ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA EKONOMICKÁ

Diplomová práce

Bankovní podvody

Banking frauds

Bc. Jolana Němcová

Plzeň 2024

Čestné prohlášení

Prohlašuji, že jsem diplomovou práci na téma

„Bankovní podvody“

vypracovala samostatně pod odborným dohledem vedoucí diplomové práce za použití pramenů uvedených v přiložené bibliografii.

Plzeň dne 19. dubna 2024 v. r. *Jolana Němcová*

Zásady pro vypracování práce

1. Vytvořte úvod do základní problematiky bankovních podvodů, definujte cíl a metodiku řešení.
2. Zpracujte teoretická východiska k problematice bankovních podvodů.
3. Představte podvodná jednání vyskytující se v bankovním styku.
4. Na základě statistických dat zpracujte vývoj bankovních podvodů.
5. Shrňte řešenou problematiku a odhadněte možný budoucí vývoj.

Studijní program

Podniková ekonomika a management

Poděkování

Ráda bych poděkovala vedoucí mé diplomové práce, Ing. Janě Šturcové, Ph.D., za její ochotu, rady, připomínky a také velmi milý a vstřícný přístup při zpracování diplomové práce.

Obsah

Úvod

V moderní ekonomice hrají banky nezastupitelnou roli. Zabezpečují platební styk, emitují bezhotovostní peníze, poskytují finanční produkty a služby, podílí se na stimulaci hospodářského růstu. Především díky široké škále poskytovaných produktů, jako jsou běžné účty, spořící účty, hypotéky či ostatní spotřebitelské úvěry a v neposlední řadě investiční možnosti, jsou banky nedílnou součástí také životů jednotlivců a firem. Podle průzkumu České bankovní asociace považuje banky až 70 % Čechů za nejdůvěryhodnější instituce. (ČBA, 2023) A právě důvěra, kterou veřejnost do bank vkládá, činí z bank, a především z jejich klientů, poměrně lákavý cíl pro podvodníky.

Podvody v sektoru bankovnictví nejsou novinkou, neboť i v tomto sektoru se vyskytují prakticky od jeho počátků. Formy podvodů se postupně vyvíjely – počínaje pravděpodobně nejstarší formou, kterou je padělání peněz, přes bankovní loupeže, zpronevěry, úvěrové podvody až po zneužití platebních karet či nejaktuálnější kybernetické podvody.

Kybernetické podvody jsou v současné době na obrovském vzestupu a představují pro společnost významnou hrozbu. Dynamický rozvoj technologií sice přináší řadu výhod, ale na druhou stranu se v jeho důsledku zároveň vyvíjejí schopnosti podvodníků a následně také rozmanitost podvodů. Zranitelní jsou v tomto ohledu úplně všichni, podvodníci jsou v dnešní době mnohem zkušenější, odvážnější, a především sofistikovanější než kdy dříve.

Diplomová práce je zpracovaná na téma, o jehož aktuálnosti nelze pochybovat. Úvodní část je věnována základním pojmům v bankovnictví, kde je specifikován bankovní systém, druhy bank a jejich úloha. Dále práce objasňuje problematiku regulace bankovního sektoru a také rizik, kterým bankovní sektor čelí. Významnou část tvoří kapitola o bankovních podvodech. Jsou zde podrobně rozebrány jednotlivé druhy podvodů, které jsou rozděleny na interní a externí podvody. Zvláštní pozornost je přitom zaměřena na aktuální kybernetické podvody. Poslední část práce se zabývá kyberkriminalitou a kybernetickými podvody v České republice. Nejprve je na základě dat od Policie ČR zmapován vývoj kyberkriminality v ČR a poté vývoj kybernetických podvodů v Plzeňském kraji. Dále je představena problematika kybernetických podvodů z pohledu České spořitelny a zmíněna je také situace v zahraničí. Závěr je věnován kyberbezpečnosti a nejčastěji se vyskytujícím typům kybernetických podvodů v ČR.

Cíl a metodika

Hlavním cílem diplomové práce bude komplexní zpracování problematiky bankovních podvodů. Dílčím cílem bude rozbor kyberkriminality a kybernetických podvodů v České republice metodou analýzy, a to na základě získaných dat od vybraných institucí.

Diplomová práce bude vycházet z předpokladu systematického zpracování teoretických východisek pro vytvoření vlastní práce. Teoretická východiska budou zpracována na základě odborné literatury, zákonů a internetových zdrojů, které souvisí s problematikou bankovních podvodů. Praktická část bude vycházet ze sekundárních dat, která poskytne Policie ČR a Česká spořitelna a také z průzkumu, který provádí Česká bankovní asociace. Metodou analýzy budou zkoumány následující oblasti.

- Registrované trestné činy v oblasti kyberkriminality a celková kriminalita v České republice v letech 2013 až 2023.
- Registrované kybernetické podvody a celkové podvody v Plzeňském kraji v letech 2019 až 2023.
- Kybernetické podvody spáchané na klientech České spořitelny a výše škod způsobené jejím klientům v důsledku podvodů v letech 2020 až 2023.
- Kyberbezpečnost a nejčastěji se vyskytující kybernetické podvody v České republice v letech 2020 až 2023.

1 Základní pojmy v bankovnictví

V této kapitole budou specifikovány základní pojmy v bankovnictví. Nejprve zde bude uvedena definice a právní úprava bank a následně bude vymezen bankovní systém, centrální a obchodní banky a jejich druhy.

1.1 Právní úprava a definice bank

Nejdůležitější institucí v bankovním systému je bezesporu banka. V nařízení Evropského parlamentu a rady (EU) č. 575/2013 o obezřetnostních požadavcích na úvěrové instituce a investiční podniky není pojem banka vymezený, neboť zmiňuje pouze úvěrovou instituci. Dle tohoto nařízení je „úvěrovou institucí podnik, jehož činnost spočívá v přijímání vkladů nebo jiných splatných peněžních prostředků od veřejnosti a poskytování úvěrů na vlastní účet."

V českém právním předpisu, konkrétně v zákoně č. 21/1992 Sb., o bankách, je uvedena následující definice bank. „Bankami se rozumějí akciové společnosti se sídlem v České republice, které

a) přijímají vklady od veřejnosti, a
b) poskytují úvěry,

a které k výkonu činností podle písmen a) a b) mají bankovní licenci."

Přičemž za **vklad** se dle výše uvedeného zákona považují svěřené peněžní prostředky, které pro banku znamenají závazek vůči vkladateli na výplatu těchto peněžních prostředků. **Úvěrem** se pak rozumí dočasně poskytnuté peněžní prostředky.

Avšak důležitou podmínkou je poslední věta definice banky, která uvádí, že kteroukoliv činnost, tedy včetně obou výše uvedených, mohou banky vykonávat pouze na základě získané **bankovní licence**. Tato licence obsahuje přesný výčet činností, které banka smí provozovat, popřípadě obsahuje podmínky, které musí splnit před zahájením výkonu dané povolené činnosti a také během něj. Bankovní licenci uděluje Česká národní banka, a to zpravidla na dobu neurčitou. K jejímu získání je potřeba splnit nejprve několik podmínek a předložit žádost. (Česká národní banka, 2023a)

Česká národní banka (2023a) uvádí, že při rozhodování o udělení licence posuzuje především tyto faktory.

- Původ a složení minimální výše základního kapitálu, která je stanovena na 500 mil. Kč.
- Strategický záměr banky, její obchodní plán a analýzu trhu, na kterém se banka chystá působit.
- Způsobilost hlavních akcionářů a osob navrhovaných do statutárních či řídících orgánů banky.
- Technické i organizační podmínky pro výkon navrhovaných činností a další.

V zákoně č. 21/1992 Sb., o bankách, jsou uvedeny další činnosti, které je banka oprávněna vykonávat, pakliže jsou uvedené v jí udělené licenci. Jedná se například o:

a) investování do cenných papírů na vlastní účet,
b) platební služby a vydávání elektronických peněz,
c) poskytování záruk,
d) pronájem bezpečnostních schránek,
e) směnárenskou činnosti a další.

Právní předpisy upravující činnost bank v ČR

Z textu uvedeného výše je patrné, že hlavním právním předpisem pro sektor bankovnictví je zákon č. 21/1992 Sb., o bankách. Tento zákon upravuje činnost a fungování bank, včetně podmínek bankovní licence, bankovního tajemství nebo pojištění vkladů. Česká národní banka, jakožto vrchol českého bankovního systému, je pověřena výkonem zvláštních činností, které jiná instituce vykonávat nemůže. Z tohoto důvodu má svůj vlastní zákon, tedy zákon č. 6/1993 Sb., o České národní bance. Stavební spořitelny, které jsou označovány jako specializované banky, poskytují klientům stavební spoření na základě bankovní licence. Díky své specializaci je nutné jejich činnost upravit dalším právním předpisem, kterým je zákon č. 96/1993 Sb., o stavebním spoření. Družstevní záložny (tzv. kampeličky) za banky považovány nejsou, ale svým členům poskytují podobné služby jako banky svým klientům. Činnost těchto institucí je tedy upravena zákonem č. 87/1995 Sb., o spořitelních a úvěrních družstvech. Samotné zákony doplňuje ještě řada vyhlášek, které vydává Česká národní banka. Jedná se například

o vyhlášku č. 55/2023 Sb., o předkládaní výkazů bankami a pobočkami zahraničních bank České národní bance nebo vyhláška č. 399/2021 Sb., o úvěrových ukazatelích.

Instituce v bankovním sektoru se řídí jednak českými právními předpisy a jednak evropskými právními předpisy. Mezi evropské právní předpisy patří nařízení Evropského parlamentu a Rady (EU) č. 575/2013 o obezřetnostních požadavcích na úvěrové instituce a investiční podniky. Toto nařízení zahrnuje obezřetnostní požadavky na instituce, které souvisejí s fungováním trhů bankovních a finančních služeb. Účelem těchto požadavků je zajištění finanční stability poskytovatelů služeb na zmíněných trzích a také značnou úroveň ochrany investorů a vkladatelů. S tímto nařízením souvisí také směrnice 2013/36/EU (CRD IV) Evropského parlamentu a Rady o přístupu k činnosti úvěrových institucí a o obezřetnostním dohledu nad úvěrovými institucemi a investičními podniky. Směrnice upravuje přístup k činnosti těchto institucí, způsob jejich řízení, správy a rámec dohledu nad nimi.

1.2 Bankovní systém

Bankovní systém představuje všechny bankovní instituce v dané zemi a uspořádání vztahů mezi nimi. Primárně je tvořen složkou institucionální a funkční, které jsou vzájemně propojené.

Do **institucionální složky** se podle Lochmannové (2018) řadí prakticky všechny banky a člení se dle hlavní náplně jejich činnosti. Obecně kromě centrálních bank existují například:

- obchodní banky,
- stavební spořitelny,
- investiční banky,
- rozvojové banky,
- hypoteční banky a další.

Složka funkční pak znamená způsob uspořádání vztahů mezi jednotlivými bankovními institucemi v dané zemi. (Lochamnnová, 2018)
Bankovní systém jako takový lze rozčlenit na jednostupňový a dvoustupňový.

- Ve **dvoustupňovém systému**, který je běžný pro většinu tržních ekonomik, funguje samostatně centrální banka a obchodní banky. Centrální banka pak nevykonává činnosti, které spadají do kompetence obchodních či jiných bank. (Revenda, 2011)

- **Jednostupňový systém** je naopak charakteristický tím, že v něm jediná banka zastává roli jak centrální, tak i obchodní banky. Neznamená to, že v tomto systému nemohou existovat i jiné banky – mohou, ale jsou plně závislé na rozhodnutí centrální banky a mají úzký rozsah činností, které mají oprávnění vykonávat. Tento systém lze také označit jako systém monobanky, jejíž funkci u nás plnila v letech 1950–1990 Státní banka československá. (Kantnerová, 2016)

Jak uvádí Syrovátková (2023a), v závislosti na poskytovaných službách lze dále bankovní systém dělit na univerzální a specializovaný.

- **Univerzální bankovní systém** – v tomto bankovním systému banka poskytuje širokou škálu finančních služeb a produktů různým klientům i podnikům. Banka tak nabízí různé druhy služeb – úvěrové, investiční, spořící či pojišťovací.
- **Specializovaný bankovní systém** – naopak specializovaný bankovní systém se zaměřuje na poskytování užšího okruhu bankovních služeb. Za specializované se považují například investiční banky.

1.3 Centrální bankovnictví

Centrální banky hrají důležitou roli v ekonomickém systému každé země. Již ve svých prvopočátcích měly centrální banky od státu svěřený emisní monopol. Poté začaly fungovat také jako banky státu, což znamená, že státu poskytovaly úvěry, vedly jeho účty nebo spravovaly státní dluh. (Kantnerová, 2016)

Jak uvádí Mejstřík, Pečená & Teplý (2015), v současnosti se rozlišují dvě základní funkce centrální banky – makroekonomická a mikroekonomická.

Funkce makroekonomická spočívá v provádění měnové politiky, emisi hotovostních peněz a devizové činnosti. Níže jsou vysvětleny jednotlivé činnosti.

- **Provádění měnové politiky**

  V rámci měnové politiky centrální banka reguluje nabídku peněz tak, aby bylo dosaženo stanovených monetárních cílů. Do monetárních cílů se řadí především zajištění cenové stability, dále pak zajištění vyrovnanosti platební bilance, udržení přijatelné míry nezaměstnanosti a podpora růstu ekonomiky. Centrální banka může pomocí nástrojů měnové politiky provádět restriktivní nebo expanzivní měnovou politiku. (Lochmannová, 2018) Nejčastěji využívá takzvané nepřímé tržní nástroje,

kam patří operace na volném trhu, diskontní nástroje, kurzové intervence a povinné minimální rezervy.

Při realizaci měnové politiky, a hlavně při zajišťování cenové stability je naprosto zásadní **nezávislost centrální banky** na vládě. Je to z toho důvodu, aby vláda například nemohla centrální banku přimět k učinění opatření, která by sice v krátkém období mohla podpořit ekonomický růst, ale následně by mohla způsobit růst inflace. Centrální banka musí tedy jednat vždy „objektivně" bez vlivu vlády. (Kantnerová, 2016)

- **Emise hotovostních peněz**

  Pravomoc vydávat národní měnu mají pouze centrální banky a to, jak bylo zmíněno výše, od jejich počátku. Lze tedy konstatovat, že jsou centrální banky takzvaní „strážci měny". (Polouček, 2013)

- **Devizová činnost banky**

  Primárním cílem devizové činnosti banky je zajištění dostatečné devizové likvidity země. Do devizové činnosti se zařazuje vytváření a správa devizových rezerv státu. Pokud je tedy potřeba, centrální banka je oprávněna nakupovat nebo prodávat národní měnu, aby stabilizovala měnový kurz. (Černohorský, 2020)

Druhou funkcí centrální banky je **funkce mikroekonomická**, do které patří především regulace a dohled nad bankami a také fungování jako banka bank a banka státu.

- **Regulace a dohled nad bankami**

  V rámci bankovní regulace má centrální banka za úkol stanovovat pravidla a podmínky pro založení a činnost obchodních bank. Provádění bankovního dohledu pak znamená, že centrální banka následně i kontroluje dodržování stanovených pravidel. (Blahová, 2018)

- **Banka bank a banka státu**

  Centrální banka také vystupuje jako banka pro obchodní banky. Znamená to, že ostatním bankám vede účty, přijímá od nich vklady a poskytuje jim úvěry. Jako banka státu vede státu účty, převádí úhrady a spravuje především státní dluh. Dále (kromě vlády) realizuje některé operace pro i centrální orgány nebo pro některé podniky působící ve veřejném sektoru. (Lochmannová, 2018)

Česká národní banka

Bankovní systém v České republice je univerzální dvoustupňový, neboť jej tvoří centrální banka, kterou je Česká národní banka (dále jen ČNB) a obchodní banky. ČNB vznikla 1. ledna 1993 a je nezávislou institucí a právnickou osobou veřejného práva, která sídlí v Praze. Nejvyšším orgánem ČNB je sedmičlenná bankovní rada, jejíž členy jmenuje prezident nejdéle na dvě šestiletá období. (Česká národní banka, 2023c)

Primárním cílem centrální banky je péče o cenovou stabilitu. ČNB má za úkol zajistit nízkou (nikoliv nulovou), stabilní a zároveň předvídatelnou inflaci. Měnovou politikou chce inflaci udržovat v blízkosti 2 %, protože tato hladina inflace vytváří žádoucí prostředí pro růst životní úrovně domácností a také pro rozvoj podnikatelských činností. (Česká národní banka, 2023b) Dále také vykonává i ostatní činnosti typické pro centrální banku. Vydává oběživo, vykonává dohled nad bankovním sektorem (vydává bankovní licenci), pojišťovnami, družstevními záložnami či směnárnami, řídí a kontroluje platební styk a peněžní oběh a v neposlední řadě také poskytuje služby státu a veřejnému sektoru. (Česká národní banka, 2023c)

Ačkoliv ČNB chce udržovat inflaci v blízkosti 2 %, dlouhou dobu se to díky řetězci událostí, které v minulých letech nastaly, nedaří. Například v roce 2022 dle Českého statistického úřadu (2023) byla průměrná roční míra inflace 15,1 %, což je vysoko nad inflačním cílem. Nicméně v srpnu 2023 dle očekávání ČNB cenová hladina meziročně vzrostla o 8,5 %, což ale znamená, že inflace sedmý měsíc po sobě zpomaluje. Návrat ke 2 % ČNB očekává nejdříve až v roce 2025. (Česká národní banka, 2023d)

1.4 Obchodní bankovnictví

Obchodní banky jsou podnikatelské subjekty, které jsou ovšem ve srovnání s ostatními podniky v mnoha ohledech odlišné. Například podmínky, které banka musí před svým založením splnit, následná nutnost získání bankovní licence, neustálý dohled a regulace centrální bankou nebo i celkové postavení v ekonomice jsou velmi specifické rysy pro instituce v sektoru bankovnictví. Zároveň tyto odlišnosti potvrzuje i fakt, že je činnost bank upravena konkrétně a přísněji (v zákoně o bankách), zatímco ostatní podniky se řídí běžnou právní úpravou podnikání, tedy zákonem o obchodních korporacích. Co však mají banky s ostatními podniky společné je jejich hlavní cíl, kterým je dosažení a maximalizace zisku.

Na banky lze nahlížet ze dvou hledisek, a to z hlediska legislativního a ekonomického. **Legislativním** přístupem je myšlena právě již dříve zmíněná definice banky vyplývající ze zákona o bankách. Znamená to tedy, že banky poskytují úvěry, přijímají vklady a musí mít přidělenou bankovní licenci. Z pohledu **ekonomického** je banka podnik, který obchoduje s penězi a zprostředkovává pohyb peněžního kapitálu mezi různým subjekty v ekonomice. (Revenda, 2011)

Základní funkce bank

Obchodní banky plní několik základních funkcí.

- **Finanční zprostředkování** – to představuje shromažďování vkladů a jejich umisťování tak, aby přinášely co nejvyšší zhodnocení. Což se děje právě proto, že jsou banky podnikatelské subjekty, které provádí finanční zprostředkování na ziskovém principu. (Černohorský, 2020)
- **Emise bezhotovostních peněz** – na rozdíl od hotovostních peněz, které emituje pouze centrální banka, peníze ve formě záznamů na bankovních účtech, tj. bezhotovostní peníze, mohou emitovat i banky. Znamená to, že banky díky emisi bezhotovostních peněz nemusí poskytovat úvěry pouze z přijatých depozit, ale i nad jejich rámec. (Revenda et al., 2023)
- **Provádění platebního styku** – banky zabezpečují jednu z velmi podstatných podmínek pro fungování tržní ekonomiky, kterou je realizace plateb. (Černohorský, 2020)
- **Zprostředkování finančního investování na peněžním a kapitálovém trhu** – banky zajišťují i emisi cenných papírů a následně pomáhají svým klientům s investováním jejich finančních prostředků, aby dosáhli zamýšlených finančních cílů. Banky také nabízejí úschovu a správu aktiv či zprostředkování nákupů a investičních obchodů. (Revenda et al., 2023)

1.4.1 Členění bank

Banky lze obecně členit na:

a) **univerzální banky** – tyto banky nabízí řadu finančních služeb – depozita, spotřebitelské i hypoteční úvěry, zprostředkování platebního styku a další. Zjednodušeně lze říct, že se věnují komerční i investiční činnosti. S univerzálními bankami se lze v České republice setkat nejčastěji. (Černohorský, 2020)

b) **specializované banky** – jak už název napovídá, specializované banky jsou zaměřené pouze na určité druhy služeb. Jedná se například o hypoteční banky, záruční, investiční či spořitelní banky. (Bankovnictví, finance – Studium, 2023)

Podle Syrovátkové (2023b) lze pak univerzální banky rozdělit na základě bilanční sumy, a to na:

a) **velké banky** – do této kategorie se řadí banky, které mají bilanční sumu nad 150 mld. Kč. V České republice to je například ČSOB, Česká spořitelna nebo Komerční banka.

b) **střední banky** – za střední banky se považují takové, které mají bilanční sumu v rozmezí 50 až 150 mld. Kč. Příkladem je GE Money Bank, Raiffeisenbank nebo Citibank.

c) **malé banky** – u malých bank pak bilanční suma nepřevyšuje 50 mld. Kč. Patří sem například Volksbank, J&T banka nebo PPF banka.

Banky se mohou členit také podle vlastnictví, a to na:

a) **soukromé banky** – banky mají formu akciových společností a jejich vlastníky jsou akcionáři. (Bankovnictví, finance – Studium, 2023)

b) **veřejnoprávní banky** – to jsou banky, které celé nebo alespoň z části vlastní či založil stát. Často se tyto banky využívají k financování veřejných projektů nebo ekonomických aktivit. (Bankovnictví, finance – Studium, 2023) Mezi tyto banky v ČR patří Česká exportní banka nebo Národní rozvojová banka.

c) **družstevní záložny** – družstevní záložny nebo také kampeličky sdružují osoby s podobnými zájmy. Také poskytují úvěry a přijímají vklady, ale tyto služby poskytují jen svým členům. (Černohorský, 2020)

Dále podle Černohorského (2020) a Šenkýřové (2010) lze banky rozčlenit z hlediska převažujících obchodů.

a) **Obchodní banky** – hlavním úkolem těchto bank je přijímání vkladů, poskytování úvěrů a zprostředkování platebního styku. Jejich klienty mohou být fyzické osoby, ale i podniky jakékoliv velikosti. V dnešní době však převládají právě univerzální banky, které kombinují komerční činnosti s investičními.

b) **Investiční banky** – mezi hlavní činnosti těchto bank se řadí správa aktiv, emise, obchodování a správa cenných papírů, investiční poradenství či poskytování dlouhodobých investičních úvěrů. Tyto banky byly populární v USA, ale dnes už se i z těchto bank staly spíše univerzální, jen se ve většině případů stále zaměřují hlavně na investiční činnosti.

c) **Spořitelny** – spořitelny byly jedny z prvních bank a zaměřovaly se především na sběr vkladů a poskytování úvěrů fyzickým osobám, o které komerční banky nejevily zájem. Dnes už se z nich většinou staly také klasické univerzální banky. Například Česká spořitelna, která v ČR působí dodnes, už nepůsobí jako klasická spořitelna, nýbrž jako univerzální banka.

d) **Hypoteční banky** – tyto banky poskytují dlouhodobé úvěry na pořízení nemovitosti, které jsou zajištěné zástavním právem k nemovité věci. Z těchto úvěrů se financuje pořízení, stavba či rekonstrukce nemovitosti. Jako zdroj financování těchto úvěrů banky používají hypoteční zástavní listy. V České republice mohou hypoteční úvěry poskytovat i univerzální banky, které tuto činnost mají uvedenou v bankovní licenci.

e) **Stavební spořitelny** – i stavební spořitelny se zaměřují na financování pořízení nebo opravy nemovitosti, ale na základě odlišného principu. Žadatel o úvěr musí být nejprve účastníkem stavebního spoření, což znamená, že musí ukládat, popřípadě jednorázově uložit dané procento budoucího úvěru u stavební spořitelny. Černohorský (2020, s. 322) dále uvádí, že „z těchto klientských vkladů tvoří stavební spořitelny fond, z kterého pak poskytují úvěry. Do tohoto systému nesmí přicházet v podstatě žádné jiné zdroje financování a zároveň takto získané zdroje nesmí být použity na nic jiného než na poskytnutí úvěru ze stavebního spoření.“ V České republice musí mít stavební spořitelny samostatnou licenci, nepůsobí tedy jako univerzální banky.

