

Kybernetická bezpečnost bankovního subjektu

Bc. Klára Chaloupková

Diplomová práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně

Fakulta logistiky a krizového řízení

Ústav ochrany obyvatelstva

Akademický rok: 2024/2025

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Bc. Klára Chaloupková
Osobní číslo:	L23036
Studijní program:	N1032A020002 Bezpečnost společnosti
Specializace:	Ochrana obyvatelstva
Forma studia:	Kombinovaná
Téma práce:	Kybernetická bezpečnost bankovního subjektu

Zásady pro vypracování

- Proveďte rešerši týkající se kybernetické bezpečnosti v bankovním sektoru.
- Definujte právní rámec kybernetické bezpečnosti pro bankovní instituce v České republice.
- Posudte současný stav kybernetické bezpečnosti ve vybraném bankovním subjektu.
- Navrhněte doporučení pro zlepšení současného stavu kybernetické bezpečnosti v tomto subjektu.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. CELE, Natile Nonhlanhla a KWENDA, Sheila. Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. Online. *Journal of Financial Crime*, 2024. 2024-12-30. ISSN 1359-0790. Dostupné z: <https://doi.org/10.1108/JFC-10-2023-0263>.
2. KOLOUCH, Jan. *CyberCrime*. Praha: Edice CZ.NIC, 2017. ISBN 978-80-88168-16-4.
3. KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. Praha: Edice CZ.NIC, 2019. ISBN 978-80-88168-31-7.
4. PORADA, Viktor a RAIS, Karel. *Právní, kriminalistické a kybernetické aspekty kybernetické kriminality a bezpečnosti: pocta Vladimíru Smejkalovi*. Brno: Akademické nakladatelství CERM, 2021. ISBN 978-80-7623-065-1.
5. ROHMEYER, Paul a BAYUK, Jennifer L. *Financial Cybersecurity Risk Management: Leadership Perspectives and Guidance for Systems and Institutions*. New York: Apress, 2018. ISBN 987-1-4842-4193-6.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání diplomové práce: **2. prosince 2024**
Termín odevzdání diplomové práce: **25. dubna 2025**

L.S.

prof. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2024

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že

- odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení diplomové práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – diplomovou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na diplomové práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne 25. dubna 2025

.....
podpis autora

ABSTRAKT

Tato diplomová práce se zabývá problematikou kybernetické bezpečnosti ve vybraném bankovním subjektu, který čelí rostoucím kybernetickým hrozbám. Teoretická část se věnuje charakteristice kybernetických útoků a právnímu rámci v bankovníctví, který upravuje bezpečnostní požadavky v tomto sektoru. Praktická část vychází z rozhovorů a analýzy dat konkrétní banky, což umožňuje detailní pohled na současný stav zabezpečení. Výsledkem práce je návrh segmentovaného komunikačního přístupu ke klientům.

Klíčová slova: bankovní sektor, DORA, kyberkriminalita, kybernetická bezpečnost, phishing, podvody

ABSTRACT

This diploma thesis focuses on the issue of cybersecurity in a selected banking institution, which faces increasing cyber threats. The theoretical part addresses the characteristics of cyberattacks and the legal framework in banking that governs security requirements in this sector. The practical part is based on interviews and data analysis from a specific bank, providing a detailed view of the current security status. The outcome of the thesis is the proposal of a segmented communication approach to clients.

Keywords: cybersecurity, cybercrime, DORA, fraud, banking sector, phishing

Poděkování

Ráda bych poděkovala všem, kteří mi pomohli při psaní této diplomové práce. Děkuji svému vedoucímu, Ing. Petru Svobodovi, Ph.D., za odborné vedení, trpělivost a cenné rady během celého procesu. Dále děkuji svým kolegům – Ing. Blance Šperlingové, Ing. Barboře Kunzové, Ph.D., a Bc. Marku Macháčkovi, kteří mi významně pomohli konzultacemi a shromažďováním podkladů pro praktickou část této práce. Velmi si vážím času, který mi věnovali, a jejich ochoty podělit se o své odborné znalosti.

OBSAH

ÚVOD.....	11
CÍLE A METODY ZPRACOVÁNÍ.....	12
I TEORETICKÁ ČÁST	14
1 KYBERNETICKÁ BEZPEČNOST V BANKOVNICTVÍ	15
1.1 BANKY JAKO CÍL KYBERNETICKÝCH ÚTOKŮ.....	16
1.2 MOTIVACE KYBERNETICKÝCH ÚTOČNÍKŮ	18
2 KYBERKRIMINALITA V ČESKÉM BANKOVNÍM SEKTORU	21
2.1 NEJČASTĚJŠÍ KYBERNETICKÉ ÚTOKY NA KLIENTY BANK	21
2.1.1 Další kybernetické útoky na klienty bank	24
2.2 KYBERNETICKÉ ÚTOKY NA BANKOVNÍ INSTITUCE	27
3 ZÁKLADY KYBERNETICKÉ BEZPEČNOSTI V BANKÁCH.....	29
3.1 TRIÁDA CIA A JEJÍ VÝZNAM V BANKOVNICTVÍ	30
3.2 MECHANISMY ŘÍZENÍ KYBERNETICKÝCH RIZIK V BANKOVNICTVÍ.....	31
4 PRÁVNÍ RÁMEC KYBERNETICKÉ BEZPEČNOSTI V ČESKÉM BANKOVNICTVÍ.....	34
4.1 SYSTÉM REGULACE FINANČNÍHO TRHU V EVROPSKÉ UNII.....	34
4.2 ZÁKON O KYBERNETICKÉ BEZPEČNOSTI	37
4.2.1 Nový zákon o kybernetické bezpečnosti	39
4.3 ZÁKON O BANKÁCH.....	39
4.4 SMĚRNICE NIS A NIS2.....	40
4.5 DIGITAL OPERATIONAL RESILIENCE ACT.....	41
4.6 NAŘÍZENÍ O TRZÍCH S KRYPTOAKTIVY	42
5 SHRUTÍ TEORETICKÝCH VÝCHODISEK	44
II PRAKTICKÁ ČÁST	46
6 CHARAKTERISTIKA VYBRANÉHO BANKOVNÍHO SUBJEKTU	47
6.1 ŘÍZENÍ KYBERNETICKÉ BEZPEČNOSTI BANKOVNÍHO SUBJEKTU	48
6.2 ZAVÁDĚNÍ BEZPEČNOSTNÍCH OPATŘENÍ	49
6.3 IMPLEMENTACE NAŘÍZENÍ DORA	50
7 PREVENCE PLATEBNÍCH PODVODŮ	54
7.1 ANALÝZA PODVODNÝCH TRANSAKCÍ	54
7.2 INVESTIGACE PODEZŘELÝCH PLATEB	58
7.3 PREVENCE PLATEBNÍCH PODVODŮ BANKOVNÍHO SUBJEKTU V PRAXI.....	59
7.4 KOMUNIKACE BANKOVNÍHO SUBJEKTU KE KLIENTŮM	62
8 NÁVRH NA ZLEPŠENÍ SOUČASNÉHO STAVU	65

8.1	METODOLOGIE A VÝSLEDKY VÝZKUMU	65
8.1.1	Zkušenost s kyberpodvody	66
8.1.2	Vnímání informací od banky	67
8.1.3	Preferované způsoby komunikace	67
8.1.4	Postoj ke školení	68
9	APLIKAČNÍ NÁVRH	69
9.1	MODELOVÝ PŘÍPAD 1	70
9.2	MODELOVÝ PŘÍPAD 2	72
9.3	MODELOVÝ PŘÍPAD 3	76
9.4	MODELOVÝ PŘÍPAD 4	78
9.5	MODELOVÝ PŘÍPAD 5	81
10	ZÁVĚREČNÁ DISKUZE	84
	ZÁVĚR	87
	SEZNAM POUŽITÉ LITERATURY A ZDROJŮ	89
	SEZNAM OBRÁZKŮ	96
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	97

ÚVOD

Kybernetická bezpečnost představuje v současné digitální éře jeden z nejzásadnějších pilířů stability finančního sektoru. Bankovní instituce se stávají stále častějším cílem kybernetických útoků, jejichž sofistikovanost i četnost meziročně narůstá. Tato skutečnost klade zvýšené nároky nejen na technické zabezpečení, ale také na prevenci, informovanost klientů a celkovou digitální odolnost bankovních systémů. V roce 2024 evidovala Česká bankovní asociace více než 87 tisíc útoků na klienty bank, přičemž škody přesáhly 1,3 miliardy korun. Tato čísla jen potvrzují, že kybernetická bezpečnost není otázkou technického detailu, ale strategickou nutností. (ČBA, 2025, online)

Téma diplomové práce bylo zvoleno s ohledem na aktuálnost problematiky i profesní zaměření autorky. Pozornost je zaměřena mimo jiné na oblast prevence podvodných transakcí a komunikaci s klienty – tedy na místa, kde i přes vysokou úroveň technického zabezpečení často přetrvávají slabiny spojené s tzv. lidským faktorem. Právě klienti bank dnes představují jeden z nejzranitelnějších článků bezpečnostního řetězce. Útočníci stále častěji využívají techniky sociálního inženýrství, manipulace a falešné identity, přičemž cílem útoků nejsou systémy samotné, ale konkrétní uživatelé.

Práce propojuje teoretické základy kybernetické bezpečnosti s praktickými příklady implementace regulací a bezpečnostních opatření v bankovním prostředí. Zkoumá, jakým způsobem banky a regulační orgány reagují na dynamicky se měnící hrozby a legislativní rámec, a která opatření se v praxi ukazují jako nejúčinnější při ochraně klientů. Součástí je rovněž analýza současné úrovně komunikace mezi bankou a klientem a hledání možností jejího zefektivnění s cílem zvýšit informovanost a odolnost vůči manipulativním technikám. Na základě poznatků z výzkumu je navržen model segmentovaného komunikačního přístupu, který může sloužit jako inspirace pro další rozvoj osvěty v oblasti kybernetické bezpečnosti v bankovním prostředí.

CÍLE A METODY ZPRACOVÁNÍ

Hlavní cíl: Hlavním cílem této diplomové práce je analyzovat současný stav kybernetické bezpečnosti ve vybraném bankovním subjektu, se zaměřením na způsoby, jimiž tato banka chrání své klienty před kybernetickými hrozbami.

Dílčí cíle práce:

- Analyzovat právní rámec a regulace týkající se kybernetické bezpečnosti, včetně aktuálních předpisů jako je nařízení DORA (Digital Operational Resilience Act).
- Zkoumat souvislosti mezi těmito regulacemi a mechanismy prevence a reakce na kybernetické hrozby v bankovním sektoru.
- Analyzovat nejčastější a nové typy kybernetických podvodů, zejména v oblasti sociálního inženýrství, které jsou častým cílem bank a jejich klientů.
- Zjistit, jak konkrétní banka implementuje nové regulace a jak chrání své klienty před kybernetickými hrozbami.
- Provést analýzu vybraných bezpečnostních opatření zavedených bankovní institucí.
- Popsat, jak banka prakticky reaguje na různé typy kybernetických útoků a podvodů.
- Navrhnout konkrétní opatření na zlepšení komunikace o kybernetických hrozbách mezi bankou a klienty.

V kontextu vytyčených cílů práce odpovídá na následující výzkumné otázky:

- Jaké jsou nejčastější formy kybernetických útoků na bankovní subjekty a jejich klienty?
- Jakým způsobem banky v současnosti řeší problematiku prevence a reakce na kybernetické hrozby?
- Jak efektivní jsou komunikační kanály banky z pohledu osvěty klientů?
- Jak lze zvýšit odolnost banky proti kybernetickým útokům prostřednictvím segmentace komunikačních přístupů pro různé typy klientů?

Metody zpracování: Teoretická část vychází z **literární rešerše**, která se zaměřuje na analýzu stávajících regulací, kybernetických hrozeb a jejich vývoje. Dále se soustředí na bezpečnostní opatření, která banky používají k ochraně jak své infrastruktury, tak svých klientů. Praktická část práce zahrnuje:

- **Polostrukturované rozhovory** s odborníky na kybernetickou bezpečnost z konkrétní banky, které přinášejí pohled na implementaci regulací, interní ochranná opatření a způsoby komunikace s klienty.
- **Kvantitativní šetření formou ankety** mezi klienty banky, zaměřené na jejich vnímání bezpečnostních opatření a efektivitu bankovní komunikace týkající se kybernetických hrozeb.

Výstup práce: V závěru této diplomové práce je zpracován návrh na zlepšení komunikace o kybernetických hrozbách mezi bankou a klienty. Tento návrh vychází z analýzy získaných aktuálních dat. Jeho cílem je optimalizovat komunikaci tak, aby byla efektivnější a lépe přizpůsobená různým typům klientů. Zvláštní důraz je kladen na prevenci kybernetických podvodů a zlepšení edukace klientů.

I. TEORETICKÁ ČÁST

1 KYBERNETICKÁ BEZPEČNOST V BANKOVNICTVÍ

Abychom mohli porozumět problematice kybernetické bezpečnosti v bankovním sektoru, je potřeba se nejprve seznámit se základní terminologií. Správné chápání nám umožní nejen lépe porozumět rizikům a hrozbám, kterým bankovní subjekty čelí, ale také pochopit, čím jsou tato rizika řízena a mitigována. Bankovní subjekty se pohybují ve specifickém prostředí, kde dochází k intenzivní výměně digitálních, finančních a osobních údajů mezi institucemi, klienty a regulačními orgány. Právě tato data jsou hlavním cílem kybernetických útoků, a proto je důležité znát klíčové pojmy související s kyberbezpečností.

Kyberprostor lze definovat jako neomezené globální virtuální prostředí, ve kterém probíhají digitální interakce mezi lidmi, technologiemi a organizacemi, včetně internetových sítí, cloudových úložišť a bankovních systémů pomocí protokolu TCP/IP, což je základní stavební kámen internetové komunikace. V kontextu bankovníctví se kyberprostor skládá z infrastruktury bank, mobilního a internetového bankovníctví, platebních sítí a databází. Nelze ho však vnímat pouze jako abstraktní prostředí, kde probíhají elektronické transakce, komunikace a uchování dat, protože je vždy vázán na materiální podstatu a lidský faktor, a to hardware a lidi, kteří jej spravují a používají. V bankovním sektoru je tato provázanost obzvláště patrná, protože moderní bankovní služby jsou kompletně závislé na propojení fyzických a digitálních komponent. (Kolouch et al., 2019, s. 36)

Kybernetická bezpečnost je jedním z největších témat poslední doby. Existuje mnoho definic, jakým způsobem tento soubor opatření, procesů, technologií, které chrání informační systémy, jejich integritu, dostupnost a důvěrnost dat, pojmenovat, nicméně zjednodušeně lze říct, že jde o ochranu ICT (Informačních a komunikačních technologií) před kybernetickými útoky a hrozbami, aby byla zachována bezpečnost informací (Vláda ČR, 2021, online). Důležité je si uvědomit, že kyberbezpečnost není jen odpovědností státu, právnických osob nebo IT pracovníků, ale každého z nás. (Kolouch et al., 2019, s. 37).

Kybernetická bezpečnost v bankovním sektoru spočívá v ochraně proti **kybernetickým hrozbám**, mezi které patří ztráta dat, jejich poškození či nežádoucí zpřístupnění, jež může nastat v důsledku softwarových chyb, lidského selhání nebo přírodních katastrof. Mezi speciální kategorii kybernetických hrozeb, kterým se tato

diplomová práce převážně věnuje, patří kybernetické útoky a kyberkriminalita. **Kybernetický útok** je srozumitelně definován jako: „Útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé informace či strategické informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků.“ (Jirásek et al., 2015, s. 71). Je to akce vedená proti konkrétním digitálním systémům s cílem poškodit, narušit nebo kompromitovat jejich fungování. **Kyberkriminalitu** je možné popsat jako jednání, při kterém jsou zneužity ICT za účelem spáchání trestného činu. Kyberkriminalita představuje širokou oblast nelegálních činností, které využívají kyberprostor jako nástroj nebo cíl útoku. Ne každý trestný čin spáchaný v kyberprostoru je klasifikován jako kybernetický útok, například jsou často ICT technologie zneužívány k tomu, aby mohla být nelegální a nemorální činnost páchána efektivněji (vydírání, online obtěžování, šíření nevhodného obsahu apod.). V kontextu bankovního sektoru kyberkriminalitu vnímáme jako kybernetické útoky motivované primárně finančním ziskem, ale i například získání citlivých informací o bankovních strategiích, technologiích či klientech. Nemusí se však pokaždé jednat o trestný čin, ale o jednání, které dnes není postižitelné žádnou právní normou a je při nejmenším nemorální. Pro přesnější klasifikaci rozlišujeme všechny kybernetické hrozby mezi kybernetickou bezpečnostní událostí a kybernetickým bezpečnostním incidentem. **Kybernetická bezpečnostní událost** představuje jakoukoli identifikovatelnou situaci, která může ohrozit bezpečnost bankovního systému, například podezřelý pokus o přístup, anomálii v síťovém provozu nebo kybernetický útok. **Kybernetický bezpečnostní incident** již znamená skutečné narušení bezpečnosti systému nebo dat, jako je únik bankovních údajů klientů nebo například úspěšný kybernetický útok, který dočasně vyřadí online bankovníctví z provozu. Zatímco bezpečnostní události mohou sloužit jako varování, bezpečnostní incidenty vyžadují okamžitou reakci, aby se minimalizovaly škody. (Kolouch et al., 2019, s. 73–83)

1.1 Banky jako cíl kybernetických útoků

V rámci pochopení potřeby kybernetické bezpečnosti v bankovních subjektech je potřeba pochopit, jaká digitální data se v bankách zpracovávají a proč je potřeba je chránit. Bankovní sektor tvoří základní pilíř finančního systému a jeho hlavním cílem je zprostředkování finančních toků mezi subjekty v ekonomice. Banky, jakožto významné instituce finančního sektoru, primárně zajišťují finanční zprostředkování mezi subjekty s přebytkem volných finančních prostředků a těmi, kteří je potřebují k financování svých

aktivit. Banky přijímají vklady od veřejnosti a poskytují úvěry jednotlivcům, podnikům i vládám, čímž podporují hospodářský růst a stabilitu.

Banky však v současné době nejsou jenom prostředníky mezi věřiteli a dlužníky, ale zajišťují řadu funkcí, které jsou zásadní pro fungování moderní ekonomiky. Mezi hlavní úkoly bankovního sektoru patří:

- Zajištění a vypořádání plateb (platební styk): Banky usnadňují bezhotovostní platební styk mezi jednotlivými subjekty, což umožňuje efektivní fungování hospodářství. Tento proces zahrnuje provádění domácích i mezinárodních plateb, spravování platebních karet a poskytování fyzického i online bankovníctví.
- Agregace a disagregace fondů: Banky shromažďují kapitál od jednotlivých vkladatelů a následně ho přerozdělují ve formě úvěrů či investic. Tento proces umožňuje efektivní využití kapitálu a zajišťuje jeho dostupnost pro ekonomické subjekty.
- Transfer fondů: Banky umožňují pohyb kapitálu mezi jednotlivými subjekty v rámci domácího i mezinárodního finančního systému. Tento proces je důležitý pro rozvoj obchodu a investic.
- Zpracování informací: Banky provádí analýzy finanční situace klientů, hodnotí jejich bonitu a poskytují investiční doporučení pro efektivní řízení rizik a rozhodování v oblasti úvěrové politiky. Kromě toho se zpracování informací využívá i pro monitorování transakcí a identifikaci podezřelých operací, které mohou souviset s praním špinavých peněz a financováním terorismu.
- Překonávání nejistoty a řízení rizik: Banky se podílejí na řízení úvěrových, tržních a operačních rizik. Poskytují produkty, jako jsou pojištění, deriváty či různé formy garancí, které pomáhají klientům chránit se před nepředvídatelnými událostmi.
- Překonávání problému principál-agent: Banky zajišťují efektivní dohled nad financovanými projekty a pomáhají řešit informační asymetrii mezi věřiteli a dlužníky. Tento proces umožňuje lepší přerozdělování kapitálu a snižuje riziko neefektivního využití finančních prostředků. (Mejstřík et al., 2014, s. 65–66)

Z výše uvedeného je patrné, že banky zpracovávají velké množství aktiv, které mají hodnotu pro nás, fyzické osoby, organizace i státy. Banky, z logiky své podstaty, vždy byly a jsou atraktivním cílem zločinců. Shromažďují finanční prostředky, citlivé informace

a jejich kolaps může vyvolat vážné ekonomické a společenské problémy. S rozvojem digitalizace bankovníctví, které může být zasazeno do 80. let 20. století, se musí vypořádávat i s problematikou nežádoucích kybernetických jevů, protože se vyvíjejí stejně rychle jako technologie samotné. Implementace moderních digitálních technologií a pokročilých analytických nástrojů umožňuje bankám nejen efektivněji obsluhovat širší spektrum klientů, ale také výrazně snižovat náklady na poskytování služeb. Bankovní služby se staly díky digitalizaci dostupnějšími a pohodlnějšími, ale ruku v ruce s tím se zvýšila rizika spojená s informační bezpečností a ochranou dat (Semenyuta et al., 2023, s. 357). Finanční sektor, jehož součástí banky jsou, je dnes vysoce propojený ekosystém, ve kterém instituce, trhy, poskytovatelé služeb a zákazníci spoléhají na komplexní technologickou infrastrukturu. Vývoj globální ICT architektury ale přináší nejen výhody, ale i výzvy v oblasti řízení rizik. (Rohmeyer et al., 2019, s. 1)

1.2 Motivace kybernetických útočníků

Kybernetické útoky na finanční instituce mají globální charakter a jejich rozsah i sofistikovanost se neustále zvyšuje a reaguje na vývoj digitalizace bankovníctví. Útočníci využívají pokročilé techniky, které se často vyvíjejí z předchozích forem útoků, čímž zvyšují jejich efektivitu a obtížnost detekce. Důležitým prvkem kybernetické ochrany je detailní porozumění současným hrozbám a jejich původcům. Vnímání kybernetických hrozeb je často zkreslené nedostatkem informací o reálných útocích. Zatímco odborníci na kybernetickou bezpečnost si jsou dobře vědomi nebezpečí, veřejnost má k dispozici pouze omezené množství konkrétních a ověřitelných údajů. Tento deficit informací vede k podceňování hodnoty dat a informačních aktiv, čímž se zvyšuje zranitelnost finančních institucí. Kybernetické hrozby mohou mít různé podoby, mohou být výsledkem neúmyslných chyb (např. softwarové chyby, lidská chyba) nebo úmyslných útoků prováděných hackery. Záměrní útočníci, tzv. "adversaries", mohou být motivováni finančním ziskem, průmyslovou špionáží či politickými a ideologickými cíli. (Rohmeyer et al., 2019, s. 2–3)

Kyberzločinci můžou být rozděleni na insidery a outsiders. Insiderem může být zaměstnanec, který má legitimní přístup k systémům, ale tuto důvěru zneužívá k nelegálním aktivitám. Naproti tomu outsideri útočí na organizaci zevnějšku, často bez předchozích znalostí o její vnitřní architektuře. Útoky zevnitř jsou obzvláště nebezpečné, protože zaměstnanci mají přístup k citlivým datům a mohou obejít tradiční

bezpečnostní opatření. Hlavní motivace kybernetických útoků může být rozdělena na tři hlavní kategorie:

- Krádež finančních prostředků: Útoky s cílem získat přímý finanční prospěch jsou v bankovníctví běžné. Útočníci dnes mají možnost využívat sofistikované digitální metody a kombinují různé metody k obejití detekčních systémů.
- Krádež dat: Osobní a finanční údaje klientů mají na trhu vysokou hodnotu, a to nejen na černém trhu. Útočníci mohou data využít k vydírání, prodeji třetím stranám nebo k dalším útokům na jednotlivé klienty. Data mohou být využita také pro získání konkurenční výhody.
- Útoky s cílem narušit provoz bank: Cílené narušení bankovních služeb je používáno jako forma vydírání, politického nátlaku či odplaty. (Rohmeyer et al., 2019, s. 4–12)

Dle motivace může být typologie útočníků rozdělena následovně:

- Black hats: Útočníci s jasným záměrem způsobit škodu nebo finanční ztráty.
- Organizované zločinecké skupiny: Využívají kyberkriminalitu k získání finančního zisku nebo k vydírání.
- Politické a teroristické skupiny: Usilují o destabilizaci protivníků či podkopání důvěry ve finanční sektor či konkrétní instituci.
- Hacktivisté: Útočí z ideologických důvodů, často jako forma protestu proti konkrétním politikám nebo institucím.

