOUCH, J.** *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016. CZ.NIC. s. 522. ISBN 978-80-88168-15-7.
8. **KREMLING, J., SHARP-PARKER, A. M.** *Cyberspace, cybersecurity, and cybercrime*. Thousand Oaks: SAGE Publications, 2017, s. 296. ISBN 978-1506347257.
9. **MCQUADE, S. C.** *Encyclopedia of cybercrime*. Westport, Conn.: Greenwood Press, 2009. s. 210. ISBN 978-0313339745.
10. **MUSIL, S.** *Počítačová kriminalita: nástin problematiky: kompendium názorů specialistů.* 1. vydání. Praha: Institut pro kriminologii a sociální prevenci, 2000, s. 6. ISBN 80-86008-80-0.
11. **POLČÁK, R. a kol.** *Právo informačních technologií*. Praha: Wolters Kluwer, 2018. Právní monografie (Wolters Kluwer ČR). s. 656. ISBN 978-80-7598-045-8.
12. **SMEJKAL, V**. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. s. 936. ISBN 978-80-7380-720-7.

13. **ŠÁMAL, P., NOVOTNÝ, O., GŘIVNA, T., HERCZEG, J., VANDUCHOVÁ, M., VOKOUN, R.** *Trestní právo hmotné*. 8., přepracované vydání. Praha: Wolters Kluwer, 2016. s. 1052. ISBN 978-80-7552-358-7.
14. **VÁLKOVÁ, H., KUCHTA, J., HULMÁKOVÁ, J.** *Základy kriminologie a trestní politiky*. 3. vydání. V Praze: C.H. Beck, 2019. Beckovy mezioborové učebnice. s. 616. ISBN 978-80-7400-732-3.
15. **ZAPLETAL, J. a kol**. *Prevence kriminality*. 2. přepracované vydání. Praha: Policejní akademie ČR, 2005, s. 108. ISBN 80-7251-200-5.

Elektronické zdroje:

16. **BARÁK, P.**, 2015. *Podvody páchané v bankách*. Brno. Seminář pro finanční trh.
17. *Cyberattack traced to hacked refrigerator, researchers report*. Phys.org [online]. Science X Network, publikováno 17. 1. 2014 [cit. 2021-11-08]. Dostupné z WWW: <https://phys.org/news/2014-01- cyberattack-hacked-refrigerator.html>.
18. **DELOITTE.** *Automatizace práce v ČR: Proč se (ne)bát robotů* [online]. 2018. Dostupné z WWW: <https://www2.deloitte.com/content/dam/Deloitte/cz/ Documents/strategy-operations/Automatizace-prace-v-CR.pdf>.
19. **DOUCHA, M.** *Deklarace nezávislosti Kyberprostoru* [online]. Pirátskélisty.cz, publ. 20. 2. 2016 [cit. 2021-10-13]. Dostupné z WWW: <https://www.piratskelisty.cz/clanek-1476-deklarace-nezavislosti-kyberprostoru>.
20. *eDemocracy*. Jaknainternet.cz [online]. CZ.NIC, z. s. p. o., © 2020 [cit. 2021-11-15]. Dostupné z WWW: <https://www.jaknainternet.cz/page/1664/edemocracy/>.
21. **HLAVÁČEK, V.** *Robotická procesní automatizace RPA – Co to je?* In: komix.cz [online]. Publikováno 5. 2. 2021 [cit. 2021-11-12] Dostupné z WWW: <https://www.komix.cz/roboticka-procesni-automatizace-rpa-co-to-je/>.
22. **HOLDEN, D**. *Estonia, six years later* [online]. Publikováno 16. 5. 2013 [cit. 2021-10-26]. Dostupné z WWW: <http://www.arbornetworks.com/asert/2013/05/ estonia-six-years-later/>.
23. **JAVŮREK, K.** *První kvantový počítač stojí deset milionů dolarů*. E15.cz [online]. CZECH NEWS CENTER a.s., © 2020 [cit. 2021-11-15]. Dostupné z WWW: <http://vtm.e15.cz/prvni-kvantovy-pocitac- stoji-deset-milionu-dolaru>.
24. **KALAMÁR Š., PETRÁK, M.** *Skimming jako jeden z druhů kybernetické kriminality.* In: Cybersecurity.cz [online]. [cit. 2022-01-05]. Dostupné z WWW: <https://www.cybersecurity.cz/data/skimming.pdf>.