2 Bankovní regulace a dohled bank

Z pohledu Revendy (2011, s. 119) zní definice regulace a dohledu následovně. „Regulací rozumíme koncipování a prosazování podmínek, pravidel a rámce činnosti bankovních institucí v dané ekonomice.“ A podle Blahové (2018, s. 18) by „regulace bank měla přispívat k zabezpečení spolehlivosti a efektivnosti bankovního systému.“

Obecně regulace bankovního sektoru představuje soubor pravidel a opatření, která mají za cíl zajistit stabilitu a bezpečnost bankovního systému a také ochranu zájmů klientů. Regulace zahrnuje například pravidla pro výpočet kapitálové přiměřenosti, požadavky na řídící a kontrolní systém banky nebo pravidla angažovanosti. (Černohorský, 2020)

Dle České národní banky (2023e) je v dnešní době regulace a dohled nad bankami nezbytnou součástí finančního sektoru, neboť bezpečnost a stabilita tohoto sektoru jsou pro fungování ekonomiky zásadními podmínkami. Avšak tyto podmínky nelze zabezpečit pouze pomocí tržních mechanismů, a právě proto činnosti poskytovatelů platebních služeb a vydavatelů elektronických peněz v České republice (ale i v ostatních vyspělých zemích) podléhají velmi značné míře regulace, která je prováděna autorizovanými orgány.

Podle Černohorského (2020) regulace obsahuje například následující pravidla.

a) Pravidla kapitálové přiměřenosti

Kapitálová přiměřenost je jedno z klíčových regulatorních pravidel. Jedná se o minimální množství kapitálu, které banka musí udržovat vzhledem k jejím aktivům. (ČBA, 2024a) Jílek (2000, s. 261) uvádí, že „podstatou koncepce kapitálové přiměřenosti je změření rizik daného subjektu a stanovení odpovídající minimální úrovně kapitálu“. Hodnota kapitálu má být tak velká, aby pokryla případné ztráty v budoucnu.

Pokud by kapitál banky regulován nebyl, je pravděpodobné, že by banky disponovaly nepřiměřeně nízkým objemem kapitálu ve srovnání s podstupovanými riziky. Avšak tím, že banka disponuje převážně cizími zdroji, je potřeba omezovat rizika ztráty vkladatelů nebo jiných věřitelů a přenést patřičnou odpovědnost za případné ztráty na majitele. (Blahová, 2018) Kromě ochrany vkladatelů přispěje kapitálová přiměřenost i k zajištění stability banky, neboť dostatečný kapitál jí bude sloužit jako „bezpečnostní polštář“.

b) Pravidla angažovanosti

Hlavní myšlenkou těchto pravidel je to, aby banka nebyla spojena s úspěšností daného klienta. Byly proto stanoveny například maximální limity úvěrů vůči jednomu klientovi, vlastníkům banky, dceřiným společnostem či vlastním zaměstnancům. (Jurošková, 2012)

c) Pravidla likvidity

Cílem je stanovení minimálních požadavků na řízení likvidity, které banky musí dodržovat, aby následně byly schopny udržovat trvalou platební schopnost. (Černohorský, 2020)

d) **Požadavky na řídící a kontrolní systém banky**

Tyto požadavky představují řádné řízení rizik, řízení a správu společnosti a také systém vnitřní kontroly. Jsou zde stanoveny například strategie řízení rizik, povinnosti a oprávnění představenstva, zásady systému vnitřní kontroly nebo bezpečnostní zásady. (Černohorský, 2020)

2.1 Bankovní regulátoři

Regulaci provádí nejčastěji centrální banky. Dohled nad bankovním sektorem mohou vykonávat centrální banky, ministerstvo financí nebo nezávislé instituce. V rámci organizace bankovní regulace a dohledu dochází ke spekulacím, zda by tyto činnosti měl vykonávat jeden nebo naopak více bankovních regulátorů. (Blahová, 2018)

Kromě počtu bankovních regulátorů se také zpochybňovalo, zda by právě tím jedním měla být centrální banka. V její prospěch hovoří několik argumentů. Podle Juroškové (2012) je argumentem například to, že má centrální banka velmi kvalifikované zaměstnance a je nezávislou institucí. Dále v její prospěch svědčí fakt, že mezi monetární a finanční stabilitou existuje významný vztah a v neposlední řadě, že centrální banka vystupuje v roli věřitele poslední instance – to znamená, že je to pro ostatní banky instituce, na kterou se obrátí v případě, že potřebují peníze. Banka tak potřebuje informace o zdraví banky, aby mohla zasáhnout, pokud by nastal problém.

Naopak dle Poloučka (2013) mezi důvody, proč by centrální banka neměla být bankovním regulátorem patří riziko, že ve prospěch bankovního sektoru bude banka provádět mírnější monetární politiku. Dalším důvodem je obava o pověst centrální banky. Výkon dohledu totiž nemusí působit jako pozitivní funkce a mohla by nastat situace, kdy

by se centrální banka rozhodla tak, aby si uchovala dobrou pověst. Tyto důvody lze označit spíše za spekulace, neboť nikdy nebyly prakticky doloženy.

Příklady zemí (kromě ČR), kde regulaci i dohled vykonává centrální banka:

- Slovensko – Národná banka Slovenska (NBS, 2024),
- Irsko – Central Bank of Ireland. (CBoI, 2024)

Příklady zemí, kde je dohled integrován i mimo centrální banku – nejčastěji se daná specializovaná instituce o výkon dohledu dělí s příslušnou centrální bankou:

- Francie – dohled provádí Autorité de Contrôle Prudentiel et de Résolution spolu s centrální bankou Banque de France (ACPR, 2024),
- Finsko – dohled provádí Finnish Financial Supervisory Authority spolu s centrální bankou Bank of Finland (FIN-FSA, 2024),
- Švédsko – dohled provádí Swedish Financial Supervisory Authority spolu s centrální bankou Riksbank. (FI, 2024)

2.2 Bankovní unie

Bankovní unie vznikla jako reakce na finanční krizi v roce 2008. Klade si za cíl vytvářet transparentnější, jednotné a bezpečné evropské bankovnictví. Transparentnosti chce bankovní unie dosáhnout uplatňováním jednotných pravidel na bankovní dohled, ozdravení a řešení krizí bank. Jednotnosti napomůže rovným přístupem ke všem bankovním aktivitám. A bezpečnějším se má evropské bankovnictví stát pomocí včasného provádění intervencí v bankách. (European Central Bank, 2024a)

Bankovní unie je tvořena všemi členskými státy eurozóny. Součástí bankovní unie se mohou stát i ostatní státy mimo eurozónu a to tím, že zahájí úzkou spolupráci s Evropskou centrální bankou (ECB). (Council of the European Union, 2024)

Česká republika součástí bankovní unie není. Podle vyjádření bývalého guvernéra ČNB Jiřího Rusnoka by se ČR měla stát součástí bankovní unie až v momentě přijetí eura. (Česká národní banka, 2021)

Jak již bylo zmíněno, v České republice provádí regulaci i dohled nad bankami centrální banka, tedy Česká národní banka. V rámci Evropské unie má na starost regulaci bankovního sektoru Evropský orgán pro bankovnictví (European Banking Authority –

EBA), jehož primárním cílem je vytvoření jednotných pravidel pro bankovní sektor pro celou EU a dohlížení na jejich dodržování. (European Banking Authority, 2024)

Bankovní unie se opírá o dva základní pilíře:

a) jednotný mechanismus dohledu,
b) jednotný mechanismus pro řešení krizí.

Oba tyto pilíře fungují na základě jednotného souboru pravidel. Jednotný soubor pravidel obsahuje pravidla zaměřené na kapitálové požadavky, ozdravení a řešení krizí ve všech zemích EU. (Haentjens & Gioia-Carabellese, 2015)

Pro bankovní dohled v Evropě byl vytvořen takzvaný jednotný mechanismus dohledu (Single Supervisory Mechanism – SSM). Součástí SSM je Evropská centrální banka (ECB) a další vnitrostátní orgány dohledu zemí, které se účastní. Automatickou účast v evropském bankovním dohledu mají všechny země eurozóny. Ostatní země EU se mohou účastnit na základě dobrovolného rozhodnutí. (European Central Bank, 2024b)

Hlavním účelem druhého pilíře, tedy jednotného mechanismu pro řešení krizí (Single Resolution Mechanism – SRM) je zajištění efektivního řešení problémů bank v krizi při minimálních nákladech pro daňové poplatníky a ekonomiku. (European Commission, 2024a)

2.3 Dohled

Mezi regulací bank a dohledem je tenká hranice, minimálně proto, že se vzájemně prolínají, ale stále jsou to rozdílné pojmy. Revenda (2011, s. 123) definuje dohled bank jako „kontrolu dodržování pravidel činnosti, včetně stanovení sankcí při neplnění pravidel.“ ČNB vykonává dohled jako dalším krok v péči o stabilitu a rozvoj finančního systému. Do výkonu dohledu spadá kontrola činnost platebních institucí, institucí elektronických peněz, vydavatelů elektronických peněz malého rozsahu a poskytovatelů platebních služeb malého rozsahu. Cílem je posilovat důvěru veřejnosti v bankovní systém, zamezovat systémovým krizím a také podporovat tržní disciplínu institucí, na které centrální banka dohlíží. (Česká národní banka, 2023c)

Dle České bankovní asociace (2021a) může ČNB jakožto bankovní regulátor vykonávat:

a) dohled na dálku,
b) dohled na místě.

Dohled na dálku

Dohled na dálku standardně probíhá pomocí pravidelných reportů, které banky mají povinnost předkládat. Na základě různých ukazatelů ČNB sleduje, zda banka dodržuje stanovená pravidla. Zároveň je ČNB schopna na základě těchto získaných informací vyhodnocovat i její ekonomickou situaci. Díky těmto opatřením je možné v případě nedostatků včas reagovat a nenaruší se a ani nehrozí stabilita finančního trhu. (ČBA, 2021a)

Dohled na místě

Jak už z názvu vyplývá, v rámci dohledu na místě provádí ČNB kontroly přímo v prostředí banky. Pravidelnými i příležitostnými kontrolami tak opět zjišťuje, zda banka dodržuje nastavená pravidla. ČNB má ovšem možnost náhledu do archivů či počítačů a také veškerých podkladů, ať už elektronických či písemných. V závislosti na tom, co ČNB aktuálně prověřuje, mohou být kontroly pouze dílčí anebo komplexní. (ČBA, 2021a)

2.4 Odůvodnění regulace

Názory na míru regulace se obecně značně liší. Mezi nejčastější argumenty opodstatňující regulaci bankovního sektoru patří:

a) poskytování specifických služeb,
b) informační asymetrie,
c) negativní externality.

Podle Revendy (2011) není regulace bankovního sektoru potřebná kvůli specifičnosti oboru podnikání, neboť je banka akciovou společností. Avšak náplň činnosti bank se oproti jiným podnikatelským subjektům zcela liší. Jelikož banky emitují bezhotovostní peníze, zabezpečují platební styk a hospodaří především s cizími zdroji v podobě klientských vkladů, je potřeba stanovit základní pravidla sloužící mimo jiné k ochraně před nelegálními transakcemi nebo před ztrátami vkladatelů. Ztráty vkladatelů je dle stejného autora vhodné případně snížit pojištěním vkladů.

Blahová (2018) uvádí například informační asymetrii jako oprávněný důvod pro regulaci. Informační asymetrie znamená, že každý subjekt v rámci daného oboru disponuje různými informacemi. V bankovním sektoru se jedná samozřejmě jednak o nedostatek informací na straně klienta a jednak nedostatku informací na straně banky. Klient jakožto

vkladatel nebude nikdy schopen sám vyhodnotit zdraví, rizikovost nebo důvěryhodnost banky. Naopak banka i přes důkladné prověřování bonity klienta nemůže stoprocentně odhadnout, zda bude klient schopen bezproblémově splatit celý svůj závazek.

Za poslední podnět hovořící ve prospěch regulace uvádí Jurošková (2012) negativní externality. Za projev negativní externality lze považovat například systémové riziko, které znamená, že krizi celého finančního sektoru může díky dominovému efektu způsobit úpadek pouze jedné instituce. Úpadek jedné banky může totiž narušit důvěru a vyvolat obavy o solventnosti ostatních bank, což může nakonec vyústit až v situaci, kdy si klienti budou chtít hromadně vybrat své vklady (jedná se o tzv. run na banku). Tím, že hlavní podíl na zdrojích bank mají právě vklady klientů, se může stát, že banka nebude schopna svým závazkům dostát.

Argumenty proti regulaci

Podle Poloučka (2013) je nejméně tolerováno pojištění vkladů bank. Uvádí, že odpůrci této podmínky argumentují tím, že banky mohou mít tendenci k provádění rizikovějších operací. Jurošková (2012) zmiňuje existenci takzvaných zastánců svobodného bankovnictví. Ti zastávali tvrzení, že kdyby banky měly větší volnost, byly by více disciplinované. Avšak toto tvrzení bylo opřené pouze o fakt, že banky v dávných dobách minimální regulace nebyly tolik náchylné k selhání. Blahová (2018) pak uvádí jako negativum náklady, které vzniknou v souvislosti s regulací. A kromě nákladů se také zvyšují administrativní povinnosti centrální banky i dalších orgánů. Dále je také zdůrazněno, že se na krize nebo kterékoliv problémy vždy reaguje novou zpřísněnou regulací místo toho, aby se například zintenzivnily průběžné kontroly.

3 Rizika v bankovním sektoru

Bankovní sektor je vystaven velkému množství rizik. Tato rizika lze rozdělit dle různých autorů do několika skupin. Blahová (2018) uvádí ve své publikaci rizika úvěrová, tržní, operační, likviditní, strategická a reputační. Dle Lochmannové (2018) lze za bankovní rizika považovat úroková, úvěrová, měnová, likviditní a kapitálová. A například dle Mejstříka, Pečené & Teplého (2015) se bankovní rizika dělí na finanční a nefinanční. Mezi finanční řadí kreditní, tržní a likviditní riziko a mezi nefinanční například riziko operační, právní, daňové, politické či vypořádací.

3.1 Členění rizik

Za čtyři základní druhy rizik, ve kterých se většina autorů shoduje, lze považovat:

a) kreditní (úvěrové),
b) likviditní,
c) tržní,
d) operační.

Kreditní neboli **úvěrové riziko** představuje možnou ztrátu vyplývající z platební neschopnosti druhé strany splácet své závazky. Toto riziko se dá označit za základní – vyskytuje se nejen v bankovním sektoru, ale v jakémkoliv oboru podnikání. Typickým příkladem v bankovnictví je nesplácení spotřebitelského či jiného úvěru spotřebitelem. V jiném podnikání by příkladem mohlo být nezaplacení obchodních faktur nebo dokonce nevyplacení mezd zaměstnancům.
Toto riziko může banka omezit pomocí důkladné prověrky bonity klienta, pomocí zajištění úvěrů (zástavou či ručením) nebo také monitorováním platební morálky či stanovením kreditních limitů. (Kantnerová, 2016)

Riziko likvidity znamená neschopnost banky dostát svým závazkům v době jejich splatnosti a daném objemu. Nejčastěji je způsobeno časovým nesouladem peněžních toků na straně aktiv a pasiv, který způsobí, že banka není schopna hromadně vyplatit vklady klientům či provést platbu z bankovního účtu na základě příkazu. (Černohorský, 2020)

Tržní riziko označuje riziko ztráty, která nastane na základě změn tržních podmínek. Může se jednat o změnu hodnoty aktiv, devizových kurzů nebo úrokových sazeb. Banka

by proto měla přizpůsobit strukturu aktiv a pasiv tak, aby jejich citlivost na změnu tržních úrokových sazeb byla alespoň částečně shodná. (Kantnerová, 2016)

Operační riziko představuje možnou ztrátu, která vznikne jako důsledek selhání, nedostatků nebo chyb ve vnitřních procesech, lidském faktoru, systémech nebo vlivem externalit. Je to riziko, které je spjaté s běžným provozem banky, respektive s jejími procesy a nejdůležitějšími prvky těchto procesů, tedy personálem, systémy a technologiemi. Toto riziko tak ovlivňuje efektivitu, kontinuitu a bezpečnost provozních činností banky, a proto také bylo nazýváno jako provozní riziko. (Blahová, 2018)

Původně bylo spíše opomíjené a řadilo se mezi „ostatní" rizika. Za ta „hlavní" rizika se považovala pouze úvěrová a tržní, protože obě tato rizika souvisela s úvěrovými, obchodními nebo investičními portfolii instituce. Operační riziko se spojovalo především s lidským faktorem, tedy ať už vědomým či nevědomým selháním a chybou lidí. Avšak díky novým formám projevů tohoto rizika, které vznikaly například s elektronickou distribucí finančních produktů a služeb a také celkovým vývojem informačních technologií, se vnímání tohoto rizika ukázalo jako nedostatečné. (Česká národní banka, 2008) Potřebná pozornost se operačnímu riziku začla věnovat po vytvoření regulatorního konceptu kapitálové přiměřenosti Basel II.

Za vybrané události operačního rizika dle České národní banky (2008) lze označit:

a) šekové podvody (skupiny retailových bank v USA),
b) zneužití klientských účtů zaměstnanci banky (ABN AMRO v Nizozemsku),
c) teroristický útok na WTC (Světové obchodní centrum),
d) selhání služby Sporoservis[1] (Česká spořitelna).

Výše uvedená rizika byla „aktuální" pravděpodobně v letech 2000–2008. Za operační rizika v roce 2024 se dle CSchlattera (2023) považují následující.

a) Kybernetické bezpečnostní hrozby – banky jsou v oblasti kybernetických útoků velmi zranitelné. V dnešním digitálním světě dochází k neuvěřitelně rychlému rozvoji hackerských útoků či podobných incidentů, které mohou ohrozit údaje, a především peníze klientů, narušit provoz banky a následně i její důvěru.

[1] Sporoservis – poskytnutí rychlého úvěru či prodeje na splátky – služba České spořitelny poskytována okolo roku 2000

b) **Technologická selhání** – inovace v oblasti technologií nesou značné příležitosti, ale stejně tak i rizika. Vývoj umělé inteligence či blockchain (distribuovaná decentralizovaná databáze) může být i pro banky velmi užitečný a jistě zvýšit efektivitu, ale existuje zde riziko selhání, výpadků nebo problémů s integritou dat.
c) **Geopolitické a ekonomické hrozby** – bankovní instituce jsou vystaveny rizikům, která plynou z politických změn, globálních ekonomických trendů nebo geopolitických konfliktů.
d) **Dodržování předpisů** – banky působí v jednom z nejvíce regulovaných prostředí. A právě i vývoj regulace například v důsledku technologického vývoje může pro banky představovat významná rizika. Banky by tak měly posilovat vnitřní kontrolní systémy, a především sledovat regulační změny.

3.2 Basilejské dohody

V roce 1974 byl centrálními bankami zemí skupiny G-10 vytvořen tzv. Basilejský výbor pro bankovní dohled (Basel Committee on Banking Supervision – BCBS), který je součástí Banky pro mezinárodní platby (Bank for International Settlements – BIS). Tento výbor je hlavním světovým orgánem pro stanovování standardů pro obezřetnostní regulaci bank a doporučení pro bankovní dohled. (BIS, 2024) Basilejským výborem bylo vypracování několik dohod o kapitálové přiměřenosti bank – Basel I, Basel II a Basel III. Cílem těchto dohod je zabezpečit, aby banky disponovaly dostatečným kapitálem vzhledem k různým typům rizik, se kterými se mohou setkat a omezilo se tak riziko bankovního selhání nebo pádu bank. (Česká národní banka, 2024)

Basel I

První z basilejských dohod vznikla již v roce 1988 pod názvem Basel I. Tato dohoda je opravdovým počátkem regulace kapitálové přiměřenosti. Zásadním úmyslem této dohody bylo, aby banka držela ke každému rizikovému aktivu danou výši kapitálu, tzn. aby vytvářela tzv. kapitálový „nárazník“. (Jurošková, 2012) Basel I byl však soustředěn pouze na nízkoriziková aktiva (která vyžadují nižší objem kapitálu) a úvěrové riziko, neboť toto riziko bylo vnímáno jako primární příčina pádu bank. (IBM, 2024) Minimální úroveň kapitálu ke krytí úvěrového rizika byla v rámci dohody stanovena na 8 %. O několik let později však vznikl dodatek k této dohodě za účelem zahrnutí i tržního rizika. Doporučení započítat i tržní riziko vzniklo kvůli aktivním obchodům bank na trzích. (Blahová, 2018)

Basel II

Rychlý vývoj finančního trhu si žádal propracovanější a komplexnější přístupy k rizikům. Nová basilejská dohoda byla po několika dřívějších neúspěšných pokusech schválena v červnu 2004. V této dohodě bylo bankám umožněno používat interní hodnocení rizik, aby byly lépe vystiženy rizikové profily jednotlivých bank. (Heffernan, 2005) Dále se také nově zahrnulo operační riziko mezi faktory, které banka musí při stanovování kapitálových požadavků zohledňovat. A v neposlední řadě byla v rámci nové dohody vytvořena třípilířová struktura kapitálových požadavků.

Obsah jednotlivých pilířů

- **Pilíř 1 – Minimální kapitálové požadavky**

  První pilíř je považován za nejdůležitější a navazuje na původní dohodu Basel I. Upravuje minimální množství kapitálu, které bance slouží k pokrytí případných ztrát plynoucích z úvěrového, tržního a nově i operačního rizika. (Jurošková, 2012)

- **Pilíř 2 – Proces dohledu**

  S druhým pilířem se začíná klást důraz na individuální rizikový profil banky. Banky by měly vypracovat vlastní procesy hodnocení kapitálových potřeb a řízení rizik. Tyto procesy jednotlivých bank by měl následně kontrolovat orgán bankovního dohledu, který by měl ověřit i správnost určování kapitálového požadavku. (Blahová, 2018)

- **Pilíř 3 – Tržní disciplína**

  Třetí pilíř se zaměřil na transparentnost a zveřejňování informací o podnikání bank. Hlavní myšlenkou je posílení tržní disciplíny tím, že banky mají v dané periodicitě a rozsahu o sobě zveřejňovat více informací. Je třeba zveřejňovat především informace, které se týkají kapitálové struktury, přiměřenosti a rizik. Tento pilíř se považuje za velmi užitečný, neboť ostatním tržním účastníkům umožní posoudit stabilitu i rizikový profil banky. (Jurošková, 2012)

Basel III

V důsledku finanční krize byl Basel II upraven a v roce 2010 byla publikovány nová pravidla v podobě Basel III. Cílem nové dohody bylo především zvýšení odolnosti bank vůči finančním krizím a také stability finančního trhu. Nově tak pro banky vznikla povinnost držet kapitálové rezervy. (Blahová, 2018)

4 Bankovní podvody

Nelegální činnosti, se kterými se lze v bankovnictví setkat, jsou bankovní podvody. Z pohledu rizik se bankovní podvody mohou zařadit do operačních rizik, neboť bance hrozí ztráta plynoucí ze selhání (nejen) lidského faktoru. Bankovní podvody existují v mnohých podobách a zahrnují širokou škálu nekalých praktik, které se nejčastěji zaměřují na neoprávněné získání nebo zneužívání finančních prostředků. V posledních letech rapidně přibývá podvodů na internetu, tedy kybernetických podvodů. Nepříznivým faktem je, že absolutní ochranu před těmito různými podvody či zneužíváním nelze vytvořit, a to i přes snahu legislativy i bankovní regulace a dohledu.

Ekonomická kriminalita

Podvod jako takový je trestným činem. Dle § 209 trestního zákoníku spáchá podvod ten „kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu“. Se samotnými bankovními podvody se lze setkat v souvislosti s ekonomickou kriminalitou.

Ekonomická kriminalita je dle Častorála (2007, s. 9) „protiprávní jednání s ekonomickými prvky, kterým je dosahováno majetkového nebo jiného prospěchu a které naplňuje skutkovou podstatu některého z trestných činů“. Ekonomická kriminalita je však rozsáhlý pojem, neboť zahrnuje také hospodářskou kriminalitu a ta zahrnuje ještě finanční kriminalitu. V tomto případě budou bankovní podvody zařazeny konkrétně do kriminality finanční, jelikož se jedná o trestný čin páchaný ve finančním sektoru.

Fryšták (2007) ve své publikaci uvádí, že za projev finanční kriminality se považuje jednání směřované proti fungování bankovního systému, kapitálového trhu a finančních institucí – především bank, pojišťoven nebo investičních fondů. Zároveň je ve stejné publikaci uvedeno, že nejčastějšími projevy finanční kriminality může být například:

- přijímání vkladů podnikatelskými subjekty bez bankovní licence za účelem jejich dalšího zhodnocení,
- bankovní podvody při zprostředkování úvěrů,
- podvody s transferem peněz, falešnými směnkami či šeky nebo bankovními zárukami,
- insider traiding,
- praní špinavých peněz.

V oblasti hospodářské kriminality jsou v § 233 až 239 trestního zákoníku definovány další trestné činnosti, které souvisí s bankovním sektorem. Jedná se například o:

- padělání a pozměňování peněz a jejich udávání do oběhu,
- neoprávněné opatření, padělání a pozměnění platebního prostředku (nejčastěji bezhotovostního platebního prostředku – např. platební karty),
- neoprávněná výroba peněz a další.