Zvláštní skupinu tvoří tzv. greyhats – etičtí hackeři, kteří mohou nelegálně testovat bezpečnost systémů, ale nemají škodlivé úmysly. (Rohmeyer et al., 2019, s. 5)

Ať už je kyberkriminalita motivovaná finančně, politicky nebo ideologicky, představuje stále větší bezpečnostní výzvu, a to nejen kvůli své technické náročnosti, ale především kvůli své organizovanosti, častému nadnárodnímu charakteru a napojení na státní či ideologické struktury. Odhalování i dokazování je obtížné, protože útočníci často pracují skrytě, mění nebo ničí důkazy. Tradiční přístupy trestního práva a vyšetřovacích metod se v tomto kontextu často ukazují jako nedostatečné. Efektivní boj s kyberkriminalitou proto vyžaduje novou organizaci práce bezpečnostních složek, vyšší úroveň odbornosti, moderní technické vybavení, a především důraz na prevenci

a mezinárodní spolupráci. Nutná je nejen harmonizace legislativy, ale také sdílení informací, včasné odhalování hrozeb a osvěta uživatelů v oblasti kybernetické bezpečnosti. (Porada, 2021, s. 116–122)

2 KYBERKRIMINALITA V ČESKÉM BANKOVNÍM SEKTORU

V posledních letech došlo k významnému nárůstu kybernetických útoků a s tím souvisejících finančních škod zaměřených nejen na bankovní sektor v České republice. Celosvětově jsou aktuální škody způsobené kriminalitou odhadovány na 6 miliard dolarů ročně (Cele et al., online, 2024). Podle údajů České bankovní asociace, které jsou uvedené v Tiskové zprávě vydané 29. ledna 2025, došlo v roce 2024 k významnému nárůstu kybernetických útoků na klienty bank. Konkrétně bylo zaznamenáno 87 407 útoků, což představuje meziroční nárůst o 25 %. Celkové škody způsobené těmito útoky dosáhly 1,39 miliardy korun. ČBA také upozorňuje na rostoucí sofistikovanost útoků a potřebu zvýšené ostražitosti ze strany klientů. (ČBA, 2025, online). Situace se nevyhýbá ani jiným segmentům, například telekomunikačním a datovým službám. Společnost T-mobile Czech Republic zaznamenala v roce 2024 30 000 bezpečnostních událostí, což představuje meziroční nárůst o 36 % (Kurzy.cz, 2025, online). Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB, 2025, online) v roce 2024 evidoval celkem 268 kybernetických bezpečnostních incidentů, což je dosud nejvyšší evidovaná hodnota (NÚKIB, 2025, online). Policie České republiky zaznamenala v roce 2024 celkem 18 495 trestných činů spáchaných v kyberprostoru, což představuje 10,7 % celkové registrované kriminality (PČR, 2025, online).

2.1 Nejčastější kybernetické útoky na klienty bank

Je zřejmé, že kybernetické hrozby jsou na vzestupu, a to jak v objemu útoků, tak v jejich sofistikovanosti. ČBA v tiskové zprávě za rok 2024 také zmiňuje, přestože jsou banky v České republice dobře zabezpečené, potřebu ochrany bankovních systémů, protože počet útoků na bankovní servery a infrastrukturu meziročně vrostl o 40 %. Nicméně dále zdůrazňuje, že v roce 2024 bylo v bankovníctví 85 % úspěšných útoků zaměřeno na klienty, což naznačuje, že hlavní slabinou nejsou technologická opatření samotných institucí, ale lidský faktor. Nejčastějšími typy podvodných útoků v roce 2024 byly:

- Phishingové e-maily napodobující oficiální komunikaci banky.
- Podvodné telefonáty vydávající se za bankovní pracovníky.
- Podvodné weby imitující internetové bankovníctví.
- SMS zprávy s falešnými výzvami k přihlášení do bankovního účtu.

ČBA rovněž upozorňuje na trend rostoucího využívání AI k podvodům, přičemž stále více útočníků využívá deepfake videa a hlasové syntézy, aby oklamali oběti a vylákali přístupové údaje. (ČBA, 2025, online)

Předpokladem pro to, aby byly kybernetické útoky úspěšné, je v mnoha případech využití sociálního inženýrství, které nemusí být samo o sobě považováno za kybernetický útok. Je to manipulační technika, která cílí na klamání lidí s cílem získat citlivé informace či přimět oběť k provedení škodlivé akce, což se týká samozřejmě i klientů bank. Útočníci místo složitého prolomení bezpečnostních technických opatření často volí jednodušší cestu, a to využití lidské důvěřivosti, strachu nebo nedostatku informací. Útoky sociálního inženýrství jsou zpravidla vedeny třemi způsoby, které jsou navzájem kombinovány:

1. Sběr veřejně dostupných dat: Útočník například sleduje sociální sítě, aby zjistil, kde oběť pracuje, s kým komunikuje a jaké má zvyky nebo vyhledává ve veřejných registrech, jako je obchodní rejstřík, katastr nemovitostí apod.
2. Fyzický útok: Útočníci mohou získat přístup k citlivým informacím fyzickou přítomností, skimmovacím zařízením nebo manipulací s hardwarem.
3. Psychologický útok: Tento způsob se zaměřuje na psychologii oběti. Útočník se snaží získat důvěru nebo vyvolat paniku, aby oběť byla méně obezřetná. (Kolouch, 2016, s. 186–187)

E-maily napodobující oficiální komunikace banky neboli **phishing**, patří mezi vůbec nejrozšířenější formy kybernetických útoků, které útočníci využívají k získání citlivých údajů o bankovních klientech. Tento typ podvodu spočívá v rozesílání falešných e-mailů, které se vizuálně i obsahově snaží napodobit legitimní komunikaci banky. Cílem útočníků je přesvědčit oběť, aby klikla na škodlivý odkaz, stáhla infikovanou přílohu nebo přímo poskytla přihlašovací údaje ke svému online bankovníctví. Phishingový útok má typicky několik fází, které jsou pečlivě promyšlené a realizované s cílem dosáhnout co nejvyšší úspěšnosti:

1. Plánování útoku: Útočníci nejprve rozhodují, kterou banku nebo finanční instituci budou napodobovat. Následně se zaměřují na shromažďování informací o potenciálních obětech, což zahrnuje získávání e-mailových adres a telefonních čísel klientů.
2. Příprava útoku: Jakmile útočníci mají dostatek informací, připravují podvodné zprávy a webové stránky, které napodobují skutečné stránky bank. Cílem je

vytvořit věrohodnou iluzi oficiální komunikace s využitím prvků, jako je napodobení vizuální identity, domény podobné skutečným webovým stránkám bank apod.

3. Spuštění útoku: V této fázi útočníci rozesílají podvodné e-maily obsahujícími odkazy na falešné stránky. Tato fáze může být doprovázena falešnými SMS zprávami, hovory apod.
4. Krádež dat: Pokud oběť klikne na podvodný odkaz a zadá své přihlašovací údaje či platební informace, útočníci tyto údaje okamžitě zaznamenávají a v této fázi může dojít i k instalaci škodlivého softwaru, který:
 - Zaznamenává stisknuté klávesy – umožňuje útočníkům získat hesla a přihlašovací údaje.
 - Monitoruje aktivitu uživatele – sleduje chování klienta a získává další citlivé informace.
 - Získává přístup k dalším službám – pokud oběť používá stejné heslo pro více služeb, útočníci mohou získat přístup k e-mailovým účtům nebo dalším online platformám.
5. Zneužití získaných údajů: Útočníci využívají získané údaje k nelegálním aktivitám, mezi které patří:
 - Okamžité převody peněz – podvodné transakce na účty útočníků, které se stávají poté téměř nevystopovatelné.
 - Prodej dat na darknetu – odcizené informace jsou nabízeny dalším kyberzločincům.
 - Zneužití údajů pro další útoky – phishing může být pouze první fází většího podvodu.
6. Zakrytí stop: Po úspěšném útoku útočníci často mažou digitální stopy, aby nemohly být bankami blokovány, případně přesměrovávají oběti na skutečné stránky, aby si nevšimly, že zadaly údaje na stránkách falešných. (Wilson, 2016, online)

Podvodný telefonát neboli vishing (voicephishing), označuje telefonický útok, při kterém útočník využívá technik sociálního inženýrství. V kontextu bankovníctví se útočníci vydávají za zaměstnance banky. Cílem je získat od obětí citlivé informace,

jako jsou přihlašovací údaje do internetového nebo mobilního bankovníctví, čísla platebních karet nebo jiné osobní údaje, které mohou být zneužity k finančním podvodům. Současné podvodné telefonáty často využívají technologii VOIP (Voiceover Internet Protocol), která umožňuje uskutečňovat hovory přes internet namísto tradičních telefonních sítí. VOIP má pro útočníky několik výhod, a to je snadné padělání telefonního čísla, nízké náklady na provoz a obtížná vystopovatelnost. (Kolouch, 2016, s. 265)

Mezi další typy kyberkriminality patří **Spear Phishing**, který je jednou z forem phishingu, ale na rozdíl od něj není plošný, ale cílený. Útočník analyzuje konkrétní oběť a vytváří důvěryhodně vypadající zprávy, v kontextu bankovníctví například falešný e-mail od banky. (Kolouch, 2016, s. 264).

Podvodné weby imitující internetové bankovníctví jsou falešné internetové stránky, které napodobují vzhled a funkce legitimních bankovních portálů. Jejich cílem je oklamat uživatele a získat od nich citlivé informace, jako jsou přihlašovací údaje, čísla platebních karet nebo osobní identifikační údaje s nejčastější motivací vylákat finanční prostředky oběti. Tyto stránky často vypadají téměř identicky jako oficiální weby bank, což zvyšuje pravděpodobnost, že nic netušící uživatelé poskytnou své důvěrné informace. Bohužel, tyto údaje zadává klient sám a dobrovolně a útočník se díky získaným údajům může pokusit získat přístupy i k dalším službám, které oběť využívá podobně stejně jako u phishingových útoků. (Kolouch, 2016, s. 266) V březnu roku 2024 sdružení CZ.NICablokovalo hned několik takových domén, které imitovaly internetové bankovníctví českých bankovních institucí, konkrétně domény jako mojeonline-csob.cz, lbfio.cz, csob-klic.cz a lbsfio.cz. (Novinky.cz, 2024, online).

SMS zprávy s falešnými výzvami k přihlášení do bankovního účtu, známé jako **smishing**, představují techniku sociálního inženýrství, při níž útočníci zasílají podvodné SMS zprávy, které se tváří jako oficiální komunikace banky. Cílem je přimět příjemce k prozrazení citlivých údajů, jako jsou přihlašovací údaje do internetového bankovníctví, čísla platebních karet nebo osobní identifikační údaje. Smishing funguje na podobném principu jako phishing a vishing, ale s využitím SMS zpráv. (Kolouch, 2016, s. 266).

2.1.1 Další kybernetické útoky na klienty bank

V předchozí kapitole byly zmíněné nejčastější kybernetické útoky na klienty evidované v českém bankovním sektoru. Nicméně kybernetických hrozeb zaměřených na klienty i systémy bank je celá řada. Z útoků zaměřených na klienty bank je potřeba zmínit

malware, což je obecné označení pro škodlivé softwarové programy, které mají za cíl narušit, poškodit nebo získat neoprávněný přístup k digitálním systémům. Existuje mnoho způsobů, jak se **malware** může šířit. Jedním způsobem jsou přenosná paměťová média, například externí disky, kdy si jejich uživatelé předávají infikované soubory v rámci počítačových sítí, typicky P2P (Peer-to-Peer) sítě, ve kterém jednotlivé uzly (počítače nebo zařízení) komunikují přímo mezi sebou bez potřeby centrálního serveru. Každý účastník sítě zároveň funguje jako klient i server, což znamená, že může sdílet, přijímat i poskytovat data ostatním uživatelům. Jedním z nejčastějších způsobů je Drive-by-download, který funguje tak, že se malware automaticky stáhne a spustí na zařízení uživatele, často při návštěvě infikované webové stránky, otevření škodlivé reklamy nebo stažením souboru skrze P2P. (Kolouch et al., 2016, s. 211)

V bankovníctví se často setkáváme s malwarem zaměřeným na krádež přihlašovacích údajů do online bankovníctví nebo sledování klávesnice uživatele. Malware má celou řadu dalších podob, jejíž název je většinou odvozen od jejich působení. **Adware** zobrazuje klientům bank nevyžádané reklamy a přesměrovává uživatele na podvodné weby napodobující bankovní stránky, čímž zvyšuje riziko phishingu. **Spyware** tajně sleduje aktivitu uživatele a zachytává přihlašovací údaje do online bankovníctví nebo citlivá data klientů. **Viry (Viruses)** se šíří mezi zařízeními a mohou infikovat bankovní či platební systémy, což může vést k výpadkům služeb a únikům dat. **Červi (Worms)** se automaticky šíří přes sítě a mohou paralyzovat bankovní infrastrukturu masivním generováním síťového provozu, což vede k nedostupnosti online bankovníctví. **Trojské koně (Trojan Horses)** se vydávají jako legitimní software a zcizují přihlašovací údaje, upravují transakce nebo instalují další škodlivé programy na klientská zařízení. **Rootkity** umožňují útočníkům získat administrátorský přístup k systémům a skrytě ovládat infikované servery, čímž ohrožují integritu sítí. **Keyloggery**, které byly již zmíněny výše, zaznamenávají stisknuté klávesy s cílem získat přihlašovací údaje, PIN kódy a další citlivé informace klientů. (Sedlák et al., 2021, s. 45; Kolouch et al., 2016, s. 204–210)

Speciálním druhem malware je **ransomware**, který šifruje data oběti a brání ji v řádném používání jeho ICT, nebo ponechá zařízení funkční, ale znepřístupní data oběti. Následně požaduje výkupné za jejich zpřístupnění. Útočníci často požadují platby v kryptoměnách, což ztěžuje jejich zpřístupnění, protože kryptoměna je virtuální měna, která není regulovaná státem ani bankami. (Kolouch et al., 2016, s. 221; Mareš, 2022, s. 221)

Man-in-the-Middle (MitM) útok je další typ útoku, při kterém se neoprávněná třetí strana vloží mezi komunikaci dvou uživatelů, klienta a banky, s cílem sledovat, přesměrovávat nebo manipulovat s přenášenými daty. Útočníkovi to může umožnit zachytit důvěrné informace. Běžné techniky MitM útoků v bankovníctví zahrnují ARP poisoning, kdy útočník propojí svou MAC adresu s legitimní IP adresou banky, čímž dokáže přesměrovat komunikaci a podvrhnout falešné bankovní stránky. Další metodou je ICMP manipulation, která umožňuje útočníkovi měnit směrování síťového provozu a monitorovat citlivá data klientů. DNS spoofing pak využívá falešné IP adresy k přesměrování obětí na podvodné webové stránky, které vypadají jako legitimní bankovní portály, což umožňuje útočníkům získat přístup k účtům klientů. (Vipin et al., 2025, online)

Nejen klienti bank se mohou často setkat se **spamem** neboli nevyžádanou, obvykle hromadnou, poštou. Nemusí se jednat vždy o útok, většina spamů je neškodná a bývá zachycena antispamovým filtrem e-mailových schránek. Nicméně mezi spamy patří neetická propagace produktů nebo služeb (reklamní spam), falešné zprávy, které příjemce vyzývají k šíření dál (hoax), podvodné nabídky, které se snaží vylákat z oběti peníze pod falešnou záminkou (scam). (Šulc, 2018, s. 63)

Botnet patří také mezi největší kybernetické hrozby, protože je kvůli automatizaci a distribuované struktuře obtížně detekovatelný. Je to síť napadených zařízení (zombie počítačů) ovládaných útočníkem přes C&C server. Slouží k DDoS útokům, šíření spamu, těžbě kryptoměn nebo krádeži dat. Komunikace botnetu je často šifrovaná a útočníci využívají rotaci IP adres v DNS či proxy servery, aby se skryli. V bankovníctví může botnet provádět DDoS útoky na bankovní servery, což dočasně znemožní přístup klientům k účtům. Také se používá k hromadnému kradení přihlašovacích údajů, například pomocí již výše zmíněných keyloggerů nebo přesměrováním uživatele na falešné přihlašovací stránky. Bankovní botnety mohou automatizovaně převádět peníze na účty podvodníků, aniž by si oběť hned všimla podezřelé aktivity. (Šulc, 2018, s. 46–49)

Je nutné zdůraznit, že výčet výše popsaných útoků zdaleka není vyčerpávající. Mezi další patří například krádeže identity (identity theft), pharming, sexting, falešné mobilní aplikace, útoky přes QR kódy nebo hybridní podvody, které rovněž představují neméně závažná rizika pro bankovní klienty a další přibývají. Vybraným dalším útokům je v této diplomové práci věnován prostor v konkrétním rámci případových studií.

2.2 Kybernetické útoky na bankovní instituce

Bankovní instituce patří mezi strategicky významné cíle kybernetických útoků. V posledních letech došlo v EU k řadě vážných „úspěšně“ provedených kybernetických útoků, při nichž útočníci narušili digitální infrastrukturu bank. Nejčastějším je DDoS útok. **DDoS**, neboli Distributed Reflected Denial of Services, kdy dochází k zahlcení serverů bank množstvím požadavků z více počítačových systémů, které jsou různě geograficky umístěny a dočasně je tak vyřadí z provozu (Kolouch, 2016, s. 296). Velký známý útok tohoto typu byl v roce 2007, kdy se terčem stalo Estonsko. V tomto případě byly ochromeny webové stránky vládních úřadů i bank. Útoky probíhaly po dobu 22 dní a cílily i na služby jako je online bankovníctví a DNS servery. Šlo především o politicky motivovaný DDoS útok. Tento incident vedl k založení NATO Cooperative Cyber Defence Centre od Excellence v Tallinnu, což je mezinárodní vojenská organizace, která se soustředí na oblast kybernetické obrany. (CCDOE, 2007, online; Wikipedia contributors, 2007, online)

Další příklad DDoS útoku představuje vyděračská kampaň skupiny Armada Collective, která v listopadu 2015 zaútočila na tři řecké banky a požadovala výkupné v bitcoinech. Útoky vyřadily z provozu internetové bankovníctví těchto napadených bank. V současné době se také objevují hacktivistické DDoS útoky spojené v souvislosti s válkou na Ukrajině. Evropský finanční sektor zaznamenal vlnu DDoS útoků od proruské hackerské skupiny NoName057 (16), která v roce 2023 napadla české banky, včetně ČNB. (ENISA, 2025, online; ESET, 2015, online)

Druhou kategorií jsou sofistikované průniky do interních sítí bank neboli **APT** (Advanced Persistent Threat). Jedná se o déle trvající, měsíce až roky, systematický kybernetický útok, který se zaměří na konkrétní ICT napadané instituce s využitím DDoS, malwaru a dalších útoků. Cílem bývá krádež citlivých dat nebo finanční zisk. V Evropě i globálně se jimi nechvalně proslavila skupina Carbanak, která v letech 2013–2015 infiltrovala až stovky finančních institucí ve 30 zemích světa. Tato skupina byla tvořená kyberzločinci převážně z Ruska a Ukrajiny a neútočila na klienty bank, ale přímo na banky samotné. Po prolomení zabezpečení bank dokázala simulovat legitimní operace (např. převody peněz) a odklonit značné sumy na účty útočníků. Na ně navázala skupina Cobalt, která působila podobně v následujících letech a zaměřila se na kompromitaci bankomatových sítí v Evropě. Známa pro útoky tohoto typu je také severokorejská skupina Lazarus (APT38), která pro útoky zneužila systém společnosti pro mezibankovní

finanční komunikaci SWIFT (Society for Worldwide Interbank Financial Telecommunication), která v reakci na to v roce 2016 zavedla přísnější bezpečnostní pravidla. Mezi známé útoky, které mohou narušit kontinuitu bankovních služeb, vyřadit zcela IT infrastrukturu nebo ovládnout bankovní systémy, patří také ransomware nebo jiný destruktivní malware. V evropském kontextu se výrazně projevil wiper malware, který maže data infikovaných ICT, nasazený spíše v rámci státem vedených útoků. Příkladem je útok Not Petya v červnu 2017, který se vydával za ransomware, ale ve skutečnosti nevratně ničil data. Tento útok primárně zasáhl infrastrukturu bank na Ukrajině a způsobil i výpadky Státní spořitelny Ukrajiny Osčadbank (Kolouch et al., 2016, s. 320–321; kaspersky, 2015, online; Wikipedia contributors, 2025, online)

Kybernetická bezpečnost se neustále vyvíjí, a každý velký útok vyvolá odezvu jak samotných institucí, tak regulačních orgánů. Dle analýzy Agentury Evropské unie pro kybernetickou bezpečnost (ENISA) je posílení v souladu s regulacemi GDPR, NIS a DORA, kterým je věnovaná část této diplomové práce, klíčové pro odolnost finančního sektoru. Kromě legislativy vznikají i specializované iniciativy, jako jsou cyber stress-testy, které mají odhalit slabiny, mezinárodní spolupráce CERT (Computer Emergency Response Team) a CSIRT (Computer Incident Response Team) týmů, pravidelná cyberrange školení nebo etický hacking, což zapadá do systémového i samostatného řízení kybernetických rizik jednotlivých finančních institucí. (ENISA, 2025, online)

3 ZÁKLADY KYBERNETICKÉ BEZPEČNOSTI V BANKÁCH

V digitální době, kdy jsou bankovní subjekty silně závislé na informačních a komunikačních technologiích, se kybernetická bezpečnost stala samozřejmostí pro zajištění stability a důvěry ve finanční sektor. Fungování bankovního sektoru je tradičně založeno na důvěře klientů a investorů, kteří očekávají, že jejich finanční prostředky a osobní údaje budou v bezpečí. Důležitost kybernetické bezpečnosti v bankovníctví potvrzuje i Evropská unie (EU), která definuje kybernetickou bezpečnost jako činnost nezbytnou k ochraně sítí a informačních systémů před kybernetickými hrozbami (EU, 2022, online).

Kybernetická bezpečnost musí být zajištěna jak v kyberprostoru, tak v reálném světě, neboť základními prvky jsou procesy, technologie a lidé. Je důležité identifikovat a hodnotit kombinace aktiv, zranitelností a hrozeb, aby bylo možné efektivně řídit rizika a chránit informace a systémy. V kontextu kybernetické bezpečnosti v bankovníctví se jedná o tyto prvky:

- **Aktivum (Asset):** Jedná se o vše, co má pro banku, klienta nebo společnost hodnotu, banka to má ve správě a musí to odpovídajícím způsobem chránit. Jedná se o fyzická zařízení, data, procesy, ale i o reputaci dané instituce.
- **Zranitelnost (Vulnerability):** Představuje slabé místo nebo nedostatek v systému, který může být zneužit hrozbou. Může se jednat o technické nedostatky, jako je neaktuální software, nebo organizační slabiny, například nedostatečné bezpečnostní metodiky.
- **Riziko (Risk):** Je kombinací pravděpodobnosti, že hrozba využije zranitelnost aktiva, a dopadu, který by ovlivnil důvěrnost, integritu nebo dostupnost informací. (Kolouch et al., 2019, s. 68–72)

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti definuje řízení rizik, jako činnost zahrnující hodnocení rizik, výběr a zavedení opatření ke zvládnutí rizik, sdílení informací o riziku a sledování a přezkoumávání rizik. V rámci tohoto zákona jsou banky povinny stanovit metodiku pro hodnocení rizik, včetně stanovení kritérií pro akceptovatelnost rizik, identifikovat relevantní hrozby a zranitelnosti s ohledem na aktiva a dle stanovených intervalů pravidelně provádět hodnocení rizik. (Česko, 2018; Kolouch et al., 2019, s. 259)

3.1 Triáda CIA a její význam v bankovníctví

Nejznámější a základní model kybernetické bezpečnosti je triáda CIA, která popisuje tři aspekty ochrany dat: Confidentiality (důvěrnost), Integrity (integritu) a Availability (dostupnost). Tento rámec je využíván v oblastech IT bezpečnosti, včetně bankovníctví, kde je zajištění ochrany citlivých finančních a osobních údajů klíčovým faktorem pro důvěru zákazníků i dodržování regulatorních požadavků. (Cochran, 2024, s. 17).