25. **KREBS, B.**, 2012. *Beware Card and Cash-Trapping at the ATM*. In: Krebs on security [online]. [cit. 2022-01-05]. Dostupné z WWW: <https://krebsonsecurity.com/2012/11/beware-card-and-cash-trapping-at-the-atm/>.
26. **KROPÁČOVÁ, A.** *CERT/CSIRT týmy a jejich role*. ROOT.CZ [online]. Publikováno 6. května 2013 [cit. 2022-01-10]. Dostupné z WWW: <https://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/>.
27. *Kyberkriminalita*. Policie ČR [online]. © 2020 Policie ČR [cit. 2021-10-20]. Dostupné z WWW: <https://www.policie.cz/clanek/kyberkriminalita.aspx>.
28. **McGUIRE, M., DOWLING, S**. *Cyber crime: A review of the evidence*, Research Report 75, Summary of key findings and implications [online]. UK Home Office, 2013, s. 5 [cit. 2021-12-20]. Dostupné z WWW: <https://ncvc.dspacedirect.org/handle/20.500.11990/871>.
29. *Memorandum o Computer Security* Incident Response Team České republiky. CZ.NIC [online]. 9. 12. 2010 [cit. 2022-01-10].
30. *Musk nás zklamal, říkají kyborgové. Jeho Neuralink dává víc otázek než odpovědí*. Forbes.cz, Darek Šmíd 07. 09. 2020 [cit. 2021-12-07]. Dostupné z WWW: <https://www.forbes.cz/musk-nas-zklamal-rikaji-kyborgove-jeho-neuralink-dava-vic-otazek-nez-odpovedi/>.
31. *NBÚ vybral provozovatele národního CERT (CSIRT.CZ), je jím CZ.NIC*. GovCERT [online]. Publikováno 27. srpna 2015 [cit. 2022-01-10]. Dostupné z WWW: <https://www.nbu.cz/cs/aktualne/820-621-nbu-vybral-provozovatele-narodniho-cert-csirtcz-je-jim-cznic/>.
32. *Neuralink Elona Muska: ovládání telefonu a počítače pouhou myšlenkou*. ALZA.cz [online]. Publikováno 8. 10. 2019 [cit. 2021-11-15]. Dostupné z WWW: <https://www.alza.cz/neuralink>.
33. **PAVLÍKOVÁ, E.** *Smart cities – inteligentní města, která nám usnadní život*. Bydlenivevate.cz [online]. Publikováno 5. 9. 2019 [cit. 2021-11-12]. Dostupné z WWW: <https://bydlenivevate.cz/lifestyle/smart-cities-inteligentni- mesta-ktera-nam-usnadni-zivot/>.
34. **RANDÁKOVÁ, R.** *#SayNo! - Celoevropská kampaň proti zneužívání dětí online*. Policie ČR [online]. Policie ČR, © 2020, publikováno 19. června 2017 [vid. 2022-02-09]. Dostupné na WWW: <https://www.policie.cz/clanek/sayno-celoevropska-kampan-proti-internetovemu-sexualnimu-natlaku-a-vydirani-deti-rekni-ne.aspx>.