Členění podvodů

V současnosti existuje několik podob, druhů i způsobů bankovních podvodů a je pravděpodobné, že jich v budoucnu přibude. Z tohoto důvodu je možné bankovní podvody rozlišit do různých skupin. Mohou se členit například podle pachatele, tedy podle toho, kdo podvod spáchal nebo naopak podle oběti, tedy na kom byl podvod spáchán. Kantnerová (2016) člení bankovní podvody na nové formy a poté nejčastější formy. Do nových forem podvodů zařazuje například phishing, malware, pharming či skimming. Za nejčastější formy pak označuje podvody s úvěry, padělání bankovek a mincí, praní špinavých peněz nebo podvodné žádosti o úvěr. Naopak Polouček (2013) ve své monografii bankovní podvody nijak specifiky nečlení a v kapitole o nelegálních činnostech v bankovnictví zmiňuje pouze insider traiding, praní špinavých peněz, korupci v bankovnictví, zpronevěry a bankovní loupeže a krádeže. V této práci jsou bankovní podvody rozděleny autorkou podle pachatele na **interní a externí podvody**.

4.1 Interní bankovní podvody

Bankovní podvody mohou být páchány jednak pachateli mimo banku, které jsou v dnešní době zřejmě častější, a jednak pachateli uvnitř banky. Interní bankovní podvody jsou tedy takové podvody, které páchají zaměstnanci banky (či jiné finanční instituce) nebo zkrátka osoby, které mají přístup k interním zdrojům nebo informacím dané instituce. Za interní podvod mohou být považovány různé formy neoprávněné manipulace s finančními prostředky, bankovními účty, informacemi či zneužití postavení zaměstnanců, které následně vede k dosažení neoprávněného prospěchu. Aby se interním podvodům dalo předcházet anebo aby bylo možné je alespoň odhalovat, je potřeba provádět důsledné interní kontroly a zároveň je i monitorovat. Banka musí aktivně pracovat na minimalizaci rizika interních podvodů, aby chránila nejen své klienty, ale i svou vlastní integritu.

Do interních podvodů lze zařadit například:

- podvodné úvěry,
- padělání dokumentů po krádeži,
- krádeže identity,
- insider traiding,
- nadměrně rizikové či nákladné obchody.

Podvodné úvěry

V případě poskytování podvodných úvěrů nastane situace, kdy nejčastěji zaměstnanec banky vytvoří nebo poskytne falešný úvěr se záměrem dosažení osobního prospěchu. Úvěr může být poskytnut například fiktivním firmám nebo na fiktivní podnikatelské aktivity.

Další možností je, že zaměstnanec napomůže k poskytnutí nebo opravdu poskytne úvěr některé spřízněné společnosti, která následně po krátké době vyhlásí bankrot. Banka tak přijde o půjčené finanční prostředky a oba pachatelé – zevnitř i zvenčí banky se o získané peníze podělí. (Kantnerová, 2016)

Padělání dokumentů po krádeži

Aby měl zaměstnanec důvod padělat dokumenty po krádeži, vyžaduje to obvykle spolupráci s dalšími externími pachateli, kteří provedou danou trestnou činnost, např. krádež finančních prostředků. Jelikož je pravděpodobné, že by krádež byla odhalena v účetnictví, zaměstnanec banky padělá dokumenty, aby tuto skutečnost zakryl. Úbytek peněžních prostředků lze zakrýt například dokumentem o poskytnutí úvěru, výběru peněžních prostředků nebo převedením na jiný účet klientem. (Kuchta, 2008) Avšak tím, že mají bankovní zaměstnanci přístup k mnohým interním dokumentům, mohou z jejich padělání získat prospěch i bez externích spolupachatelů.

Krádež identity

Krádež identity je možné zařadit jak mezi interní podvody, tak i mezi externí. V obou případech se jedná o neoprávněné získání a využívání informací jednotlivců – opět se záměrem osobního prospěchu nebo páchaním dalších trestních činností. Při „interní“ krádeži identity může zaměstnanec banky sám nějakým způsobem zneužít osobní informace klienta anebo je může předávat či prodávat třetím osobám. (Kantnerová, 2016) Mezi osobní informace patří kterýkoliv údaj, který se týká identifikované nebo

identifikovatelné žijící osoby – například jméno, adresa, rodné číslo, číslo bankovního účtu atp. (European Commission, 2024b) A všechny tyto osobní údaje se dají zneužít. V případě „externí“ krádeže identity se může jednat o phishing či smishing (viz kapitola o kybernetických podvodech).

Insider traiding

Insider traiding nebo také insider obchody označují obchodování nebo smlouvy, při kterých jsou zneužity neveřejné informace a dochází k manipulaci s trhem. Tento bankovní podvod se týkají především obchodování s cennými papíry a jen zřídkakdy dochází k insider traiding při jiných bankovních aktivitách (např. při poskytování úvěrů, úniku informací). Insider traiding nejčastěji spočívá v obchodování s cennými papíry na základě důvěrných informací, ke kterým obchodníci získali přístup díky své pozici. Tito obchodníci, tzv. primární insider osoby mohou být členové dozorčí rady, pracovníci vnitřní kontroly nebo členové managementu instituce. Vystupují zde i takzvané sekundární insider osoby, kterými jsou osoby, které přijímají neveřejné informace od primárních insider osob. Jedním z příkladů insider obchodu může být prodej cenných papírů na základě neoprávněného získání informací o budoucích změnách kurzu. Například obchodníci mohou prodat cenné papíry za vyšší kurz ještě před tím než informace, která způsobí pokles kurzu daných cenných papírů, bude zveřejněná. Nebo v opačném případě mohou obchodníci nakoupit cenné papíry za nízký kurz s vědomím, že zanedlouho nastane situace, která kurz těchto cenných papírů zřejmě zvýší. (Polouček, 2013)

Nadměrně rizikové či nákladné obchody

V tomto případě zaměstnanec banky může například překračovat bankou stanovené limity pro spekulativní obchody. V případě, že bude obchod prodělávat a existuje hrozba, že se tato skutečnost odhalí, zaměstnanec začne provádět další nepovolené aktivity a transakce jménem banky, aby nahradil ztrátu z původního nepodařeného obchodu. (Kantenrová, 2016) V jiné situaci může zaměstnanec banky zneužít důvěry, kterou v něj klienti či investoři mají, a uzavírat velmi rizikové či neetické obchody bez jejich vědomí.

4.2 Externí bankovní podvody

Externí bankovní podvody jsou podvody, které se odehrávají mimo banku, ale s cílem banku či jejího klienta poškodit. Tyto podvody páchají externí jednotlivci či skupiny, kteří nejsou s bankou nijak spojeni a chtějí dosáhnout především finančního prospěchu. Pachatelé používají různé metody a techniky, které s rozvojem informačních technologií neustále zdokonalují. Banky k minimalizaci rizika externích podvodů musí neustále implementovat nové bezpečnostní opatření, monitorovat neobvyklé aktivity, a především o těchto skutečnostech informovat své klienty.

Mezi externí podvody patří například:

- padělání a pozměňování peněz,
- krádeže,
- legalizace výnosů z trestné činnosti – praní špinavých peněz,
- podvodné žádosti o úvěr,
- podvody s platebními kartami.

Padělání a pozměňování peněz

Pravděpodobně nejstarším bankovním podvodem a zároveň druhým nejstarším řemeslem je padělání či pozměňování peněz. Jedná se o činnost, při které se padělatel snaží vytvořit co nejvěrohodnější kopii bankovek či mincí, které bude následně vydávat za skutečné peníze. Motivace k padělání peněz je jasná – vidina zisku, kterého lze dosáhnout přeměněním kousku kovu či papíru v něco cenného. Vzhledem k tomu, že je padělání peněz téměř stejně staré jako peníze samy, již v dávných dobách vznikla potřeba se proti padělkům bránit. Vznikly tak zákony, které regulovaly vydávání platidel, byly ukládány velmi přísné tresty a zároveň se vylepšovalo provedení platidel tak, aby padělání nebylo jednoduché. (Česká spořitelna, 2011)

V současnosti existuje několik opatření proti padělání peněz, aby bylo možné národní měnu chránit. V České republice platí, že oprávnění k vydávání bankovek i mincí má pouze Česká národní banka a jakákoliv snaha o padělání či pozměnění peněz se dle § 233 trestního zákoníku považuje za trestný čin proti měně. Bankovky jsou také vybaveny několika ochrannými prvky, mezi které patří především samotný bankovkový papír, vodoznak, iridiscentní pruh, ochranný proužek, skrytý obrazec, opticky proměnlivá barva

nebo soutisková značka. V případě mincí by se za ochranný prvek mohl považovat samotný materiál, gramáž anebo hrany, které se liší dle jednotlivých druhů mincí.

Dnes padělání peněz již není tak častý jev, ale přesto se každoročně několik padělků odhalí. V roce 2023 se zadrželo celkem 3 608 padělaných či pozměněných bankovek a mincí různých měn. Z toho padělky české měny tvořilo 1 189 českých mincí a 1 787 českých bankovek, které byly padělány nebo pozměněny. Oproti roku 2022 došlo k mírnému nárůstu zadržených padělků. (Česká národní banka, 2023e)

Podle tiskové zprávy České národní banky (2023f) se v roce 2022 padělala nejvíce tisícikoruna a hned na druhém místě dvoutisícikoruna. Nejčastěji padělatelé používali k tisku inkoustové tiskárny a v několika případech i barevné tonerové kopírky. Česká národní banka také hodnotí nebezpečnost padělků na stupnici 1–5. První stupeň označuje velmi nebezpečné padělky a pátý stupeň jsou velmi nezdařilé tzv. „neumělé padělky“. Padělkům české měny je převážně přiřazen čtvrtý stupeň z pěti – jedná se tedy o méně zdařilé padělky.

Krádeže

Další z nejstarších bankovních podvodů je bankovní krádež či loupež. Situace často vypadá tak, že pachatel přepadne pobočku banky a vyžaduje finanční hotovost za doprovodu výhružek nebo dokonce ohrožování přítomných osob zbraní. V jiném případě mohou v bankovní loupeži figurovat i zaměstnanci banky, kteří mají daleko lepší přístup k finančním prostředkům než externí pachatelé. V ČR je podle § 173 trestního zákoníku loupež i její příprava považován za trestný čin, za který hrozí odnětí svobody v rozmezí 2 až 10 let.

Legalizace výnosů z trestné činnosti

Legalizaci výnosů z trestné činnosti se přezdívá praní špinavých peněz, přičemž v angličtině je používán výraz „money laundering“, doslova tedy praní peněz. Praní špinavých peněz lze považovat za externí bankovní podvod, avšak jistě může nastat i situace, kdy by do tohoto procesu byli zapojeni i zaměstnanci banky či jiné finanční instituce.

Pojem legalizace výnosů z trestné činnosti představuje jednání, kterým je sledováno zakrytí nezákonného původu výnosu z trestné činnosti se záměrem vzbudit dojem, že se jedná o příjem nabytý v souladu se zákonem. Trestnou činností v tomto případě mohou

být například obchody s drogami, daňové podvody, korupce či jakákoliv krádež. (Častorál, 2007)

Proces praní špinavých peněz lze dle Financial Crime Academy (2023) rozdělit do tří fází.

1. **Fáze: umístění (placement) nebo také „namáčení“** – cílem první fáze je dostat příjem z trestné činnosti do finančního systému. Příkladem může být otevření nového účtu a následné vložení hotovostních peněžních prostředků.
2. **Fáze: vrstvení (layering) nebo také „mydlení“** – v druhé fázi jsou prováděny řetězce převodů (často mezinárodních) či přesunů finančních prostředků, což slouží k zakrytí nebo alespoň zamlžení jejich původu. Kromě převodů bývají často finanční prostředky přeměňovány na aktiva jako je zlato, kryptoměny či nemovitosti.
3. **Fáze: integrace (integration) nebo také „ždímání“** – v poslední fázi se peněžní prostředky navrátí k majiteli, který je použije k investici do legální činnosti. Pachatel tak vytvoří dojem, že výnos pochází z té legální činnosti, do které investoval. A právě tímto postupem došlo k legalizování výnosů z trestné činnosti.

K zamezení praní špinavých peněz byly vypracovány tzv. „Anti-Money Laundering“ (AML) povinnosti. V boji proti praní špinavých peněz je klíčová mezinárodní spolupráce, neboť tato kriminalita často přechází i do zahraničí, a proto jej upravuje několik mezinárodních smluv včetně legislativy Evropské unie. Základní principy, které byly následně implementovány i do českého zákona, udává směrnice EU 91/208EHS o předcházení zneužití finančního systému k praní peněz. V České republice jsou AML povinnosti zakotveny v zákoně č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. Tento zákon může být také nazýván jako zákon proti praní špinavých peněz nebo AML zákon. Český zákon udává nejen bankám, ale i dalším institucím několik povinností například:

- uskutečňovat identifikaci klienta,
- uskutečňovat kontrolu klienta (tj. zjišťovat původ majetku a účel transakce, skutečného majitele právnické osoby apod.)
- neustále vyhodnocovat, zda obchod nevykazuje znaky podezřelého obchodu,
- v případě podezřelého obchodu provést odpovídající postup a podat oznámení o podezřelém obchodu a další. (ČBA, 2024b)

Podvodné žádosti o úvěr

Podvodné žádosti o úvěr jsou známé také pod termínem úvěrové podvody. Úvěrový podvod je trestný čin spočívající v poskytnutí zkreslujících či nepravdivých údajů, případě v zamlčení důležitých údajů klientem. Přičemž podle § 211 trestního zákoníku nezáleží na tom, zda úvěr byl či nebyl poskytnut, neboť pro dokonání trestného činu není nutný vznik škody.

Ještě před samotným sjednáním úvěru podává klient žádost o úvěr, ve které uvádí několik podstatných údajů, na základě kterých banka vyhodnotí, zda klientovi úvěr poskytne či nikoliv. Každá banka má svůj originální formulář, avšak údaje, které je potřeba uvést, se zpravidla neliší. Například v žádosti o úvěr u banky ČSOB (2024) je nutné uvést mimo jiné:

- osobní údaje,
- druh úvěru (kontokorent, kreditní karta či spotřebitelský úvěr) a jeho účel (pakliže je účelový),
- výši úvěru v Kč,
- údaje o zaměstnání nebo podnikatelské činnosti,
- výši měsíčních příjmů,
- výši měsíčních výdajů (splátky dalších úvěrů, výživné atp.)

Nejčastější informací, kterou klienti uvádí nepravdivě je výše příjmů a výdajů. Je to dáno tím, že výše příjmů je prakticky jednou z nejpodstatnějších informací, která zřejmě rozhodne o poskytnutí či neposkytnutí úvěru. S tím souvisí další často zatajované informace, kterými jsou ostatní závazky, tj. další úvěry nebo vyživovací povinnost. Přitom skutečnost, že žadatel splácí i další úvěry či jiné závazky není negativní – tedy pouze v případě, že je splácí řádně. Pakliže klient již existující úvěry či závazky řádně splácí, je považován za spolehlivého dlužníka. Pokud však klient není schopen dostát svým závazkům, dle Kantnerové (2016) se tuto skutečnost často snaží zatajit pozměněním svých osobních údajů tak, aby například informaci o nesplaceném úvěru nebylo možné dohledat. Banka však v procesu schvalování úvěru ověřuje především klientovu bonitu, tedy to, zda bude úvěr schopen splácet. V rámci procesu ověřování bonity klienta důkladně prověřuje příjmy klienta a samozřejmě i úvěrové registry. Lze se domnívat, že v dnešní době pozměnění nebo falšování údajů tak, aby na to banka nepřišla, není jednoduchou záležitostí, zejména pro „obyčejné“ žadatele o úvěr. V každém případě je

velký nerozum uvádět nepravdivé údaje či polopravdy, neboť banka tento podvod s velkou pravděpodobností odhalí a klientovi nejenže úvěr neposkytne, ale oznámí tuto skutečnost Policii ČR.

Podvody s platebními kartami

Mezi známé podvody patří i podvody s platebními kartami. Kantnerová (2016) ve své monografii zmiňuje například takzvanou libanonskou smyčku. Principem libanonské smyčky je umístění blokovacího zařízení do čtečky karty v bankomatu, které pomůže pachateli neoprávněně získat něčí platební kartu. Toto zařízení po vložení kartu totiž „zasekne“ tak, že karta už nejde zpět vytáhnout, ale ani se nedostane do bankomatu tak, jak by měla. Pachatel stojí opodál a držiteli karty, který chtěl z bankomatu vybrat peníze, nabídne ochotně pomoc s vyndáním karty. Přičemž se snaží, aby držitel zkusil zadat svůj PIN, který si pachatel zapamatuje a následně kartu odcizí. Jiná varianta je, že pachatel s držitelem karty neiniciuje kontakt a jen čeká až bude moct platební kartu odcizit. (Komerční banka, 2024)

Dalším podvodem může být například tzv. skimming. Skimming je forma podvodu, která spočívá ve zkopírování údajů z magnetického proužku platební karty, aniž by si toho byl její držitel vědom. Podvodníci následně neoprávněně získané údaje překopírují na vyrobený padělek platební karty. Ke skimmingu dochází především u bankomatů, kam podvodníci umístí tzv. skimmovací zařízení, které údaje zkopíruje. (CyberSecurity.CZ, 2012)

4.3 Kyberkriminalita a kybernetické podvody

Některé z druhů kybernetických podvodů se také dají zařadit mezi externí bankovní podvody. Avšak proto, že jejich počet v současnosti extrémně narůstá, jsou zařazeny do samostatné podkapitoly.

Kybernetická kriminalita nebo také kyberkriminalita je pojem, který je samozřejmě úzce spojen informačními technologiemi. Podle Policie ČR (2024a) je kyberkriminalita definována jako „trestná činnost, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí“. Přičemž oblast těchto technologií může být buď předmětem útoku, anebo je trestná činnost páchaná právě za významného využití informačních a komunikačních technologií.

Ministerstvo vnitra (2022) uvádí následující druhy kyberkriminality.

- **Podvody** – mezi podvody patří různé druhy podvodů, které jsou páchané v online prostředí (phishing, podvodné e-shopy, podvodné investiční příležitosti či inzeráty).
- **Hacking** – za hacking se považuje neoprávněný vstup do počítačového systému a jeho zneužití (zavirování, krádež dat atd.).
- **Blagging** – blagging je označení pro podvodné žádosti o finance.
- **Mravnostní trestné činy** – jsou to trestné činy, které ohrožují výchovu dětí (činy spojené s dětskou pornografií, navazováním nedovolených kontaktů).
- **Trestné činy proti autorskému právu** – znamená to jakékoliv porušení autorského práva a práv, které s ním souvisejí (sdílení hudby, filmů, software).
- **Násilné projevy a hatecrime** – do této kategorie patří například vydírání, vyhrožování nebo šíření poplašné zprávy.

S dynamickým rozvojem technologií a digitalizace, kterým je současná doba charakteristická, se objevují i nové příležitosti pro podvodníky. Stále více služeb, komunikace a transakcí se přesouvá na online platformy s cílem tyto činnosti zjednodušit, mít takzvaně „po ruce“, na jednom místě a moci je pohodlně ovládat z domova. Avšak vše má i svá negativa – těmi jsou v kontextu technologických pokroků právě rozvíjející se schopnosti a možnosti podvodníků.

Kyberkriminalita je označena za nejstrměji rostoucí trestnou činnost, a to v České republice i ve světe. V roce 2022 tvořila kyberkriminalita více než 10 % z celkové registrované kriminality v ČR. Bylo odhaleno celkem 18,5 tisíce případů této trestné činnosti a meziročně tento typ kriminality vzrostl o 94,9 %. (Ministerstvo vnitra ČR, 2023)

Avšak o kybernetických podvodech a kyberkriminalitě obecně se hovoří již několik let. Policie ČR kybernetickou kriminalitu sleduje od roku 2011. Také například Kantnerová (2016) ve své publikaci z roku 2016 uvádí v kapitole o nových formách podvodů například phishing, či smishing a zdůrazňuje, že mezi nejdiskutovanější bankovní podvody patří podvodné e-maily.

Dříve byly také podle Kantnerové (2016) známé takzvané **Nigerijské dopisy**, které se ale v určité míře objevují dodnes. Nigerijský dopis je taková forma podvodu, kdy se podvodník z oběti snaží (většinou přes dopis nebo e-mail) vylákat finanční prostředky. Název vychází z toho, že mnoho z těchto podvodů mělo dříve nějaké spojení s Nigérií.

Podvodník se například vydával za nigerijského konzula, vdovu nigerijského velvyslance atp. Podvodník k vylákání peněz používá různé záminky a hlavní informací bývá, že disponuje mimořádným finančním obnosem. Samotný podvod pak probíhá tak, že oběť obdrží e-mail, ve kterém se podvodník představí například jako údajný velvyslanec, lékař či voják ze zahraničí a naléhavě žádá o pomoc s převedením finančních prostředků s příslibem finanční odměny. Podvodník často apeluje na soucit, lásku a také vidinu odměny za pomoc při provedení transakce. Následně je oběť vyzvána, aby poskytla své bankovní údaje, osobní informace nebo předem zaplatila různé poplatky (např. administrativní poplatky), aby mohla být transakce provedena. Když oběť pošle peníze, podvodníci se odmlčí a zmizí. Oběť nakonec ve snaze pomoc přijde o své finanční prostředky. (Policie, ČR, 2023)

Kybernetické podvody

Mezi aktuální kybernetické podvody, které ČNB označuje také jako podvody v platebním styku, lze zařadit:

- phishing,
- smishing
- vishing a spoofing,
- falešné investiční příležitosti.

Phishing

Phishing je podvodná technika, při které útočníci používají informační a komunikační technologie, aby získali citlivé informace od jiných uživatelů. Tento typ útoku je zaměřen především na získání přihlašovacích údajů, hesel, platebních informací či jiných citlivých dat. (ESET, 2024a) Název této podvodné techniky vznikl na základě kombinace dvou anglických slov „fishing“ (rybaření) a „phreaking“, což je výraz pro krádež telefonní služby. (Kantnerová, 2016)

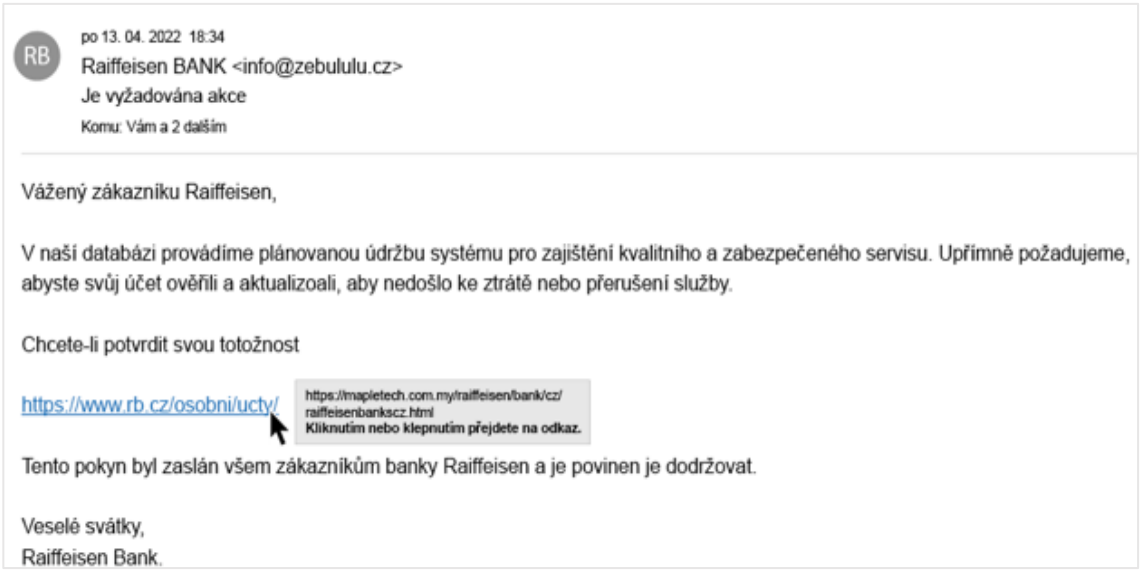
Nejčastěji je phishingový útok prováděn pomocí falešných e-mailů. Útočníci posílají podvodné e-maily, které na první pohled vypadají jako legitimní elektronická pošta od banky, nějaké firmy či instituce. Tyto e-maily obsahují sdělení, jehož cílem je přimět uživatele k zadání svých přihlašovacích údajů, čísla platební karty atp. Dále obsahují odkaz na falešné webové stránky, které však na první pohled mohou opět vypadat jako opravdové.