Důvěrnost dat v bankovním sektoru znamená, že citlivé informace, jako jsou údaje o bankovních účtech, osobní identifikační údaje nebo transakční historie, jsou přístupné pouze oprávněným osobám a systémům. Banky k dosažení důvěrnosti používají:

- Šifrování: Transakce a citlivé údaje jsou šifrovány pomocí protokolů jako TLS/SSL s cílem znemožnit jejich přečtení neoprávněným osobám.
- Přístupové kontroly: Banky používají vícefaktorovou autentizaci (MFA), biometrické prvky nebo chytré karty k omezení neoprávněného přístupu.
- Klasifikaci dat: Různé úrovně citlivosti dat určují, kdo a jakým způsobem k nim může přistupovat. (Cochran, 2024, s. 18-19)

Integrita dat zajišťuje, že informace nejsou neoprávněně změněny nebo manipulovány během přenosu či uložení. To je důležité například pro finanční transakce, kde i malá změna může vést k podvodům nebo finančním ztrátám. V současném bankovním sektoru to představují například tato zabezpečení:

- Hashovací funkce: Bankovní systémy využívají kryptografické hashe (SHA) k ověřování integrity transakcí.
- Digitální podpisy: Elektronické transakce v bankovníctví jsou podepsány digitálními certifikáty, aby bylo možné ověřit jejich pravost.
- Řízení verzí: Banky zaznamenávají změny v databázích, aby bylo možné zpětně ověřit správnost údajů. (Cohran, 2024, s. 20–21)

Dostupnost dat zajišťuje, že bankovní systémy a služby jsou neustále k dispozici pro klienty i pro zaměstnance. Banky implementují řadu opatření k prevenci výpadků a zajištění kontinuity provozu:

- Redundance a zálohy: Bankovní servery jsou rozmístěny v několika datových centrech s automatickým přepínáním v případě selhání.

- Řízení dostupnosti (SLA): Banky stanovují minimální úroveň dostupnosti služeb ve svých smlouvách s dodavateli služeb.
- Řízení provozuschopnosti: Nepřetržité monitorování serverů, automatické procesy obnovy a rychlé zásahy zodpovědných týmů v případě detekovaných problémů, banky zabezpečují k tomu, aby zajistily, že systémy a zdroje banky zůstanou nepřetržitě funkční a dostupné. (Cochran, 2024, 22-23)

Dle vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti je stanovena povinnost hodnotit aktiva v kontextu kybernetických rizik a přijímat opatření k jejich ochraně. Je zde také obsažena stupnice pro hodnocení důvěrnosti, integrity a dostupnosti. (Česko, 2018)

3.2 Mechanismy řízení kybernetických rizik v bankovníctví

Pro finanční sektor má integrita, dostupnost a důvěrnost dat klíčový význam pro stabilitu a důvěru zákazníků. Žádné ICT prostředí není zcela imunní, proto je potřeba neustále monitorovat hrozby a umět na ně reagovat. Efektivní řízení kybernetických rizik musí být integrální součástí strategického a vrcholového řízení banky, protože dozorčí rady a představenstvo nesou odpovědnost za stanovení kybernetické strategie. Moderní řízení kybernetických rizik v bankách vychází z několika základních principů, které zahrnují standardizované přístupy jako je Enterprise Risk Management (ERM) a COSO ERM Framework. Tyto rámce poskytují metodiku pro integrované řízení rizik napříč celou organizací a podporují strategické plánování v oblasti bezpečnosti. (ECB, online, 2024)

Je potřeba stanovení tolerance rizik a jejich akceptovatelné úrovně neboli definování **Cybersecurity Risk Appetite**. Interně musí být definované metodické předpisy a pravidla, **cybersecurity policy**, která stanovují odpovědnosti při řízení kybernetických hrozeb a implementují tři základní linie obrany: První linie, které jsou součástí provozní útvarů, jsou odpovědné za denní řízení rizik. Druhá linie, která zahrnuje nezávislé řízení a compliance. Třetí linie, což je interní nezávislý audit, který hodnotí účinnost opatření.

Banky musí neustále aktivně vyhodnocovat a kategorizovat kybernetická rizika podle jejich potenciálního dopadu na obchodní model. Pro identifikaci a hodnocení rizik jsou používané metodiky zahrnující **NIST Cybersecurity Framework**, který strukturuje bezpečnostní opatření do pěti oblastí: identifikace, ochrana, detekce, reakce a obnova. Účinná preventivní ochrana vyžaduje nepřetržitý monitoring sítě a systémů, což vyžaduje potřebu pokročilých analytických nástrojů, jako je **Security Information and Event**

Management (SIEM) systém pro včasné odhalování bezpečnostních událostí. Zavádí se také **Incident Response Plány (IRP)** pro rychlou reakci k řízení a mitigaci incidentů. Tyto mechanismy jsou určeny zejména pro incidenty spojené s únikem dat klientů, které mohou mít právní důsledky podle nařízení GDPR, či pro technické incidenty, jako jsou DDoS útoky, způsobující finanční ztráty a narušení služeb. Kroky efektivního řízení incidentů zahrnují detekci (identifikace podezřelých aktivit prostřednictvím SIEM a dalších bezpečnostních systémů), reakci (izolace kompromitovaných systémů a minimalizace dopadu), forenzní analýzu (vytváření incidentu s cílem zjistit příčinu a rozsah škod), obnovu (návrat k normálnímu provozu) a posílení ochranných opatření, aby se podobné incidenty neopakovaly. (Kolouch et al., 2019, s. 85–89)

Součástí řízení incidentů jsou odborníci a specializované týmy, a to nejen v bankovním sektoru. Security Operations Center (SOC) je centrální tým odborníků, který monitoruje kybernetické hrozby a reaguje na incidenty. **CERT** je specializovaný tým, který reaguje na kybernetické incidenty, analyzuje hrozby a poskytuje doporučení pro jejich zmírnění. Národní CERTy existují v mnoha zemích (např. GovCERT.CZ v ČR). **CIRST** funguje obdobně, ale zaměřuje se na konkrétní organizace (např. banky), kde koordinuje reakce na bezpečnostní incidenty, zajišťuje forenzní analýzu a spolupracuje s externími bezpečnostními složkami. (Kolouch et al., 2016, s. 506–516)

Pro ochranu dat a transakcí musí banky zajistit **end-to-end šifrování** finančních transakcí, přísnou kontrolu přístupu k datům a monitorování podezřelých aktivit. Šifrování dat jak při přenosu, tak v úložištích, je dnes nezbytnou praxí, která vyžaduje i právní rámec. Dále také **MFA a biometrii** k zabezpečení přístupu k účtům a jiným poskytovaným službám, jako je kombinace hesla, telefonu, biometrických údajů apod. V EU je od roku 2019 požadováno tzv. silné ověření klienta (Strong Customer Authentication), což výrazně zvyšuje bezpečnost v online bankovníctví a snižuje riziko i v případě úniku hesla. (Tanker, online, 2018; ECB, online, 2018)

Školení a osvěta mezi zaměstnanci, stejně jako zavádění bezpečnostních standardů nebo nových technologií (blockchain, AI apod.) je v EU již standardní součástí řízení rizik bankovních institucí. Důležitá je také spolupráce a sdílení informací. Banky si prostřednictvím specializovaných platforem, jako je Financial Services Information Sharing and Analysis Center (FS-ISAC), vyměňují aktuální varování a indikátory kompromitace, aby mohly rychle aplikovat ochranná opatření. Regulační orgány, jako Bank for International Settlements (BIS), podporují sdílení informací o kybernetických

hrozbách mezi finančními institucemi. Banky by se měly aktivně zapojit do kybernetických cvičení a simulací. Měly by také využívat Threat Intelligence Platformy (TIP) pro analýzu hrozeb a implementovat SWIFT Customer Security Programme (CSP) pro bezpečnost mezinárodních platebních transakcí. (OCC, online, 2022)

4 PRÁVNÍ RÁMEC KYBERNETICKÉ BEZPEČNOSTI V ČESKÉM BANKOVNICTVÍ

Bankovní sektor patří mezi nejvíce regulované odvětví ekonomiky, a to nejen v České republice. Mezi hlavní důvody regulací bankovního sektoru patří informační asymetrie, vysoká zadluženost s nízkým podílem vlastního kapitálu a systémové riziko, které může ohrozit, například při selhání velké banky, stabilitu hospodářství. Hlavními regulačními mechanismy jsou bankovní regulace, které stanovují pravidla pro fungování bank a bankovní dohled, který kontroluje dodržování pravidel a ukládá sankce. V České republice je hlavním regulačním a dohledovým orgánem Česká národní banka (ČNB). Nicméně vzhledem k závazkům České republiky plynoucím z jejího členství v mezinárodních organizacích a faktu, že 90 % aktiv českých bank je v zahraničních rukou, je nezbytná úzká spolupráce ČNB s regulátory domovských států. (Mejstřík et al., 2014, s. 208–217)

Regulace bank se v průběhu let vyvíjí v reakci na změny geopolitického a ekonomického prostředí, zkušenosti z finančních krizí a technologický pokrok. Právě technologický pokrok a stále více používané ICT zvýšily riziko, že se jednotlivci, podniky (vč. bankovních subjektů) a veřejné orgány stávají obětí kybernetických hrozeb. První principy bezpečnosti sítí začaly být formulovány v USA na konci 80 let 20. století. Dnes už je kybernetická bezpečnost a digitální autonomie věcí strategického významu i pro EU a její členské státy. (NKÚ, 2020, online)

4.1 Systém regulace finančního trhu v Evropské unii

České banky jsou součástí komplexního systému regulace a dohledu, který zahrnuje jak národní, tak evropské instituce. ČNB představuje, dle zákona č. 6/1993 Sb., o České národní bance, hlavní regulační autoritu na národní úrovni a vykonává dohled nad bankovním trhem. Nad ní stojí Evropský systém centrálních bank (ESCB) a Evropská centrální banka (ECB), které se podílejí na koordinaci měnové politiky a stability finančního trhu. Důležitou roli hraje také Evropský systém finančního dohledu (ESFS), v němž působí specializované orgány jako Evropský orgán pro bankovnínictví (EBA), Evropský orgán pro cenné papíry a trhy (ESMA) a Evropský orgán pro pojišťovnictví a zaměstnanecké penzijní pojištění (EIOPA), které zajišťují jednotné standardy a regulace v rámci EU. Evropská rada pro systémová rizika (ESRB) pak monitoruje a vydává doporučení ke zmírnění potenciálních hrozeb. Společně tak tyto instituce vytvářejí

víceúrovňovou ochrannou síť nad českým bankovním sektorem, která nejen reguluje tradiční bankovní operace, ale stále více se zaměřuje i na nové výzvy spojené s digitalizací a kybernetickými hrozbami. (ČNB, 2025, online; MFČR, 2012, online)

Regulace finančního trhu se tedy opírá o různé právní prameny, formy regulace a dohledové mechanismy, které by měly pomoci zajistit stabilitu finančního systému, ochranu investorů, spotřebitelů a snižovat systémová rizika. Lze je rozdělit na dva základní prameny: **Hard Law** (závazné) a **Soft Law** (nezávazné). Mezi **Hard Law** patří právní předpisy jako zákony, nařízení a směrnice EU, které jsou přímo aplikovatelné nebo transportované do národního právního řádu. Primární evropské právo obsahuje Smlouvu o fungování Evropské unie, sekundární právo zahrnuje směrnice a nařízení EU, které harmonizují regulaci finančních trhů v členských státech. Český právní řád obsahuje zákony o bankách, kapitálovém trhu či pojišťovnictví, které upravují fungování jednotlivých subjektů na finančním trhu. Jedním z dalších důležitých regulačních nástrojů jsou opatření obecné povahy, které vydává ČNB. Tato opatření mají správní povahu a určují konkrétní pravidla pro finanční instituce, například kapitálové požadavky bank. Opatření obecné povahy nejsou zákonem, ale svou povahou mají obdobné účinky. (Janovec, 2023, s. 3–12)

Níže jsou uvedené aktuální platné hard law pro bankovní subjekty v ČR, které jsou více přiblíženy v následujících kapitolách:

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti: Základní právní rámec pro kybernetickou bezpečnost v ČR.
- Zákon č. 21/1992 Sb., o bankách: Upravuje regulaci bankovních subjektů, včetně jejich povinnosti zajistit bezpečnost informačních systémů a ochranu citlivých dat klientů.
- Směrnice Evropského parlamentu a Rady (EU) 2016/1148 (NIS) a její aktualizace NIS2 (2022/2555/EU): Tato směrnice tvoří základní rámec pro zajištění kybernetické bezpečnosti v EU. Směrnice NIS2 zintenzivňuje požadavky na ochranu sítí a informačních systémů v rámci NIS a rozšiřuje povinnosti, které se vztahují na finanční instituce, včetně bank.
- Nařízení Evropského parlamentu a Rady (EU) 2022/2554 (DORA – Digital Operational Resilience Act): Zavádí jednotná pravidla pro digitální provozní odolnost finančních subjektů, včetně bank.

- Směrnice o platebních službách č. 2015/2366/EU (PSD2 – Payment Services Directive 2): Závazný právní předpis EU upravující oblast platebních služeb na vnitřním trhu EU.
- Nařízení o trzích s kryptoaktivy (MiCA, 2023): Reguluje poskytovatele služeb v oblasti digitálních aktiv a stanovuje bezpečnostní požadavky pro obchodování s kryptoaktivy. Banky, které nabízejí služby spojené s kryptoaktivy, musí splnit nové požadavky na transparentnost a ochranu investorů.
- Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury: Stanovuje pravidla pro určování prvků kritické infrastruktury, do nichž spadají i významné bankovní instituce.

Soft law zahrnuje doporučení a standardy vydávané regulátory, jako je ČNB, Evropský orgán pro bankovníctví (EBA) nebo Evropský orgán pro cenné papíry a trhy (ESMA). Ačkoliv soft law není právně závazné, v praxi má značný regulační účinek a instituce jsou povinny se jím řídit nebo vysvětlit, proč se jím neřídí. Vzhledem k rychle se vyvíjejícímu bankovnímu sektoru mají v současné době soft law a globální bezpečnostní standardy důležitou roli v regulaci bankovních subjektů. Doporučení a standardy vydávané mezinárodními i evropskými institucemi umožňují pružnější reakci na změny trhu než legislativní proces. Mezi významné instituce vydávající soft law patří Basilejský výbor pro bankovní dohled, Mezinárodní organizace komisí pro cenné papíry (IOSCO) či Evropská komise. ČNB se také podílí na tvorbě soft law prostřednictvím výkladových stanovisek a metodických pokynů. (Janovec, 2023, s. 4-5).

Níže jsou uvedené vybrané soft law pro bankovní subjekty v ČR:

- Doporučení České národní banky k řízení kybernetických rizik: ČNB vydává pokyny a doporučení pro banky, které se týkají řízení kybernetických hrozeb, ochrany dat a kontinuity provozu.
- Standardy ISO/IEC 27001 a 27002: Mezinárodní normy pro řízení bezpečnosti informací (ISMS – Information Security Management System), což je přístup zabezpečení informací.
- Pokyny Evropského orgánu pro bankovníctví (EBA) k řízení ICT a bezpečnostních rizik: Definují opatření, která musí banky implementovat k řízení a mitigaci kybernetických rizik.

- Memoranda a spolupráce mezi ČNB a NÚKIB: Společné metodické pokyny a spolupráce mezi ČNB a NÚKIB k posílení kybernetické odolnosti bankovního sektoru.
- Bezpečnostní normy vydané karetními asociacemi Payment Card Industry Data Security Standard (PCI-DSS).

Výše uvedené právní předpisy představují základní a aktuální právní rámec zaměřený primárně na kybernetickou bezpečnost. Zároveň je však třeba si uvědomit, že kybernetická bezpečnost v bankovním sektoru je průřezovým tématem zasahujícím do mnoha dalších oblastí. Proto se na ni vztahuje i řada dalších právních předpisů, směrnic a nařízení na úrovni EU i ČR. Patří sem například obecné nařízení o ochraně osobních údajů (GDPR), směrnice o platebních službách (PSD2), legislativa proti praní špinavých peněz (AML) či právní úprava digitálních služeb a elektronických identit. Tyto normy, přestože se primárně zaměřují na jiné aspekty, zahrnují také důležité požadavky týkající se kybernetické bezpečnosti v bankovním sektoru. Oblast kyberbezpečnosti je navíc velmi dynamická a právní rámec se průběžně aktualizuje tak, aby reagoval na nové hrozby i technologický vývoj.

4.2 Zákon o kybernetické bezpečnosti

V České republice první legislativní krok v oblasti kybernetické bezpečnosti nastal v roce 2000, kdy byl přijat zákon č. 365/2000 Sb. o informačních systémech veřejné správy, který měl za cíl definovat základní pravidla pro bezpečnost státních informačních systémů. Ministerstvem vnitra ČR byla přijata Koncepce boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření. Od té doby začal v ČR vývoj kybernetické bezpečnosti na národní úrovni. V roce 2011 byla Vládou ČR zřízena Rada pro kybernetickou bezpečnost a byla přijata Strategie pro oblast kybernetické bezpečnosti České republiky na období let 2011 až 2015, mimo jiné s cílem vytvoření právního rámce, ze které pak v roce 2014 vzešel důležitý milník pro bankovní instituce v ČR v oblasti kybernetické bezpečnosti. Před rokem 2014 bankovní sektor podléhal z pohledu českého práva obecným právním předpisům a regulatorním opatřením, jako je například zákon č. 21/1992 Sb., o bankách, zákon č. 101/2000 Sb., o ochraně osobních údajů nebo doporučení ČNB, které sice zahrnovaly aspekty informační bezpečnosti a ochrany, ale z pohledu kyberbezpečnosti nebyly dostatečné. (Kolouch, 2019, s. 87–91)

V roce 2014 byl přijat zákon č. 181/2014 Sb., o kybernetické bezpečnosti, což byl první komplexní zákon zaměřený na kybernetickou bezpečnost a vstoupil v platnost 1. ledna 2015. V tomto zákoně jsou ustaveny práva a povinnosti osob a orgánů veřejné moci v oblasti kybernetické bezpečnosti, zapracovány příslušné předpisy EU, například transpozice směrnice NIS. Zákon byl v roce 2017 významně novelizován, byly do něj zakotveny některé funkce Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB), který v tomto roce vznikl, a jeho působnost byla rozšířena na subjekty, jejichž služby jsou podmíněny využíváním sítí elektronických komunikací nebo informačních systémů. Narušení by znamenalo významný dopad na zabezpečení všech společenských nebo ekonomických dat i celý český bankovní sektor. V zákoně jsou také uvedeny zvláštní opatření a povinnosti, kterým podléhají prvky kritické informační struktury (KII) definované dle nařízení vlády č. 422/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. Konkrétní seznam prvků KII není veřejně publikován, ale obecně lze předpokládat, že v něm jsou uvedeny největší banky v ČR s ohledem na jejich význam pro finanční systém země. (Česko, 2017)

Mezi hlavní povinnosti bank z pohledu tohoto zákona patří:

- Zavedení bezpečnostních opatření: Banky musí implementovat odpovídající opatření k zajištění kybernetické bezpečnosti svých ICT. Konkrétní požadavky na tato opatření jsou specifikována vyhláškou č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti.
- Vedení bezpečnostní dokumentace: Banky jsou povinny vést dokumentaci o zavedených bezpečnostních opatřeních.
- Detekce a hlášení kybernetických bezpečnostních incidentů: Banky musí být schopny detekovat kybernetické bezpečnostní incidenty ve svých systémech a bezodkladně je hlásit Národnímu úřadu pro kybernetickou a informační bezpečnost (NÚKIB). Pokud incident významně ovlivní poskytování základní služby, musí o tom informovat NÚKIB.
- Zohlednění bezpečnostních požadavků při výběru dodavatelů: Při výběru partnerů pro informační a komunikační systémy jsou banky povinny brát

v úvahu bezpečnostní požadavky a promítnout je do smluvních podmínek s danými dodavateli.

- Plnění opatření NÚKIB: Banky jsou povinny provádět opatření nařízená NÚKIB, jako jsou varování, reaktivní opatření nebo ochranná opatření, zejména v případě kybernetických bezpečnostních incidentů. (Česko, 2017; EPRAVO.CZ, 2017, online)

4.2.1 Nový zákon o kybernetické bezpečnosti

Předpokládá se, že v polovině roku 2025 vstoupí v platnost nový zákon o kybernetické bezpečnosti, který byl schválen vládou v červenci 2024 a nyní prochází legislativním procesem v Poslanecké sněmovně. Návrh zákona a související vyhlášky připravil NÚKIB. Nový zákon vychází z aktuálně platného zákona č. 181/2014 Sb., o kybernetické bezpečnosti, implementuje zkušenosti, nové poznatky a požadavky evropské směrnice NIS2 do českého právního řádu. Směrnice NIS2 rozšířila okruh regulovaných odvětví a služeb, což znamená, že se nově dotkne minimálně 6 000 českých firem a samozřejmě všech bank a finančních institucí. (NÚKIB, 2025, online)

4.3 Zákon o bankách

Zákon č. 21/1992 Sb., o bankách, stanovuje pravidla pro vznik, činnost a zánik bank v České republice. I když v době jeho přijetí nebyl pojem „kybernetická bezpečnost“ běžně používán, zákon obsahuje ustanovení týkající se bezpečnosti a ochrany dat, jako jsou:

- Banky jsou povinny zavést efektivní systém řízení rizik a vnitřní kontroly, který zahrnuje identifikaci, hodnocení, sledování a řízení rizik spojených s jejich činnostmi, včetně rizik týkajících se informačních systémů a ochrany dat.
- Pracovníci bank a další pověřené osoby jsou vázáni povinností mlčenlivosti o všech informacích týkajících se klientů, které získali v rámci výkonu své profese nebo funkce. Tato povinnost zahrnuje i ochranu osobních údajů klientů před nepovoleným zpřístupněním a zajištění důvěrného zacházení s těmito informacemi.
- Česká národní banka je oprávněna uložit bance opatření k nápravě, pokud zjistí nedostatky v jejím fungování, včetně oblastí týkajících se řízení rizik

a ochrany dat. Tato opatření mohou zahrnovat požadavky na zlepšení systémů vnitřní kontroly a bezpečnosti informací. (Česko, 1992)

4.4 Směrnice NIS a NIS2

Směrnice NIS (Network and Information Security Directive) byla vydána EU s hlavním záměrem dosáhnout vysoké společenské úrovně kybernetické bezpečnosti v členských státech. Tato směrnice se zaměřovala na zajištění bezpečnosti sítí a informačních systémů v odvětvích, která jsou považována za klíčová pro fungování společnosti, jako jsou energetika, doprava, bankovníctví nebo zdravotnictví. Směrnice NIS, která ji nahrazuje, byla přijata v roce 2022 s cílem reagovat na rostoucí kybernetické hrozby a technologický vývoj. Mezi klíčové požadavky směrnice NIS na banky patřila implementace bezpečnostních opatření, oznamovací povinnost závažných incidentů příslušným orgánům a spolupráce s nadnárodními autoritami. Směrnice NIS byla v České republice implementována prostřednictvím novely zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Tato novela stanovila povinnost, nejen bankám, identifikovat kritická aktiva, zavést bezpečnostní opatření a oznamovat kybernetické bezpečnostní incidenty NÚKIB. (Evropský parlament a Rada EU, 2016)

Vzhledem k rychlému vývoji kybernetických hrozeb a potřebě posílit odolnost kritických infrastruktur byla přijata nová směrnice Evropského parlamentu a Rady EU 2022/2555 ze dne 14. prosince 2022, známá jako směrnice NIS2. Tato směrnice rozšiřuje působnost původní směrnice NIS a zavádí přísnější požadavky na kybernetickou bezpečnost. Mezi hlavní změny patří:

- Rozšíření působnosti: Směrnice NIS2 zahrnuje širší spektrum odvětví a typů subjektů, které jsou považovány za kritické, včetně většího počtu finančních institucí.
- Přísnější bezpečnostní požadavky: Subjekty musí zavést pokročilejší bezpečnostní opatření, včetně řízení rizik dodavatelského řetězce a pravidelného hodnocení zranitelností.
- Harmonizace sankcí: Směrnice zavádí jednotný rámec sankcí za nedodržení požadavků, což zajišťuje konzistentní přístup napříč členskými státy.
- Zlepšení spolupráce: Posiluje se spolupráce mezi členskými státy nejen prostřednictvím vytvoření Evropské sítě pro kybernetickou bezpečnost.