35. **SOUČKOVÁ, K.**, 2017. *Přibývá podvodů s platebními kartami. Rizikem jsou univerzální bankomaty*. In: iRozhlas [online]. [cit. 2021-12-21]. Dostupné z WWW: <https://www.irozhlas.cz/ekonomika/pribyva-podvodu-s-platebnimi-kartami-rizikem-jsou- univerzalni-bankomaty_1707251034_mos>.
36. **SVÍZELOVÁ, S.**, 2018. *Operační riziko v bankovnictví*. In: MUNI.cz [online]. [cit. 2021-12-20]. Dostupné z WWW: <https://is.muni.cz/th/zx42p/ Svizelova-DP_5_1__FINAL_.pdf>.
37. **TŮMA, O.**, 2013. *Dávejte si pozor na platební kartu! Podvodníci jsou stále vynalézavější*. In: Peníze.cz [online]. [cit. 2022-01-05]. Dostupné z WWW: <https://www.penize.cz/platebni-karty/248343-davejte-si-pozor-na-platebni-kartu!- podvodnici-jsou-stale-vynalezavejsi>.
38. *V Brně bylo otevřeno Národní centrum kybernetické bezpečnosti*. Krajský úřad Jihomoravského kraje [online]. Publikováno 13. 5. 2014 [cit. 2022-01-10]. Dostupné z WWW: <https://www.kr-jihomoravsky.cz/ Default.aspx?ID=230019&TypeID=2>.
39. **VÁCLAVÍK, L.** *Většina internetu je skrytá. Co jsou to deep a dark web?* CNEWS.cz [online]. Publikováno 8. 10. 2018 [cit. 2021-10-14]. Dostupné z WWW: <https://www.cnews.cz/co-je-to-deep-invisible-hluboky-dark-temny-web>.
40. **VIMMEROVÁ, V.** *Síť jménem 5G vstoupí do našich životů a změní je. Odpor je marný, ostražitost nutná.* Aktuálně.cz [online]. Publikováno 29. 11. 2019 [cit. 2021-11-15]. Dostupné z WWW: <https://zpravy.aktualne.cz/ekonomika/bezpecnost-site-5g-co-si-sami-neuchranime-je-v-ohrozeni/r~8738a046f73511e9ac60ac1f6b220ee8/>.
41. Zdroj: (PwC, ©2016) PricewaterhouseCoopers.
42. Zdroj: iDnes.cz, 2007.

Legislativní zdroje:

43. ČESKO. VLÁDA. *Usnesení Vlády ČR č. 205 ze dne 15. března 2010 o řešení problematiky kybernetické bezpečnosti České republiky*.
44. ČESKO. VLÁDA. *Usnesení Vlády ČR č. 380 ze dne 24. května 2010 o zřízení Meziresortní koordinačńí rady pro oblast kybernetické bezpečnosti*.

45. ČESKO. VLÁDA. *Usnesení Vlády ČR č. 781 ze dne 19. října 2011 č. 781 o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast*.
46. *Úmluva Rady Evropy č. 185 o kybernetické kriminalitě ze dne 23. listopadu 2001*. In: Council of Europe [Treaty Office]. Official website of the Treaty Office [cit. 2021-10-16]. Dostupné z WWW: <https://www.coe.int/en/web/conventions/>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ICT – Informační a komunikační technologie (Information and Communication Technologies)

TCP/IP – Primární přenosový protokol/protokol síťové vrstvy (Transmission Control Protocol/Internet Protocol)

MIT - Massachusetts Institute of Technology

RPA - Robotická Procesní Analýza (Robotic Process Automation)

IoT – Internet věcí (Internet of Things)

DoS – odmítnutí služby (Denial of Service)

PIN – osobní identifikační číslo (Personal Identification Number)

DNS – systém doménových jmen (Domain Name System)

SMS – služba krátkých textových zpráv (Short Message Service)

FTP – protokol pro přenos souborů (File Tranfer Protocol)

P2P – typ počítačové sítě, kde spolu komunikují jednotlivý klienti (Peer-to-Peer)

VNC – program ke vzdálenému připojení k jinému počítači (Virtual Network Connection)

CSIRT – tým pro řešení počítačových bezpečnostních incidentů (Computer Security Incident Response Team)

HTTP – internetový protokol určený pro komunikaci s webovými servery (Hypertext Transfer Protokol)

CERT – tým pro řešení počítačových havarijních situací (Computer Emergency Response Team)

ZoKB – zákon o kybernetické bezpečnosti

NBÚ – Národní bezpečnostní úřad

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ

SEZNAM PŘÍLOH

PŘÍLOHY

Příloha č. I. Vzory HOAXu

Předmět: Neplaťte pokuty

Neplaťte pokuty...!