Příkladem může být zpráva o tom, že byl uživateli např. zablokován bankovní účet, e–mailová schránka nebo účet na sociální síti. Nemusí se jednat samozřejmě jen o zablokování účtu – jinou záminkou může být například aktualizace nebo ověření účtu z různých důvodů. Dále je k e-mailu připojen falešný odkaz a uživatel je vyzván, aby na tomto odkazu vyplnil své přihlašovací údaje, díky čemuž získá svůj účet zpět, ověří jej či aktualizuje. Problémem je, že uživateli jistě žádný účet zablokován nebyl a útočníci využívají pouze jeho strachu a ochoty udělat proti zablokování jeho účtu cokoliv. A když tato záchrana vyžaduje pouze zadání svých přihlašovacích (či jiných údajů), není to nic těžkého. Jenže tímto postupem uživatel své údaje plně přenechá útočníkům a ty je zneužijí ku vlastnímu prospěchu.

Výše zmíněný popis je charakteristický pro klasický tedy „náhodný“ phishingový útok. Náhodným útokem je myšleno to, že dané osobě může přijít podvodný e-mail například kvůli zablokování e-mailové schránky u společnosti Google, ale přitom tato osoba u společnosti Google žádný e-mail nebo účet vedený nemá. A kromě náhodného phishingu existuje i takzvaný **cílený phishing,** který představuje situaci, kdy si útočníci cíleně zjistí několik informací o konkrétní osobě, které následně v podvodném e-mailu použijí a zvýší tak věrohodnost tohoto podvodu. Dále se ještě hovoří o **whalingu**, což je typ phishingového útoku, který se zaměřuje přímo na vrcholové manažery či vlastníky firem, tedy takzvané velké ryby. (ESET, 2024a)

Na obrázku 1, který se nachází na straně 39, je uveden příklad podvodného e-mailu. Po pozornějším prohlédnutí si lze všimnout několika chyb, díky kterým lze podvod rozpoznat. Prvním náznakem podvodu je zvláštní e-mailová adresa, neboť adresu „info@zebululu.cz“ jistě žádný bankéř mít nebude. Aby e-mailová adresa byla seriózní, skládá se většinou ze jména a příjmení dané osoby, popřípadě také názvu organizace jejímž jménem daná osoba jedná. Dalším znakem může být i fakt, že stejný e-mail je podle kolonky „Komu“ odeslán dalším 2 osobám. I v případě hromadných e-mailů od různých institucí většinou nelze zobrazit v kolonce „Komu“, zda byl e-mail odeslaný i někomu dalšímu. Dále je mimo jiné překlep ve slově „aktualizovali“ a také je poměrně zvláštní „rozkaz“, že je klient povinen tento pokyn dodržovat. Smluvní podmínky je nutné dodržovat, neboť při jejich porušení mohou klientovi hrozit penále, ale aktualizace a ověření účtu už zřejmě bude fungovat na dobrovolné bázi. Klient se sice vystaví situaci, kdy mu (podle e-mailu) nebude „zajištěn kvalitní a zabezpečený servis“, ale pravděpodobně nic neporuší.

Obr. 1: Příklad podvodného e-mailu od banky



Zdroj: Kybertest (2024a)

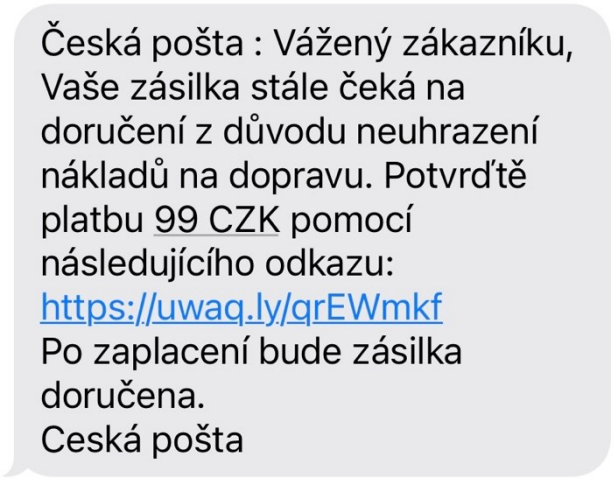
Smishing

Smishing, také nazývaný jako „SMS phishing“ je kybernetický útok, který k podvodu využívá krátké textové zprávy (SMS). Smishing je tedy podobný phishingu, ale namísto e-mailů jsou používány textové zprávy, opět s cílem přimět oběť k poskytnutí osobních informací po otevření falešných odkazů. V roce 2022 byl tento typ podvodu v ČR velmi rozšířený. Za tento rok se podvodnými SMS zprávami nechalo nachytat několik klientů bank a celkové škody pak činily až stovky milionů korun. (Kopecký, 2022) Naopak Kantnerová (2016) ve své monografii zmiňuje, že se dříve podvodné SMS zprávy objevovaly pouze v USA.

Kromě podvodných zpráv od bankovních institucí, rozesílají podvodníci i zprávy jménem dopravních společností – jako je například Česká pošta, PPL či Zásilkovna. Server Kybertest (2024b) uvádí, že v případě podvodných zpráv od dopravních společností záleží také na načasování. Největšího „úspěchu“ tyto podvody dosahují v období před Vánocemi, kdy lidé nejvíce nakupují online a nechávají si zásilky posílat.

Obrázek 2, který se nachází na straně 40, uvádí konkrétní příklad podvodné SMS zprávy vypadající jako od České pošty. Zde bylo podvod poměrně jednoduché odhalit, neboť dle zprávy má být zaplaceno za doručení zásilky, avšak žádná zásilka, kterou by měla doručit Česká pošta, objednána nebyla. Dále je dobré poznamenat, že při objednávce z e-shopu bývá často cena za dopravu součástí celkové ceny k zaplacení.

Obr. 2: Příklad podvodné SMS zprávy



Zdroj: soukromá SMS zpráva autorky (2023)

Vishing a spoofing

Vishing a spoofing jsou dvě různé techniky, které však mohou být kombinovány. Pojem vishing vznikl spojením slov "voice phishing" a jedná se o typ kybernetického útoku, který využívá hlasovou komunikaci opět nejčastěji k získání citlivých informací od oběti. Vishing je prováděn pomocí telefonních hovorů, při kterých se volající představí jako zaměstnanec banky, úřadu nebo jiných důvěryhodných institucí, a snaží se oběť přinutit k poskytnutí citlivých údajů, jako jsou hesla, PIN kódy nebo údaje o bankovních účtech. Tato forma podvodu je poněkud sofistikovanější než ty předchozí, kdy podvodníci rozesílali zprávy a e-maily. Útočníci, tedy volající, jsou často velmi dobře seznámeni s psychologií, neboť využívají především psychologického nátlaku, který na oběť vytvářejí, aby ji přiměli k okamžité reakci. (Chvalkovská, 2021)

Spoofing je pak technika, při které útočníci zfalšují svou identitu a úspěšně se identifikují jako jiná osoba, aby vytvořili zdání legitimní komunikace. Podvodníci například využijí tzv. spoofingu telefonního čísla, což tedy znamená, že jsou schopni napodobit kterékoliv telefonní číslo. Příchozí hovor následně vypadá opravdu tak, že přichází od důvěryhodné instituce, například od banky nebo nějakého úřadu. (ProComputing, 2023)

Policie ČR (2021) už v roce 2021 uváděla, že podvody jako vishing a spoofing byly aktuálním trendem a zaznamenala i případy s milionovými škodami. Dále také eviduje případy, kdy podvodný telefonát od falešného bankéře doprovázel následně i telefonát od falešného policisty, který oběť již naprosto přesvědčil o věrohodnosti telefonátů.

Pokud útočníci tyto dvě metody zkombinují, mohou podvod dovést téměř k dokonalosti. Pro většinu lidí je velmi obtížné jej odhalit i bez zfalšovaného telefonního čísla, natož s ním. A především starší osoby mohou mít s odhalováním podvodu velké potíže. Jsou jistě v tomto ohledu zranitelnější a méně odolné vůči nátlaku, který je nutí reagovat okamžitě a bez času na rozmyšlení.

Falešné investiční příležitosti

K aktuálním podvodům také patří falešné investice. Jedná se o typ podvodu, kdy jednotlivci nebo společnosti lákají lidi či investory na neexistující nebo nelegitimní investiční příležitosti s cílem pouze získat jejich peníze. Na falešné investiční příležitosti lze narazit různými způsoby. Mohou se objevit například jako e-mailová nabídka, telefonní hovor či reklama na internetu. Podle České spořitelny (2024a) bývá v reklamě často nabízena příležitost k velmi výhodnému investování, které přislibuje bezpečí a zároveň „supervýhodné“ zúročení. V případě telefonního hovoru může volat někdo jménem investiční společnosti a nabízet různé možnosti výhodných investic, přičemž zároveň může požadovat instalaci aplikace či softwaru do telefonu či počítače oběti. Avšak tyto aplikace a softwary ve skutečnosti neslouží ke kontrolování stavu investice nebo k jiné zámince, kterou podvodník uvede, ale k získání vzdáleného přístupu do telefonu či počítače podvedené osoby. A v neposlední řadě lze narazit na nabídku zaslanou například e-mailem, který obsahuje odkaz na falešnou webovou stránku. Na webové stránce, kde oběť najde opět možnost výhodné investice, bude vyžadováno zadání údajů k platební kartě či přístupu do bankovnictví. Údaje o platební kartě mohou být vyžadovány například pod záminkou, aby mohl být později připsán příjem z investice.

Za novinku lze v současnosti považovat takzvaná deepfake videa. Deepfake videa jsou vytvořená za pomoci umělé inteligence a může je jednoduše vytvořit téměř každý. Spočívají ve vytváření falešných videí (či v případě deepfake nahrávek ve vytváření hlasových nahrávek), které jsou záměrně upraveny tak, aby vypadaly jako opravdové. Nejčastěji se obětmi deepfake videí i nahrávek stávají známé osobnosti, politici či jiní veřejní činitelé. (PilsFree, 2023) Výsledkem je pak video, kde známá osobnost mluví svým přirozeným hlasem, ale sděluje nepravdivá nebo nesmyslná prohlášení.

Například v lednu 2024 bylo zveřejněno deepfake video, ve kterém prezident ČR Petr Pavel sliboval, že si občané s pomocí speciální investiční aplikace mohou vydělat třičtvrtě milionu korun měsíčně. (Economia, 2024) Pro většinu lidí bylo pravděpodobně

evidentní, že by prezident takovéto prohlášení zřejmě nevydal, na druhou stranu vyšlo alespoň najevo, že umělá inteligence může být v tomto ohledu opravdu nebezpečná a jednoduše s ní lze manipulovat lidi.

Dále například server Kybertest (2024c) upozorňuje i na následující podvody.

- **Bazarové podvody –** při prodeji zboží na internetu předstírá podvodník jakožto kupující zájem o dané zboží. Nejčastěji prodávajícího kontaktuje přes mobilní aplikaci WhatsApp nebo Messenger. Po dohodě o koupi podvodník sdělí prodávajícímu informaci, že si zboží nevyzvedne sám, ale že jej vyzvedne kurýr vybrané dopravní společnosti. Dále také slíbí, že zboží zaplatí předem, ale nejprve potřebuje, aby na zaslaném odkazu prodávající vyplnil své údaje k platební kartě, kam mu peníze za zboží přijdou. Samozřejmě se opět jedná o způsob, jakým se podvodníci snaží vylákat z lidí bankovní údaje, neboť daný odkaz je falešný a pokud je prodejce uvede, akorát je předá podvodníkovi.
- **Podvodné e-shopy –** nebezpečí hrozí i při nákupu na e-shopu, který může vypadat jako normální nebo jako nově spuštěný e-shop, ale přitom je podvodný. Pokud si člověk před nákupem tento e-shop neověří alespoň pomocí recenzí, může snadno přijít o peníze. Nejhorší variantou je zaplacení za dané zboží na neověřeném e-shopu předem platební kartou. V lepším případě přijde kupující pouze o zaplacenou částku za zboží, v horším případě vyplněné bankovní údaje získá podvodník a kupujícímu odcizí peníze z jeho bankovního účtu.
- **Podvodné veřejné Wi-Fi sítě** – na veřejných místech jako je obchodním centrum nebo letiště rozhodně nejsou Wi-Fi sítě zabezpečené, a proto mohou být jednoduše zneužity podvodníky. Po připojení na podvodnou veřejnou Wi-Fi síť může podvodník získat přístup k různým datům z připojeného mobilního telefonu nebo počítače. Může se jednat o fotografie, hesla ale samozřejmě i o přístupy do bankovnictví.
- **Podvodné aplikace –** spolu se stažením některých mobilních aplikací si lze stáhnout do telefonu například i malware Antasa, tedy škodlivý vir. Jedná se například o aplikace k údajnému „čistění“ telefonu nebo k práci s PDF soubory. Poté, co si uživatel stáhne škodlivou aplikaci a následně ji aktualizuje, dostane se do mu telefonu zároveň i malware, který se zaměřuje na napadení bankovních aplikací. (ESET, 2024b)

4.4 Prevence proti bankovním podvodům

Prevence proti bankovním podvodům je v době, kdy digitální prostředí nabývá stále většího významu, naprosto klíčová. Kybernetické útoky se stávají hůře odhalitelnými a podvodníci jsou velmi přesvědčiví a vynalézaví.

Jelikož podle Policie ČR (2022) došlo od roku 2018 do roku 2022 k nejméně čtyřnásobnému navýšení trestných činností páchaných v kyberprostoru, začala se prevenci proti kybernetickým podvodům věnovat potřebná pozornost. V roce 2022 tak Česká bankovní asociace (ČBA) vytvořila ve spolupráci s Policií ČR a Národním úřadem pro kybernetickou a informační bezpečnost interaktivní vzdělávací server s názvem Kybertest. Tento server seznamuje veřejnost s nejčastějšími druhy kybernetických podvodů, které detailně popisuje. Velmi přínosným je také samotný kybertest, na kterém si veřejnost může vyzkoušet, zda bezpečně pozná různé formy kybernetických podvodů. Test obsahuje celkem deset otázek, přičemž každá z nich prezentuje jeden reálný druh podvodu. (Kybertest, 2024d) ČBA (2024c) uvedla, že v roce 2023 průměrná úspěšnost v kybertestu byla 74 %. Test absolvovalo přes 110 tisíc lidí, přičemž nejlepších výsledků dosahovala věková skupina 26–55 let a nejslabší skupinou byli mladí mezi 12–17lety a také věková skupina 56+.

Příklady konkrétních rad, jak se proti bankovním podvodům bránit, uvádí například Česká spořitelna (2024b). Co se týče například vishingu, tedy podvodného telefonátu, jako první zdůrazňuje, že banka ani jiná instituce by citlivé údaje týkající se platební karty nebo bankovního účtu nikdy chtít neměla. Pokud takováto situace nastane a někdo jménem banky bude informace požadovat, stejně tyto údaje nikdo v žádném případě sdělovat nemá. Dále také zmiňuje, že ani vzdálený přístup ke svému počítači nemá nikdo za žádných okolností povolovat. I přesto, že volající může tvrdit, že je z technické podpory, je téměř jisté, že se jedná o podvod.

Podle serveru Dvojklik (2023) provozovaný společností ESET, která se specializuje na antivirové programy, je zásadní při podezření na podvodný telefonát zachovat klid. Dále je potřeba ověřit si, kdo skutečně volá. Je tedy dobré se zaměřit na jméno volajícího nebo instituci, kterou má zastupovat. Pokud volá někdo jménem instituce je nutné si uvědomit, zda má člověk u této instituce uzavřené nějaké smlouvy nebo využívá některý z jejich produktů. Pokud ano, je dobré se zeptat na nějakou interní informaci, kterou by měla vědět jen ta konkrétní instituce – např. číslo smlouvy. A samozřejmostí je se soustředit

na to, v jaký čas hovor probíhá a také jakým jazykem volající mluví. Zaměstnanci banky totiž volají zpravidla v úředních hodinách, a i v rámci telefonního hovoru mluví formálně a především česky. Pokud však někdo neumí reagovat pohotově nebo přemýšlet „za pochodu“ během hovoru, je lepší volbou zavěsit a obrátit se na infolinku dané instituce.

Prevence kriminality v České republice (2024) zmiňuje jednoduchý princip 4P, který může pomoci se vyhnout případným problémům při setkání s bankovním podvodem. Tento princip minimální důvěry a maximálního možného ověření reprezentuje slova: PŘEMÝŠLEJ, PROVĚŘUJ, PORAĎ SE a pak až PLAŤ. V případě phishingu či smishingu, tedy příchozích e-mailů či SMS zpráv, se tento princip aplikuje celkem snadno, neboť si lze oba typy zpráv v klidu několikrát přečíst a v případě pochybností se obrátit na infolinku banky či dané instituce. Naopak v případě vishingu, tedy telefonních hovorů, to snadný úkol není, ale je potřeba mít na paměti, že je klíčové nepodlehnout nátlaku, který je při podvodu cíleně vyvíjen.

Základní pravidla pro bezpečné chování v online prostředí shrnuje deset základních zásad bezpečnosti, jež uvádí České bankovní asociace (2022a).

1. Péče o bezpečí svého počítače – je potřeba mít nainstalované a pravidelně aktualizované antiviry na počítačích.
2. Zabezpečení mobilního telefonu – většinu účtů lidé ovládají právě z telefonu, takže je vhodné mít i v něm nainstalované bezpečnostní aplikace.
3. Ověřování původu aplikací – stahování aplikací je bezpečné pouze z oficiálních obchodů s aplikacemi (Google Play nebo AppStore). I tak je dobré věnovat pozornost například počtu stažení dané aplikace a jejím recenzím.
4. Ochrana přihlašovacích údajů – přihlašovací ani osobní údaje není vhodné komukoliv sdělovat nebo ukládat na zařízeních ve veřejných sítích.
5. Ochrana PIN kódu – je dobré si PIN kód pouze pamatovat, ale pokud vznikne potřeba si jej někam zapsat, rozhodně je nutné napsaný PIN pečlivě uschovat.
6. Bezpečné heslo – základem bezpečného hesla je to, aby se nedalo odhadnout. Delší hesla, kde budou zkombinována velká a malá písmena s různými speciálními znaky jsou ideální. A také je důležité mít pro různé platformy rozdílná hesla.
7. Neznámé přílohy – není dobré otevírat e-mail od podezřelých odesílatelů či stahovat v něm uvedené přílohy a klikat na odkazy.

8. Nákupy je vhodné provádět pouze u důvěryhodných online prodejců – jejich důvěryhodnost lze ověřit například jednoduchým vyhledáním daného e-shopu na internetu nebo ověřením recenzí.
9. Je potřeba věnovat pozornost upozorněním banky, vlastního počítače či mobilního telefonu.
10. Informování banky – při sebemenším podezření, že je s bankovním účtem něco v nepořádku, je nejlepší reakcí kontaktovat přímo banku.

5 Vývoj kybernetických podvodů

V následující části práce bude zmapován vývoj kyberkriminality v České republice a vývoj kybernetických podvodů, které evidovalo Krajské ředitelství policie Plzeňského kraje. Poté bude představena problematika kybernetických podvodů z pohledu České spořitelny a bude zmíněna i situace v zahraničí. Poslední část kapitoly bude věnována kyberbezpečnosti a nejčastějším kybernetickým podvodům v ČR.

5.1 Kyberkriminalita v ČR

Policejní prezidium ČR je pověřeno vytvářením statistických přehledů kriminality za každý kalendářní měsíc a poté souhrnně za celý rok. V rámci této statistiky je evidován počet registrovaných (oznámených) trestných činů, což jsou trestné činy, které byly Policii ČR nahlášené a bylo u nich zahájeno trestní řízení. Dále statistiky uvádí způsobené škody či míru objasněnosti. Objasněnost se dělí na dvě skupiny, tedy na objasněno a dodatečně objasněno. Objasněno znamená, že registrovaný skutek byl objasněn ve sledovaném období, a naopak objasněno dodatečně znamená, že byl ve sledovaném období objasněn skutek registrovaný v minulých letech. Dále je ve statistice evidováno, zda byl trestný čin spáchán nezletilými, mladistvými, dětmi, cizinci či opakovaně trestanými osobami. A také, zda byl trestný čin spáchán pod vlivem (obecně), pod vlivem alkoholu či firmou. (Police ČR, 2024b)

Policie ČR člení trestnou činnost na základě takticko-statistické klasifikace (TSK), která pomáhá podrobněji sledovat druhy kriminality, přičemž každá kategorie má přidělené trojčíselné označení. Do jedné kategorie TSK může být zahrnuto více paragrafů trestního zákoníku, a naopak jeden paragraf trestního zákoníku lze rozčlenit do několika kategorií TSK. Například § 209 trestního zákoníku, který odkazuje na trestný čin podvodu, je rozdělen do tří kategorií TSK, a to: 511 – podvod (v rámci majetkové kriminality), 815 – podvody v sociálním zabezpečení a nemocenském pojištění, 830 – podvod (v rámci hospodářské kriminality). Naopak kategorie TSK 750 – ublížení na zdraví z nedbalosti (pracovní úraz) obsahuje § 143, § 147 § 148, § 274 a § 360. (Policie ČR, 2024b)

Podle vedoucího oddělení tisku Policejního Prezidia ČR plukovníka PhDr. Ondřeje Moravčíka (osobní komunikace, 8. 3. 2024), se v případě aktuálních podvodů, jako je phishing, vishing či smishing, vždy jedná o trestný čin podvodu podle § 209 trestního zákoníku. Statisticky tedy nejsou sledovány údaje, zda se jedná o podvody v platebním

styku spáchané formou vishingu, phishingu atd., protože statistiky jsou členěny pouze na základě konkrétních druhů trestných činů.

Z tohoto důvodu nebylo možné získat od Policie ČR statistiku podvodů v platebním styku, ze které by bylo patrné, kolik podvodů, které byly spáchány formou phishingu, vishingu či pomocí podvodných e-shopů, Policie ČR eviduje. Nicméně tyto podvody jsou zahrnovány do oblasti kybernetické kriminality, ke které data evidována jsou. Proto plukovník Moravčík za Policejní Prezidium ČR poskytl na žádost autorky data tykající se počtu všech trestných činů v oblasti kyberkriminality v ČR od roku 2013 do roku 2023, neboť tato data nejsou součástí zveřejňovaných statistik.

5.1.1 Struktura kyberkriminality v ČR

Před zobrazením výše uvedených dat bude pro představu zmíněna nejprve struktura kyberkriminality, neboť se obecně do kyberkriminality zahrnuje více druhů trestných činů. Jak již bylo zmíněno v podkapitole 4.1.3 o kyberkriminalitě a kybernetických podvodech, těmito trestnými činy jsou podvody (kam patří právě phishing, podvodné e-shopy, podvodné inzerce atd.), hacking, mravnostní trestné činy, trestné činy proti autorskému právu, násilné projevy a hatecrime a poslední kategorií jsou ostatní trestné činy, kam se řadí například blagging. Zjednodušeně řečeno, patří sem trestné činy, které jsou páchané ve vztahu k datům a často je k jejich páchání použit počítač.

V tabulce 1, která je umístěna na další straně, jsou uvedeny počty registrovaných trestných činů v letech 2015 až 2020 patřící do oblasti kyberkriminality. Z celkových počtů registrovaných trestných činů lze pozorovat, že v jednotlivých letech narůstají nejen případy podvodných jednání, ale také ostatních druhů kyberkriminality a tím pádem i celkové kyberkriminality. Obecně je ve všech druzích registrovaných trestných činů nárůst poměrně pozvolný, pokud se bere v potaz, že se jedná o data za celou ČR. V letech 2019 až 2020 došlo k viditelnému nárůstu všech druhů kyberkriminality, kromě autorskoprávních deliktů, kterých v těchto letech ubývalo. Podvodných jednání bylo registrováno nejvíce v roce 2019. Například ve srovnání s rokem 2015, bylo v roce 2019 registrováno o 1 625 případů podvodného jednání více. Celkově v roce 2019 bylo spácháno nejvíce trestných činů v oblasti kyberkriminality v rámci pozorovaných šesti let. Krádeží dat či cíleného zavirování počítače s cílem získat peníze také přibývá. Na tyto skutečnosti odkazuje hacking, který je od roku 2018 na vzestupu. Za zmínku stojí také kategorie ostatní kyberkriminalita, kam patří například blagging (podvodné žádosti

o finance), neboť zde je také viditelný nárůst počtu případů. V roce 2019 bylo těchto ostatních trestných činů evidováno 955, což je o 355 skutků více než v roce 2015.