Členské státy EU, včetně České republiky, mají povinnost transponovat směrnici NIS2 do svého národního práva do 17. října 2024. V České republice budou nové požadavky směrnice NIS2 zohledněny v rámci nového zákona o kybernetické bezpečnosti, který nabude účinnosti v 2025. Banky budou muset přizpůsobit své bezpečnostní strategie a procesy tak, aby splňovaly tyto nové požadavky, včetně rozšíření bezpečnostních opatření a zlepšení schopnosti reagovat na kybernetické incidenty. (Evropský parlament a Rada EU, 2022)

4.5 Digital Operational Resilience Act

Nařízení Evropského parlamentu a Rady Evropské unie 2022/2554 známé jako Digital Operational Resilience Act (DORA), představuje komplexní rámec zaměřený na posílení digitální provozní odolnosti finančního sektoru v EU. Toto nařízení se netýká státní správy a bylo přijato s cílem zajistit, aby finanční instituce byly schopny odolat, reagovat a zotavit se z různých druhů rizik a hrozeb souvisejících s informačními a komunikačními technologiemi. Nařízení bylo přijato 14. prosince 2022 a vstoupilo v platnost 17. ledna 2023. Bankovní instituce, pojišťovny a investiční společnosti, měly povinnost implementovat požadavky tohoto nařízení do 17. ledna 2025 pod kontrolou ČNB. (ČNB, 2025, online)

Hlavní požadavky tohoto nařízení zahrnují:

- Řízení rizik ICT: Finanční subjekty musí zavést a udržovat robustní rámec pro řízení rizik informačních a komunikačních technologií, který zahrnuje identifikaci, ochranu, detekci, reakci a obnovu.
- Hlášení incidentů: Subjekty jsou povinny oznamovat významné incidenty v oblasti ICT příslušným orgánům, včetně informací o povaze incidentu, jeho dopadu a přijatých opatřeních.
- Testování digitální provozní odolnosti: Pravidelné testování systémů a procesů ICT je vyžadováno k ověření jejich odolnosti vůči kybernetickým hrozbám.
- Řízení rizik třetích stran: Finanční subjekty musí posoudit a monitorovat rizika spojená s využíváním služeb třetích stran v oblasti ICT, včetně zavedení smluvních opatření k zajištění souladu s nařízením.

- Sdílení informací: Podpora sdílení informací o kybernetických hrozbách a zranitelnostech mezi finančními institucemi s cílem zvýšit kolektivní odolnost sektoru.(Evropský parlament a Rada EU, 2022)

4.6 Nařízení o trzích s kryptoaktivy

Dalším, relativně novým, nařízením v oblasti finančních trhů je nařízení Evropského parlamentu a Rady Evropské unie 2023/1114 o trzích kryptoaktiv. Toto nařízení bylo přijato 31. května 2024 a jeho ustanovení se začala postupně uplatňovat od roku 2024. Nařízení Markets in Crypto-Assets Regulation (MiCA) představuje komplexní právní rámec pro kryptoaktiva v EU. Jeho cílem je poskytnout právní jistotu subjektům, které vydávají kryptoaktiva nebo nabízejí s nimi související služby, podpořit technologický rozvoj a zároveň zajistit ochranu investorů a udržení stability finančního systému. (Evropský parlament a Rada EU, 2023)

- Rozsah působnosti: Toto nařízení upravuje pravidla pro emisi, veřejnou nabídku a zařazení kryptoaktiv k obchodování, stejně jako pro poskytování služeb spojených s různými druhy kryptoaktiv.
- Požadavky na vydavatele kryptoaktiv: Nařízení stanovuje požadavky na vydavatele kryptoaktiv, jako je:
 - Musí být právnickou osobou.
 - Jsou povinni zveřejňovat na svých webových stránkách bílou knihu kryptoaktiv a všechna veškerá marketingová sdělení.
 - Jsou zavázáni jednat poctivě, transparentně a profesionálně. Komunikace se současnými i potenciálními investory musí být srozumitelná, spravedlivá a nesmí být zavádějící. Zároveň musí aktivně identifikovat, řídit, předcházet a zveřejňovat případné střety zájmů.
 - Odpovídají za škody, které mohou vzniknout v důsledku nepřesných nebo chybných informací uvedených v bílé knize, a zároveň musí investorům umožnit odstoupit od smlouvy.
 - Požadavky na vydavatele tokenů vázaných na aktiva:
 - Musí mít právní formu a sídlo v některém z členských států EU.

- Jsou povinni získat povolení od příslušného orgánu ve svém domovském státě EU, nebo musí být úvěrovou institucí, která připravila bílou knihu schválenou příslušným národním regulátorem.
- Na požádání držitelů tokenů musejí být kdykoli schopni tyto tokeny zpětně odkoupit za tržní hodnotu krytých aktiv, případně poskytnout samotná aktiva. (Evropský parlament a Rada EU, 2023)

Evropský orgán pro cenné papíry a trhy (ESMA) ve spolupráci s Evropským orgánem pro bankovníctví (EBA) zveřejňuje do jednoho roku od nabytí účinnosti nařízení a následně každý rok zprávu přístupnou veřejnosti, která se věnuje uplatňování příslušné legislativy a aktuálním trendům na trzích s kryptoaktivy. (Evropský parlament a Rada EU, 2023)

V České republice bude za dozor a dodržování nařízení MiCA opět odpovědná Česká národní banka (ČNB). Tato povinnost jí byla přidělena na základě zákona č. 31/2025 Sb., o implementaci předpisů Evropské unie v oblasti digitalizace finančního trhu (zákon o digitalizaci finančního trhu), který zapracovává požadavky tohoto nařízení do českého právního systému. Návrh tohoto zákona byl schválen Poslaneckou sněmovnou 6. prosince 2024 a následně postoupen Senátu. Po jeho schválení Senátem a podpisu prezidenta zákon nabude účinnosti dnem následujícím po jeho vyhlášení ve Sbírce zákonů. Subjekty, které již poskytují služby v oblasti kryptoaktiv na základě živnostenského oprávnění, budou mít povinnost požádat ČNB o povolení k činnosti poskytovatele služeb souvisejících s kryptoaktivy (CASP) do 31. července 2025. Pokud podají žádost včas, mohou pokračovat ve své činnosti až do rozhodnutí o žádosti, nejpozději však do 1. července 2026. (ČNB, 2025, online)

5 SHRNUÍ TEORETICKÝCH VÝCHODISEK

Teoretická východiska této diplomové práce se opírají o českou i zahraniční odbornou literaturu, aktuální právní úpravy a regulatorní rámce kybernetické bezpečnosti, jakož i o dokumenty vydané institucemi působícími v oblasti finanční stability a ochrany informačních systémů. Při rešerši byly využity odborné publikace z akademického prostředí a výstupy České národní banky (ČNB), České bankovní asociace (ČBA), Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB), Evropské unie (EU) a dalších relevantních institucí.

Napříč odbornou literaturou a institucionálními zdroji panuje shoda, že kybernetická bezpečnost je jedním z nejzásadnějších pilířů stability bankovního sektoru. Podle Koloucha (2019) spočívá kybernetická bezpečnost v ochraně informačních systémů a dat před úmyslným či neúmyslným narušením jejich důvěryhodnosti, integrity a dostupnosti. Dle Evropské centrální banky patří digitální rizika dlouhodobě mezi hlavní hrozby ohrožující stabilitu finančního systému EU. Z hlediska praxe pak ČNB potvrzuje, že odolnost vůči kybernetickým hrozbám je důležitou součástí dohledu nad ICT a řízením bank.

Z mnoha zdrojů dále vyplývá, že současným trendem jsou primárně útoky cílené nikoliv přímo na bankovní infrastrukturu, ale na koncové uživatele – klienty. Sociální inženýrství v podobě phishingu, smishingu či vishingu je typickým příkladem hrozby založené na manipulaci s lidským faktorem. Lidská chyba je v oblasti kybernetické bezpečnosti opakovaně označována jako nejzranitelnější článek – a to napříč domácími i evropskými zdroji. Například NÚKIB (2024) ve své Zprávě o stavu kybernetické bezpečnosti v ČR za rok 2023 konstatuje, že „lidský faktor zůstává významným příčinným prvkem většiny incidentů“. Stejně tak ENISA (2024), agentura Evropské unie pro kybernetickou bezpečnost, ve své zprávě z roku 2024 uvádí, že právě lidský faktor je trvalou slabinou a současně výzvou pro organizace v celé EU

Banky se těmto hrozbám brání zaváděním kombinace technologických a procesních opatření. Mezi běžně používaná patří vícefaktorová autentizace, šifrování komunikace, monitoring aktivit nebo zavádění politik přístupu. Současně je kladen důraz na edukaci a informovanost nejen zaměstnanců, ale také klientů. Dle ČNB je součástí účinného řízení rizik i to, jakým způsobem instituce pracují s bezpečnostní kulturou uvnitř banky a jak informují veřejnost o hrozbách.

Rámec kybernetické bezpečnosti je zároveň silně ovlivněn regulatorními požadavky. Směrnice NIS2 (EU 2022/2555) rozšiřuje požadavky na zabezpečení systémů v kritické infrastruktuře včetně bankovního sektoru. Česká republika musela tuto směrnici do svého práva transponovat do října 2024 prostřednictvím nové verze zákona o kybernetické bezpečnosti, který vejde v platnost v polovině roku 2025. Další klíčový předpis, nařízení DORA (EU 2022/2554), vstoupil v účinnost od ledna 2025 a zavádí jednotný rámec digitální provozní odolnosti finančních institucí. Vedle těchto předpisů hraje stále větší roli i regulační rámec týkající se trhu s kryptoaktivy, konkrétně nové nařízení MiCA (EU2023/1114), které vstupuje v platnost v českém prostředí zákonem č. 31/2025 Sb., o implementaci předpisů Evropské unie v oblasti digitalizace finančního trhu.

Z výše uvedených poznatků vyplývá, že kybernetická bezpečnost bank je podmíněna kombinací technologických, legislativních i lidských faktorů. Nejde pouze o ochranu systémů, ale také o strategii, která propojuje technickou připravenost, regulaci a informovanost. Právě na tento komplexní rámec navazuje praktická část diplomové práce, která analyzuje, jak tyto principy uplatňuje konkrétní bankovní instituce v praxi.

II. PRAKTICKÁ ČÁST

6 CHARAKTERISTIKA VYBRANÉHO BANKOVNÍHO SUBJEKTU

Vybraným bankovním subjektem praktické části této diplomové práce je Komerční banka, a. s. (KB), která je dále v práci označována jako „Banka“. Banka je jedním z největších a nejznámějších bankovních subjektů působících na českém kapitálovém trhu. Nabízí služby retailového, podnikového i investičního bankovníctví, ale také další specializované služby. Služby Banky využívá v současné době přes 1,7 milionu klientů.

Banka byla založena 1. ledna 1990 jako samostatná instituce, která vznikla oddělením obchodních aktivit tehdejší Státní banky československé. Tento krok byl součástí širších ekonomických reforem, které vedly k postupné transformaci československého bankovního sektoru. V roce 1992 došlo k transformaci Banky na akciovou společnost, přičemž hlavními akcionáři se staly Fondy národního majetku České a Slovenské republiky a její akcie byly zařazeny do systému kuponové privatizace. O tři roky později, v roce 1995, Banka vstoupila na mezinárodní kapitálové trhy prostřednictvím emise globálních depozitních certifikátů, čímž si zajistila přístup k zahraničním investorům. Na přelomu tisíciletí, v roce 2001, došlo k zásadní změně vlastnické struktury. Mezinárodní finanční skupina Sociétés Générales (dále označována jako „Skupina“) koupila 60% podíl a stala se majoritním vlastníkem, kterým je dodnes. (KB, 2025, online)

Díky příslušnosti k mezinárodní skupině Banka získala silného strategického partnera, který jí umožnil další expanzi a modernizaci služeb. Od roku 2001 Banka postupně začala zavádět inovace v oblasti digitalizace. Ve stejném roce spustila internetové bankovníctví MojeBanka, čímž nabídla klientům možnost spravovat své finance online. S rozvojem digitálních technologií přicházelo zaměření i na kybernetickou bezpečnost. V roce 2015 Banka jako první banka v České republice nabídla svým klientům zdarma bezpečnostní software Trusteer Rapport od IBM, který chránil proti phishingu, malware a keyloggerům. V roce 2018 spustila aplikaci Banka Klíč, což je aplikace pro bezpečnější přihlašování do internetového bankovníctví bez nutnosti zadávat SMS kódy. Tyto změny zvýšily bezpečnost klientů a přispěly k modernizaci uživatelského prostředí. (KB, 2023, online)

V roce 2023 Banka oznámila veřejnosti svou transformaci označovanou jako nová éra bankovníctví. Tento proces je součástí strategie Banka Change 2025, která klade důraz na digitalizaci a zefektivnění bankovních služeb. Jedním z hlavních kroků bylo nasazení

nového moderního core banking systému od společnosti Temenos AG, který poskytuje nepřetržitou dostupnost a modulární architekturu podporující digitalizaci a personalizaci produktů. Další velkou investicí byla výměna karetního systému – nově má Banka platformu pro zpracování platebních karet TSYs Prime v aplikaci společnosti Global Payments Europe. Ta zajišťuje primárně bezpečnost a efektivitu zpracování. (KB, 2023, online)

Další klíčovou součástí této transformace je zavedení inovativní platformy Banka+, která poskytuje klientům přístup k bankovním službám prostřednictvím jednoho intuitivního rozhraní. Tato aplikace umožňuje například digitální správu dokumentů, čímž Banka podporuje nejen bezpečná, ale také ekologická řešení. Modernizací a agilním zaváděním změn Banka nejen zajišťuje komfortní správu financí, ale také ochranu svých klientů před podvodnými aktivitami a digitálními hrozbami. (KB, 2023, online)

6.1 Řízení kybernetické bezpečnosti bankovního subjektu

V roce 2023 schválilo představenstvo Banky strategii kyberbezpečnosti pro roky 2023, 2024 a 2025. Zároveň pokračuje v realizaci programu neustálého zlepšování bezpečnosti „wing to wing“, který byl schválen Evropskou centrální bankou, a zapojila se tak do celoevropské iniciativy zaměřené na zlepšení zabezpečení IT infrastruktur a sjednocení bezpečnostních standardů v rámci celé finanční Skupiny. Zároveň v tomto roce započaly přípravy na implementaci nového nařízení DORA, které přináší zpřísněné požadavky na digitální odolnost finančních subjektů. (KB, 2024, online)

V Bance je kybernetická a informační bezpečnost řízena od nejvyšší úrovně managementu. Za tuto oblast má odpovědnost vrchní ředitel a Chief Digital Officer, který je zároveň členem představenstva. Klíčovým řídicím orgánem je oddělení Security Center of Expertise, jehož úkolem je definovat celkovou strategii kybernetické bezpečnosti, šířit její principy napříč celou institucí, identifikovat a hodnotit bezpečnostní rizika a kontrolovat dosažení požadovaných úrovní ochrany. Banka zároveň prosazuje princip individuální odpovědnosti, kdy se každý zaměstnanec musí řídit zásadami bezpečného chování při práci s interními a klientskými daty. (KB, 2024, online)

Banka se soustředí na začlenění bezpečnostních prvků do všech vývojových a provozních procesů s cílem chránit data, informace o klientech a veškerou komunikaci s nimi před známými a předvídatelnými hrozbami. Přístup Banky vychází ze standardů ISO/IEC 27000, přičemž klíčovými pilíři jsou důvěrnost, integrita, dostupnost

a neodmítnutelnost dat. Využívá k tomu vícevrstvý bezpečnostní model, který kombinuje preventivní i detekční mechanismy. Pravidelně monitoruje uživatelské chování a vyhodnocuje rizika spojená s interními i externími hrozbami. Důraz je kladen také na řízení dodavatelských rizik, kontrolu přístupu k citlivým datům a prevenci jejich úniku. (KB, 2024, online)

6.2 Zavádění bezpečnostních opatření

Jak již bylo uvedeno v předchozí kapitole této práce, Banka průběžně implementuje nové bezpečnostní technologie, regulace a postupy s cílem zvýšit svoji digitální odolnost. Digitální prostředí je pod stálým dohledem operačního centra. Důsledné dodržování jak fyzické, tak digitální bezpečnosti je pravidelně kontrolováno sadou bezpečnostních automatizovaných kontrol různých úrovní. Dle interního benchmarkového hodnocení společnosti BitSight, která se specializuje na hodnocení kybernetické bezpečnosti organizací a poskytuje na základě analýzy objektivní pohled na úroveň zabezpečení, dosahuje Banka již od roku 2020 hodnocení „advanced“. (KB, 2024, online)

V roce 2023 byly v prostředí Banky modernizovány základní bezpečnostní prvky, včetně EDR na serverech s operačním systémem Windows. V oblasti detekce a reakce na kybernetické hrozby došlo ke sjednocení bezpečnostních protokolů v rámci skupiny SG a zavedení standardizované úrovně výstrah v Security Information and Event Management s cílem efektivněji reagovat na nejkritičtější bezpečnostní incidenty. Dále byla zpřísněna kontrola zpracování nejcitlivějších informací, včetně pravidel pro využívání cloudových služeb SaaS. Byly posíleny mechanismy prevence úniku dat DLP (Data Loss Prevention) a zavedeny kontroly v souladu s regulačními požadavky Schrems II, což je označení pro rozhodnutí Soudního dvora Evropské unie upravující přenos osobních údajů mezi EU a USA. (KB, 2024, online; Chander, 2020, s. 771–784)

Důraz byl rovněž kladen na bezpečnost aplikací, kde se uplatňují principy Secure by Design. Secure by Design je princip vývoje softwaru a IT systémů, který zajišťuje, že bezpečnostní opatření jsou integrována do aplikací již od první fáze návrhu a vývoje produktu. Místo toho, aby byla bezpečnost řešena dodatečně jako reakce na objevené zranitelnosti, je pevně zakotvena do samotné architektury systému. Například nová platforma Banka+ využívá vestavěné zabezpečení. Při vývoji této aplikace se dodržují také principy Agile@Scale, což umožňuje rychlé zavádění inovací, lepší spolupráci mezi týmy, ale také efektivní řízení bezpečnostních požadavků. V rámci vývoje aplikace je dodržování

bezpečnostních standardů kontrolováno experty na danou problematiku, kteří jsou přiřazeni k jednotlivým vývojovým týmům. Průběžně identifikované nedostatky a zranitelnosti jsou zaznamenávány v rámci systému řízení rizik informační bezpečnosti. Následně jsou jednotlivé zjištěné problémy ohodnoceny dle své závažnosti a zařazeny dle priorit k odstranění za dohledu managementu (KB, 2024, online).

I přes technologicky pokročilé bezpečnostní systémy představuje jednu z největších výzev v oblasti kybernetické bezpečnosti lidský faktor, neboť útoky mohou být založené na manipulaci zaměstnanců, kteří mohou neúmyslně umožnit přístup útočníkům k citlivým datům nebo bankovním systémům. V Bance je proto kladen také důraz na vzdělávání zaměstnanců a budování silné kybernetické kultury.

6.3 Implementace nařízení DORA

S ohledem na to, že bankovní sektor podléhá celé řadě regulatorních požadavků, je nezbytné, aby i Banka průběžně implementovala nové právní předpisy a přizpůsobovala jim své interní procesy. Jedním z nejvýznamnějších předpisů této oblasti současné doby je nařízení DORA, jehož cílem je zvýšit digitální provozní odolnost finančních institucí v celé EU. Jeho plná účinnost nastává v roce 2025, přičemž všechny finanční instituce v EU se na něj musely v předstihu připravit. Pro účely této diplomové práce byla vybrána implementace právě tohoto nařízení, protože představuje zásadní změnu v přístupu k řízení ICT rizik a kybernetické bezpečnosti ve finančních institucích. Nařízení DORA sjednocuje požadavky na digitální odolnost napříč celým finančním sektorem a klade důraz na prevenci, detekci a zvládání kybernetických incidentů. Jeho uvedení do praxe vyžaduje komplexní přístup zahrnující nejen technologické aspekty, ale i organizační a procesní změny.

Banka, jako součást mezinárodní Skupiny, zahájila přípravy na implementaci tohoto nařízení s dostatečným předstihem. V roce 2023 provedla analýzu existujících bezpečnostních opatření a identifikovala oblasti, které je nutné přizpůsobit novým regulatorním požadavkům. V rámci této analýzy bylo rovněž sladěno řešení této problematiky se skupinovými standardy a vytvořené specializované týmy pro řízení reakce na incidenty a obnovu provozu. Banka si kladla za cíl začlenit procesy digitální odolnosti do standardního řízení kontinuity provozu a postupně zavádět opatření, která budou plně integrována do běžného fungování banky. Přestože Banka disponovala a disponuje rozsáhlým bezpečnostními mechanismy, implementace DORA přinesla výzvy spojené se

sjednocením regulatorních požadavků napříč evropským finančním sektorem. To zahrnuje nejen technologické úpravy a zavedení bezpečnostních kontrol, ale také změny v interních procesech, odpovědnostech jednotlivých týmů a přizpůsobení bezpečnostní politiky banky.

Pro hlubší pochopení tohoto procesu v prostředí Banky byla využita kvalitativní výzkumná metoda ve formě polostrukturovaného rozhovoru s paní Ing. Barborou Kunzovou, Ph.D., která v Bance působí na pozici Digital Transformation Lead a její hlavní odpovědností je úspěšné zavedení regulace DORA a koordinace napříč Skupinou.

- **Profesní role a strategie implementace**

Jaký byl Váš osobní přístup k implementaci DORA v Bance a jaké jste vnímala hlavní výzvy v průběhu tohoto procesu? *Můj osobní přístup byl v tomto případě Learning by doing. Pro všechny z nás, v Bance i na trhu, byla regulace DORA nové téma. Bylo těžké najít na trhu odborníky. Velká část DORA regulace nebyla ještě v lednu 2024 schválena EU. Výzev bylo opravdu mnoho. Mezi největší patřila koordinace celé aktivity napříč Bankou a ve spolupráci se Skupinou. Dále práce s nejistým scopem řešení. Velká část finální dokumentace byla vydána EU až v červenci 2024 a ještě nyní dochází ke změnám. Další velkou výzvou byl rozdílný výklad nařízení mezi odborníky nebo celková komplexita změny.*

Jakým způsobem byla nastavena strategie implementace nařízení DORA? Jaké hlavní fáze implementace zahrnovala? *Implementace řešení byla rozdělena podle kapitol DORA na streamy a každý stream měl svého stream Leadera. Celé řešení jsme rozpadli na tzv. Compliance checklisty a provedli tzv. gap analýzu oproti stávajícímu stavu v Bance. Na základě výstupů gap analýzy jsme si vydefinovali naše MVP k 17. lednu.2025.*

Jak probíhala koordinace implementace mezi Bankou, jejími dceřinými společnostmi a Skupinou? *Koordinace probíhala ve třech rovinách: 1) Koordinace uvnitř Banky – implementační SW změny, metodika, procesní změny. 2) Dceřiné společnosti – metodický support, koordinace a příprava reportů na regulátora. 3) Se Skupinou – implementace požadavků napříč celou skupinou. Harmonizace rozdílných přístupů.*

Na co se v rámci implementace kladl největší důraz – technologická opatření, změny procesů, nebo lidský faktor? *Kladli jsme důraz na vyvážený přístup. Snažili jsme se navrhnout řešení tak, aby bylo udržitelné a stavěli jsme na stávajících řešeních. Důležité pro nás bylo proces dobře nastavit*

V jakých oblastech banky vyžadovala implementace největší změny a jak se s nimi Banka vypořádala? *Změn bylo opravdu mnoho. Největší změny přišly v oblastech: 1) Řízení třetích stran, změny v evidencích a úpravy ICT smluv, tvorba registru informací o smlouvách, reporting na regulátora. 2) Incident management systému – nová metodika pro posuzování kandidátů na DORA major incidenty. Nový DORA komunikační dashboard. 3) Testování digitální provozní odolnosti – vznikala nová metodika na TLPT testování. Bude koordinováno ČNB.*

- **Dopady na provozní a kybernetickou bezpečnost Banky:**

Musela Banka zavádět nové technologie nebo upravovat stávající systémy v reakci na požadavky nařízení DORA? *Banka upravovala stávající systémy. Snažili jsme se záměrně, i z důvodu nákladů, o maximální použití stávajícího řešení a technologií.*

Jak se změnil proces hlášení kybernetických incidentů v důsledku implementace DORA? Jaké nové mechanismy Banka v této oblasti zavedla? *Došlo ke zpřísnění časového intervalu pro reporting na regulátora. Dochází ke sloučení hlášení u některých incidentů na regulátora. Všechny nově nastavené časové tresholdy pro eskalaci a reporting DORA incidentů v Bance kopírují pravidla nařízení DORA. Došlo k úpravě metodik, nastavení rolí a odpovědností.*

Nařízení DORA zavádí také přísnější požadavky na řízení dodavatelů ICT služeb. Jak se změnila spolupráce s externími partnery? *Došlo k úpravě požadavků na smluvní dokumentaci a zároveň došlo k zvýšení požadavků hodnocení rizik dodavatelů a dodávaných služeb.*

- **Interní a externí komunikace**

Jakým způsobem Banka interně komunikovala změny vyplývající z implementace nařízení DORA směrem k zaměstnancům? *Pravidelně jsme informovali zaměstnance prostřednictvím intranetu formou aktualit a zajímavých článků. Vše probíhalo ve spolupráci s naším útvaru Interní komunikace, která nám velmi pomáhala. Co se týká vývojových nebo metodických změn, tak jsme využívali informační kanál v Microsoft Teams.*

Jak probíhalo školení zaměstnanců ohledně nových bezpečnostních opatření? *Pro všechny útvary Banky mimo distribuční síť jsme připravili školení formou e-learningu.*

Jak se změnila externí komunikace Banky směrem ke klientům v oblasti kybernetické bezpečnosti v souvislosti s DORA? *Banka má velmi aktivní kampaně v oblasti kybernetické bezpečnosti směrem ke klientům bez ohledu na DORA. Došlo k úpravám metodik týkající se komunikace, ale přímé změny se klientům nekomunikovali.*

- **Výzvy a přínosy implementace nařízení DORA pro Banku**

Jaké byly největší výzvy při zavádění DORA v Bance a v čem byl tento proces nejnáročnější? *Největší výzvy byli v koordinaci v Bance a v celé Skupině (přes 150 lidí). Dále najít vlastníky procesů poté, co přestane fungovat DORA tým a komunikace se stakeholdery, neustále vysvětlování vyvíjejících se výkladů požadavků.*

Jakým způsobem nařízení přispělo ke zvýšení bezpečnosti a provozní odolnosti banky? *Došlo ke zvýšení kvality informací o dodavatelích a smlouvách. Došlo ke zlepšení procesů a jasné definice odpovědností. Podařilo se nám sjednotit některé přístupy napříč Skupinou. Zvýšilo se zapojení i zapojení managementu a runové (operační) části banky do tématu digitální provozní odolnosti.*

7 PREVENCE PLATEBNÍCH PODVODŮ

Tato práce se také zabývá oblastí prevence platebních podvodů. Rozhodnutí vychází ze skutečnosti, že právě platební podvody představují jednu z nejrozšířenějších a nejvíce dopadajících forem kybernetické kriminality vůči běžným uživatelům finančních služeb. Jejich četnost, sofistikovanost a schopnost přizpůsobovat se měnícím se technologiím i návykům uživatelů z nich činí vážnou výzvu jak pro regulátory, tak pro samotné bankovní instituce.