Víte, že vůbec nemusíte platit pokuty za "přiměřeně" rychlou jízdu?

Taky jsem se to dozvěděla nedávno a řeknu Vám, že mě mrzí, že jsem těm bídákům zeleným dala peníze za něco na co vůbec nemají ze zákona právo. V zákoně č.361/2000 o pozemních komunikacích je sice napsáno, že máme povinnost jezdit v obci 50 km/hod., na okresce 90 km/hod. a na dálnici max 130 km/hod.. Jenže kluci zelení nás můžou pokutovat jen za přestupek. A v přestupkovém zákoně č.200/1990 je přestupek definován jako překročeni rychlosti v obci o 30 km/hod a mimo obec o 50 km/hod. Jo jo, to je ta naše legislativa. Takže, když se fakt budete mírnit a v obci pojedete do 79 km/hod, na okresce do 119 km/hod a na dálnici do 179 km/hod, tak jim nemusíte dávat nic a místo peněz vyhozených za pokutu zajít radši na zmrzlinu.

Ověřovala jsem si to u naší právničky a je to skutečně tak. Opět zase stát spoléhá na to, že neznáme dobře zákony. Jo a kdyby Vám chtěli argumentovat tím, že celá tato věc je ošetřena v nějaké vyhlášce, tak to klidně může být, ale zákon je vyhlášce nadřazen. Tak a mají smůlu. Teď už jen připravit lékárničky, technický stav vozidla, aby si rozčilení "neléčili" na něčem jiném.Tak a hurá na rychlejší, ale stále bezpečnou jízdu.

Předmět: BANKOMAT + PIN - Může to být užitečné...

Verze 1

Jakmile se ocitnete v situaci, kdy jste přinuceni násilníkem a musíte pod nátlakem vybrat peníze z Bankovního automatu, zadejte svůj PIN opačně: tzn. od konce - > např. máte-li 1234, tak zadáte 4321 a automat vám peníze přesto vydá, ale též současně přivolá policii, která vám přijede na pomoc.

Tato zpráva byla před nedávnem vysílána v TV, přesto ji využili doposud jen 3 lidé, protože se o této skutečnosti mezi lidmi neví.

Přepošlete co nejvíce lidem.

Verze 2

Předmět: BANKOMAT + PIN - Může to být užitečné...

Jakmile se ocitnete v situaci, kdy jste přinuceni násilníkem a musíte pod nátlakem vybrat peníze z Bankovního automatu, zadejte svůj PIN opačně: tzn. od konce - např. máte-li 1234, tak zadáte 4321 a automat vám peníze přesto vydá, ale též současně přivolá policii, která vám přijede na pomoc!!!

Tato zpráva byla před nedávnem vysílána v TV, přesto ji využili doposud jen 3 lidé, protože se o této skutečnosti mezi lidmi neví.

Přepošlete co nejvíce lidem.

Příloha č. II. Dotazníkové šetření z oblasti počítačové kriminality

Dobrý den, jmenuji se Petr Maloň a pracuji jako policista v oblasti informačních a komunikačních technologií. V současné době studuji vysokou školu a jsem studentem III. ročníku oboru „bezpečnostně právní činnost“. Výstupem mého studia bude bakalářská práce zabývající se problematikou počítačové kriminality jako nového druhu trestné činnosti.

Rád bych Vás touto cestou požádal o vyplnění níže uvedeného dotazníku, který se zaměřuje na klíčové prvky z oblasti páchání trestné činnosti počítačové kriminality. U otázek můžete křížkem označit svoji odpověď, některé otázky umožňují označení více možností (uvedeno u otázky). Veškeré vyplněné údaje jsou anonymní a budou sloužit pouze pro účely mé bakalářské práce. Děkuji Vám za Váš čas a ochotu.