Tab. 1: Počty registrovaných trestných činů v oblasti kyberkriminality v ČR v letech 2015-2020

Druh kyberkriminality	**Rok**					
	2015	**2016**	**2017**	**2018**	**2019**	**2020**
Podvodná jednání	2 932	3 300	3 464	3 544	4 557	4 399
Hacking	582	513	608	682	852	1 057
Mravnostní delikty	355	336	561	743	822	751
Autorskoprávní delikty	345	236	301	613	474	190
Nás. projevy a hatecrime	209	247	349	647	757	756
Ostatní	600	358	371	586	955	920
CELKEM	**5 023**	**4 990**	**5 654**	**6 815**	**8 417**	**8 073**

Zdroj: vlastní zpracování (2024) dle Hejduka (2020)

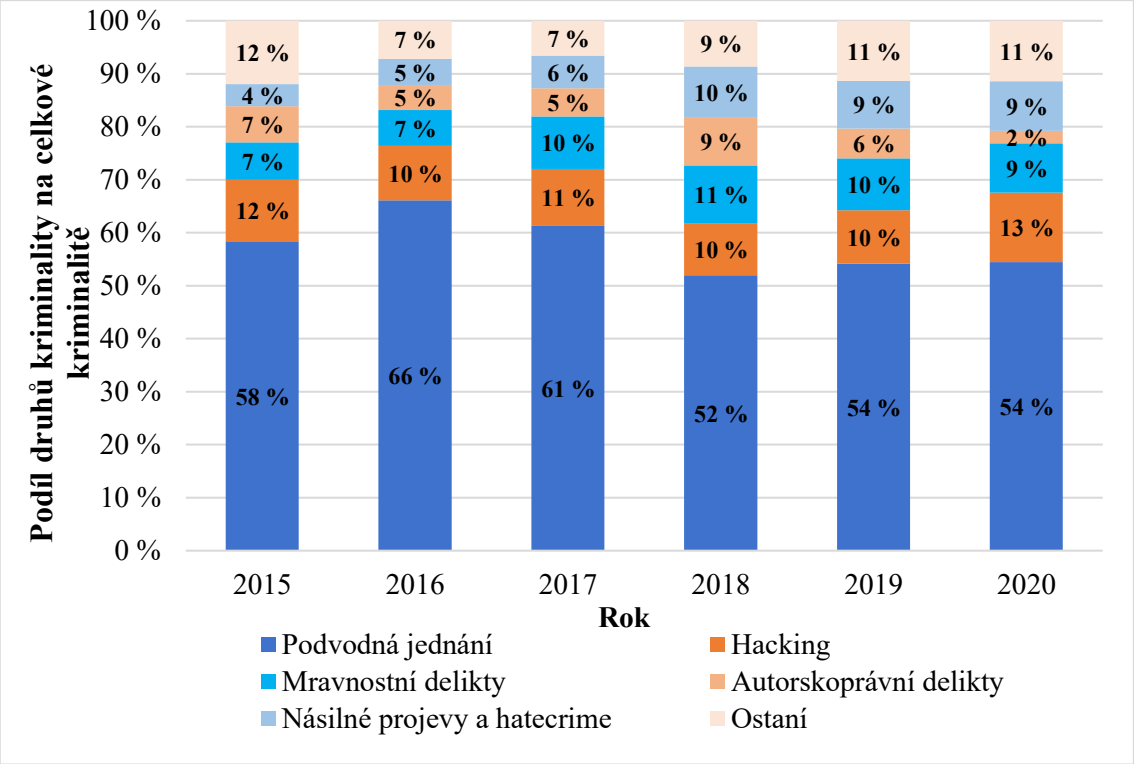
Na straně 49 je umístěn obrázek 3, který zobrazuje graf struktury kyberkriminality v letech 2015 až 2020 z hlediska registrovaných případů v ČR. V grafu jsou vyobrazeny procentuální podíly jednotlivých druhů kyberkriminality na celkové kyberkriminalitě, které podávají lepší obraz o struktuře kyberkriminality nežli samotné počty registrovaných trestných činů v předcházející tabulce.

Na první pohled je patrné, že nejvýraznější jsou jednoznačně podvodná jednání. Druhé místo pak každoročně (kromě roku 2018) zaujímá hacking. K největší změně došlo v roce 2016, kdy oproti přechozímu roku 2015 podíl podvodů na celkové kyberkriminalitě vzrostl o 8 procentních bodů, tedy z 58% podílu na 66% podíl. Není to způsobeno tím, že by početně případy podvodného jednání o tolik narostly (což je patrné z předcházející tabulky), ale proto, že ubylo autorskoprávních deliktů a ostatní kyberkriminality, takže mírně poklesl celkový počet trestných činů.

V dalších letech podíl podvodných jednání na celkové kyberkriminalitě mírně klesá, neboť především v roce 2018 vzrostl počet případů násilných projevů a hatecrime a také mravnostních deliktů. Konkrétně v roce 2018 podíl podvodných jednání klesl

o 9 procentních bodů. Následně pak v roce 2019 a 2020 se podíl podvodných jednání na celkové kyberkriminalitě nemění, a to i přes nárůst ostatních druhů kyberkriminality.

Obr. 3: Struktura kyberkriminality v ČR v letech 2015-2020



Zdroj: vlastní zpracování (2024) dle Hejduka (2020)

Tato data měla za cíl ukázat, že navzdory tomu, že se kyberkriminalita skládá z několika druhů trestných činů, z tabulky 1 a obrázku 3 vyplývá, že právě **podvody tvoří vždy více než polovinu** celkové kyberkriminality. Hned za podvody je umístěn hacking a následně ostatní kriminalita. Je tedy patrné, že v popředí jsou trestné činy, kdy je cílem pachatelů zisk peněžních prostředků prostřednictvím podvodných jednání (phishing, podvodné e-shopy atp.), či podvodných žádostí o finance a krádeže dat.

5.1.2 Kybernetická a celková kriminalita v ČR

Následující tabulka 2 zobrazuje vývoj kybernetické a celkové kriminality v ČR v letech 2013 až 2023. Jak bylo zmíněno dříve, data o kybernetické kriminalitě byla na žádost poskytnuta plukovníkem PhDr. Ondřejem Moravčíkem. Data o celkové kriminalitě vychází ze statistických přehledů kriminality.

Tab. 2: Počty trestných činů kybernetické a celkové kriminality v ČR v letech 2013-2023

Rok	Kybernetická kriminalita (KK)	Celková kriminalita (CK)	Podíl KK na CK (v %)
2013	3 108	325 366	0,96
2014	4 348	288 660	1,51
2015	5 023	247 628	2,03
2016	4 990	218 162	2,29
2017	5 654	202 303	2,79
2018	6 815	192 405	3,54
2019	8 417	199 221	4,22
2020	8 073	165 525	4,88
2021	9 518	153 233	6,21
2022	18 554	181 991	10,20
2023	19 592	181 417	10,80

Zdroj: vlastní zpracování (2024) dle Moravčíka (osobní komunikace, 8. 3. 2024) a Policie ČR (2024b)

Kyberkriminalita

Z tabulky 2 lze pozorovat, že v případě kyberkriminality každoročně docházelo k nárůstu, kdežto celková kriminalita v průběhu sledovaných let klesala. V letech 2013 až 2018 se nárůst kyberkriminality dá považovat za méně výrazný, pokud jej srovnáme s následujícími roky. Rostoucí tendenci v tomto období narušil pouze rok 2016, kdy bylo registrováno o 33 případů méně než v předcházejícím roce. Následně od roku 2017 skutků opět přibývalo.

V období let 2019 až 2023 jsou číselné údaje poněkud „zajímavější“. V roce 2019 bylo evidováno o 1 602 případů kybernetické kriminality více než v roce 2018. V roce následujícím, tedy 2020, byla rostoucí tendence opět mírně narušena, neboť Policie ČR registrovala o 344 skutků méně než v roce 2019. Avšak v roce 2021 byl opět zaznamenán nárůst a to o 1 445 případů oproti roku 2020. Postupný nárůst v následujících letech mohl být odstartovaný díky potřebě práce z domova. Přibližně od podzimu 2020 a především

pak v roce 2021 probíhala druhá, silnější vlna koronavirové epidemie, v jejímž důsledku hodně firem přecházelo na home office. Často se k práci využívaly vzdálené přístupy, které pro kyberpodvodníky představovaly větší množství příležitostí např. pro krádeže dat s cílem získání finančních prostředků. Bezesporu nejvyšší nárůst registrovaných případů kyberkriminality nastal v roce 2022, kdy počet případů vzrostl o 9 036 případů, což je bez mála dvojnásobek počtu případů roku 2021. Rok poté, tedy v roce 2023, se počet skutků mírně zvýšil, konkrétně jich bylo evidováno o 1 038 více. Přestože v posledním roce nebyl počet případů o tolik vyšší, jistě to naznačuje pokračující trend nárůstu. Srovná-li se první a poslední sledovaný rok, tedy rok 2013 a 2023, počet registrovaných případů kyberkriminality v roce 2023 stoupl dramaticky, a to celkem o 16 484 případů.

Celková kriminalita

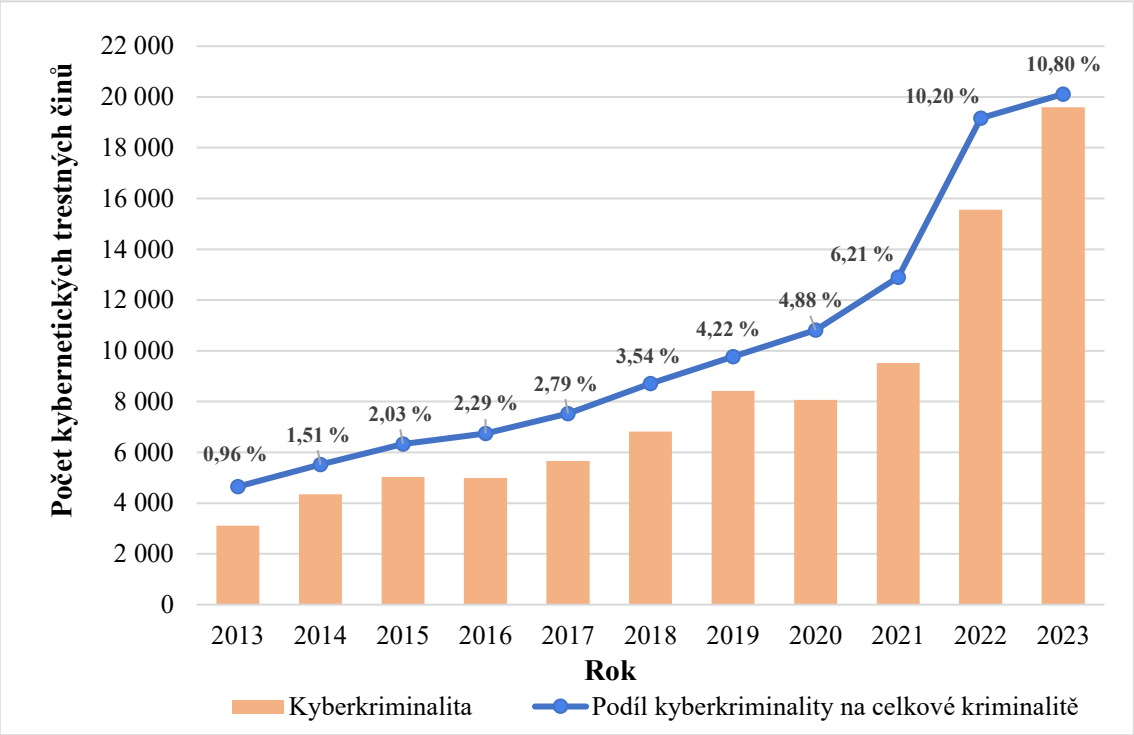
Celková kriminalita se ve sledovaných letech nevyvíjela tak pravidelně jako tomu bylo v případě kyberkriminality. Je však evidentní, že právě v kontrastu s kyberkriminalitou celková kriminalita v ČR postupně klesala, až na několik výjimek. Pravidelný pokles byl pozorován od roku 2013 do 2018, a to z 325 366 případů na 192 405. K nepatrnému nárůstu došlo v roce 2019, konkrétně na 199 221 případů. Avšak ihned v následujících letech 2020 a 2021 se počty případů opět propadly a to na 165 525 případů a poté v roce 2021 na 153 233 případů. V letech 2022 a 2023 byla celková kriminalita na úrovni téměř 182 000 případů. Lze pozorovat opětovný nárůst, nicméně v obou letech je počet podobný, nemuselo by to tedy naznačovat enormní růst celkové kriminality do budoucna.

Podíl kyberkriminality na celkové kriminalitě

Obrázek 4, který se nachází na straně 52, zobrazuje graf, kde je uveden počet registrovaných trestných činů v oblasti kyberkriminality spolu s podílem kyberkriminality na celkové kriminalitě. Jak bylo zmíněno výše, zatímco celková kriminalita víceméně klesá, kyberkriminalita je naopak na vzestupu. Kyberkriminalita tím pádem tvoří stále větší část celkové kriminality v ČR. Což také vypovídá o ústupu „tradičních“ forem kriminality a přesunu kriminálních aktivit do kyberprostoru. Zatímco v roce 2013 se kyberkriminalita podílela necelým procentem na celkové kriminalitě, v minulém roce, tedy v roce 2023, tvořila téměř 11 % kriminality v ČR. Prudké zvýšení jejího podílu nastalo samozřejmě již v roce 2022, neboť počet registrovaných kybernetických trestných činů se téměř zdvojnásobil a celková kriminalita nebyla příliš

vysoká. Ještě o dva roky dříve, v roce 2020, byl podíl kyberkriminality o polovinu nižší, činil necelých 5 %. Opět to poukazuje na fakt, že je kyberkriminalita rostoucí problém, neboť její vzestup je ohromný.

Obr. 4: Kyberkriminalita a její podíl na celkové kriminalitě v letech 2013-2019

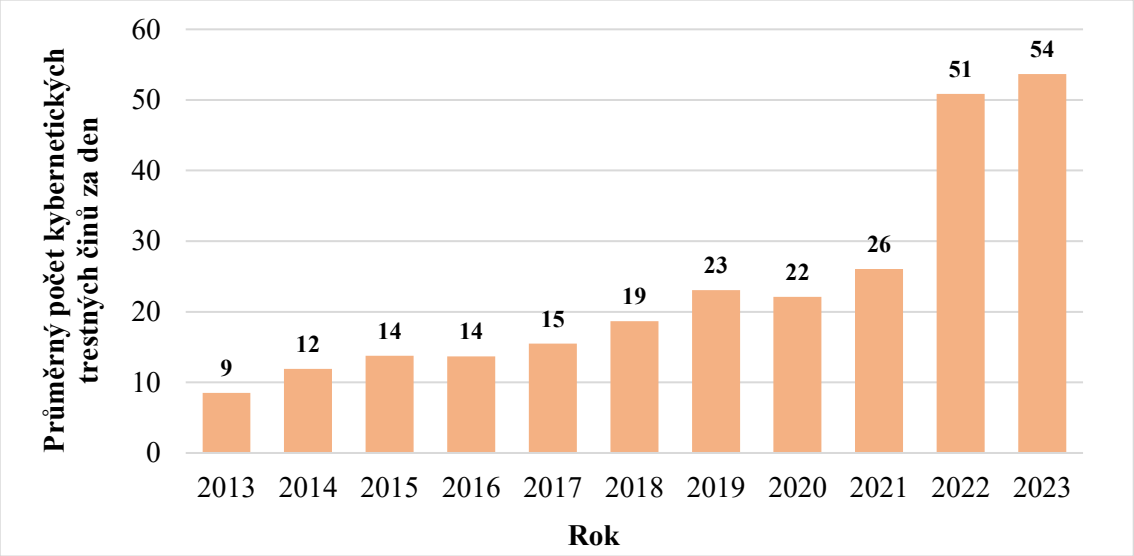


Zdroj: vlastní zpracování (2024) dle Moravčíka (osobní komunikace, 8. 3. 2024)

Počet kybernetických trestných činů za den

Obrázek 5, který se nachází na straně 53, zobrazuje graf, kde jsou uvedeny počty registrovaných kybernetických trestných činů v letech 2013 až 2023 přepočítané na dny. Je zřejmé, že průměrný denní počet registrovaných trestných činů stoupá s rostoucím počtem případů kyberkriminality. Zatímco v letech 2014 až 2018 se průměrný počet skutků udržoval pod hranicí 20 skutků za den, v dalších sledovaných letech už tomu tak nebylo. V období let 2019 až 2021 se průměrný denní počet registrovaných kybernetických trestných činů pohyboval mezi hodnotami 22 až 26 případů za den. Opět největší skok nastal v roce 2022, kdy bylo denně evidováno v průměru 51 kybernetických skutků, tedy téměř dvakrát více než v předcházejícím roce. V posledním sledovaném roce 2023 vycházelo, že bylo průměrně registrováno 54 kybernetických trestných činů za den. Frekvence kybernetických trestných činů zůstala v posledním roce tedy poměrně stabilní, avšak je pravděpodobné, že v dalších letech budou počty případů přibývat.

Obr. 5: Průměrný počet kybernetických trestných činů v ČR za den v letech 2013-2023



Zdroj: vlastní zpracování (2024) dle Moravčíka (osobní komunikace, 8. 3. 2024)

5.1.3 Prognóza vývoje kyberkriminality v ČR

Tím, že jsou k dispozici data o vývoji kyberkriminality v minulosti, lze predikovat jejich pravděpodobný budoucí vývoj. V této podkapitole bude predikován možný budoucí vývoj počtu kybernetických trestných činů v letech 2024 až 2030 a k jeho vytvoření bude využita funkce FORECAST.ETS v MS Excel. Tato funkce dokáže predikovat budoucí vývoj na základě existujících historických dat s využitím algoritmu ETS, tedy exponenciálního vyrovnání. Se všemi údaji, které se do funkce dosazují, vypadá funkce následovně.:

FORECAST.ETS (cílové_datum; hodnoty; časová osa; [sezónnost]; [dokončení_dat]; [agregace]).

- **Cílové datum** představuje vždy rok (nebo jiný datový údaj), pro který bude hodnota predikována (v prvním řádku se zvolí 2024).
- **Hodnoty** představují historická data, která jsou k dispozici (zde se označují všechny počty kybernetických trestných činů, tj. od roku 2013 do 2023)
- **Časová osa** je v tomto případě rok 2013 až 2023 (označí se tedy všechna pole s roky, tj. 2013 až 2023),
- **Sezónnost, dokončení dat a agregace** jsou nepovinné argumenty, neboť se používají především v případě chybějících dat, která se v počtu kybernetických trestných činů nenachází. Budou tam ponechány výchozí hodnoty argumentů.

Kromě samostatné prognózy bude vypočten i 95% interval spolehlivosti. Interval spolehlivosti ukazuje, že se skutečná hodnota (v tomto případě počet kybernetických trestných činů) bude s 95% pravděpodobností pohybovat v daném intervalu. Dolní hranice spolehlivosti bude označovat hodnotu, pod kterou se s 95% pravděpodobností predikovaný počet kybernetických trestných činů nebude nacházet. Horní hranice spolehlivosti naopak označí hodnotu, nad kterou se s 95% pravděpodobností predikovaný počet kybernetických trestných činů nebude nacházet.

Pro výpočet horní i dolní hranice bude použita funkce FORECAST.ETS.CONFINT, ve které se vyplňují totožné argumenty jako ve funkci pro predikci dat. Jedinou změnou je, že v při výpočtu dolní hranice spolehlivosti je potřeba funkci odečíst od predikované hodnoty (v roce 2024 je tato hodnota 24 358). Naopak při výpočtu horní hranice spolehlivosti se funkce k predikované hodnotě přičítá. Výsledná tabulka 3 je zobrazena níže.

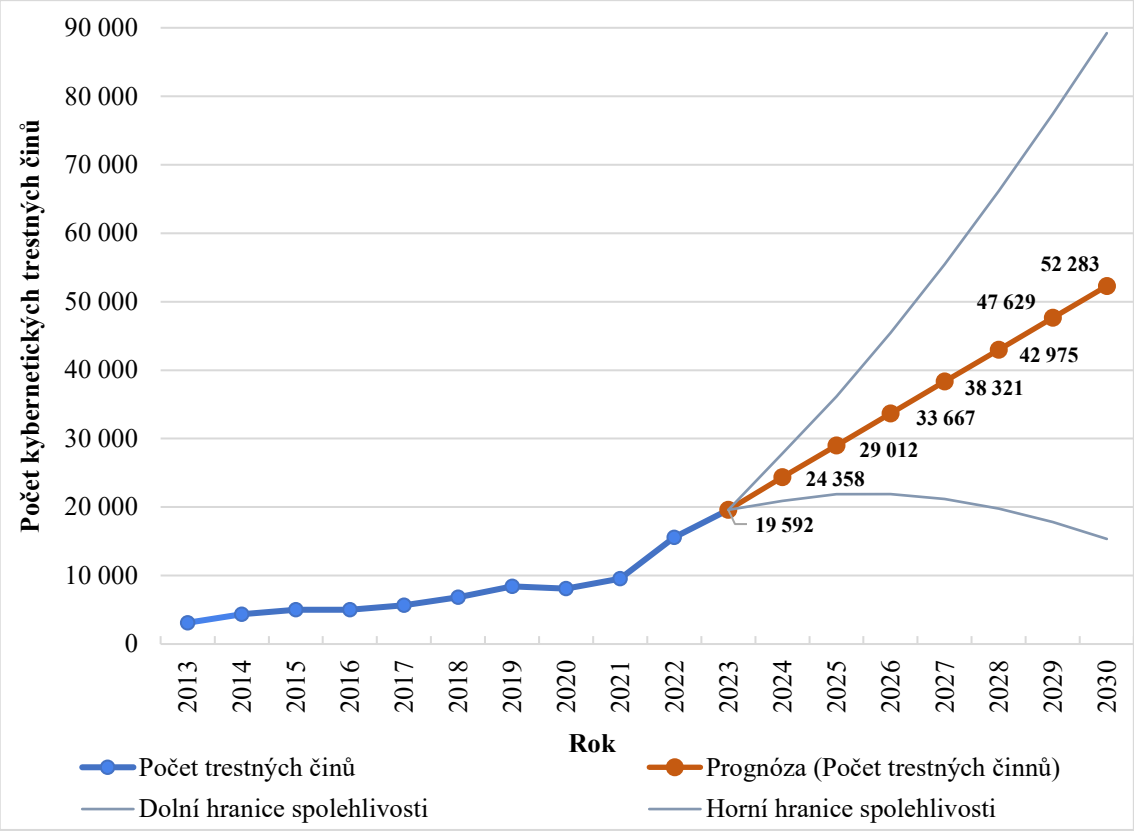
Tab. 3: Prognóza vývoje kyberkriminality v ČR v letech 2024-2030

Rok	Počet kybernetických trestných činů	Prognóza kyberkriminality	Dolní hranice spolehlivosti	Horní hranice spolehlivosti
2013	3 108			
2014	4 348			
2015	5 023			
2016	4 990			
2017	5 654			
2018	6 815			
2019	8 417			
2020	8 073			
2021	9 518			
2022	15 557			
2023	19 592	19 592	19 592	19 592
2024		24 358	20 890	27 827
2025		29 012	21 873	36 152
2026		33 667	21 896	45 437
2027		38 321	21 169	55 473
2028		42 975	19 793	66 156
2029		47 629	17 837	77 421
2030		52 283	15 349	89 217

Zdroj: vlastní zpracování (2024) dle Moravčíka (osobní komunikace, 8. 3. 2024)

Pro přehlednost byl vytvořen také graf s predikovanými počty kybernetických trestných činů v letech 2024 až 2030. Tento graf zobrazuje obrázek 6.

Obr. 6: Prognóza vývoje kyberkriminality v ČR v letech 2024-2030



Zdroj: vlastní zpracování (2024) dle Moravčíka (osobní komunikace, 8. 3. 2024)

Historická data v letech 2013 až 2023 byla rozebrána v přecházejících kapitolách a je tedy známo, že vykazují evidentní rostoucí trend. V následujících letech bude tento trend zřejmě pokračovat, což je znázorněno oranžovou čarou, která zobrazuje nejpravděpodobnější vývoj kyberkriminality. Predikované hodnoty vykazují poměrně strmý růst počtu kybernetických trestných činů, neboť by počty měly stoupat každoročně v průměru o 4 650 případů. Pokud by tomu opravdu tak bylo, v roce 2030 by bylo evidováno přes 52 tisíc případů za rok, což je téměř třikrát více případů než v roce 2023. Denně by průměrný počet případů vycházel na 143 případů. Jestliže by obecně kriminalita v ČR stagnovala či stále mírně klesala, znamenalo by to, že se kyberkriminalita bude stále výrazněji podílet na celkové kriminalitě.