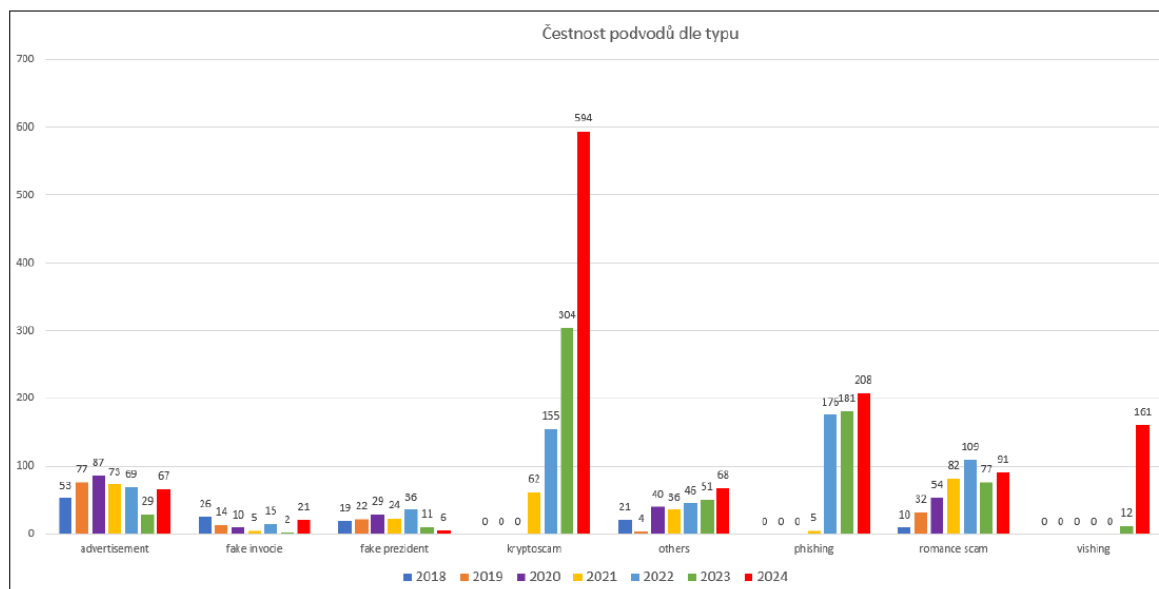
Zatímco legislativa a technologická opatření minimalizují rizika na systémové úrovni, v ochraně klientů hraje důležitou roli prevence, konkrétně včasná a účinná komunikace. Úspěšnost podvodů totiž často závisí na chování a rozhodování jednotlivce, tedy na tom, zda dokáže podvod rozpoznat a adekvátně na něj reagovat. Tato oblast proto vyžaduje specifický přístup, který zohledňuje různé úrovně digitální gramotnosti, zkušenosti a zranitelnosti klientů.

Metodologicky je tato kapitola postavena na analyticko-deskriptivním přístupu. Vychází z dostupných odborných zdrojů, poznatků z praxe bankovního sektoru a případových scénářů, na jejichž základě je popsáno, jak prevence platebních podvodů aktuálně funguje a jaké komunikační nástroje jsou využívány.

7.1 Analýza podvodných transakcí

Jak můžeme vidět na grafu na Obrázku 1 níže, aktuálním trendem mezi Bankou zachycenou kyberkriminalitou jsou kryptopodvody. U kryptopodvodů, kdy útočník láká oběť na rychle dostupný zisk prostřednictvím investic do kryptoměn přes falešné investiční nabídky, Banka zaznamenala největší nárůst pokusů z 0 případů v roce 2018–2020 na 594 případů v roce 2024. Stabilně s vysokým výskytem je phishing, od roku 2018 (176 případů) s mírným růstem v dalších letech, kulminující v roce 2024 na 208 případech. Ukazuje se jako trvale rozšířená forma útoku. Rychlý růst vishingu také naznačuje trend mezi útočníky. Nebyl zachycen vůbec až do roku 2023, kdy bylo zaznamenáno 12 případů, v roce 2024 prudký nárůst na 161 případů. Mezi další časté pokusy o podvody patří romance scam, což je typ podvodu, kdy pachatel naváže s obětí fingovaný milostný vztah prostřednictvím online seznámk, sociálních sítí nebo e-mailu, s jasným cílem opět podvést a získat od ní peníze (Kopp et al, 2016, s. 148). Počet pokusů narostl z 10 případů v roce 2018 na 109 případů v roce 2023, v roce 2024 pak mírně poklesl na 91 případů. Také Advertisement podvody neboli bazarové podvody, se

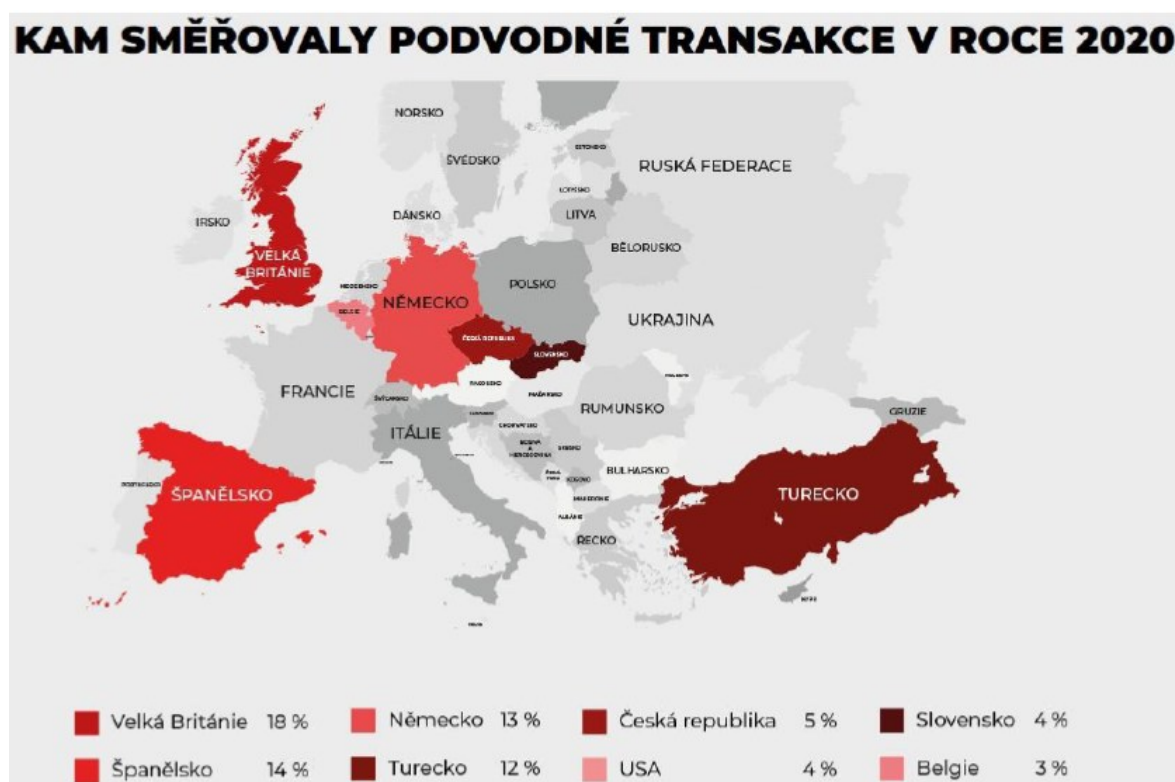
vyskytují poměrně stabilně mezi 53–87 případy v letech 2018–2023, v roce mírně 2024 poklesly na 67 případů. Advertisement podvody obvykle spočívají v tom, že podvodník uveřejní falešný inzerát na legitimním inzertním webu (např. láká na levně nabízené auto, loď či jiné zboží). Když oběť na nabídku reaguje, podvodník tvrdí, že zboží odešlo po obdržení platby. Pokud oběť zaplatí, o peníze přijde, žádné zboží nedostane a prodejce přestane komunikovat (ACC, 2015, s. 45). Roste také CEO fraud, neboli Fake prezident, z 21 případů v roce 2018 na 36 případů v roce 2023, v roce 2024 pak mírně výskyt poklesl na 6 případů. CEO fraud je druh kybernetického útoku, při němž se podvodník vydává za vysokého firemního činitele (např. ředitele) a zmanipuluje zaměstnance, aby na základě falešných příkazů odeslal finanční prostředky nebo citlivé informace (MIMECAST, 2025, online). Méně časté mezi klienty Banky patří Fake invoice, neboli podvržená faktura, s výskytem do 26 případů ročně. Podvod s falešnou fakturou nastává ve chvíli, kdy se podvodník úmyslně snaží oklamat firmu a vylákat z ní peníze nebo bankovní údaje prostřednictvím podvržené či pozměněné faktury, na jejímž základě požaduje úhradu (Tuytel, 2023, online). Do kategorie ostatní spadají nové či méně známé typy podvodů, jako je falešná rodina, podvodný antivirus, smyšlené dědictví a další.



Obrázek 1 - Četnost podvodů dle typu v letech 2018-2024 (KB, interní zdroj, 2025)

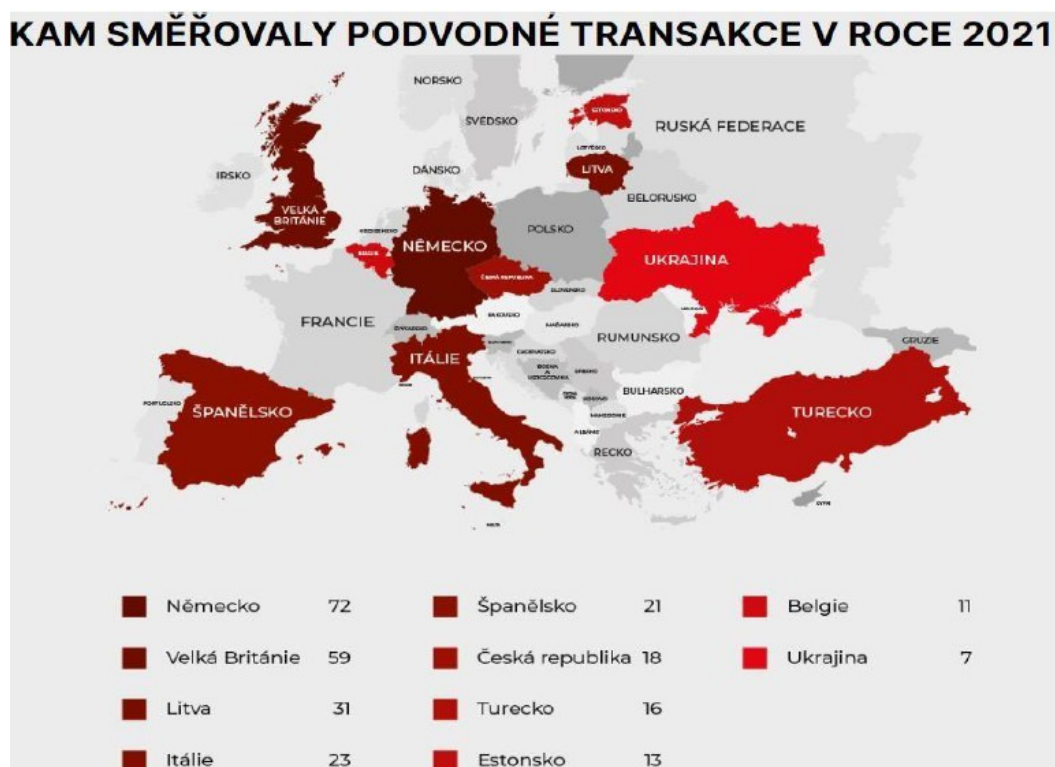
Jak zobrazuje Obrázek 2 a Obrázek 3 v roce 2020 nejčastěji směřovaly podvodné transakce do Velké Británie (18 %), Španělska (14 %), Německa (13 %), Turecka (12 %), České republiky (5 %), USA (4 %), Slovenska (4 %) a Belgie (3 %). V roce 2021 sestupně do Německa, Velké Británie, Litvy, Itálie, Španělska, České republiky, Turecka, Estonska, Belgie a Ukrajiny. Změny ve směřování podvodných transakcí můžeme přičítat mnoha

faktorům, které reflektují mezinárodní finanční prostředí, technologické trendy a kybernetickou kriminalitu. V roce 2020 bylo nejvíce podvodných transakcí směřováno do Velké Británie, Španělska, Německa a Turecka, přičemž podíl těchto zemí lze vysvětlit jejich významnou rolí v globálním finančním systému a vysokému objemu mezinárodních transakcí. V této době také pandemie COVID-19 vytvořila nové příležitosti pro finanční podvody, zejména v souvislosti s nárůstem online plateb, podvodných e-mailů či falešných investičních nabídek.



Obrázek 2 – Směrování podvodných transakcí v roce 2020 (KB, interní zdroj, 2025)

V roce 2021 se vedle tradičních finančních center mezi cílové země také dostaly Litva, Ukrajina, Česká republika a Estonsko. Tento posun naznačuje přesun podvodných aktivit do zemí s méně přísnou regulací nebo do regionů, kde tou dobou docházelo k častějším kybernetickým útokům. Ukrajina v té době byla upozorňována na nedostatky v boji proti praní špinavých peněz a financování terorismu, podobně jako Litva. (Europol, online, 2021; FATF, online, 2022–2024)



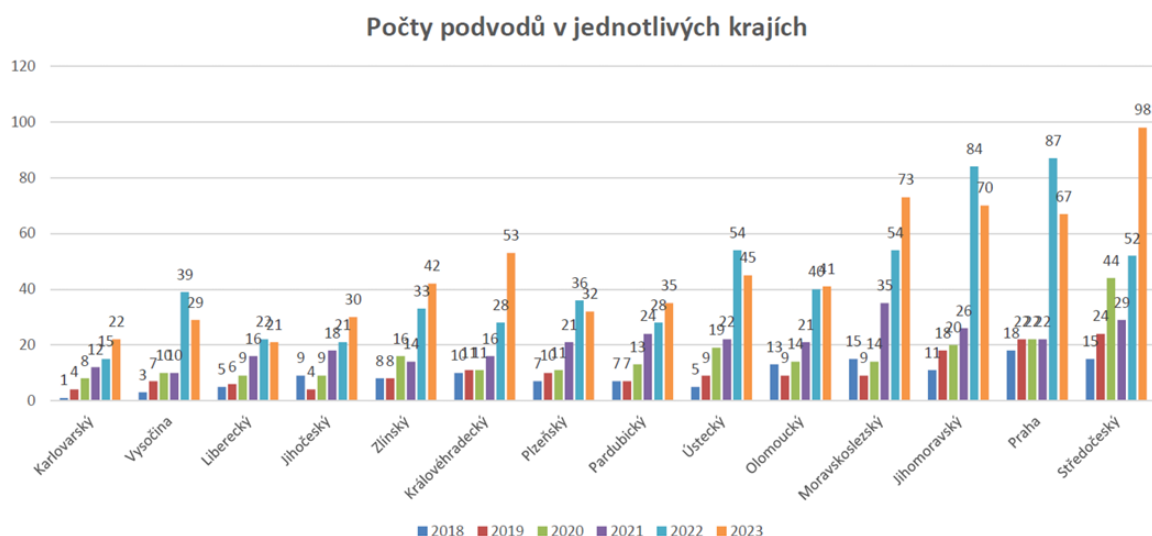
Obrázek 3 - Směrování podvodných transakcí v roce 2021 (KB, interní zdroj, 2025)

Jak ukazuje graf na Obrázku 4 nejvyšší koncentrace nahlášených pokusů o podvody je patrná u klientů ve věkové skupině 35–45 let. Klienti v tomto věku jsou nejvíce aktivními klienty bank, což koncentraci vysvětluje.



Obrázek 4 - Četnost věkových kategorií (KB, interní zdroj, 2025)

Největší koncentraci výskytu podvodů v jednotlivých krajích za období let 2018 až 2023 ukazuje graf na Obrázku 5. Tento graf vysvětluje fakt, že v Praze a Středočeském kraji je vyšší koncentrace jak klientů, tak firem.



Obrázek 5 - Počty podvodů v jednotlivých krajích (KB, interní zdroj, 2025)

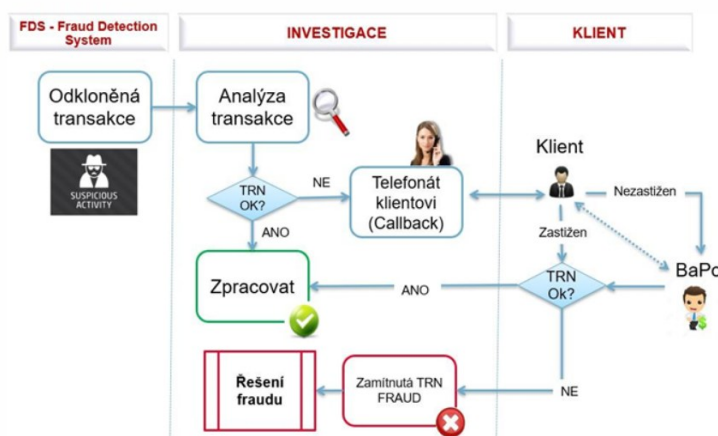
7.2 Investigace podezřelých plateb

Specializovaný tým v Bance, který má na starosti prevenci platebních podvodů, ve spolupráci s dalšími odděleními Banky denně prověří přes 700 tisíc transakcí. K 1. lednu 2025 se díky nim podařilo odhalit 3 888 podvodů a klientům zachránili přes 503 milionu korun. Tým prevence platebních podvodů se zaměřuje na detekci, analýzu a řešení podezřelých transakcí. Tento proces je rozdělen do několika fází:

1. Monitoring a detekce podezřelých transakcí (FDS – Fraud Detection System): Banka využívá FDS, který automaticky sleduje transakce a identifikuje podezřelé platby na základě vzorců chování, geografické polohy, neobvyklých částek nebo neobvyklého času transakce.
2. Analýza transakce: Podezřelá transakce je následně analyzována a ověřuje se, zda obsahuje známky podvodu.
3. Ověření transakce u klienta: Pokud není možné jednoznačně rozhodnout, tým prevence kontaktuje klienta prostřednictvím telefonátu (callback). Klient je dotázán, zda transakci skutečně autorizoval. Pokud klient není zastižen, může být transakce dočasně pozastavena nebo eskalována k dalšímu šetření (Bankovní poradce).

4. Rozhodnutí o transakci: Pokud klient potvrdí, že transakce je v pořádku, banka ji zpracuje a povolí. Pokud klient transakci neautorizuje, je označena jako podvodná a tím ji zamítne. V případě podvodu je transakce postoupena k řešení, což zahrnuje interní vyšetřování, právní kroky nebo spolupráci s policií.

Přehledně jsou tyto fáze také vyobrazené na Obrázku 6.



Obrázek 6 – Schéma procesu zpracování podezřelé platby (KB, interní zdroj, 2025)

7.3 Prevence platebních podvodů bankovního subjektu v praxi

Kybernetická bezpečnost ve finančním sektoru se stále více stává záležitostí prevence, vzdělávání a efektivní komunikace s klienty. Banky čelí nejen technickým hrozbám, ale i sociálnímu inženýrství, které se stává stále sofistikovanější, a útočníci cíleně manipulují klienty k provedení podvodných transakcí. Zatímco regulatorní požadavky, jako je nařízení DORA, pomáhají v posilování provozní odolnosti bankovních systémů, jedním z nejdůležitějších prvků v ochraně klientů před kybernetickými útoky zůstává prevence platebních podvodů. Z tohoto důvodu byl v rámci této diplomové práce zpracován následující polostrukturovaný rozhovor, který umožňuje zachytit komplexitu tématu a vnímání jednotlivých aspektů prevence platebních podvodů v reálném provozním prostředí.

Banka má v této oblasti proaktivní strategii na ochranu svých klientů v detekci podezřelých transakcí, v systémové kontrole podvodných aktivit a v přímé osvětě klientů. Za účelem detailnějšího pochopení interních procesů a strategie Banky v oblasti prevence platebních podvodů byl veden rozhovor s Bc. Markem Macháčkem, supervizorem prevence platebních podvodů, který vede tým prevence platebních podvodů. Kromě chodu

týmu má na starosti také řešení podezřelých nebo podvodných transakcí přes mobilní a internetové bankovníctví, podvodné hovory, e-maily, SMS a další podezřelé případy, které klienti Banky hlásí.