		OTÁZKY DOTAZNÍKU	
1.		Pohlaví	označte X
	a)	žena	
	b)	muž	
	c)	neuvedl/a	
2.		Věk	označte X
	a)	15 - 30	
	b)	31 - 45	
	c)	46 - 60	
	d)	61 a více	
	f)	neuvedl/a	
3.		Vzdělání	označte X
	a)	základní	
	b)	vyučen/a	
	c)	středoškolské odborné s maturitou	
	d)	středoškolské všeobecné s maturitou (gymnázium)	
	e)	vyšší odborné	
	f)	vysokoškolské	
	g)	neuvedl/a	
4.		Pracovní a sociální zařazení ve společnosti	označte X
	a)	student	
	b)	zaměstnanec	
	c)	podnikatel/ka - OSVČ, jednatel/ka společnosti	
	d)	důchodce/důchodkyně	
	e)	nezaměstnaný/á	
	f)	neuvedl/a	
5.		Na jakém zařízení nejčastěji používáte internet?	označte X
	a)	PC/iMac	
	b)	Notebook/MacBook	
	c)	Mobilní telefon	
	d)	Tablet/iPad	
	e)	Internet nepoužívám	
	f)	neuvedl/a	

6.		Využíváte internetové bankovnictví (dále jen „IB“)?	označte X
	a)	ano	
	b)	ne	
	c)	neuvedl/a	
7.		Je podle Vaše názoru přihlašování do Internetového bankovnictví z Vaší strany dostatečně zabezpečeno?	označte X
	a)	ano	
	b)	ne	
	c)	nejsem si jistý	
	e)	neuvedl/a	
8.		Používáte antivirovou ochranu?	označte X
	a)	ano	
	b)	ne	
	c)	neuvedl/a	
9.		Pokud používáte antivirovou ochranu, na jakém zařízení ji máte nainstalovanou? (Máte možnost výběru více odpovědí)	označte X
	a)	PC/iMac	
	b)	Notebook/MacBook	
	c)	Mobilní telefon	
	d)	Tablet/iPad	
	f)	neuvedl/a	
10.		Otevíráte přílohy v emailových zprávách zaslané od neznámých odesílatelů?	označte X
	a)	ano	
	b)	ne	
	c)	Několikrát se mi to už stalo	
	g)	neuvedl	

11.		Označte křížkem, pokud jste se někdy stal/a obětí některé z níže uvedených situací? (Máte možnost výběru více odpovědí)	označte X
	a)	zašifrování disku na PC	
	b)	Spam (nevyžádaná pošta)	
	c)	Phishing (podvodný mail, který Vás přesměroval na infikovanou stránku)	
	d)	počítačový vir	
	e)	odcizení či prolomení přihlašovacích údajů do sociálních sítí nebo jiných účtů	
	f)	odcizení či prolomení přihlašovacích údajů do internetového bankovnictví	
	g)	odcizení a následné zneužití Vaší platební karty	
	h)	kyber šikana	
	i)	odcizení soukromých dat z počítače/mobilu	
	j)	Vydírání, vyhrožování v souvislosti s internetem	
	e)	**neuvedl**	
12.		**Byla Vám někdy kyber útokem způsobena nějaká finanční škoda?**	**označte X**
	a)	ano	
	b)	ne	
	g)	**neuvedl**	
13.		**Pokud jste uvedl/a, že Vám díky kyber útoku vznikla nějaká finanční škoda, vyberte z možností, v jakém rozmezí korun se tato škoda pohybovala:**	**označte X**
	a)	méně než 10.000	
	b)	více než 10.000 a méně než 50.000	
	c)	více než 50.000 a méně než 100.000	
	d)	více než 100.000 a méně než 500.000	
	e)	více než 500.000 a méně než 1.000.000	
	f)	více než 1.000.000	
	g)	**neuvedl**	
14.		**Pokud Vám byla kyber útokem způsobena nějaká finanční škoda, řešil/a jste tuto skutečnost s Vaší bankovní institucí?**	**označte X**
	a)	ano	
	b)	ne	
	c)	**neuvedl**	
15.		**Pokud Vám byla kyber útokem způsobena nějaká finanční škoda, řešil/a jste tuto skutečnost s orgány činnými v trestním řízení?**	**označte X**
	a)	ano	
	b)	ne	
	c)	**neuvedl**	