Vzhledem k tomu, že je interval spolehlivosti velmi široký, je pravděpodobné, že budoucí počty případů kyberkriminality mohou být poměrně rozdílné. Přece jen byl zaznamenán prudký nárůst počtu případů až posledních dvou letech, tedy v roce 2022 a 2023, a do této

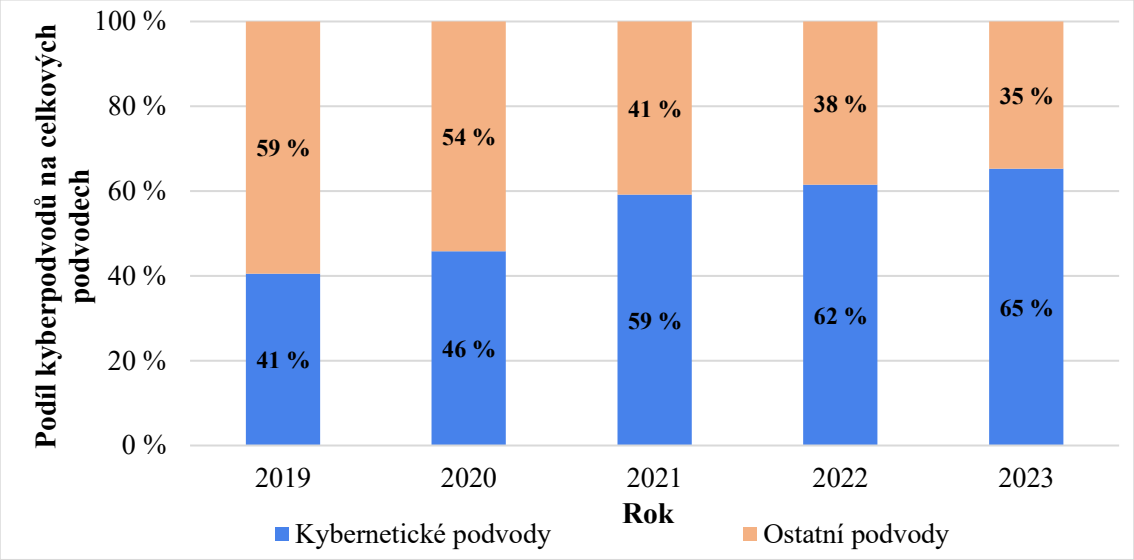
doby byl nárůst celkem postupný. Je to tedy víceméně nepravidelný trend, což může jistě zkreslit výsledky prognózy. V každém případě v budoucnu lze očekávat spíše nárůst, avšak až v dalších letech se ukáže, kolik přesně případů bude přibývat. Kyberkriminalita je tak bezesporu velkým rizikem. Nutno znovu připomenout, že se celou dobu pracuje s registrovanými trestnými činy, tj. oznámenými. Je tedy více než pravděpodobné, že jich ve skutečnosti bylo v minulých letech spácháno více, ale nebyly nahlášeny Policii ČR.

5.2 Kyberkriminalita v Plzeňském kraji

Vedoucí odboru analytiky a kybernetické kriminality Krajského ředitelství policie Plzeňského kraje (KŘP PK) major Bc. Luděk Hrabák, DiS (osobní komunikace, 18. 3. 2024), taktéž potvrdil, že aktuální podvody (phishing, vishing či smishing) jsou vždy označeny za trestný čin podvod a konkrétně se nesleduje, zda se jednalo o phishing či jiný podvod. Dále major Hrabák uvedl, že KŘP PK v případě podvodů eviduje, zda podvodné jednání bylo spáchané internetem či jinak (např. na ulici). Podvody spáchané internetem následně označuje jako kyberkriminalitu.

Následně na žádost autorky pan major Hrabák poskytl za KŘP PK údaje o **podvodech spáchaných internetem,** které KŘP PK registrovalo v letech 2019 až 2023. Pro dokreslení podílu podvodů spáchaných internetem byly poskytnuty také údaje o **celkově registrovaných podvodech** za stejné období. Předtím než budou podrobněji rozebrány získané údaje, na obrázku 7 je zobrazen graf, kde je vyjádřen procentuální podíl kybernetických podvodů na celkových podvodech.

Obr. 7: Podíl kybernetických podvodů na celkových podvodech v letech 2019-2023



Zdroj: vlastní zpracování (2024) dle Hrabáka (osobní komunikace, 18. 3. 2024)

Jak je vidno v grafu, v prvních dvou sledovaných letech 2019 a 2020 tvořily kybernetické podvody vždy bezmála polovinu celkových podvodů. Mírně vyšší podíl v roce 2020 byl způsoben tím, že se zvýšil počet kybernetických podvodů a zároveň poklesly případy ostatních podvodů. Poté v roce 2021 podvody páchané internetem dosáhly 59% podílu a v následujících letech 2022 a 2023, kdy počet kybernetických podvodů výrazně rostl, tvořily vždy přes 60 % všech registrovaných podvodů.

Registrované podvody

Počty všech registrovaných podvodů spolu s objasněností a celkovou škodou jsou uvedeny v tabulce 4.

Tab. 4: Celkové podvody registrované Krajským ředitelstvím policie PK v letech 2019–2023

Rok	Registrováno	Objasněno	Objasněno dodatečně	Celková objasněnost (v %)	Škoda (v tis. Kč)
2019	343	130	58	54,81	53 818
2020	312	77	58	43,27	261 070
2021	404	66	84	37,13	90 749
2022	853	79	73	17,82	166 787
2023	946	75	122	20,82	169 806

Zdroj: vlastní zpracování (2024) dle Hrabáka (osobní komunikace, 18. 3. 2024)

Značný nárůst podvodů byl zaznamenán i v Plzeňském kraji. V letech 2019 až 2021 byl vývoj mírně nepravidelný. Rok 2020 totiž opět porušil rostoucí trend, neboť bylo registrováno o několik podvodů méně než v roce 2019. Nicméně poté v roce 2022 došlo ke skokovému nárůstu a počet registrovaných podvodů se zdvojnásobil. Počty poté mírně vzrostly i v roce 2023, avšak už jen o stovku případů.

Celková objasněnost v průběhu let naopak klesala. V roce 2019 Policie ČR objasnila polovina případů, avšak a v roce 2023 bylo objasněno pouze necelých 21 % podvodů. Co se škod týče, zde byla nejvyšší hodnota zjištěna v roce 2020, kdy škody přesahovaly 260 milionů Kč. V dalším roce došlo k viditelnému snížení celkové škody na 90 milionů Kč. Avšak v letech 2022 2023 s narůstajícím počtem registrovaných podvodů škoda opět vzrostla.

Kyberkriminalita

V tabulce 5 jsou uvedeny počty podvodů spáchaných internetem v Plzeňském kraji v letech 2019 až 2023 včetně objasněnosti a celkové škody.

Tab. 5: Kyberkriminalita registrovaná Krajským ředitelstvím policie PK v letech 2019–2023

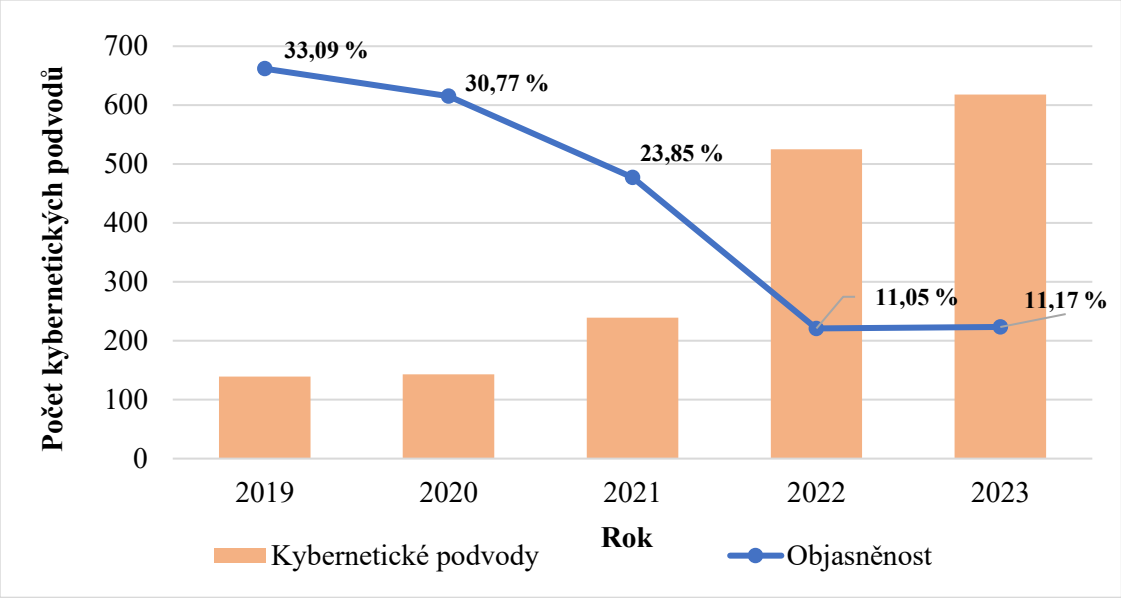
Rok	Registrováno	Objasněno	Objasněno dodatečně	Celková objasněnost (v %)	Škoda (v tis. Kč)
2019	139	29	17	33,09	5 526
2020	143	27	17	30,77	219 972
2021	239	24	33	23,85	40 448
2022	525	24	34	11,05	91 912
2023	618	22	47	11,17	85 273

Zdroj: vlastní zpracování (2024) dle Hrabáka (osobní komunikace, 18. 3. 2024)

Není výjimkou, že ve sledovaných letech docházelo v počtu registrovaných kybernetických podvodů opět k postupnému nárůstu. Srovná-li se rok první a poslední sledovaný rok, v roce 2023 bylo registrováno o 479 podvodů spáchaných internetem více, což je více než trojnásobek kybernetických podvodů v roce 2019. S přibývajícím počtem kybernetických podvodů se sice zvyšuje absolutní počet objasněných případů, ale viditelně klesá míra celkové objasněnosti. Zatímco v roce 2019 byla objasněna třetina případů, v letech 2022 a 2023 Policie ČR byla schopna objasnit pouze 11 % případů. Může to poukazovat na to, že jsou podvody i jejich pachatelé sofistikovanější a je výrazně složitější případy těchto podvodů objasnit. O tom také může svědčit i rostoucí počet případů, které byly objasněny až dodatečně, neboť je možné, že případy vyžadovaly více času na vyřešení. Opět až na výjimku v roce 2020, celková škoda spojená s kyberkriminalitou stoupá. Může to být jednak důsledkem většího množství podvodů a jednak možným zvýšením škod, které byly způsobeny jednotlivými případy. Za zmínku také stojí fakt, že v roce 2022 tvořila škoda způsobená kybernetickými podvody 55 % škody způsobené všemi podvody.

K vizualizaci těchto dat slouží obrázek 8 na straně 59, kde je zobrazen graf s počtem registrovaných kybernetických podvodů a mírou celkové objasněnosti.

Obr. 8: Vývoj kybernetických podvodů a jejich objasněnosti v PK v letech 2019-2023



Zdroj: vlastní zpracování (2024) dle Hrabáka (osobní komunikace, 18. 3. 2024)

Z dat, která byla poskytnuta Policií ČR, jednoznačně vyplývá, že i v Plzeňském kraji je kyberkriminalita na velkém vzestupu. Zatímco počet registrovaných kybernetických podvodů strmě roste, jejich objasnění se zdá být obtížné a celková míra objasněnosti klesá. Je víceméně logické, že trestné činy páchané v kyberprostoru lze prozatím jen těžko objasnit – pachatelé jsou v tomto oboru bezesporu napřed a Policie ČR spolu s bankami a jinými institucemi musí reagovat často na nové provedení podvodů za pochodu. Také nárůst celkové škody, který ukazuje finanční dopad na oběti, je celkově u všech podvodů velmi výrazný. Bohužel se lze domnívat, že i v následujících letech bude podvodů v kyberprostoru i způsobených škod přibývat.

5.3 Podvody v České spořitelně

Česká spořitelna a. s. je nejstarší česká banka, která vznikla v roce 1825. Sama se označuje za „banku s nejdelší tradicí“ a v roce 2025 oslaví 200 let existence na českém trhu. Z pohledu počtu klientů je považována za největší banku v ČR, neboť jich čítá přes 4,5 milionu. (Česká spořitelna, 2022) Česká spořitelna dále také uvádí, že se stará o finanční zdraví svých klientů. Aktivně se podílí na finančním vzděláváním obyvatel ČR a apeluje především na finanční vzdělávání dětí. Snaží se o to, aby Češi, a především její klienti, pochopili důležitost vytváření finančních rezerv na neočekávané výdaje, šetření peněžních prostředků na důchod, porozumění úvěrům atp. Všechny tyto přísliby Česká spořitelna shrnuje do několika hesel, například „Ať rozbitá pračka nepřipraví děti o kroužky.“, „Ať se děti mají lépe než rodiče.“ nebo „Na penzi by se měl člověk těšit.“ (Česká spořitelna, 2023)

5.3.1 Škody způsobené kybernetickými podvody

Česká spořitelna je také jediná z oslovených bank v ČR, která poskytla autorce údaje z vlastního reportu týkající se kybernetických útoků. Grafy poskytl za Českou spořitelnu pan Lukáš Kropík (osobní komunikace, 18. 3. 2024), který působí v týmu pro externí komunikaci. První graf se týká celkové škody, která byla způsobena klientům banky v důsledků různých druhů podvodů. Tento graf zobrazuje obrázek 9 na straně 61.

Modrá část grafu vyznačuje objemy škod, které klientům banky vznikly v důsledku **fraudů** (podvodů) jako je například zneužití platební karty, a to na základě různých forem útoků od family fraudu, po vyplnění citlivých údajů na neověřených webech apod. Podle České spořitelny (2024c) je family fraud označení pro (ve většině případů) neúmyslné zneužití platební karty osobou blízkou, nejčastěji pak dětmi. Rodič má například uloženou kartu v mobilním telefonu, který se dětem může dostat do rukou. V případě, že přístupy do různých aplikací v zařízení nejsou zabezpečeny heslem, děti si následně mohou stahovat placenou hudbu, hry, filmy či zaplatit předplatné streamovacích služeb atd.

Růžová část grafu poté zachycuje škody, které vznikly v důsledku ostatních podvodů neboli **scamů**. Klienti například poslali peníze na účet podvodníka či vybrali a vložili peníze do bitcoinmatu nebo na jiný falešný investiční produkt. Stejně tak se ale může

jednat o různé typy scamu/phishingu, tedy komunikace podvodníků s klienty prostřednictvím SMS zpráv, e-mailu nebo falešných telefonátů.

Obr. 9: Škody způsobené klientům České spořitelny v letech 2020-2024

Zdroj: Kropík (osobní komunikace, 18. 3. 2024)

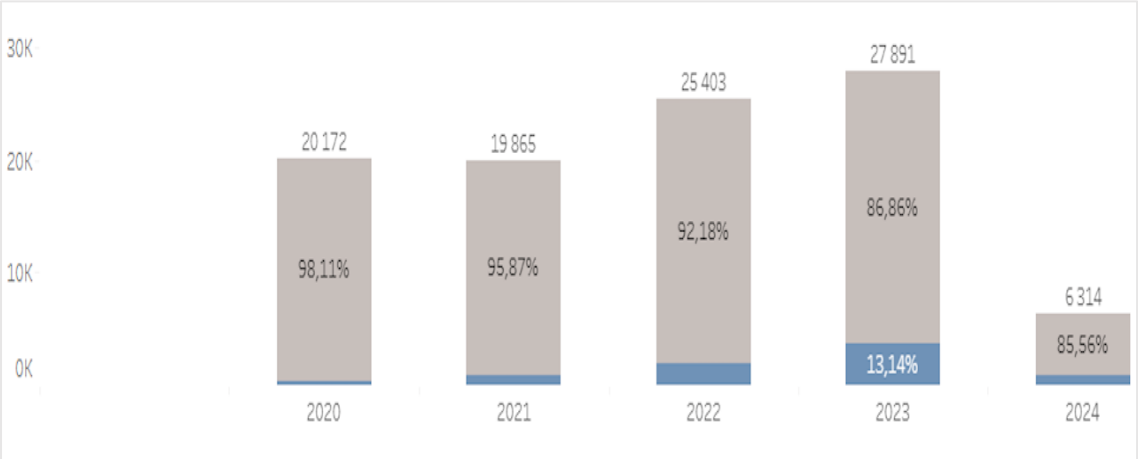
Dle barevného vyznačení byly každoročně největší škody způsobeny scamy, tj. posláním peněz podvodníkovi, phishingem, falešnou investiční příležitostí apod. Velmi prudký nárůst škod byl zaznamenán mezi roky 2021 a 2022. O nejvíce peněz přišli klienti banky právě v roce 2022, kdy výše celkové škody dosahovala 454 milionů Kč, což je v průměru 37 milionů za měsíc. Z toho škody způsobené právě phishingem či podobným podvodem měly na této enormní škodě 85% podíl. Zbylých 15 % škod bylo způsobeno zneužitím platebních karet. V roce 2023 celková škoda klesla o čtvrtinu, a to na částku 330 milionů Kč, přičemž 24 % škody bylo způsobeno zneužitím platebních karet a 76 % škody představuje opět ostatní podvodná jednání. V roce 2023 průměrná měsíční škoda činila 27,5 milionu Kč. Na obrázku 9 je zobrazen i počáteční vývoj v roce 2024, kde je škoda vyčíslena přibližně do poloviny března a činí prozatím 71 milionů Kč. Škoda zjištěná v roce 2024 může v této chvíli naznačovat podobný průběh jako v roce předchozím, neboť prozatímní výše škody ukazuje, že měsíčně klienti přišli průměrně

o 27 milionů Kč. Je taktéž zajímavé pozorovat, že škoda ve výši 94 milionů, která byla zjištěna za celý rok 2021, je velmi blízko škodě zjištěné za necelé tři měsíce v roce 2024.

5.3.2 Počty kybernetických podvodů

Druhý graf z reportu kybernetických útoků, který je zobrazen na obrázku 10, ukazuje počty podvodů spáchaných na klientech banky v letech 2020-2024. **Modré pole v grafu** symbolizuje stejně jako v předchozím grafu **fraudy**, tedy podvody s platebními kartami, a **šedivé pole v grafu** značí opět **scamy.**

Obr. 10: Počet scamů a fraudů spáchaných na klientech České spořitelny v letech 2020-2024



Zdroj: Kropík (osobní komunikace, 18. 3. 2024)

Z grafu vyplývá, že i kybernetické podvody páchané na klientech České spořitelny postupně narůstají, pomine-li se jejich nepatrný pokles v roce 2021. Jak se dalo očekávat na základě předchozího obrázku 9 se způsobenými škodami, každý rok tvořily dominantní část scamy, kterých během sledovaných let bylo dohromady spácháno bezmála 100 000. Případů zneužití platebních karet pak bylo dohromady zjištěno zhruba 5 000. V roce 2020 bylo na klientech banky spácháno lehce přes 20 000 podvodů a v roce 2021 přibližně o 300 méně. Avšak v případě škod tomu bylo naopak, neboť v roce 2021 byla způsobená škoda o třetinu vyšší nežli v roce 2020. Významný nárůst podvodů byl poté zaznamenán v roce 2022, kdy bylo oproti roku 2021 nahlášeno přibližně o 5 000 podvodů více. Zatímco se v roce 2023 počet podvodů opět mírně zvýšil, v předchozím grafu způsobených škod bylo možné sledovat, že celková klientská škoda se meziročně viditelně snížila. Podle Kropíka (osobní komunikace, 18. 3. 2024) to bylo způsobeno především kombinací vzdělávacích kampaní a neustálé vzdělávací komunikace přímo na klienty, do níž Česká spořitelna investovala desítky milionů korun, a zároveň nasazením

nových technologií (včetně AI, tedy umělé inteligence) pro odhalení potenciálně podvodných plateb. Do zhruba půlky března roku 2024 bylo odhaleno okolo 6 000 podvodů, což je ve srovnání s minulými roky podobné tempo nárůstu podvodů.

Dále Kropík (osobní komunikace, 18. 3. 2024) také uvedl, že v roce 2023 poprvé Česká spořitelna zaznamenala rozšířené využívání umělé inteligence mezi kyberpodvodníky. Příkladem byla vlna falešných telefonátů, při nichž se podvodníci vydávali za zaměstnance České spořitelny.

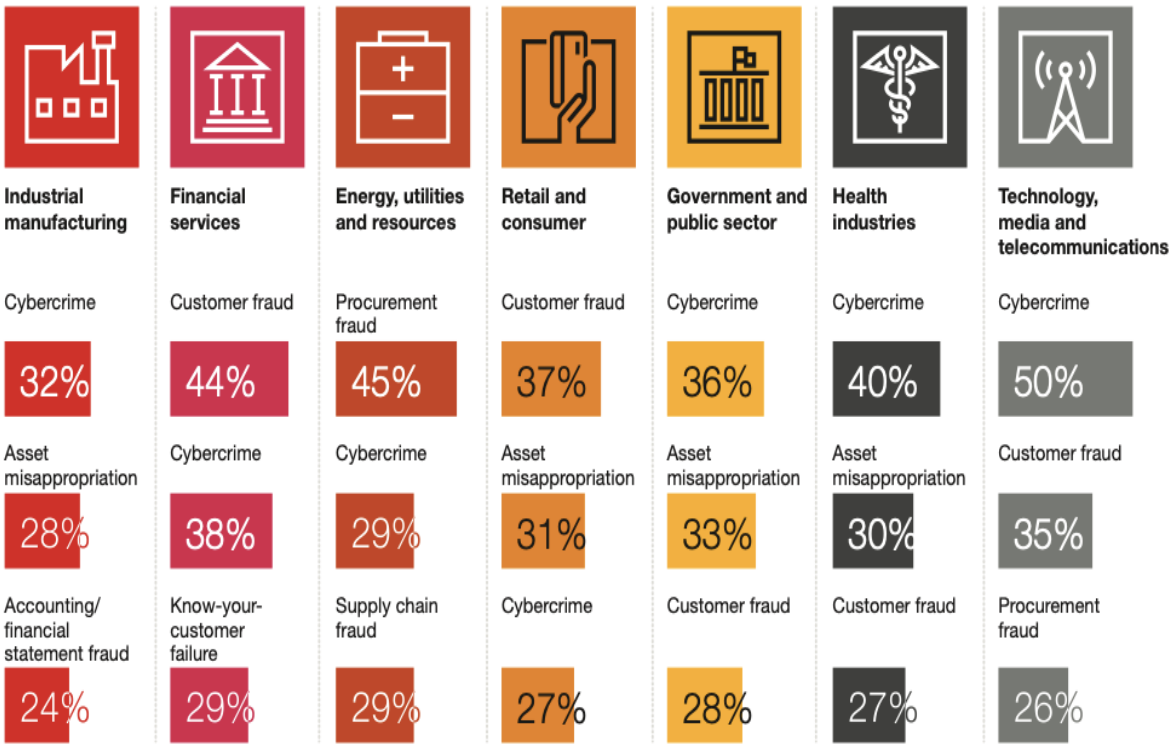
Zvýšený výskyt podvodů souvisel dle Kropíka (osobní komunikace, 18. 3. 2024) především s přechodem klientů na novou bankovní aplikaci, kterého podvodníci využili. Téměř dva miliony klientů totiž přecházely z aplikace George klíč, která byla dříve používána pro ověřování plateb a identity, na novou aplikaci George v mobilu, která nyní slouží ke správě plateb i k ověření identity klientů v rámci bankovních služeb. Aby kyberpodvodníci získali přístup k digitálnímu bankovnictví, kontaktovali klienty prostřednictvím SMS zpráv, telefonátů nebo také využívali předem nahrané telefonické zprávy, k jejichž vytvoření používali právě AI. Pod falešnou záminkou potřeby dokončení přechodu na novou aplikaci, vyzývali klienty k uvedení jejich přihlašovacích údajů a aktivních kódů k aplikaci George.

V roce 2024 byl přechod klientů na novou aplikaci dokončen a širší využití umělé inteligence v kybernetických útocích Česká spořitelna neidentifikuje. Naopak, jak bylo zmíněno výše, sama Česká spořitelna začala AI využívat v boji proti kyberpodvodům.

5.4 Podvody v zahraničí

Mezinárodní společnost PwC, která poskytuje auditorské, daňové a poradenské služby, provádí Global Economic Crime and Fraud Survey, tedy globální průzkum hospodářské kriminality a podvodů. Poslední průzkum byl proveden v roce 2022, kde bylo vyzdvihováno především riziko kyberkriminality. Z průzkumu vyplývá, že kybernetické podvody v menší či větší míře postihovaly všechna odvětví. Zvláště v odvětvích technologií, médií a telekomunikací je kybernetická kriminalita označena 50 %, což je nejvyšší procento mezi všemi odvětvími. Hned na druhém místě jsou pak zdravotnická zařízení se 40 %. V odvětví finančních služeb, kam lze zařadit i banky, se nejvíce společností setkalo nejčastěji s podvodem ze strany klienta a hned poté s kybernetickým podvodem. Finanční služby, odvětví energetiky, veřejných služeb a zdrojů a také obchod jsou tedy oblasti, které nemají na prvním místě kybernetické podvody. Avšak je velmi pravděpodobné, že pokud by byl průzkum proveden v roce 2023 nebo až v roce 2024, kybernetické útoky by zaujímaly minimálně v oblasti finančních služeb první místo.