- **Interní strategie a opatření KB**

Jakým způsobem banka interně monitoruje podezřelé transakce a jak probíhá jejich vyhodnocení? *Máme systém (FDS – Fraud Detection Systém), který denně prověří a tzv. „oskóruje“ veškeré transakce, které klienti během dne provedou. Zhruba se bavíme o cca 700 000 transakcích denně. Z nich systém každý den vyhodnotí cca 200–400 transakcí podezřelých, které následně prověřujeme. Sledujeme taktéž podvodné účty a pokud chce někdo z klientů zaslat finance na takovýto účet, je platba pozastavena a klient kontaktován s tím, že zasílá finance na podvodné číslo účtu a je i varován, že je zde velké riziko, že o své finance přijde.*

Jak probíhá spolupráce mezi týmem detekce a prevence platebních podvodů a dalšími útvary banky při řešení podvodných transakcí? *To závisí na tom, co aktivně řešíme. Náš přesah je poměrně veliký. Často komunikujeme s kolegy z karetních podvodů, kdy klient kromě vyplnění karetních údajů podvodníkovi předá své přihlašovací údaje. Pak samozřejmě čteně spolupracujeme s kolegy z prevence praní špinavých peněz a kolegy ze zahraničních plateb. Velice často taktéž komunikujeme s kolegy z prevence podvodů dalších bank v rámci mezibankovní spolupráce, kdy řešíme podvody, které směřovaly z KB nebo do KB. Často také komunikujeme s kolegy z poboček, kteří mají přímý kontakt s klienty a samozřejmě i se samotnými klienty, se kterými řešíme podvodné jednání. Tady bych určitě vyzdvihl, že nám při řešení ochrany našich klientů i případně podvodného jednání pomáhají ve velké míře na všech frontách všechna oddělení.*

Jakým způsobem se banka připravuje na nové typy podvodů, například deepfake nebo AI generované phishingové kampaně? *Víme o těchto podvodech a samozřejmě je zahrnujeme v preventivních kampaních směřujících na naše klienty, i ve spolupráci s ČBA. Podporujeme akci nePINdej! a s tím spojený Kybertest.cz, který slouží jako edukativní nástroj. Musím říct, že je někdy těžké se připravit na budoucí typ podvodu specificky, protože my vždy musíme reagovat až na to, co podvodníci vlastně vytvoří. Připodobnil bych to k šachům, kdy podvodník má spoustu možných tahů a my reagujeme až na jejich tah, konkrétně abychom případně nemrhali časem na tahy, které podvodník vůbec neudělá.*

Samozřejmě zabezpečení bankovníctví je na takové úrovni, že drtivá většina útoků je směřována na ten nejslabší článek zabezpečení – klienta. Pokud dokážete nějakým způsobem klienta přesvědčit, přinutit ho k zaslání peněz dobrovolně ze svého účtu, není moc možností, jak klientovi v takovém jednání s jeho financemi zamezit. Nejsilnější zbraň je ale prevence, pokud víte, že podvodník využívá určitou formu videa např. s prominentními politiky, je jednoduché klienty varovat, že takto peníze opravdu nezískají, což výrazně snižuje účinnost podvodníků při těchto druzích podvodů.

- **Prevence platebních podvodů u klientů**

Jaké jsou hlavní hrozby, kterým klienti Banky v současnosti nejvíce čelí? Zjednodušeně, momentálně jsou nejhorší tzv. kryptopodvody či v rámci jiného názvosloví investiční podvody, podvodné volání (vishing) a pak stále klasické bazarové podvody (phishing).

Když banka identifikuje podezřelou platbu, jaký je další postup? Jakým způsobem se spojíte s klientem a jak probíhá ověření transakce? Pokud se jedná o podezřelou platbu, která není zachycená přímo na tzv. „watchlist“, tedy nevíme předem, zda příjemce je již hlášen jako podvodný účet, tak takovou transakci prověřujeme. Sledujeme, zda je pro klienta typická částka, příjemce, země. Dále například, kdo je firma, kam a za jakým účelem finance směřují, zda nesplňuje taková transakce určité typické podvodné scénáře. Pokud se nám něco na transakci nezdá, tak se klientům přímo ozýváme a situaci s nimi řešíme telefonicky, výjimečně přes bankovní poradce nebo e-mailem.

Jaké nejčastější chyby dělají klienti, které vedou k úspěšným podvodům? Nejčastěji klienti věří podvodníkům, kteří jim slibují závratné zisky v podstatě bez práce. Rád říkám, že bez práce nejsou koláče. Každý den řešíme desítky případů, kdy klienti věří cizím lidem po telefonu, které nikdy neviděli osobně, neví, jak se jmenují, kde sedí, a i přes naše varování jsou i tak schopni takovým podvodníkům poslat v mžiku své životní úspory. Pustit takové lidi do svého domu by určitě neudělali, ale pustit takové lidi do svého počítače a do svého bankovníctví jim problém nedělá, a podvodníkům pak nedělá problém takových možností okamžitě využít.

Jak Banka školí zaměstnance pracující v přímém kontaktu s klienty, aby dokázali správně reagovat na podezřelé situace?

S kolegou z karetních podvodů máme pravidelná školení o platebních a karetních podvodech. Snažíme se klienty varovat preventivními kampaněmi a ty zasíláme také našim kolegům, aby byli informováni o nejnovějších trendech.

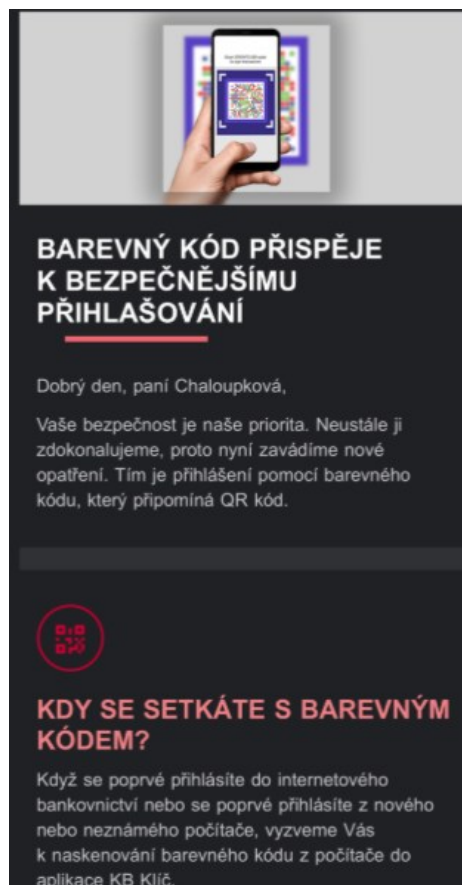
Jakou roli podle Vás hraje vzdělávání klientů v oblasti kybernetické bezpečnosti?

Obrovskou! Rád říkám, že znalost a informace v rámci podvodů jsou to nejcennější, co každý z nás v boji s podvody má. Když vím, jak určitý podvod funguje, a někdo se ho na mě pokusí použít, můj mozek vyhodnotí stejný pattern (vzorec), rozpozná ho (v tom jsme jako lidé opravdu skvělí) a dojde mi, že tady něco nehraje, jsem varován a podvodu se nejčastěji vyhnu. Pokud nevím, že se např. objevují Deepfake videa s podvodnou nabídkou investic, tak je o dost pravděpodobnější, že na takovou nabídku přistoupím, protože žádná „červená dioda“ v mé hlavě mě nevaruje. Tedy informace, které banky, policie a média klientům a všeobecně veřejnosti zasílají a doslova „pumpují“ jsou opravdu to nejlepší co je proti podvodům ideální dělat. Sám vystupuji na žádost médií v TV, rádiu, podcastech apod. a snažím se tuto osvětu sdělit uchopitelným přednesem tak, aby si každý dokázal situace připodobnit a sít se s nimi.

7.4 Komunikace bankovního subjektu ke klientům

Banka dlouhodobě investuje do ochrany finančních prostředků svých klientů, zabezpečení digitálních platforem a osvěty v oblasti kybernetických hrozeb. Klade důraz nejen na moderní bezpečnostní technologie, ale také na pravidelné informování svých klientů o aktuálních hrozbách a způsobech ochrany.

Banka používá Below the Line komunikaci (dále jen „BTL“), mimo jiné, jako nástroj pro cílenou edukaci a ochranu svých klientů. Poskytuje informace prostřednictvím e-mailové komunikace, SMS, push-up notifikací, zpráv v internetovém a mobilním bankovníctví, webu apod. Touto cestou Banka informuje klienty i o nových zabezpečeních, viz Obrázek 7.



Obrázek 7 - BTL komunikace bezpečnostních prvků (E-mailová komunikace KB zaslaná klientům, 2022)

Stránka Bezpečnost na oficiálním webu Banky slouží jako přehledný a praktický průvodce kybernetickou bezpečností pro klienty banky i širokou veřejnost. Jejím hlavním cílem je informovat uživatele o aktuálních hrozbách v online prostředí a poskytnout jim konkrétní rady, jak chránit své finance, osobní údaje a digitální zařízení. Stránka se zaměřuje na edukaci o nejčastějších typech podvodů, mezi které patří phishing, podvodné e-maily, telefonáty nebo falešné nabídky v internetových bazarech. Uživatelé se zde dozvědí, jak tyto útoky rozpoznat a jak na ně správně reagovat. Součástí obsahu je i tzv. „Desatero bezpečnosti na internetu“, tedy soubor základních pravidel pro bezpečné chování v digitálním světě, včetně doporučení, jako je používání silných hesel, pravidelná aktualizace softwaru nebo upozornění na obezřetnost při otevírání nevyžádaných zpráv. Stránka rovněž nabízí konkrétní návody na zabezpečení počítače, mobilního telefonu, platebních karet. V případě, že uživatel zaznamená podezřelé chování na svém účtu nebo se stane obětí podvodu, najde zde jasný postup, jak situaci řešit, včetně kontaktů na zákaznickou linku nebo návodů na blokaci karty. Dále jsou zde pravidelně aktualizovány informace o aktuálních hrozbách, které pomáhají uživatelům být v obraze

a lépe se chránit před nově vznikajícími typy útoků. Celkově stránka představuje důležitý nástroj prevence, který podporuje bezpečné digitální chování a zvyšuje povědomí o rizicích spojených s online prostředím. (KB, online, 2025)

Mediální komunikace Above the Line (dále jen „ATL“) zahrnuje masová média, jako jsou televize, rádio, tisk a další. Mimo jiné spustila v únoru roku 2025 rozsáhlou ATL kampaň zaměřenou na kyberbezpečnost, ve které pomocí vizuálních „příšer“ upozorňuje na vybrané digitální hrozby. Kampaň probíhá napříč různými komunikačními kanály, je ji možné vidět v televizi nebo na billboardech. V rámci kampaně banka upozorňuje na možné hrozby, ale zároveň klade důraz na využívání bezpečnostních opatření a služeb, jako je „Ověření bankéře“, které klientům umožňuje okamžité potvrzení identity zaměstnanců Komerční banky při telefonickém hovoru prostřednictvím mobilního bankovníctví. (KB, online, 2025)

8 NÁVRH NA ZLEPŠENÍ SOUČASNÉHO STAVU

Kybernetická bezpečnost je jedním z pilířů moderního bankovního sektoru, kde nejen technologická opatření, ale také informovanost a obezřetné chování klientů hrají zásadní roli v ochraně finančních prostředků a citlivých údajů. Přestože se banky soustředí na zajištění robustních bezpečnostních systémů, jedním z nejslabších článků kybernetické bezpečnosti zůstává lidský faktor. Klienty bank jsou častým cílem kybernetických podvodů, přičemž úspěšnost těchto útoků závisí především na míře jejich informovanosti, schopnosti rozpoznat hrozbu a správné reakci na potenciální riziko. Z tohoto důvodu byla v rámci této diplomové práce zvolena aplikační strategie zaměřená na posílení bezpečnostního povědomí klientů Banky jakožto klíčového prvku celkového bezpečnostního ekosystému banky.

Za účelem návrhu zlepšení současné komunikace kybernetických hrozeb směrem ke klientům byl proveden průzkum formou ankety a moderované diskuse. Hlavními cíli výzkumu bylo zjistit, jaké mají respondenti povědomí o kyberpodvodech, jak hodnotí informace poskytované Bankou a jaké formy předávání informací by vnímali jako nejefektivnější. Dotazování se soustředilo na konkrétní zkušenosti s podvody, subjektivní vnímání rizik a preference v oblasti edukace.

8.1 Metodologie a výsledky výzkumu

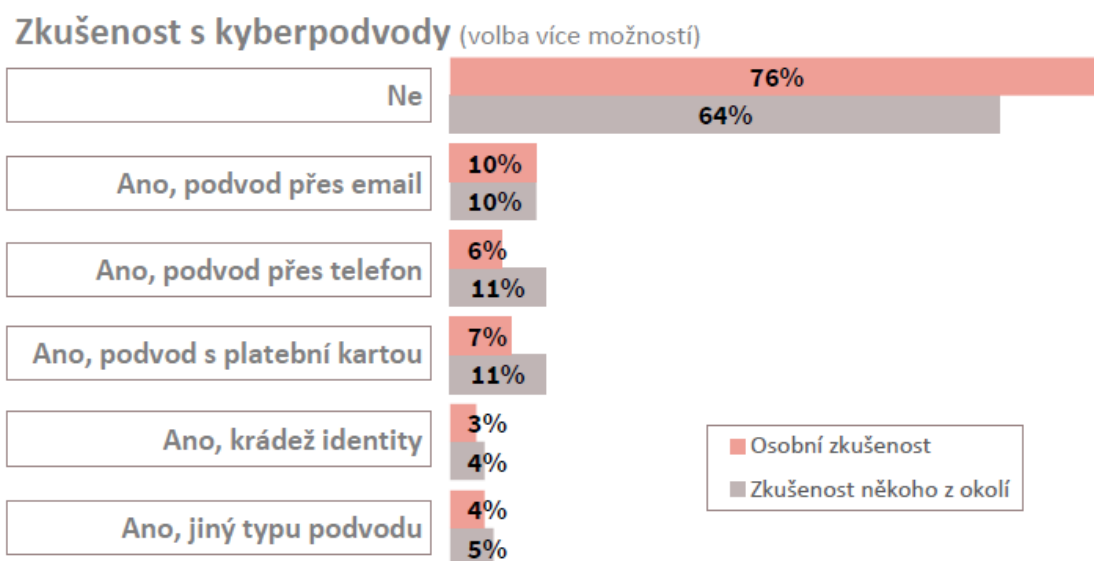
Výzkum byl realizován prostřednictvím Konzulátu. Konzulát je moderovaná online komunita, ve které klienti Banky a zároveň konkurence diskutují nad danými bankovními tématy, hodnotí předložené materiály, testují novinky, odpovídají na dotazníky a popisují zážitky spojené s bankovníctvím. Jedná se o dlouhodobou komunitu 200 respondentů, kteří si, kromě příležitostných průzkumů, píší pravidelné deníky bankovních zážitků, které slouží k dalšímu rozvoji bankovních služeb a zlepšení klientské zkušenosti. Průzkum, který byl nazván „Kyberbezpečnost a kyberpodvody“ byl rozdělen na dvě části, a to anketu a moderovanou diskuzi. Sběr odpovědí probíhal v období 18. prosince 2024 až 2. ledna 2025 a zapojilo se do něj 154 členů Konzulátu a do moderované diskuse se zapojilo 49 Konzulů.

8.1.1 Zkušenost s kyberpodvody

V anketě byly respondentům položeny následující tři otázky: Stali jste se někdy Vy osobně obětí kyberpodvodu? O který typ se jednalo? Víte o někom z Vašeho okolí, kdo se někdy stal obětí kyberpodvodu?

Většina respondentů uvedla, jak ukazuje graf na Obrázku 8, že se nikdy osobně nestala obětí kyberpodvodu. Přesto však značná část z nich má zkušenost s tím, že se podvod vyskytl v jejich blízkém okolí. Nejčastěji uváděné typy podvodů zahrnují telefonické útoky, podvody spojené s využíváním platebních karet, phishingové e-maily a falešné online obchody. Respondenti často uváděli, že se snaží být obezřetní a dodržovat základní pravidla kybernetické bezpečnosti, jako neotevírání podezřelých e-mailů či neklikání na neznámé odkazy. Přesto však mnozí z nich nedokázali přesně popsat jednotlivé typy podvodů, což svědčí o určitém nedostatku systematického přehledu. Otázky byly navrženy autorem této práce a autorizovány odborníky na vybranou oblast.

Respondenti uvedli, že při zmínce o kyberpodvodu se jim vybaví následující typy podvodů: Vylákání údajů o platební kartě přes podvodné zprávy nebo aplikace, falešné bankovní aplikace, zprávy od falešného pracovníka banky, podvodné SMS/mail/hovory, deepfake videa pomocí AI, falešné e-shopy a podvodné prodeje (např. na platformě Marketplace).



Obrázek 8 – Zkušenost respondentů s kyberpodvody (KB, interní zdroj, 2025)

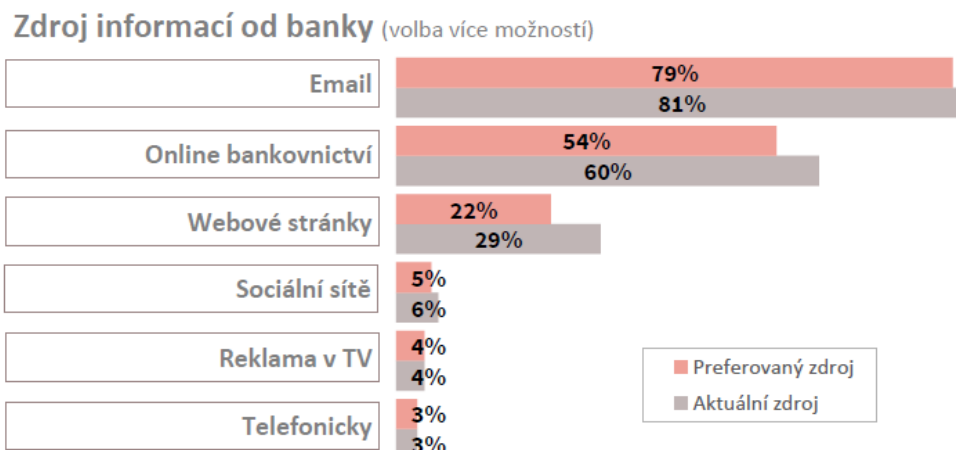
8.1.2 Vnímání informací od banky

Drtivá většina dotázaných (94 %) uvedla, že od své banky pravidelně dostává informace o kyberbezpečnosti. Tyto informace jsou vnímány jako důležité a užitečné, avšak mnozí respondenti zároveň kritizují jejich obecnost a nedostatek konkrétních příkladů. Často zaznívaly požadavky na přehlednější, názornější a praktičtější formu komunikace. Někteří klienti si přejí, aby banka poskytovala více vizuálních materiálů, jako jsou například screenshoty podvodných zpráv nebo krátká videa zachycující modelové situace. Výzkum zároveň ukazuje, že klienti by uvítali, kdyby jim banka ukazovala reálné případy podvodů, které byly aktuálně zaznamenány na trhu.

8.1.3 Preferované způsoby komunikace

Nejčastější formou, jakou banky poskytují informace, je e-mail. Jak představuje graf na Obrázku 9, tento kanál je zároveň vnímán jako nejpohodlnější, protože umožňuje informace si přečíst v klidu a v čase, který klientovi vyhovuje. „Preferovaný zdroj“ v grafu zastupuje odpovědi respondentů na otázku: Jakým způsobem Vás banka o kyberpodvodech informuje? Aktuální zdroj představuje výsledky odpovědí respondentů na položený dotaz: Jakou formou byste chtěli informace o kyberpodvodech od své banky dostávat? Další oblíbenou formou jsou notifikace v online bankovníctví, i když zde dochází ke kolizi zájmu, pokud klient spěchá například na provedení platby, často informační zprávu ignoruje.

Respondenti se shodli na tom, že ideální formou komunikace je kombinace e-mailu a notifikace v bankovní aplikaci, která zajistí, že klientovi informace neuniknou, ale zároveň ho nebudou rušit v nevhodný moment. Klienti informace považují za všeobecné, ocenili by přidání více praktických typů nebo přímo ukázek. Respondenti se shodují, že by konkrétní ukázky podvodů měly obsahovat následující: Screenshoty aktuálně šířících se podvodů, videa s ukázkou podvodů a návod na jejich řešení, články, jaké podvody v minulosti proběhly a praktické ukázky podvodů a jejich odhalení.



Obrázek 9 – Preferovaný zdroj informací (KB, interní zdroj, 2025)

8.1.4 Postoj ke školení

Na otázku, jestli by ocenili nějakou formu školení s odborníkem z banky, který by jim problematiku kyberbezpečnosti přiblížil (např. besedu, školení) neprojevali respondenti výrazný zájem, a to především z důvodu nedostatku času a neochoty cestovat. Naopak velmi pozitivně byly hodnoceny online formy školení, zejména krátká instruktážní videa s praktickými ukázkami podvodů a doporučeným postupem, jak se zachovat v případě jejich výskytu.

Za inspirativní příklad byla opakovaně zmiňována kampaň společnosti Air Bank „Podvody, které zrovna letí“, stejně jako televizní pořad České televize „Tohle radši nezkoušejte“. Tyto formáty jsou vnímány jako srozumitelné, názorné a účinné při zvyšování povědomí o rizicích.

9 APLIKAČNÍ NÁVRH

Tato část diplomové práce se zaměřuje na konkrétní oblast komunikace Banky směrem ke klientům, konkrétně na podlinkovou (BTL) komunikaci v kontextu kybernetické bezpečnosti. Tento výběr vychází z přesvědčení, potvrzené jak posouzením interního stavu kybernetické bezpečnosti vybrané bankovní instituci, tak provedenou anketou, že efektivní a cílená komunikace představuje jeden z nejúčinnějších nástrojů prevence v oblasti kyberpodvodů. BTL komunikace umožňuje oslovit klienty individuálně prostřednictvím digitálních kanálů, které pravidelně využívají nebo i dopisem. Právě tyto kanály jsou jedna z cest, jak posilovat digitální gramotnost, zvyšovat obezřetnost uživatelů a poskytovat jim konkrétní nástroje k rozpoznávání rizikových situací.

Pro zpracování návrhu pro zlepšení současného stavu kybernetické bezpečnosti byla využita metoda Service Desing. „*Service Desing je interdisciplinární přístup, jehož účelem je navrhovat služby tak, aby byly z pohledu uživatele užitečné, použitelné a žádoucí, a z pohledu poskytovatele efektivní a účinné*“ (Mager et al., 2011, online). Jedná se o proces, který pomáhá poskytovatelům služeb, v tomto případě Banky, vytvořit promyšlený a cílený návrh služby včetně všech jejích kontaktních bodů. Právě tato uživatelsky orientovaná povaha Service Designu je vhodná při navrhování komunikačních zásahů v oblasti prevence kybernetických hrozeb. Nejde pouze o informování klienta, ale o vytváření prostředí, ve kterém se klient cítí bezpečně, je edukován přístupnou formou a dostává informace v čase a způsobem, který odpovídá jeho digitálním návykům i zranitelnosti vůči podvodům. (Mager et al., 2011, online)

Na základě moderované diskuse s klienty, ankety, analýzy dat a využitím metody Service Design je definovány modelové případy typických uživatelů, kteří představují prototypy obětí různých podvodů: Modelový případ 1: Seniorní klientka s nízkou digitální gramotností, Modelový případ 2: Firemní klient ohrožený falešnými fakturami, Modelový případ 3: Digitálně zdatný klient s preferencí online komunikace, Modelový případ 4: Klientka ohrožená romance scamem a Modelový případ 5: Klient aktivní na online bazarech s rizikem podvodných plateb. Tyto modelové případy pomohou lépe pochopit chování, potřeby a komunikační zvyklosti jednotlivých skupin klientů. Každý případ reprezentuje specifický profil klienta s různou mírou digitální gramotnosti, odlišnými životními okolnostmi a jinou úrovní zranitelnosti vůči kybernetickým útokům. Vytvoření modelových případů umožňuje přenést konkrétní poznatky do lidsky uchopitelné roviny a slouží jako zástupný model určité množiny reálných typů klientů,

jehož chování, potřeby, motivace a obavy jsou systematicky popsány a propojeny s konkrétními riziky kybernetických podvodů. Pro daný segment klientů bude tak možné účinněji a lépe nastavit obsah, formu a načasování komunikace. Například senior klient bude pravděpodobně potřebovat více opakování, jednodušší jazyk a přímé ukázky, zatímco mladý digitální zákazník ocení interaktivní a vizuálně atraktivní formáty. Modelové případy tak zajišťují, že komunikace nebude založena na domněnkách, ale na reálných datech a behaviorálních charakteristikách různorodých skupin. Slouží jako základ pro tvorbu scénářů, mapování zákaznické cesty (customer journey) a identifikaci klíčových kontaktních bodů, ve kterých má smysl komunikovat preventivní sdělení. V konečném důsledku modelové případy pomohou přizpůsobit preventivní komunikaci tak, aby byla pro každou cílovou skupinu relevantní, srozumitelná a motivující k žádoucímu chování.

9.1 Modelový případ 1

Modelový případ 1 reprezentuje personu „Seniorní klientka s nízkou digitální gramotností“, která byla vytvořena na základě výzkumných rozhovorů, diskusí s klienty a analýzy dat. Persona popisuje klientku, která je ohrožena specifickými typy kybernetických podvodů a reaguje na bankovní komunikaci odlišným způsobem než mladší nebo technicky zdatnější skupiny.

Demografie: Tato persona je 68letá bývalá učitelka, která žije v malém městě na okraji větší aglomerace. Po odchodu do důchodu si cení klidu a stability, přičemž často žije sama. I když má solidní vzdělání a dlouholeté zkušenosti, její digitální gramotnost není na úrovni mladších klientů, což ji staví do situace, kdy je ohrožena podvodnými praktikami, se kterými se setkávají klienti starší 65 let.