Obr. 11: Typy podvodů v jednotlivých odvětvích v roce 2022



Zdroj: PwC – Global Economic Crime and Fraud Survey (2022)

Britská společnost AAG (2023), která je ve Velké Británii specialistou v oblasti technologií a bezpečnosti, provedla v roce 2022 průzkum týkající se kyberbezpečnosti ve světě. Výsledky jsou následující.

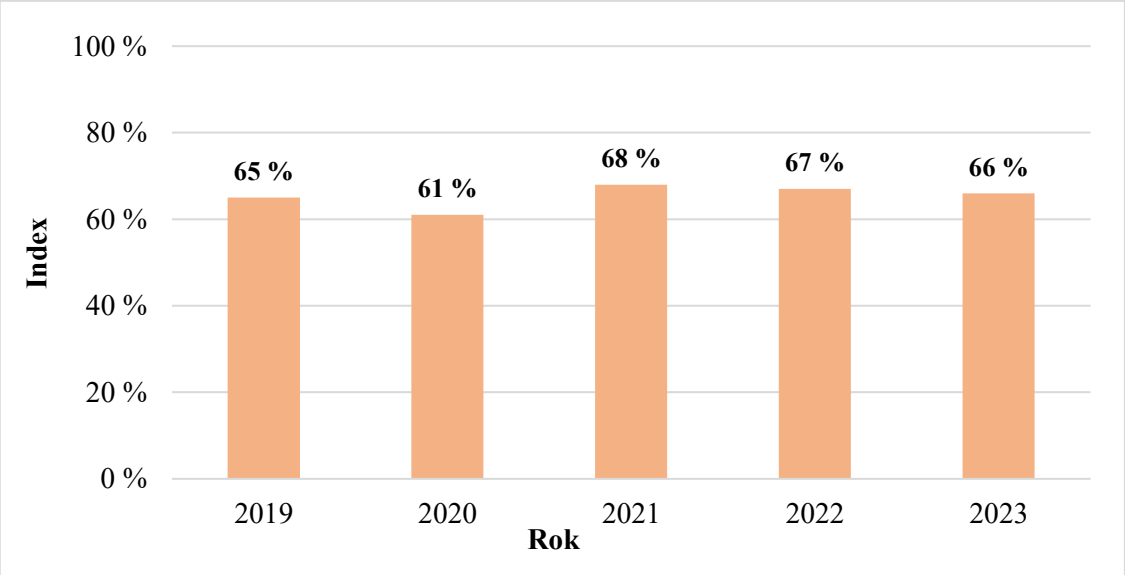
- V Asii se kybernetická kriminalita stává čím dál tím vážnějším problémem. V zemích jako Pákistán, Indie, Malajsie a Nepál roste počet případů finančních podvodů, hackingu, online obtěžování a útoků ransomware. Například v Indii bylo v prvních dvou měsících roku 2022 nahlášeno více kybernetických trestných činů než v celém roce 2018.
- Také v Americe se zvyšuje počet kybernetických trestných činů, zejména v Kanadě, kde mezi lety 2017 a 2021 vzrostl počet nahlášených případů o 153 %. Alarmujícím problémem jsou stejně jako v ČR phishing a online podvody. Kanadské organizace v roce 2020 přišly kvůli kybernetické kriminalitě o bezmála 1,5 miliardy dolarů.
- V rámci Oceánie je nejčastějším cílem kybernetických útoků Austrálie, s průměrným výskytem kybernetického útoku každých 10 minut. Scamy, zejména falešné investiční příležitosti, stály Australany v roce 2022 více než 48 milionů dolarů.
- Afrika je také vystavena vysokému riziku kybernetické kriminality. Především země jako Nigérie a Zambie se setkávají s obrovským nárůstem datových krádeží a finančních ztrát v důsledku podvodů.
- V Evropě je největším terčem útoků Rusko, ale například i Německo se potýká s vysokou mírou kybernetických trestných činů. Rusko zažívá obrovský počet především datových krádeží a v Německu vedou spamy a phishing.

Dále například v rámci Microsoft Digital Defense Reportu (2022) bylo zkoumáno, které evropské země jsou z hlediska kybernetické bezpečnosti pro občany nejvíce bezpečné. Microsoft konkrétně zkoumal procenta počítačů, které každý měsíc čelily útokům spojeným s kryptoměnami, malwarem a ransomwarem. Za kyberneticky nejisté země jsou dle tohoto reportu považovány nejčastěji méně vyspělé země, neboť zde byly počítačové útoky zjištěny ve velké míře. Patří mezi ně Bulharsko, Bělorusko, Ukrajina, Bosna a Hercegovina, Litva, Rumunsko, Maďarsko a Chorvatsko. Naopak mezi nejbezpečnější země patří ČR a spolu s ní také Irsko, Norsko, Dánsko, Švýcarsko, Island, Švédsko s Lucembursko.

6 Kyberbezpečnost v ČR

Česká bankovní asociace (ČBA) pravidelně již několik let pozoruje chování a obezřetnost Čechů v online prostoru. V této souvislosti provádí ČBA každý rok průzkum prostřednictvím strukturovaného online dotazníku, jehož cílovou skupinou je reprezentativní vzorek populace ČR ve věku 18-79 let, který tvoří vždy přibližně 1 000 lidí. Na základě tohoto průzkumu od roku 2015 ČBA sestavuje index kyberbezpečnosti, který vypovídá o schopnosti zodpovědného chování Čechů v kyberprostoru. Od roku 2019 se počty kybernetických podvodů zvyšují, a tak ČBA přidala do dotazníku několik nových otázek. (ČBA, 2023) Jak se hodnota indexu kyberbezpečnosti vyvíjela v letech 2019-2023 ukazuje graf, který je zobrazen na obrázku 12.

Obr. 12: Vývoj indexu kyberbezpečnosti v ČR v letech 2019-2023



Zdroj: vlastní zpracování (2024) dle ČBA (2019, 2020, 2021b, 2022b, 2023)

Přestože od roku 2019 začalo kybernetických podvodů přibývat, na hodnotě indexu se to nepodepsalo. Oproti roku 2018 totiž jeho hodnota stoupla o 5 procentních bodů na 65 % ze sta. Avšak podle ČBA (2019) to nebylo považováno za příliš velký úspěch, neboť je to stále průměrný výsledek ve srovnání s ostatními zeměmi. V roce 2020 opět index klesl na průměrnou hodnotu 61 %, ale rok poté Češi začali vykazovat obezřetnější chování v kyberprostoru, neboť index kyberbezpečnosti dosáhl 68 %. ČBA (2021b) toto zlepšení přisuzuje i pandemii koronaviru, v důsledku které se přesunula spousta aktivit online a mnoho lidí se tak naučilo lepší orientaci v online světě. V letech 2022 a 2023 index

mírně poklesl, avšak veřejnost v tomto období čelila výrazně vyššímu počtu kyberútoků oproti nejzdařilejšímu roku 2021. Lze tedy konstatovat, že to nejsou špatné výsledky.

6.1 Otázky bezpečnosti

V tabulce 6 je uvedeno, jak Češi v letech 2020 až 2023 odpovídali na vybrané otázky týkající se základních bezpečnostních návyků v kyberprostoru.

Tab. 6: Výsledky vybraných otázek z průzkumu ČBA v letech 2020-2023

Otázka	2020	2021	2022	2023
Upozornění od banky si čte:				
pravidelně	51 %	52 %	48 %	51 %
občas	44 %	44 %	46 %	43 %
Bankovní účet si kontroluje:				
pravidelně	65 %	65 %	64 %	69 %
příležitostně	33 %	33 %	34 %	29 %
Přílohy od neznámého neotevře:				
nikdy	82 %	78 %	74 %	76 %
občas	14 %	17 %	19 %	18 %
Do internetového bankovnictví se přihlašuje přes:				
zabezpečenou Wi-FI síť	53 %	46 %	–	–
datový tarif	33 %	43 %	–	–
Do internetového bankovnictví se přihlašuje:				
pouze na svém zařízení	–	–	79 %	81 %
na pracovním zařízení	–	–	10 %	9 %

Zdroj: vlastní zpracování (2024) dle ČBA (2020, 2021b, 2022b, 2023)

V případě základních návyků, které by měly být v rámci bezpečnosti na internetu dodržovány, dopadli Češi v průběhu let 2020 až 2023 následovně. Upozorněním, které

vydává banka, Češi tolik pozornosti nevěnují. Pravidelně je četlo v každém roce okolo 50 % a občas si upozornění přečetlo v průměru 44 %. S přihlédnutím k počtům podvodů lze toto považovat za nerozumné. Svůj bankovní účet nebo bankovní výpis pravidelně kontrolovalo průměrně 65 % respondentů a příležitostně 32 %. Znamená to, že pouhá 3 % respondentů stavu na svém účtu nevěnuje pozornost. Pokud někomu přišel e-mail od neznámého odesílatele, pak v průměru 75 % Čechů neotevřelo nikdy jeho přílohu a přibližně 17 % se občas do přílohy podívalo. Otázky ohledně internetového bankovnictví se mírně odlišovaly. V roce 2020 a 2021 bylo zkoumáno, jaké připojení respondenti používají při vstupu do internetového bankovnictví, kdežto v letech 2022 a 2023 otázka směřovala na zařízení, ze kterého se do bankovnictví přihlašují. V každém případě jsou výsledky poměrně uspokojující. Jedině přes zabezpečenou Wi-Fi síť se připojovala přibližně polovina Čechů. Datového tarifu využívalo 33 % Čechů v roce 2020 a 43 % v roce 2021. Není to vyloženě špatný výsledek, ale z odpovědí je bohužel jasné, že se v obou letech několik respondentů přihlásilo do svého bankovnictví na veřejné Wi-Fi síti, což by se v žádném případě stávat nemělo. V letech 2022 a 2023 respondenti využívali pro přihlášení do internetového bankovnictví nejčastěji pouze své zařízení (mobilní telefon, počítač či tablet). Z pracovního zařízení, o kterém vědí, jak je zabezpečeno, se přihlašovalo 10 % (2022) a 9 % (2023). Z průzkumu vyplývá, že se chování Čechů v otázkách základních bezpečnostních návyků v průběhu let víceméně nemění a lze jej považovat za průměrné. Bylo by vhodné věnovat zprávám od bank větší pozornost a opravdu pravidelně si kontrolovat svůj bankovní účet. To je v bezpečnostních návycích jistě neprosté minimum.

Hesla k účtům a zabezpečení zařízení

Odpovědi na otázky ohledně hesel k účtům ve všech letech dopadly opět velmi podobně a poměrně dobře. Pro internetové bankovnictví používali Češi silná sofistikovanější hesla, která si pamatovali a tím pádem nikam nezapisovali. Negativní stranou byla frekvence změny hesel – nejčastěji si hesla v aplikacích respondenti měnili jednou ročně. Pro ostatní média jako jsou sociální sítě či e-maily mívají Češi klidně stejná hesla a změní si je často až v případě, že je daná aplikace či webová stránka vyzve. (ČBA, 2020, 2021b, 2022b, 2023) V případě zabezpečenosti zařízení Češi takzvaně pohořeli. Každý rok se najde přibližně čtvrtina lidí, kteří svá zařízení jako mobilní telefon, počítač nebo tablet nezabezpečují a důvěřují pouze v ochranu samotným operačním systémem. Nejméně

chráněné pak bývají většinou mobilní telefony, a naopak nejvíce si Češi zabezpečují své počítače.

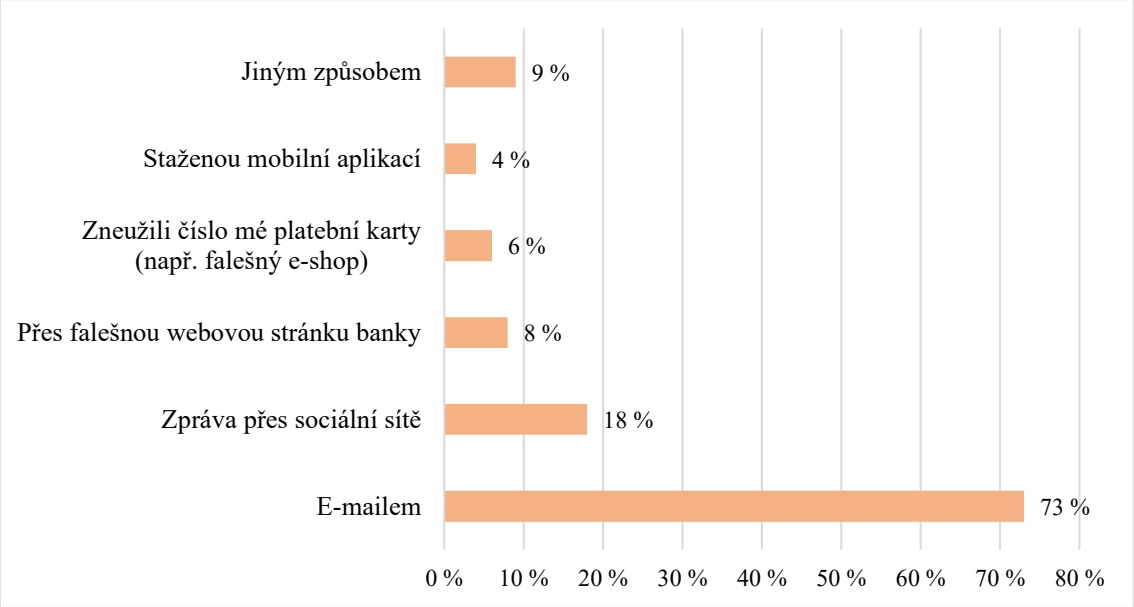
6.2 Kyberútoky

Ve sledovaných letech se každoročně s kyberútokem setkala polovina Čechů. Nejčastěji se s jakýmkoliv typem útoku setkávali mladí lidé ve věku 18-34 let, a naopak nejméně se s podvody a útoky setkávali lidé starší 65 let. Pokud doje na ochranu dat, podle průzkumu přibližně 70 % Čechů důvěřuje nejvíce bankám. Podle ČBA (2022b) to může být důvod, proč se podvodníci v e-mailech nebo v hovorech stále častěji vydávají za pracovníky banky.

6.2.1 Druhy kyberútoků v roce 2020

Nejčastější druhy útoků, kterým byli respondenti, jež se setkali s útokem, vystaveni v roce 2020, jsou zobrazeny na následujícím obrázku 13.

Obr. 13: Nejčastější způsoby kyberútoků v roce 2020



Zdroj: vlastní zpracování (2024) dle ČBA (2020)

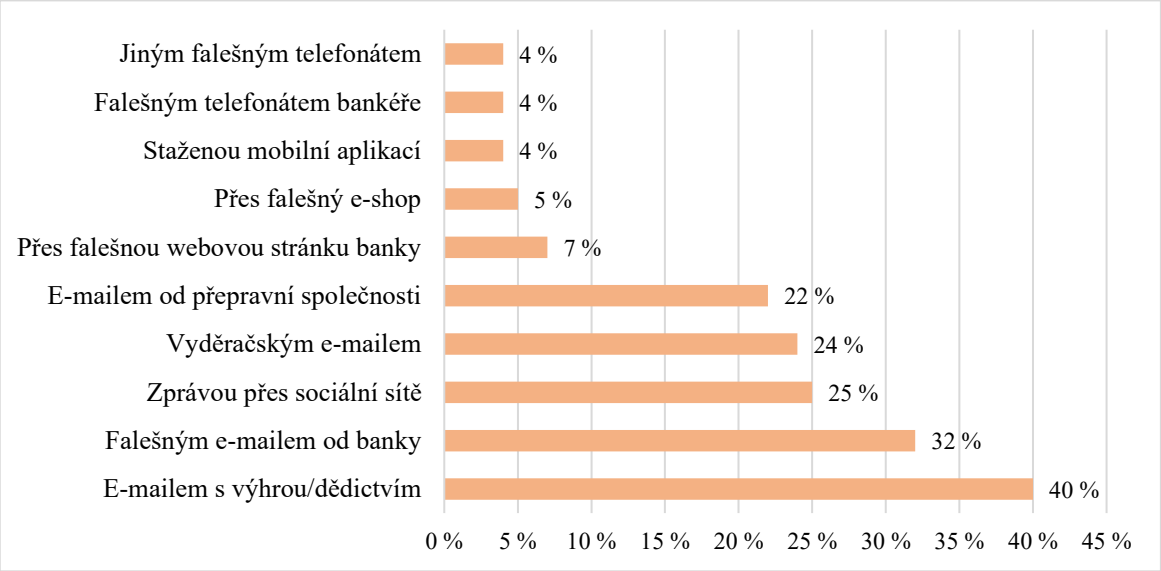
V roce 2020 se s kyberútokem setkalo 49 % Čechů a v 73 % případů se jednalo o podvodný e-mail, tedy phishing. V tomto roce nebylo členění tolik podrobné jako v dalších letech, ale podle ČBA (2020) byly registrované ve velké míře e-maily sdělující, že má dotyčný zablokovaný bankovní účet a přes uvedený falešný odkaz si jej může odemknout. Také bylo několik případů falešných e-mailů od přepravních služeb nebo

vyděračských e-mailů. Dále se nejvíce Češi setkávali s podvodnou zprávou na sociálních sítích a falešnou webovou stránkou banky. V důsledku stažení mobilní aplikace byla podvedena pouze 4 % respondentů.

6.2.2 Druhy kyberútoků v roce 2021

Kybernetické útoky se v roce 2021 opět odehrávaly nejčastěji prostřednictvím phishingových e-mailů. V tomto roce je členění podrobnější a lze tedy pozorovat, že se nejvíce Čechů setkalo s e-mailem s příslibem odměny nebo dědictví. Dalšími nejčastějším e-mailem byl falešný e-mail od banky. Lze se domnívat, že na podvodný e-mail s dědictvím či výhrou by mělo být jednodušší nereagovat nebo podvod odhalit, a to hlavně v případě, kdy není žádné dědictví či výhra očekávána. Odhalení falešných e-mailů od banky tak snadné není, ale jak bylo uvedeno v podkapitole 4.1.3 o kybernetických podvodech, téměř vždy lze v e-mailu nalézt několik nesrovnalostí. S podvodnou zprávou na sociálních sítích se setkalo 25 % respondentů, přičemž třetinu tvořili mladí lidé ve věku 18-34 let. Dalšími častými útoky byly vyděračské e-maily a falešné e-maily od přepravních společností. Právě tyto druhy e-mailů se vyskytovaly nejvíce mezi staršími ve věku 50-64 let. Poprvé v roce 2021 se lidé začali aktivně setkávat s vishingem, tedy falešnými telefonáty od bankéřů, policistů nebo pracovníků ČNB. Pozitivní zprávou je, že 83 % respondentů, kteří se s útokem setkali, dokázalo podvod včas rozpoznat a nebyla jim tak způsobená žádná škoda. Nejčastější způsoby kyberútoků v roce 2021 jsou shrnuty v grafu, který zobrazuje obrázek 14.

Obr. 14: Nejčastější způsoby kyberútoků v roce 2021

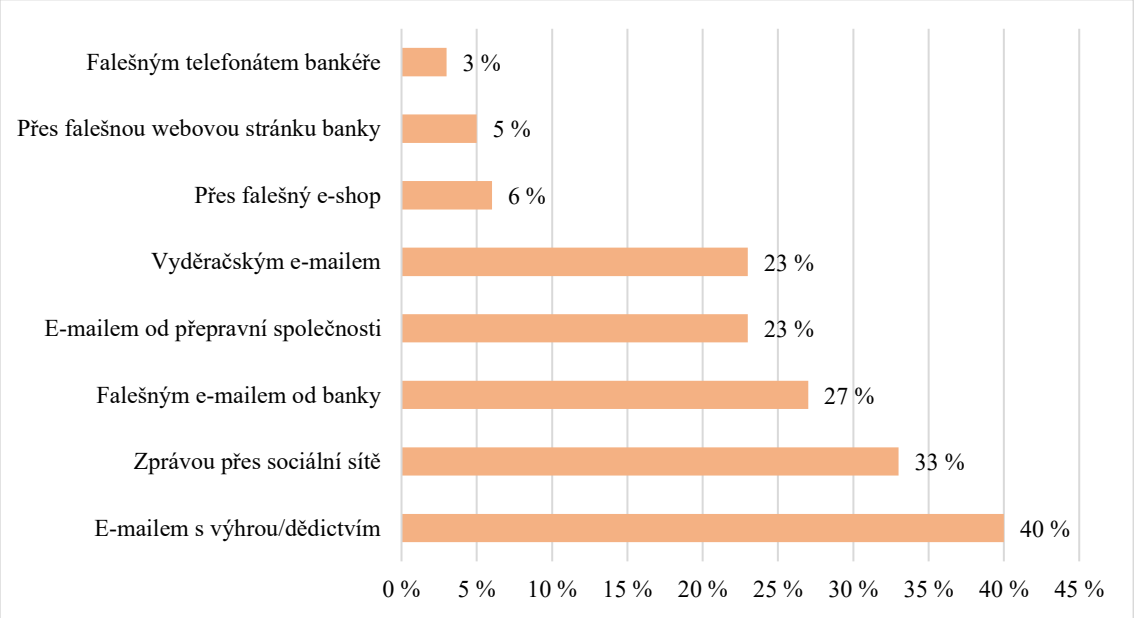


Zdroj: vlastní zpracování (2024) dle ČBA (2021b)

6.2.3 Druhy kyberútoků v roce 2022

V roce 2022 bylo celkově zaznamenáno nejvíce útoků. Jejich počty se za dva roky zvýšily čtyřnásobně a škoda na jednoho podvedeného klienta v průměru činila 162 000 Kč. (ČBA, 2022b) Dle obrázku 15 je patrné, že stejně jako v předešlých letech, se lidé nejvíce setkávali s různými formami phishingu, přičemž nejčastějším cílem podvodníků bylo získání přihlašovacích údajů do bankovnictví a čísel platební karty. Nárůst byl zaznamenán v případě útoků provedených přes zprávy na sociálních sítích, jejichž výskyt se oproti minulému roku zvýšil o 7 procentních bodů. Případů vishingu spíše nepřibývalo a z průzkumu také vyplynulo, že podvodné telefonáty Češi většinou odhalí, avšak 4 % z nich by při hovoru osobní informace sdělila. Počet útoků prostřednictvím falešné webové stránky banky nebo falešného e-shopu je víceméně stabilní.

Obr. 15: Nejčastější způsoby kyberútoků v roce 2022



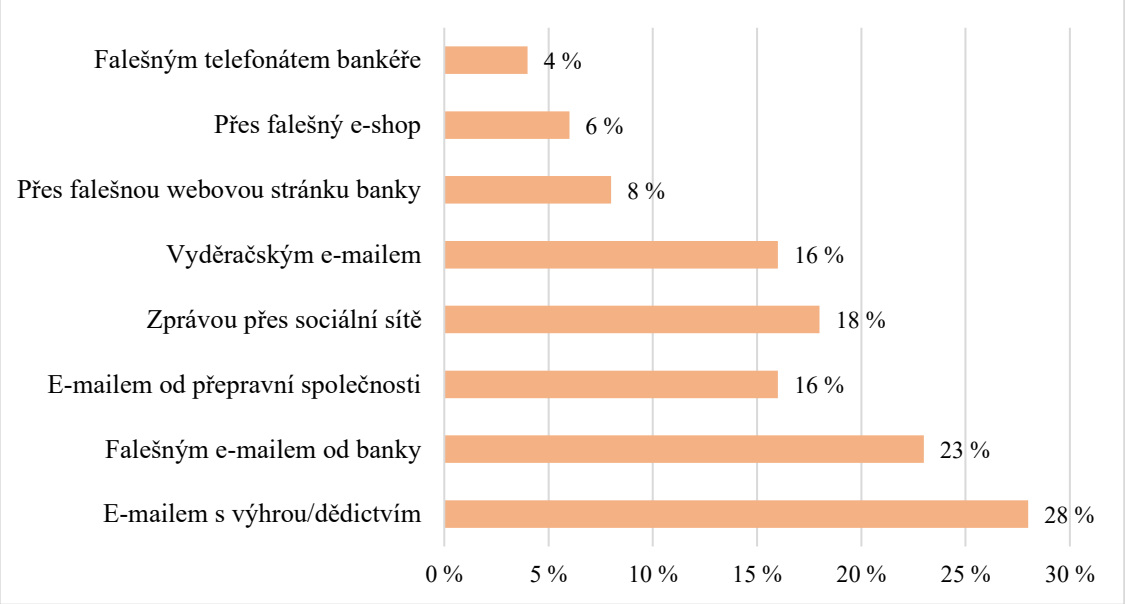
Zdroj: vlastní zpracování (2024) dle ČBA (2022b)

6.2.4 Druhy kyberútoků v roce 2023

Počty kyberútoků se v roce 2023 opět zvýšily – v září tohoto roku jich bylo evidováno bezmála 50 000. Škoda, která byla napadeným způsobena, dosahovala průměrně 20 786 Kč. (ČBA, 2023) Nejčastějším útokem byly opět phishingové e-maily s výhrou, od banky či přepravní společnosti. Podvodů páchaných přes zprávy na sociálních sítích v tomto roce ubylo o 15 procentních bodů. Jejich druhé místo v počtu útoků v roce 2022 vystřídaly falešné e-maily od banky. S falešným telefonátem se stejně jako v minulém

roce setkaly 4 % respondentů a stejně tak je to stále nejméně se vyskytující podvod. Opět z průzkumu vyplynulo, že téměř nikdo (96 %) neposkytl žádné informace během telefonátu. Opět čtyři procenta Čechů by podvodníkovi (nebo samozřejmě komukoliv jinému) požadované informace sdělila. Avšak i takto málo „ochotných“ lidí může sobě způsobit potenciálně obrovské škody. Nejčastější způsoby kyberútoků v roce 2023 jsou shrnuty v grafu, který zobrazuje obrázek 16.