Chování: Persona se spoléhá především na tradiční formy komunikace se svou bankou. Raději navštěvuje pobočky, přijímá tištěné dopisy a telefonické hovory, než aby využívala internetové bankovníctví či mobilní aplikace. Oceňuje osobní kontakt a jasně strukturované informace, přičemž se snaží dodržovat bezpečnostní doporučení, která dostává od banky.

Rizika: Nejčastější oběť vishingu a phishingu. Přestože se tato persona snaží být obezřetná, její reakce na naléhavé situace může být někdy impulzivní. Když obdrží telefonát nebo dopis s výzvou k okamžitému ověření údajů, její pocit znepokojení a potřeba jednat rychle mohou vést k unáhleným rozhodnutím. Její schopnost rozeznat

jemné rozdíly v komunikaci je omezená, což ji činí zranitelnou vůči podvodným praktikám, jako jsou falešné telefonáty či e-maily.

Geografické zaměření: Nejvíce případů v Moravskoslezském a Středočeském kraji.

Doporučená prevence:

- **Tištěné letáky na pobočkách:** Letáky by měly obsahovat jednoduché a jasné instrukce, jak rozeznat podezřelé zprávy, a měly by být vizuálně přitažlivé. Primárně na pobočkách v Moravskoslezském a Středočeském kraji, kde je těchto případů hlášeno nejvíce.
- **Informativní dopisy s reálnými příběhy:** Dopisy, ve kterých jsou prezentovány příběhy reálných obětí, mohou působit jako silný varovný prvek a pomoci personě lépe si zapamatovat důležité bezpečnostní informace.
- **Telefonické hovory od bankovních poradců:** Osobní přístup přes telefon umožňuje ověřit autenticitu komunikace a poskytuje možnost konzultovat každý podezřelý případ.

Doporučení pro komunikaci: Pro personu Seniorní klientka s nízkou digitální gramotností, která upřednostňuje tradiční formy komunikace, jsou tištěné letáky a dopisy vhodným nástrojem pro prevenci podvodů, zejména phishingu. Tyto materiály by měly být navrženy tak, aby byly vizuálně přitažlivé a snadno čitelné, s velkým, jasným písmem a jednoduchým jazykem s případným vysvětlením anglicismů. Leták by měl obsahovat stručné a srozumitelné instrukce, jak rozeznat podezřelé e-maily, např. upozornění, že podvodné e-maily často obsahují odkazy, které vás mají „přesměrovat“ na falešnou stránku, a varovné výrazy jako „Vaše finance jsou v ohrožení“. Součástí letáku by měl být také vyhrazený prostor pro ilustrativní obrázek podvodné komunikace, viz Obrázek 10, na kterém budou jasně vyznačeny podezřelé prvky, jako je nesprávná adresa odesílatele, naléhavý tón, gramatické chyby nebo neobvyklý formát odkazu. Dopis zasílaný poštou by měl být podobně strukturován a obsahovat detailnější vysvětlení, včetně reálných příkladů z praxe, které pomáhají klientce zapamatovat si, jaké varovné signály sledovat. V textu dopisu by mělo být zdůrazněno, že pokud tato persona obdrží zprávu s neobvyklými požadavky na ověření údajů, měla by se vždy obrátit na svého bankéře nebo oficiální kontaktní kanály banky a ověřit pravost komunikace.



Obrázek 10 - Příklad phishingu (vlastní zdroj)

Telefonická komunikace je pro tuto personu také velmi důležitá, neboť preferuje osobní kontakt a svého bankéře zná. Proto je třeba, aby bankéři, kteří ji kontaktují, měli připravené detailní a srozumitelné call scripty. Takový skript by měl začínat přátelským a uklidňujícím tónem, kdy bankéř představí své jméno, oddělení a vysvětlí, proč volá. Dále by měl bankéř vysvětlit, že podvodníci často používají taktiky, jako je naléhavý tón, volání v brzkých ranních hodinách, často používají taktiku „zastavení podvodu“ či jiných naléhavých situací, aby vyvinuli časový tlak, vyvolali paniku a přiměli klientku k impulzivnímu jednání, jako je potvrzení požadované akce v internetovém bankovníctví. Bankéř by měl zdůraznit, že skuteční zástupci banky nikdy nebudou požadovat sdělení citlivých údajů přes telefon a že pokud si persona není jistá, měla by hovor okamžitě ukončit a zavolat zpět na oficiální číslo, které má uvedeno na vizitce nebo v jiných oficiálních materiálech od své banky.

9.2 Modelový případ 2

Modelová případ 2 reprezentuje personu označenou jako „Firemní klient ohrožený falešnými fakturami“, která byla vytvořena na základě poznatků z analýzy incidentů, podnětů od klientů a výsledků průzkumu mezi firemní klientelou. Persona představuje typického podnikatele, který se každodenně pohybuje v prostředí firemního bankovníctví a je vystaven specifickým kybernetickým hrozbám spojeným s fakturační agendou.

Demografie: Persona patří do střední věkové skupiny a působí jako majitel menší či střední firmy. Nese vysokou zodpovědnost za finanční řízení podniku a denně zpracovává faktury a platební operace. Je zvyklá využívat digitální nástroje a má vysokou odbornou způsobilost v oblasti podnikání a ekonomiky. Vzhledem k pracovnímu vytížení však může dojít k poklesu pozornosti a snížení obezřetnosti při vyhodnocování elektronické komunikace.

Chování: Persona pravidelně vyřizuje faktury a provádí platby, zejména prostřednictvím e-mailové komunikace. Využívá notifikace v internetovém bankovníctví a aktivně se účastní online seminářů zaměřených na firemní klientelu. Část svých operativních úkolů deleguje, například asistentka má oprávnění k provádění platebních transakcí, což sice zvyšuje efektivitu, ale zároveň představuje významný bezpečnostní faktor.

Rizika: Persona je zvláště ohrožena podvody typu „fake prezident“ s podvrženými fakturami. Podvodníci často využívají podvržené e-maily, ve kterých se vydávají za banku nebo obchodního partnera a vyžadují rychlou reakci, například změnu platebních údajů. Tyto podvody patří podle dat banky k nejčastějším a zároveň nejvýnosnějším. V hektickém pracovním režimu může snadno dojít k unáhlené reakci bez dostatečného ověření pravosti výzvy. Navíc fakt, že persona často deleguje pravomoci na další osoby v organizaci, zvyšuje pravděpodobnost, že útočníci zneužijí nepozornost těchto osob k získání neoprávněného přístupu a odčerpání finančních prostředků.

Doporučená prevence:

- **Povinná bezpečnostní školení pro firemní zaměstnance:** Školení zaměřená na rozpoznání konkrétních scénářů podvodů ve firemní praxi a zvýšení finanční gramotnosti uvnitř organizace. Může ho zprostředkovávat banka, obdobným způsobem jako již funguje vzdělávací projekt od České bankovní asociace Bankéři do škol, případně může školení probíhat online formou.
- **E-mailová upozornění s ukázkami podvodných faktur:** Poskytování konkrétních příkladů falešných faktur, což usnadní identifikaci podvodných komunikací, zejména vzhledem k tomu, že persona pracuje s fakturami denně.
- **Doplnění tématu bezpečnosti na schůzkách s bankovními poradci:** Kromě zaměření na obchodní a servisní záležitosti, by měly být pravidelné schůzky s bankovními poradci zaměřené i na pravidelnou revizi klientova bezpečnostního nastavení a doporučení. Např. zavedení dodatečných ověřovacích mechanismů, aby

každá změna platebních údajů byla potvrzena prostřednictvím vícefaktorového ověřování, čímž se sníží riziko zneužití přístupu, který má asistentka.

Doporučení pro komunikaci: Persona Firemní klient ohrožený falešnými fakturami reprezentuje typického firemního klienta banky a představuje specifickou cílovou skupinu, která denně pracuje s fakturami, provádí elektronické platby a zároveň často deleguje přístup k firemnímu bankovníctví. Komunikace určená této personě by měla být praktická, názorná a zároveň profesionální, důraz by měl být kladen na srozumitelnost a rychlou využitelnost v praxi. Banka by měla volit komunikační kanály a obsah, které odpovídají pracovním podmínkám této osoby, jejím digitálním návykům a roli ve firmě.

E-mailová upozornění s ukázkami podvodných faktur představují klíčový komunikační nástroj, neboť persona je zvyklá zpracovávat faktury prostřednictvím e-mailu na denní bázi. Tato forma komunikace odpovídá jak jejímu pracovnímu rytmu, tak typickému vektoru útoků, kterým čelí. Banka by měla pravidelně zasílat personalizované e-mailové zprávy s konkrétními příklady aktuálně cirkulujících podvodných faktur například jako na Obrázku 11. Tyto e-maily by měly být vizuálně přehledné a obsahovat jasně označené rizikové prvky jako například nečekanou změnu čísla účtu dodavatele, časový tlak na provedení platby, výhradní komunikaci prostřednictvím e-mailu nebo kombinaci názvu firmy a banky ze dvou různých zemí.

Datum: 31.10.2024 11:14

Příjemce:

Kopie:

Předmět: **Platba faktur**

Potvrďte, že jste včera obdrželi náš níže uvedený e-mail ohledně platby.

Dobré odpoledne

Přiložené faktury jsou splatné zítra a upřednostníme příjem prostředků v naší aktualizované bance níže:

Název účtu:

Ceská sporitelna, A.S.

Olbrachtova 1929/62, 140 00 Praha 4

CZ7508000000005539225003

BIC: GIBACZPX

Náš starý bankovní účet je nefunkční, proto vám doporučujeme převádět všechny platby do naší výše aktualizované banky.

S pozdravem

Obrázek 11 – Příklad fake invoice (vlastní zdroj)

Dalším důležitým informačním kanálem jsou pravidelná osobní setkání s bankovním poradcem, která by neměla být zaměřena pouze na obchodní záležitosti, ale měla by cíleně zahrnovat také téma bezpečnosti. Bankéř by mohl při každé schůzce otevřít otázku digitální bezpečnosti firmy, ověřit aktuální nastavení přístupových oprávnění, schvalovacích limitů a způsobů autorizace transakcí. Jedním z doporučených kroků je například zavedení vícefázového ověřování při změně platebních údajů. Toto opatření snižuje riziko podvodného zásahu, zejména v případech, kdy má k bankovníctví přístup více osob, například asistentka. Ve spojení s tímto doporučením by měl bankéř nabízet i revizi oprávnění v rámci firemních profilů a doporučovat využití dodatečných bezpečnostních prvků, jako je Cronto kód, který významně zvyšuje úroveň zabezpečení přihlášení a autorizace.

Pro dlouhodobé posílení finanční gramotnosti firmy by bylo vhodné, aby banka zprostředkovala povinná bezpečnostní školení pro zaměstnance. Tato persona obvykle deleguje vybrané úkoly na své spolupracovníky, například asistentku nebo účetní, které pak mohou být nejslabším článkem celého bezpečnostního řetězce. Banka by měla nabídnout možnost absolvovat krátké, prakticky orientované školení, ať už prezenční nebo formou webináře nebo e-learningu, zaměřené na reálné scénáře podvodů: jak vypadá

„fakeprezident“, jak rozeznat podvodný telefonát (vishing) nebo jak identifikovat phishingovou stránku napodobující přihlášení do bankovníctví. Tato školení mohou navazovat na osvědčené iniciativy, jako je projekt České bankovní asociace „Bankéři do škol“, ovšem adaptovaný pro firemní (B2B) prostředí.

Jak dokládají statistiky banky, pouze za rok 2024 bylo díky včasnému zásahu zachráněno více než 503 milionů korun – což podtrhuje význam prevence i na úrovni menších firem.

V neposlední řadě by banka měla s touto personou komunikovat také prostřednictvím kontextových varování přímo v internetovém bankovníctví, která by mohla v reálném čase detekovat podezřelé transakce. Například při zadání nové platby na neznámý účet by se mohla objevit push notifikace s výstrahou typu: „Tato faktura se výrazně liší od předchozích faktur daného příjemce, zkontrolujte prosím údaje s protistranou.“ Taková chytrá výstraha využívá analýzu transakční historie a pomáhá klientovi zastavit se v kritickém momentu bez narušení jeho obvyklého pracovního postupu.

9.3 Modelový případ 3

Modelový případ 3 vychází z osoby označené jako „Digitálně zdatný klient s preferencí online komunikace“. Persona reprezentuje mladého klienta s vysokou mírou digitální aktivity a technologického sebevědomí, který je současně zranitelný vůči specifickým formám online podvodů, zejména v oblasti investic a kryptoměn.

Demografie: Persona reprezentuje muže ve věku 25 let, studuje vysokou školu a při studiu pracuje. Je plně obeznámen s moderními technologiemi, aktivně využívá digitální nástroje a věnuje se investování, zejména v oblasti kryptoměn. Právě tento aktivní přístup a zájem o nové formy zhodnocení financí jej staví do popředí skupiny, u které kryptopodvody představují rychle rostoucí riziko.

Chování: Tomáš aktivně investuje do kryptoměn a pravidelně sleduje online influencery, kteří ho informují o aktuálních trendech a investičních příležitostech. Je zvyklý využívat internetové bankovníctví a mobilní aplikace ke správě svých finančních operací. Jeho digitální aktivita a zájem o nové technologie však také znamenají, že je náchylný k podvodům, zejména nabízející rychlý jednoduše dostupný zisk.

Rizika: Hlavními riziky, kterým tato persona čelí, jsou kryptopodvody a phishing. Útočníci často zneužívají její zájem o online investice a oslovují ji prostřednictvím falešných investičních nabídek nebo e-mailů slibujících vysoké výnosy. Cílem těchto útoků je získat přístup k finančním prostředkům nebo osobním údajům klienta.

Komunikační kanály: Push notifikace, cílené reklamy na YouTube a Instagramu, edukace v internetovém bankovníctví.

Doporučená prevence:

- **Krátká videa na YouTube a Instagramu:** Video, která vizuálně přitahují pozornost a poskytují jasná varování před podvodů. Tato videa by měla obsahovat konkrétní příklady a varovné signály, aby Tomáš mohl snadno rozeznat falešné zprávy.
- **Push notifikace v mobilní aplikaci:** Personalizovaná upozornění, která mu okamžitě sdělí důležité bezpečnostní informace, a která jsou navržena tak, aby byla stručná, ale účinná.
- **Interaktivní chatbot v mobilním bankovníctví:** Chatbot, který je schopný okamžitě reagovat na jeho dotazy a poradit, jak postupovat v případě podezřelých situací. Tento systém umožní personě rychle získat relevantní informace bez zbytečného čekání a bez kontaktu s bankovním poradcem, který tato věková skupina zpravidla tolik nevyhledává.

Doporučení pro komunikaci: Pro personu označenou jako Digitálně zdatný klient s preferencí online komunikace, která představuje mladého, technologicky zdatného klienta se zájmem o investování a kryptoměny, by měla banka volit moderní a dynamické formy komunikace s důrazem na rychlost, přehlednost a interaktivitu. Persona je aktivní online, denně využívá mobilní aplikace, sleduje influencery a je zvyklá hledat informace v reálném čase. Právě díky tomuto stylu života je zranitelná vůči kryptopodvodům a phishingovým útokům, které často využívají „clickbaitovou“ strategii – tedy lákavé výnosy, známé osobnosti a zdánlivě důvěryhodné platformy.

Jedním z nejúčinnějších komunikačních kanálů v tomto případě jsou krátká videa na platformách YouTube a Instagram, která mají atraktivní vizuální styl a přímý obsah. Tato videa by měla této personě ukazovat konkrétní scénáře, jak vypadá podvodná nabídka na „rychlý zisk“ v kryptoměnách, jak funguje vzdálená správa (např. instalace AnyDesk pod záminkou pomoci) nebo jak rozeznat falešný e-mail od tzv. „investičního poradce“. Video mohou být postavena na reálných případech, které banka řešila, a zakončena jasným poselstvím typu: „*Nenech se nachytat, ověřuj si informace, než klikneš!*“

Kromě vizuálních médií je důležité, aby banka komunikovala svými kanály, jako jsou push notifikace v mobilní aplikaci, na kterou tato persona spoléhá pro každodenní správu financí. Notifikace by měly být stručné, ale jasné. Tato forma je vhodná pro okamžité doručení důležité zprávy v reálném čase, a zároveň personu nezahluje – ideálně by notifikace obsahovala i možnost „kliknout pro více informací“, což by ji odkázalo na blog banky nebo přímo do edukačního rozhraní v aplikaci.

Pro mladší generaci klientů je přirozeným komunikačním nástrojem také interaktivní chatbot integrovaný přímo do mobilního bankovníctví nebo na oficiální web banky. Persona zpravidla nekontaktuje bankovního poradce telefonicky, ale raději si informace vyhledává sama. Chatbot by měl být vybaven konkrétními scénáři, např. „*Mám podezřelý e-mail o investici, co mám dělat?*“ nebo „*Nabízejí mi pomoc s kryptem přes TeamViewer.*“. Důležitá je okamžitá reakce, doporučení ověřených kroků (např. zablokování přístupů, kontaktování IT podpory banky) a odkazy na další obsah. Tento nástroj by zároveň mohl sloužit i jako vstupní bod k e-learningovým modulům zaměřeným na bezpečnost.

9.4 Modelový případ 4

Modelový případ 4 reprezentuje personu označenou jako „Klientka ohrožená romance scamem“. Persona představuje specifickou skupinu klientek, které jsou aktivní na sociálních sítích a online seznamkách a hledají partnerský vztah, přičemž se tím zároveň stávají cílem psychologicky sofistikovaných typů kybernetických podvodů.

Demografie: Persona je žena ve věku 40 let, která aktivně hledá partnerský vztah. Aktivita na sociálních sítích a online seznamkách jí umožňuje být v kontaktu s potenciálními partnery, avšak zároveň ji vystavuje riziku, že se stane obětí podvodných praktik, jako jsou romance scam a sextortion.

Chování: Persona aktivně využívá sociální sítě a online seznamky k navazování nových kontaktů. Její online prezentace je pečlivě sestavená, zveřejňuje fotografie a profily, které odrážejí její zájmy a osobnost. Ráda čte články a sleduje blogy, které jí poskytují rady ohledně vztahů a bezpečnosti v online prostředí.

Rizika: Útočníci často vytvářejí falešné profily, které se tváří jako potenciální partneři, aby získali důvěru persony a následně ji přiměli k finančním převodům nebo ke sdílení citlivých informací. Persona může být snadno zmanipulována příběhy, které se zdají být upřímné, a proto potřebuje mít k dispozici jasné varovné signály, které jí pomohou rozeznat podvodné zprávy.

Komunikační kanály: Upozornění v internetovém bankovníctví, články na bankovním webu, e-mailová varování.

Doporučená prevence:

- **Cílené e-maily s reálnými příběhy obětí:** Tyto e-maily by měly obsahovat konkrétní příklady falešných profilů a podvodných situací, které pomohou personě rozeznat varovné signály a posílit její schopnost se chránit. Emočně rezonují a pomáhají rozpoznat varovné signály podvodu.
- **Varovná upozornění v internetovém bankovníctví a mobilním bankovníctví:** Při provádění transakcí by měla být zobrazena upozornění, která ji varují před neobvyklými platbami a naléhavými výzvami, a to v takovém formátu, který není rušivý, ale informativní.
- **Specializovaná sekce na webu banky:** Tato sekce by měla obsahovat detailní články, videa a další materiály, které jsou dostupné kdykoli a poskytují komplexní informace o podvodech, jejich varovných signálech a způsobech, jak se proti nim bránit.
- **Doporučení na sociálních sítích:** Protože persona pravidelně navštěvuje sociální síť a online seznamky, jsou tyto kanály vhodné k aktivnímu šíření bezpečnostních informací. Krátká videa, grafické příspěvky, zacílené na tuto personu, by měly poskytovat konkrétní varovné signály.

Doporučení pro komunikaci: Persona Klientka ohrožená romance scamem představuje skupinu klientek, které jsou aktivní na sociálních sítích a online seznamkách a hledají partnerský vztah. Právě tato aktivita ji činí zranitelnou vůči tzv. romance scamům a případům sextortion, které patří k psychologicky nejzákladnějším typům podvodů. Útočníci v těchto případech často působí velmi důvěryhodně, vystupují jako zahraniční lékaři, vojáci, vdovci nebo podnikatelé, a po navázání emocionálního kontaktu začnou zneužívat důvěru pro vlastní finanční prospěch.

Vzhledem k jejímu digitálnímu chování – čtení blogů, aktivitě na sociálních sítích a citlivosti na osobní příběhy – je vhodné zaměřit bankovní komunikaci na cílené e-maily s reálnými příběhy jiných obětí, viz Obrázek 12. E-maily by měly být emočně rezonující, vyprávět skutečný scénář, ve kterém se oběť zamilovala do falešného profilu, postupně posílala finance a až pozdě zjistila, že šlo o podvod. Zároveň by měl e-mail jasně poukazovat na varovné signály: příliš rychlé budování důvěry, žádosti o peníze kvůli

„životnímu neštěstí“ nebo snaha přesunout komunikaci mimo oficiální platformy. Tyto příběhy nejen informují, ale i emočně zapojují, což je u této osoby klíčové pro zapamatování.

Dětský domov okradla o miliony. Peníze posílala neexistujícímu námořníkovi



Patrik Biskup
+ sledovat 165



Dnes 13. 8., 14:37 • Plzeň

Naletěla podvodníkovi vydávajícímu se za důstojníka amerického námořnictva a postupně mu poslala přes sedm milionů korun. Padly na to její úspory, brala si půjčky a nakonec okradla o peníze i svého zaměstnavatele.



Obrázek 12 – Článek o oběti romance scamu (Novinky.cz, 2024, online)

Dalším důležitým kanálem jsou varovná upozornění přímo v internetovém a mobilním bankovníctví, která by se měla objevovat v případě, že persona zadává podezřelé platby, např. opakující se částky na zahraniční účty neznámého příjemce nebo převody spojené s naléhavým komentářem. Upozornění by mělo být srozumitelné, neagresivní a mělo by obsahovat konkrétní formulace, jako například: „*Platba na účet v zahraničí, ověřte, zda znáte příjemce. Podvodníci se často vydávají za zahraniční partnery.*“ Cílem není personě zabránit v transakci, ale zastavit ji na okamžik a nabídnout šanci na přehodnocení situace, ideálně s možností kliknout na odkaz „Zjistit více“ vedoucí na oficiální web banky. Právě specializovaná sekce na webových stránkách banky je dalším klíčovým prvkem komunikace. Tato sekce by měla být graficky atraktivní, přehledná a obsahovat články, videa, případové studie a jednoduché kontrolní seznamy (např. „5 signálů, že váš online partner může být podvodník“). Vhodné je zde také umístit možnost stáhnout si PDF brožuru nebo si přehrát instruktážní video.

Další oblastí jsou sociální sítě, které persona denně navštěvuje. Banka by měla využít formát krátkých příspěvků nebo videí cílených konkrétně na prevenci vztahových podvodů. Podobný formát je efektivní i jako placená reklama na Facebooku a Instagramu, kde se tato persona pohybuje nejčastěji. Obsah by měl být srozumitelný, lidský a empatický, nikoliv technokratický či moralizující.

9.5 Modelový případ 5

Modelový případ 5 reprezentuje personu označenou jako „Klient aktivní na online bazarových platformách“, která reflektuje potřeby a rizika klientů využívajících služby jako Bazoš, Sbazar, Vinted nebo Marketplace na Facebooku. Persona reprezentuje skupinu klientů, kteří často provádějí drobné transakce v online prostředí, především v oblasti nákupu a prodeje, a jsou specificky ohroženi reverzními inzerátovými podvody.

Demografie: Persona je muž ve věku 42 let, který má zálibu v autech a aktivně nakupuje a prodává díly na automobily přes online bazary. Je aktivním uživatelem platform jako Bazoš, Sbazar, Vinted a Marketplace na Facebooku. I když je aktivní v oblasti prodeje a nákupu autodílů, příslušenství či jiných produktů, jeho znalosti moderních digitálních nástrojů jsou omezené. Zaměřuje se především na tradičnější formy online bankovníctví a komunikace prostřednictvím e-mailu. Preferuje kombinaci e-mailového varování a zprávy v internetovém bankovníctví, aby informace neminul, ale zároveň nebyly rušivé.

Chování: Persona pravidelně vyřizuje transakce přes internetové bankovníctví a kontroluje e-mail, kam dostává důležitá upozornění. Telefon využívá primárně k volání a SMS, chytré aplikace běžně nepoužívá.