Obr. 16: Nejčastější způsoby kyberútoků v roce 2023



Zdroj: vlastní zpracování (2024) dle ČBA (2023)

Z průzkumu ČBA v letech 2020 až 2023 jednoznačně vyplývá, že nejčastějším podvodem v ČR je phishing, neboť se každý rok drží na prvních místech. Konkrétně je nejčastějším útokem e-mail slibující výhru nebo dědictví a hned poté falešný e-mail od banky. Telefonáty od falešných bankéřů se od roku 2021 objevují v menším měřítku každý rok, nicméně většina lidí jej odhalí. Mladí lidé mají potíže s podvody v rámci sociálních sítích a starší lidé čelí nejvíce e-mailům od přepravních společností. Celkově z průzkumu jednoznačně vyplývá, že se kybernetické útoky každým rokem zvyšují, a proto je nesmírně důležité dbát na svou bezpečnost mimo jiné i v rámci kyberprostoru.

Závěr

Diplomová práce byla zaměřena na bankovní podvody, kdy hlavním cílem bylo komplexně zpracovat problematiku těchto podvodům a dílčím cílem byl rozbor kyberkriminality a kybernetických podvodů v České republice. Prokázalo se, že podvody páchané v kyberprostoru jsou v současné době na výrazném vzestupu. Tato skutečnost se týká i České republiky a je patrná nejen z médií a upozornění bank, ale také z dat o registrované kyberkriminalitě a kybernetických podvodech. Z dat Policie ČR i České spořitelny a také z průzkumu České bankovní asociace vyplývá, že nejvíce kyberpodvodů a potažmo případů kyberkriminality bylo zaznamenáno především v letech 2022 a 2023.

Data o kyberkriminalitě ukázala, že v roce 2023 Police ČR zaznamenala o 60 % více případů kybernetické kriminality než v roce 2020 a o 85 % více případů ve srovnání s rokem 2013. Tento nárůst lze přisuzovat dynamickému rozvoji informačních technologií a částečné také pandemii koronaviru. Tyto okolnosti jistě vedly k přesunu velkého množství aktivit do online prostoru a zvýšenému využívání režimu home office, který většinou vyžadoval vzdálený přístup. Tento vzdálený přístup k firemním počítačům se stal častým terčem podvodníků, protože byly opakovaně hlášeny krádeže dat či průniky do interních firemních sítí. Na straně druhé, celková kriminalita v posledních letech spíše klesala, což vedlo k tomu, že se zvyšoval podíl kyberkriminality na celkové kriminalitě. V roce 2023 představovala kyberkriminalita téměř 11 % všech registrovaných trestných činů, zatímco v roce 2020 to bylo jen necelých 5 % a v roce 2013 méně než 1 %.

Situace v Plzeňském kraji se v kontextu kybernetických podvodů vyvíjela obdobně, neboť v roce 2023 byl zaznamenán trojnásobek kybernetických podvodů oproti roku 2020. Navíc s rostoucí sofistikovaností kyberpodvodů dramaticky klesala míra jejich objasněnosti, což jistě naznačuje, že bylo pro Policii ČR velmi obtížné trestné činy v kyberprostoru vyšetřovat.

Průzkum České bankovní asociace prokázal, že od roku 2020 lze považovat za nejčastější kyberpodvod jednoznačně phishing, a to především v podobě podvodného e-mailu. Tuto skutečnost potvrdila také data z reportu České spořitelny, která ukázala, že se i její klienti setkávali nejčastěji se scamy, tedy phishingem, zatímco případů zneužití karet bylo minimum. Lze konstatovat, že phishing je pro podvodníky poměrně nenáročná metoda provedení podvodu, ale ukázalo se, že v mnoha případech byla účinná. Dále se Češi velmi

často setkávali s phishingem na sociálních sítích a v několika případech také s telefonáty od falešných bankéřů, tedy vishingem.

Obecně data naznačují, že v budoucnu lze očekávat spíše pokračující nárůst kybernetických podvodů. V současné době se však banky, Policie ČR i Česká bankovní asociace intenzivně zaměřují na vzdělávací kampaně a komunikaci s veřejností ohledně prevence kybernetických podvodů, a zdá se, že jsou tyto metody každým rokem účinnější. Svědčí o tom také index kyberkriminality, který v letech 2022 a 2023, i přes masivní nárůst kyberpodvodů, vykazoval mírně vyšší hodnotu než v předchozích letech.

Je zřejmé, že nejúčinnější obranou proti kybernetickým podvodům je neustálé vzdělávání v kombinaci s technickými opatřeními a dodržováním základních bezpečnostních zásad. Technická opatření zahrnují například instalaci antivirových programů v používaných zařízeních, používání silných a jedinečných hesel nebo také bezpečné používání Wi-Fi sítě. Jednou z klíčových bezpečnostních zásad je ochrana platebních a osobních údajů, a především nesdělování těchto údajů cizím osobám. Banky ani jiné instituce nikdy nebudou vyžadovat informace jako PIN k platební kartě, přihlašovací údaje do bankovnictví nebo jakákoliv hesla či údaje prostřednictvím e-mailu, zprávy nebo telefonního hovoru. Dále je také vhodná pravidelná kontrola stavu bankovního účtu a pravidelné sledování všech upozornění, která vydávají banky a další instituce. Dodržováním těchto opatření lze výrazně snížit pravděpodobnost, že se jedinec stane obětí kybernetického podvodu.

Seznam použité literatury

Monografie

Blahová, N. (2018). *Rizika bank a jejich regulace*. Ekopress.

Černohorský, J. (2020). *Finance: od teorie k realitě*. Grada Publishing.

Častorál, Z. (2007). *Ekonomická kriminalita (z pohledu řízení a správy).* Vysoká škola finanční a správní, o.p.s.

Fryšták, M. (2007). *Hospodářská kriminalita z pohledu teorie a praxe.* Key Publishing s.r.o.

Haentjens, M. & Gioia-Carabellese, P. D. (2015). *European banking and financial law*. Routledge.

Heffernan, S. (2005). *Modern Banking.* John Wiley & Sons, Ltd.

Jílek, J. (2000). *Finanční rizika.* Grada.

Jurošková, L. (2012). *Bankoví regulace a dohled.* Auditorium.

Kantnerová, L. (2016). *Základy bankovnictví: teorie a praxe.* C.H. Beck.

Kuchta, J. (2008). *Nové jevy v hospodářské a finanční kriminalitě*. Masarykova univerzita.

Lochmannová, A. (2018). *Bankovnictví: základy bankovnictví*. Computer Media.

Mejstřík, M., Pečená, M. & Teplý, P. (2015). *Bankovnictví v teorii a praxi.* Karolinum.

Šenkýřová, B. (2010). *Bankovnictví.* Vysoká škola finanční a správní.

Polouček, S. (2013). *Bankovnictví.* (2. vydání). C.H. Beck.

Revenda, Z. (2011). *Centrální bankovnictví.* (3. aktualiz. vyd). Management Press.

Revenda, Z., Mandel M., Kodera, J., Musílek, P., & Dvořák, P. (2023). *Peněžní ekonomie a bankovnictví* (Sedmé přepracované vydání). Ekopress.

Internetové zdroje

AAG (2023). *The Latest Cyber Crime Statistics.* Dostupné 17. 3. 2024 z https://aag-it.com/the-latest-cyber-crime-statistics/

ACPR (2024). *PRÉSENTATION DE L'ACPR*. Dostupné 19. 1. 2024 z https://acpr.banque-france.fr/page-sommaire/presentation-de-lacpr

Bankovnictví, finance – Studium. (2023). *Charakteristika typů obchodních bank.* Dostupné 27.9. 2023 z https://bankovnictvi-finance.studentske.eu/2008/04/5-charakteristika-typ-obchodnch-bank_27.html

BIS (2024). *Basel Committee Charter. Dostupné 16. 1. 2024 z https://www.bis.org/bcbs/charter.htm*

CBoI (2024). *What does the Central Bank of Ireland do?* Dostupné 19. 1. 2024 z https://www.centralbank.ie/about

Council of the European Union (2024). *Banking union.* Dostupné 19. 1. 2024 z https://www.consilium.europa.eu/en/policies/banking-union/

CSchlatter, C. (2023). *Top 5 operational risks for banks in 2024.* Intuition. https://www.intuition.com/top-5-operational-risks-for-banks-in-2023/

CyberSecurity.CZ (2012). *Skimming*. Dostupné 25. 1. 2024 z https://www.cybersecurity.cz/data/skimming.pdf

ČBA (2019). *Kyberbezpečnost a index bezpečnosti 2019*. Dostupné 4. 4. 2024 z https://cbaonline.cz/kyberbezpecnost-a-index-bezpecnosti-2019

ČBA (2020). *Průzkum ČBA: Češi a jejich chování v on-line 2020*. Dostupné 4. 4. 2024 z https://cbaonline.cz/cesi-a-jejich-chovani-v-on-line-prostredi-2020

ČBA (2021a). *Bankovní dohled.* Dostupné 17. 9. 2023 z https://www.financnivzdelavani.cz/bankovni-dohled

ČBA (2021b). *Průzkum ČBA: Češi jsou oproti kybernetickým hrozbám obezřetnější*. Dostupné 4. 4. 2024 z https://cbaonline.cz/pruzkum-cba-cesi-jsou-oproti-kybernetickym-hrozbam-obezretnejsi

ČBA (2022a). *Desatero bezpečnosti.* Dostupné 4. 2. 2024 z https://www.kybertest.cz/desatero-bezpecnosti-na-internetu

ČBA (2022b). *Index kyberbezpečnosti 2022*. Dostupné 4. 4. 2024 z https://cbaonline.cz/index-kyberbezpecnosti-2022

ČBA (2023). *Index kyberbezpečnosti 2023*. Dostupné 4. 4. 2024 z https://cbaonline.cz/index-kyberbezpecnosti-2023

ČBA (2024a). *Kapitálová přiměřenost.* Dostupné 17. 1. 2024 z https://cbaonline.cz/kapitalova-primerenost

ČBA (2024b). *Jak dnes vypadá boj proti praní špinavých peněz.* Dostupné 17. 1. 2024 z https://cbaonline.cz/banky-a-aml

ČBA (2024c). *Průměrná úspěšnost v Kybertestu byla 74 %.* Dostupné 4. 2. 2024 z https://mailchi.mp/cbaonline/cba-news-202402_cz

Česká národní banka (2021). *ČR by měla vstoupit do bankovní unie až v okamžiku přijetí eura.* Dostupné 10. 1. 2024 z https://www.cnb.cz/cs/cnb-news/tiskove-zpravy/CNB-CR-by-mela-vstoupit-do-bankovni-unie-az-v-okamziku-prijeti-eura/

Česká národní banka (2023a). *Licencování.* Dostupné 10. 9. 2023 z https://www.cnb.cz/cs/dohled-financni-trh/vykon-dohledu/postaveni-dohledu/dohled-nad-uverovymi-institucemi/licencovani/

Česká národní banka (2023b). *Měnová politika.* Dostupné 19. 9. 2023 z https://www.cnb.cz/cs/menova-politika/

Česká národní banka (2023c). *O ČNB.* Dostupné 17. 9. 2023 z https://www.cnb.cz/cs/o_cnb/

Česká národní banka (2023d). *Inflace v srpnu 2023 v souladu s prognózou dále klesla.* Dostupné 12. 9. 2023z https://www.cnb.cz/cs/verejnost/servis-pro-media/komentare-cnb-ke-zverejnenym-statistickym-udajum-o-inflaci-a-hdp/Inflace-v-srpnu-2023-v-souladu-s-prognozou-dale-klesla/

Česká národní banka (2023e). *Zadržené padělky v roce 2023.* Dostupné 12. 1. 2024 z https://www.cnb.cz/cs/bankovky-a-mince/padelky/pad_ctvrtletni_sum/

Česká národní banka (2023f). *Padělků bankovek výrazně ubylo, padělatelé nejčastěji napodobují tisícikorunu.* Dostupné 12. 1. 2023 z https://www.cnb.cz/cs/cnb-news/tiskove-zpravy/Padelku-bankovek-vyrazne-ubylo-padelatele-nejcasteji-napodobuji-tisicikorunu/

Česká národní banka (2008) *Operační riziko a jeho dopady do finanční stability.* Dostupné 20. 1. 2024 z https://www.cnb.cz/export/sites/cnb/cs/financni-stabilita/.galleries/zpravy_fs/fs_2007/FS_2007_clanek_4.pdf

Česká národní banka (2024) *Basilejský výbor.* Dostupné 20. 1. 2024 z https://www.cnb.cz/cs/dohled-financni-trh/vykon-dohledu/mezinarodni-aktivity/basilejsky-vybor/

Český statistický úřad (2023). *Průměrná roční inflace v ČR v roce 2022 byla 15,1 %*. Dostupné 26. 9. 2023 z https://www.czso.cz/csu/xe/prumerna-rocni-mira-inflace-v-cr-v-roce-2022-byla-151-

ČSOB (2024). *Žádost o poskytnutí úvěru.* Dostupné 20. 1. 2024 z https://www.csob.cz/documents/10710/498467/csob-zadost-poskytnuti-uveru.pdf

Česká spořitelna (2011). *Padělání peněz/Druhé nejstarší řemeslo*. Dostupné 17. 1. 2024 z https://www.galerieceskesporitelny.cz/galerie/vystavy/35/skladacka.nahled.pdf.pdf

Česká spořitelna (2022). *Všeobecná prezentace o FS ČS*. Dostupné 20. 3. 2024 z https://www.csas.cz/static_internet/cs/Obecne_informace/FSCS/CS/Prilohy/vseobecna_prezentace.pdf

Česká spořitelna (2023). *Zlepšeme finanční zdraví Čechů*. Dostupné 20.3. 2024 z https://financnezdravejsi.csas.cz/cs/web/zlepseme-financni-zdravi-cechu

Česká spořitelna (2024a). *Zbohatnutí přes internet, falešné nabídky investic*. Dostupné 27. 1. 2024 z https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat/zbohatnuti-pres-internet-falesne-nabidky-investic

Česká spořitelna (2024b). *Jak se bránit proti moderním typům podvodů.* Dostupné 27. 1. 2024 z https://financnezdravejsi.csas.cz/cs/jsem-v-bezpeci/bezpecne-finance-jak-se-branit-proti-modernim-typum-podvodu

Česká spořitelna (2024c). *Family Fraud.* Dostupné 20. 3. 2024 z https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat/family-fraud

Dvojklik (2023). *Vishing: Podvodné telefonáty nás připraví o peníze i data*. Dostupné 27. 1. 2024 z https://www.dvojklik.cz/podvodne-telefonaty-vas-pripravi-o-data-a-casem-i-o-penize/

Economia (2024). *Nečekaně přesvědčivý podvod. Video s Pavlem se na sítích „utrhlo“. A bude hůř.* Dostupné 25. 1. 2024 z https://domaci.hn.cz/c1-67285590-necekane-presvedcivy-podvod-video-s-pavlem-se-na-sitich-utrhlo-a-bude-hur

ESET (2024a). *Phishing*. Dostupné 23. 1. 2024 z https://www.eset.com/cz/phishing/

ESET (2024b). *Přehled hrozeb pro Android: Chytré telefony v Česku nově ohrožuje trojský kůň, který napadá bankovní aplikace* Dostupné 23. 1. 2024 z https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/prehled-hrozeb-pro-

android-chytre-telefony-v-cesku-nove-ohrozuje-trojsky-kun-ktery-napada-bankovni-aplikace/

European Banking Authority (2024). *EBA at a glance*. Dostupné 12. 1. 2024 z https://www.eba.europa.eu/eba-glance-1

European Commission (2024a). *Single resolution mechanism*. Dostupné 12. 1. 2024 z https://finance.ec.europa.eu/banking/banking-union/single-resolution-mechanism_en

European Commission (2024b). *What is personal data?* Dostupné 23. 1. 2024 z https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en

European Central Bank (2024a). *Banking union.* Dostupné 12. 1. 2024 z https://www.bankingsupervision.europa.eu/about/bankingunion/html/index.en.html

European Central Bank (2024b). *Single Supervisory Mechanism*. Dostupné 12. 1. 2024 z https://www.bankingsupervision.europa.eu/about/html/index.en.html

Financial Crime Academy (2023). *The Three Stages of Money Laundering and How Money Laundering Works.* Dostupné 23. 1. 2024 z https://financialcrimeacademy.org/the-three-stages-of-money-laundering/

FI (2024). *About FI.* Dostupné 19. 1. 2024 z https://www.fi.se/en/about-fi/

FIN-FSA (2024). *About FIN-FSA*. Dostupné 19. 1. 2024 z https://www.finanssivalvonta.fi/en/about-the-fin-fsa/

Hejduk, M. (2020). Počítačová mravnostní kriminalita – kybergrooming. *Bezpečnostní teorie a praxe*, *2020*(1), 57-83.

Chvalkovská, P. (2021). *Co je to vhishing. Další cesta, jak na vás vyzrát.* Kybez.cz https://kybez.cz/co-je-to-vishing-dalsi-cesta-jak-na-vas-vyzrat/

IBM (2024) *Basel I summary.* Dostupné 17. 1. 2024 z https://www.ibm.com/docs/en/bfmdw/8.10?topic=accord-basel-i-summary

Komerční banka (2024). *Jak chránit platební kartu.* Dostupné 29. 1. 2024 z https://www.kb.cz/cs/podpora/bezpecnost/vase-platebni-karta

Kopecký, K. (2022). *Smishing čili phishing realizovaný prostřednictvím SMS opět řádí.* E-Bezpečí. https://e-bezpeci.cz/journal/pdf.php?article=2625&

Kybertest (2024a). *Podvodné e-maily – phishing*. Dostupné 28. 1. 2024 z https://www.kybertest.cz/nejcastejsi-typy-podvodu/phishing-podvodne-e-maily

Kybertest (2024b). *Podvodné SMS (tzv. smishing)*. Dostupné 28. 1. 2024 z https://www.kybertest.cz/nejcastejsi-typy-podvodu/smsishing-podvodne-sms-zpravy

Kybertest (2024c). *Nejčastější typy podvodů*. Dostupné 28. 1. 2024 z https://www.kybertest.cz/nejcastejsi-typy-podvodu/smsishing-podvodne-sms-zpravy

Kybertest (2024d). *Buďte na internetu v bezpečí*. Dostupné 28. 1. 2024 z https://www.kybertest.cz

Microsoft (2022). *Microsoft Digital Defense Report 2022.* Dostupné 27. 3. 2024 z https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022

Ministerstvo vnitra ČR (2022). *Kybernetická kriminalita.* Dostupné 10. 2. 2024 z https://www.youtube.com/watch?v=4_dFiDX4vpQ

Ministerstvo vnitra ČR (2023). *Na nebezpečí kryberkriminality upozorní Den bezpečnějšího internetu.* Dostupné 24. 1. 2204 z https://www.mvcr.cz/clanek/na-nebezpeci-kyberkriminality-upozorni-den-bezpecnejsiho-internetu.aspx

NBS (2024). *Dohľad nad finančným trhom.* Dostupné 19. 1. 2024 z https://nbs.sk/dohlad-nad-financnym-trhom/

PilsFree (2023). *Co je to deepfake a jak ho poznat.* Dostupné 26. 1. 2024 z https://www.pilsfree.net/novinky/272-co-je-to-deepfake-a-jak-ho-poznat

Policie ČR (2021). *Vishing a spoofing.* Dostupné 29. 1. 2024 z https://www.policie.cz/clanek/vishing-a-spoofing.aspx

Policie ČR (2022). *#nePINdej!* Dostupné 28. 1. 2024 z https://www.policie.cz/clanek/nepindej.aspx

Policie ČR (2023). *Pozor na „Nigerijské dopisy“.* Dostupné 29. 1. 2024 z https://www.policie.cz/clanek/pozor-na-nigerijske-dopisy.aspx

Policie ČR (2024a). *Kyberkriminalita.* Dostupné 23. 1. 2024 z https://www.policie.cz/clanek/kyberkriminalita.aspx

Policie ČR (2024b). *Statistické přehledy kriminality*. Dostupné 24. 3. 2024 z https://www.policie.cz/statistiky-kriminalita.aspx

Prevence kriminality v České republice (2023). *Jak být v bezpečí před podvody na internetu v každém věku.* Dostupné 30. 1. 2024 z https://prevencekriminality.cz/jak-byt-v-bezpeci-pred-podvody-na-internetu-v-kazdem-veku/

ProComputing (2023). *Jak nenaletět na metody zvane vhishing či spoofing*. Dostupné 24. 1. 2024 z https://procomputing.cz/jak-nenaletet-na-metody-zvane-vishing-ci-spoofing/

PwC (2022). *Global Economic Crime and Fraud Survey* 2022. Dostupné 20. 1. 2024 z https://www.pwc.com/gx/en/forensics/gecsm-2022/PwC-Global-Economic-Crime-and-Fraud-Survey-2022.pdf

Syrovátková, J. (2023a). *Základy finančních dovedností pro nefinančníky.* Technická univerzita v Liberci. Dostupné 27. 9. 2023 z https://turbo.cdv.tul.cz/mod/book/view.php?id=5979&chapterid=6360

Syrovátková, J. (2023b). *Základy finančních dovedností pro pro nefinančníky.* Technická univerzita v Liberci. Dostupné 27. 9. 2023 https://turbo.cdv.tul.cz/mod/book/view.php?id=5979&chapterid=6364

Zákony

Nařízení Evropského parlamentu a Rady (EU) č. 575/2013 o obezřetnostních požadavcích na úvěrové instituce a investiční podniky

Směrnice 2013/36/EU (CRD IV) Evropského parlamentu a Rady o přístupu k činnosti úvěrových institucí a o obezřetnostním dohledu nad úvěrovými institucemi a investičními podniky

Směrnice EU 91/208EHS o předcházení zneužití finančního systému k praní peněz

Vyhláška č. 55/2023 Sb., o předkládaní výkazů bankami a pobočkami zahraničních bank České národní bance

Vyhláška č. 399/2021 Sb., o úvěrových ukazatelích

Zákon č. 21/1992 Sb., o bankách

Zákon č. 6/1993 Sb., o České národní bance

Zákon č. 96/1993 Sb., o stavebním spoření

Zákon č. 87/1995 Sb., o spořitelních a úvěrních družstvech

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

Trestní zákoník č. 40/2009 Sb.

Seznam tabulek

Seznam obrázků

Abstrakt

Němcová, J. (2024). *Bankovní podvody* [Diplomová práce, Západočeská univerzita v Plzni].

Klíčová slova: banky, podvody, kybernetické podvody, kybernetická kriminalita, bezpečnost

Diplomová práce je zaměřena na bankovní podvody a klade si za cíl tuto problematiku komplexně zpracovat. Práce je rozdělena na teoretickou a praktickou část. V teoretické části jsou nejprve vymezeny základní pojmy v bankovnictví, druhy bank a jejich úloha. Poté je objasněna problematika bankovní regulace, dohledu a rizik v bankovním sektoru. Dále jsou v práci podrobně popsány bankovní podvody, které jsou členěny na interní a externí podvody. Zvláštní pozornost je zaměřena na aktuální kybernetické podvody. Praktická část práce je věnována rozboru kyberkriminality a kybernetických podvodů v České republice. Je zde využito sekundárních dat poskytnutých Policií ČR a Českou spořitelnou a průzkumu České bankovní asociace.

Abstract

Němcová J. (2022). *Banking frauds* [Master's Thesis, University of West Bohemia].

Key words: banks, fraud, cyber fraud, cybercrime, security

This thesis is focused on bank fraud and aims to provide a comprehensive overview of this issue. The thesis is divided into theoretical and practical parts. In the theoretical part the basic concepts in banking, types of banks and their role are first defined. Then the issues of banking regulation, supervision and risks in the banking sector are explained. Next, the thesis describes in detail bank fraud, which is divided into internal and external fraud. Particular attention is focused on current cyber frauds. The practical part of the thesis is devoted to the analysis of cybercrime and cyber fraud in the Czech Republic. It uses secondary data provided by the Police of the Czech Republic and Česká spořitelna and a survey of the Czech Banking Association.