Rizika: Hlavní riziko pro tuto personu spočívá v podvodech spojených s reverzními inzerátovými praktikami. Podvodníci často zasílají falešné e-maily či SMS, které napodobují oficiální komunikaci banky, a varují před naléhavými změnami platebních údajů. Tyto zprávy mohou vnést zmatek a vést k impulzivnímu jednání, což je u osoby riskantní, neboť ne vždy pečlivě ověřuje pravost zasílaných upozornění a nemusí spolehlivě rozpoznat znaky podvodného obsahu.

Doporučená prevence:

- **E-mailová upozornění s ukázkami falešných zpráv:** Poskytování konkrétních příkladů podvodných e-mailů pomůže snadněji rozeznat varovné signály.
- **SMS varování:** Krátké, jasné zprávy, které upozorní na podezřelé transakce, aby persona nezmeškala důležité informace. Např. SMS varování při pokusu

o platbu na podezřelý účet. Persona často reaguje pod časovým tlakem a krátká zpráva ji může zastavit.

- **Doporučení v internetovém bankovníctví:** Zprávy v internetovém bankovníctví, které obsahují konkrétní příklady falešných zpráv a upozorňují na neobvyklé změny platebních údajů.

Doporučení pro komunikaci: Persona Klient aktivní na online bazarových platformách reprezentuje typického klienta, který se aktivně pohybuje na online bazarových platformách jako Bazoš, Sbazar nebo Marketplace na Facebooku, a zaměřuje se na prodej a nákup autodílů a příslušenství. Jeho záliba v autech a transakční aktivita v online prostředí jej staví do rizikové skupiny z hlediska reverzních inzerátových podvodů. Ačkoliv má persona určitou zkušenost s internetem a bankovníctvím, jeho znalosti v oblasti digitální bezpečnosti a nových technologií jsou omezené. Upřednostňuje přehlednost, stručnost a tradiční kanály jako e-mail, SMS a zprávy v internetovém bankovníctví.

Jedním z nejúčinnějších způsobů, jak bankou informovat personu o rizicích, jsou tedy e-mailová upozornění s ukázkami podvodných zpráv. E-maily by měly obsahovat konkrétní, realistické příklady falešných e-mailů a SMS, které se tváří jako notifikace o přijetí platby nebo potvrzení objednávky, viz Obrázek 13. Důraz by měl být kladen na vizuální označení varovných prvků – např. neznámý odesílatel, podvodný odkaz, který údajně vede na stránky „Zásilkovny“, nebo tlačítko „Přijmout platbu“, které ve skutečnosti směřuje na phishingovou stránku banky.



Obrázek 13 - Příklad smishing útoku (vlastní zdroj)

Dále je vhodné využít vnitřní zprávy v internetovém bankovníctví, které může persona zkontrolovat při každém přihlášení. Tyto zprávy by měly obsahovat jak aktuální upozornění, tak i preventivní doporučení. Tato doporučení by měla být pravidelně aktualizována, ideálně doplněna o jednoduchou infografiku, která ukazuje rozdíl mezi pravou a podvodnou zprávou.

Z hlediska stylu komunikace je u této osoby důležité, aby banka vystupovala jako praktický a srozumitelný partner, který přináší jasné rady bez zbytečného balastu. Emoce zde nehrají tak velkou roli jako u osoby výše. Tato persona chce vědět, co přesně má udělat, čemu se vyhnout a kde najde ověřené informace. Klíčem k efektivitě je opakování, názornost a kombinace napříč všemi kanály – e-mailem, SMS i prostředím bankovníctví.

10 ZÁVĚREČNÁ DISKUZE

Získaná zjištění diplomové práce poskytly ucelený pohled na současný stav kybernetické bezpečnosti ve vybraném bankovním subjektu z pohledu ochrany klientů. Ukázalo se, že zabezpečení banky na technické úrovni je robustní, instituce důsledně aplikuje regulační požadavky a má zavedené účinné procesy prevence a detekce útoků. Přímé útoky na bankovní systémy byly dle analýzy vzácné, dominantním problémem však zůstávají útoky využívající sociální inženýrství – phishing, vishing, smishing nebo falešné investiční nabídky. Cílem těchto útoků jsou primárně klienti banky. Výzkum ukázal, že ačkoliv klienti vnímají hrozby a deklarují obezřetnost, často nedokážou rozpoznat konkrétní typy podvodů a postrádají systematický přehled. Komunikační strategie banky se ukázala jako převážně plošná a zaměřená na všechny klienty stejně – nejčastěji prostřednictvím e-mailů, webových stránek a informačních kampaní. Z diskusí však vyplynulo, že klienti by uvítali praktičtější a konkrétnější obsah, například vizuální ukázky podvodů nebo krátká instruktážní videa. Klíčovým zjištěním bylo také to, že kombinace více komunikačních kanálů (např. e-mail a notifikace v mobilním bankovníctví) je účinnější než jednostranná forma, a že načasování a forma sdělení mají zásadní vliv na jeho dopad.

Tato zjištění korespondují s teoretickými východisky práce. V teoretické části byla identifikována hlavní hrozba v podobě sociálního inženýrství a role lidského faktoru jako klíčového zranitelného místa. Práce se opírala o odborné zdroje, které zdůrazňují, že i nejlépe zabezpečené systémy selhávají, pokud jsou uživatelé neinformovaní nebo snadno manipulovatelní. Výsledky řešerši tento předpoklad potvrdily – útoky mířené na klienty se vyskytují výrazně častěji než útoky na samotné systémy. Zároveň se v praxi ukázalo, že i přes množství distribuovaných informací klienti nemusí využít osvětu efektivně, protože jim není přizpůsobena. Teoretická část upozorňovala na význam personalizované komunikace, a praktická část přinesla konkrétní návrh, jak tohoto cíle dosáhnout.

Tvorba cílených person představuje osvědčený a efektivní nástroj pro cílenou BTL komunikaci v rámci metody Service Designu a může významně přispět k optimalizaci preventivní komunikace v oblasti kybernetické bezpečnosti v bankovním sektoru. Využití kombinace datových analýz, behaviorální typologie a zpětné vazby od klientů by mohlo bankám pomoci přizpůsobit strategii jednotlivým skupinám uživatelů na základě jejich zranitelnosti a preferencí. Personalizovaná edukace prostřednictvím preferovaných kanálů

výrazně zvyšuje pravděpodobnost pochopení a přijetí bezpečnostního sdělení. Implementace takového přístupu může významně přispět ke snížení finančních ztrát, posílení důvěry klientů a zvýšení celkové kybernetické odolnosti bankovní instituce. Je však třeba zdůraznit, že tvorba těchto person není zaměřena na stereotypizaci či diskriminaci jednotlivých skupin, ale slouží jako analytický nástroj, který pomáhá lépe porozumět různorodým potřebám klientů. Z pohledu dalšího rozvoje a případného využití návrhu by bylo vhodné, aby daná banka nadále pravidelně vytvářela a aktualizovala persony na základě nově získaných dat, vývoje digitálních hrozeb a změn v chování klientů a čtenosti komunikace, která je v bance datově sledována. Současně by měla být věnována pozornost integraci těchto poznatků do návrhu uživatelského rozhraní internetového a mobilního bankovníctví, včetně testování efektivity různých typů zásahů a forem edukace.

Z hlediska naplnění stanovených výzkumných cílů lze konstatovat, že práce odpověděla na všechny čtyři výzkumné otázky a nabídla konkrétní návrh řešení. Segmentovaný komunikační model, který vznikl na základě výzkumných dat, představuje prakticky využitelný rámec, jenž zohledňuje různorodé potřeby klientů. Mezi přínosy patří především potenciál zvýšení relevance sdělení, vyšší pravděpodobnost porozumění obsahu a posílení důvěry mezi bankou a klientem. Model je zároveň navržen jako flexibilní a otevřený budoucím úpravám, což jej činí adaptabilním na dynamické prostředí kybernetických hrozeb.

I přes přínosné výsledky je však třeba reflektovat některá omezení výzkumu. Výzkumný vzorek byl tvořen klienty jedné banky, kteří byli součástí online komunity a pravděpodobně se více zajímají o bankovní dění než běžný klient. Zjištění proto nelze bez dalšího generalizovat na celou populaci bankovních klientů. Výzkum byl rovněž časově vymezen a reflektuje situaci v konkrétním období, přičemž kybernetické hrozby se rychle vyvíjejí. Omezením může být i subjektivní povaha interpretace kvalitativních dat. Vzhledem k citlivosti tématu rovněž nebylo možné zveřejnit některé konkrétní informace a interní postupy banky, což mohlo omezit míru detailu v některých částech analýzy. Tyto limity však neumenšují hodnotu výsledků, ale spíše ukazují směr dalšího výzkumu – například provedení širšího kvantitativního šetření, ověření modelu v praxi nebo hlubší analýzu právních a technologických aspektů implementace cílené komunikace.

Věřím, že práce nejen splnila svůj akademický účel, ale přinesla i konkrétní návrh řešení s praktickou využitelností, který bude ve vybraném bankovním subjektu dále

rozvíjen. Osvěta v oblasti kybernetické bezpečnosti je klíčovým prvkem obrany proti podvodům a navržený model může být inspirací pro efektivnější a „lidštější“ komunikaci bankovních institucí směrem ke klientům.

ZÁVĚR

Tato diplomová práce se komplexně zabývala problematikou kybernetické bezpečnosti v bankovním sektoru, a to s důrazem na rostoucí počet útoků cílených na klienty bank. V teoretické části byla provedena rešerše týkající se kybernetické bezpečnosti v bankovním sektoru, byly představeny klíčové pojmy, právní rámec kybernetické bezpečnosti včetně aktuálních evropských regulací, a rovněž byly analyzovány nejčastější hrozby, jimž bankovní sektor čelí, zejména ve formě sociálního inženýrství. Tato část tak vytvořila ucelený teoretický rámec pro pochopení současných výzev a přístupů v oblasti ochrany klientů a informačních systémů.

Na teoretický základ navázala praktická část práce, která prostřednictvím kombinace kvalitativních a kvantitativních metod umožnila podrobněji nahlédnout do současné praxe v oblasti zabezpečení, osvěty a komunikace s klienty vybraného bankovního subjektu. Na základě získaných dat byl v aplikační části navržen segmentovaný přístup ke klientům, který by mohl přispět ke zvýšení relevance a účinnosti preventivní komunikace. Tento návrh vychází ze zjištění, že různé skupiny klientů mají odlišné potřeby a způsoby vnímání rizik, a je koncipován jako inspirativní podklad pro případné další rozpracování v praxi.

V rámci výzkumné části byly zodpovězeny všechny čtyři výzkumné otázky. Výsledky ukázaly, že nejčastěji využívané formy útoků (např. phishing, vishing či falešné investice) směřují primárně na klienty, nikoli na technickou infrastrukturu bank. Zároveň bylo potvrzeno, že ačkoliv jsou technická bezpečnostní opatření na vysoké úrovni, samotná edukace a komunikace na klienty je plošná a mohla by být více cílená a diferencovaná. Univerzální přístup snižuje účinnost prevence a může přispívat k chybným reakcím klientů.

Na základě těchto zjištění byl navržen model segmentovaného přístupu ke klientům prostřednictvím pěti typových modelových případů. Tento návrh vychází z kombinace dostupných dat, zpětné vazby klientů a konzultací s odborníky. Slouží jako ilustrativní rámec, který by mohl bankovním institucím pomoci lépe cílit preventivní komunikaci na specifické potřeby různých skupin klientů – např. seniorů, podnikatelů nebo digitálně zdatných uživatelů. Model může sloužit jako inspirace pro další rozpracování či pilotní implementaci v praxi.

Závěrem lze konstatovat, že práce naplnila stanovené cíle a nabídla konkrétní podněty pro zlepšení klientské komunikace v oblasti kybernetické bezpečnosti. Získané poznatky

potvrzují, že kromě technických opatření je třeba klást důraz i na promyšlenou práci s informovaností klientů, která může významně přispět ke zvýšení celkové odolnosti bankovního sektoru vůči kybernetickým hrozbám.

SEZNAM POUŽITÉ LITERATURY A ZDROJŮ

2007 cyberattacks on Estonia. Online. In: Wikipedie. Stránka byla naposledy editována 24. 3. 2024 v 11:22. Dostupné z: https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia [cit. 2025-04-01].

2017 Ukraine ransomware attacks. Online. In: Wikipedie. Stránka byla naposledy editována 14. 3. 2024 v 21:16. Dostupné z: https://en.wikipedia.org/wiki/2017_Ukraine_ransomware_attacks [cit. 2025-04-01].

AUSTRALIAN COMPETITION & CONSUMER COMMISSION. *Targeting scams: report of the ACCC on scams activity 2014*. Online. Canberra: ACCC, 2015. Dostupné z: <https://www.accc.gov.au/system/files/Targeting%20Scams%202014%20report.pdf>. [cit. 2025-04-01].

BISKUP, Patrik. *Dětský domov okradla o miliony. Peníze posílala neexistujícímu námořníkovi*. Online. In: Novinky.cz. 2024. Dostupné z: <https://www.novinky.cz/clanek/krimi-detsky-domov-okradla-o-miliony-penize-posilala-neexistujicimu-namornikovi-40483957>. [cit. 2025-04-20].

CELE, Natile Nonhlanhla a KWENDA, Sheila. Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. Online. *Journal of Financial Crime*, 2024. 2024-12-30. ISSN 1359-0790. Dostupné z: <https://doi.org/10.1108/JFC-10-2023-0263>

COCHRAN, Kodi A. The CIA Triad: Safeguarding Data in the Digital Realm. In: *Cybersecurity Essentials*. Berkeley (CA): Apress, 2024. Dostupné z: https://doi.org/10.1007/979-8-8688-0432-8_2. [cit. 2025-01-23].

ČESKÁ BANKOVNÍ ASOCIACE. Banky loni klientům zachránily téměř 8 miliard korun, kyberútoků meziročně přibylo o čtvrtinu. *Česká bankovní asociace*. Online. 2025. Dostupné z: <https://www.cbaonline.cz/clanky/banky-loni-klientum-zachranily-temer-8-miliard-korun-kyberutoku-mezirocne-pribylo-o-ctvrtinu>. [cit. 2025-03-01].

ČESKÁ NÁRODNÍ BANKA. *Dohled nad finančním trhem*. Online. 2025. Dostupné z: <https://www.cnb.cz/cs/dohled-financi-trh/>. [cit. 2025-04-02].

ČESKÁ NÁRODNÍ BANKA. *Nařízení DORA nabývá účinnosti*. Online. 2025. Dostupné z: <https://www.cnb.cz/cs/cnb-news/aktuality/Narizeni-DORA-nabyva-ucinnosti/>. [cit. 2025-03-16].

ČESKÁ NÁRODNÍ BANKA. *Působnost ČNB podle nařízení o trzích kryptoaktiv (MiCA)*. Online. 2025. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/novinky/pusobnost-cnb_podle_narizeni_o_trzich_kryptoaktiv_mica/. [cit. 2025-03-31].

ČESKÁ NÁRODNÍ BANKA. *Regulace a dohled nad platebními institucemi a institucemi elektronických peněz*. Online. 2025. Dostupné z: <https://www.cnb.cz/cs/dohled-financni-trh/vykon-dohledu/postaveni-dohledu/regulace-a-dohled-nad-platebnimi-institucemi-a-institucemi-elektronickych-penez/>. [cit. 2025-03-25].

ČESKO, 2014. Zákon č. 181 ze dne 23. července 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Online. In: *Zákony pro lidi*. Dostupné z: <https://www.zakonyprolidi.cz/cs/2014-181>. [cit. 2025-04-01].

ČESKO. 1992. Zákon č. 21 ze dne 20. prosince 1991 o bankách. Online. In: *Zákony pro lidi*. Dostupné z: <http://www.zakonyprolidi.cz/cs/1992-21>. [cit. 2025-04-01].

EPRAVO.CZ. *Nové povinnosti bank podle zákona o kybernetické bezpečnosti*. Online. In: *Epravo.cz* [online]. 2017. Dostupné z: <https://www.epravo.cz/top/clanky/nove-povinnosti-bank-podle-zakona-o-kyberneticke-bezpecnosti-106221.html>. [cit. 2025-03-10].

ESET. *Armada Collective launches DDoS attacks against Greek banks*. Online. 2015. Dostupné z: <https://www.welivesecurity.com/2015/12/01/armada-collective-launches-ddos-attacks-greek-banks/> [cit. 2025-03-26].

EUROPEAN CENTRAL BANK. *Speech by Elizabeth McCaul – ECB Banking Supervision: strengthening resilience in an interconnected world*. Online. 2024. Dostupné z: <https://www.bankingsupervision.europa.eu/press/speeches/date/2024/html/ssm.sp241022~8a6df2f788.en.pdf>. [cit. 2025-03-26].

EUROPEAN CENTRAL BANK. *The revised Payment Services Directive (PSD2) and the transition to stronger payments security*. Online. 2018. Dostupné z: https://www.ecb.europa.eu/press/intro/mip-online/2018/html/1803_revisedpsd.en.html. [cit. 2025-03-26].

EUROPEAN UNION AGENCY FOR CYBERSECURITY. *ENISA Threat Landscape: Finance Sector: January 2023 to June 2024*. Online. 2025. Dostupné z: https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf [cit. 2025-03-29].

EUROPOL. *Pandemic profiteering: how criminals exploit the COVID-19 crisis*. Online. 2021. Dostupné z: <https://www.europol.europa.eu/publications-events/publications/pandemic-profiteering-how-criminals-exploit-covid-19-crisis>. [cit. 2025-03-31].

EVROPSKÝ PARLAMENT a RADA EU. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Online. In: *EUR-Lex*. Dostupné z: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L1148>. [cit. 2025-04-01].

EVROPSKÝ PARLAMENT a RADA EU. Directive (EU) 2022/2555 on cybersecurity and network resilience. Online. In: *EUR-Lex*. Dostupné z: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555>. [cit. 2025-04-01].

EVROPSKÝ PARLAMENT a RADA EU. Nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (EU) č. 1093/2010, (EU) č. 1094/2010 a (EU) č. 1095/2010 (nařízení DORA). Online. In: *Úřední věstník Evropské unie*. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?from=EN&uri=CELEX%3A32022R2554>. [cit. 2025-03-31].

EVROPSKÝ ÚČETNÍ DVŮR. *Kybernetická bezpečnost orgánů, institucí a jiných subjektů EU: úroveň připravenosti obecně není úměrná hrozbám*. Online. 2022. Dostupné z: <https://op.europa.eu/webpub/eca/special-reports/hack-proofing-eu-institutions-05-2022/cs/>. [cit. 2025-02-18].

FATF. *Lithuania*. Online. 2024. Dostupné z: <https://www.fatf-gafi.org/en/countries/detail/Lithuania.html>. [cit. 2025-03-31].

FATF. *Ukraine*. Online. 2022. Dostupné z: <https://www.fatf-gafi.org/en/countries/detail/Ukraine.html>. [cit. 2025-03-31].

CHANDER, Anupam, 2020. Is Data Localization a Solution for Schrems II? *Journal of International Economic Law*. Online. Vol. 23, no. 3, s. 771–784. Dostupné z: <https://doi.org/10.1093/jiel/jgaa024>. [cit. 2025-04-01].

JANOVEC, Michal. *Finanční trh a jeho stabilita*. Právní monografie. Praha: Wolters Kluwer, 2023. ISBN 978-80-7676-597-9.

JIRÁSEK, Petr, NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti*. 3. aktualizované vydání. Praha: AFCEA, 2015. Online. Dostupné z: https://afcea.cz/wp-content/uploads/2015/03/Slovník_Final_screen_v2_0.pdf. [cit. 2025-02-18].

KASPERSKY. The Great Bank Robbery: Carbanak cybergang steals \$1bn from 100 financial institutions worldwide. Online. 2015. Dostupné z: <https://www.kaspersky.com/about/press-releases/the-great-bank-robbery-carbanak-cybergang-steals-1bn-from-100-financial-institutions-worldwide>. [cit. 2025-03-29].

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

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

KOMERČNÍ BANKA, a. s. *Historie KB*. Online. 2025. Dostupné z: <https://www.kb.cz/cs/o-bance/historie-kb>. [cit. 2025-01-23].

KOMERČNÍ BANKA, a. s. *Komerční banka spouští inovativní kampaň na podporu kyberbezpečnosti a prevence proti rizikům finančních podvodů*. Online. 2025. Dostupné z: <https://www.kb.cz/cs/o-bance/tiskove-zpravy/komercni-banka-spousti-inovativni-kampan-na-podporu-kyberbezpecnosti-a-prevence-proti-rizikum-financ>. [cit. 2025-04-01]

KOMERČNÍ BANKA, a. s. *Kybernetická bezpečnost*. Online. 2025. Dostupné z: <https://www.kb.cz/cs/podpora/bezpecnost>. [cit. 2025-03-31].

KOMERČNÍ BANKA, a. s. *Výroční finanční zpráva 2023*. Online. 2024. Dostupné z: <https://www.kb.cz/getmedia/460b8633-cb30-4b55-a9b6-902a495a6f8a/Vyrocní-zpráva-KB-2023.pdf>. [cit. 2025-01-23].

KOMERČNÍ BANKA, a. s.. *KB 3Q & 9M 2023 results and KB 2025 strategy update*. Online. 2023. Dostupné z: <https://www.kb.cz/getmedia/c0cdebc9-1fe3-4e5e-870e-0c44f365ff92/KB-Results-3Q2023-cz.pdf>. [cit. 2025-01-23].

KOPP, Kelly, SILLITOE, Steve, GONDAL, Sadia a LAYTON, Robyn, 2016. Perceptions of vulnerability to online romance scams. *Journal of Psychology and Educational Research*. Online. Roč. 24, č. 2, s. 144–161. Dostupné z: https://www.marianjournals.com/files/JPER_articles/JPER_24_2_2016/Kopp_Sillitoe_Gondal_Layton_JPER_2016_24_2_144_161.pdf. [cit. 2025-04-01].

KURZY.CZ. T-Mobile: Meziroční nárůst bezpečnostních incidentů o 36 % i největší útok v historii – rok 2024 v kostce. *Kurzy.cz*. Online. 2025. Dostupné z: <https://zpravy.kurzy.cz/801938-t-mobile-mezirocni-narust-bezpecnostnich-incidentu-o-36-i-nejvetsi-utok-v-historii--rok-2024-v/>. [cit. 2025-04-02].

Mager, B., & Sung, T. J. (2011). *Special issue editorial: Designing for services*. *International Journal of Design*, 5(2), 1-3.

MAREŠ, Petr. *Kyberkultura, hackeři a digitální revoluce: Informace chce být svobodná*. Praha: Grada, 2022. ISBN 978-80-271-4900-1.

MEJSTŘÍK, Michal; PEČENÁ, Magda a TEPLÝ, Petr. *Bankovníctví v teorii a praxi*. Praha: Karolinum, 2014. ISBN 978-80-246-2870-7.

MIMECAST. *What is CEO fraud?* Online. 2025. Dostupné z: <https://www.mimecast.com/content/what-is-ceo-fraud/>. [cit. 2025-03-31].

MINISTERSTVO FINANCÍ ČESKÉ REPUBLIKY. *Důvodová zpráva k návrhu zákona, kterým se mění zákon č. 6/1993 Sb., o České národní bance, ve znění pozdějších předpisů, a další související zákony*. Online. 2012. Dostupné z: https://www.mfcr.cz/assets/attachments/Duvodova-zprava_2012-01-06_Duvodova-zprava.pdf. [cit. 2025-03-09].

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *NÚKIB v roce 2024 zaznamenal více kybernetických incidentů než v předchozích letech*. Národní úřad pro kybernetickou a informační bezpečnost. Online. 2025. Dostupné z: <https://nukib.gov.cz/cs/infoservis/aktuality/2215-nukib-v-roce-2024-zaznamenal-vice-kybernetickych-incidentu-nez-v-predchozich-letech>. [cit. 2025-04-02].

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Průvodce novým zákonem o kybernetické bezpečnosti*. Online. Dostupné z: <https://portal.nukib.gov.cz/pruvodce-novym-zakonem-o-kyberneticke-bezpecnosti>. [cit. 2025-03-16].

NOVINKY.CZ. *Podvodníci to zkouší znovu. Přes tyto weby se snažili napálit důvěřivce.* 2024. Online. Dostupné z: <https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-podvodnici-to-zkousi-znovu-pres-tyto-weby-se-snazili-napalit-duverivce-40472565>. [cit. 2025-03-05].

OFFICE OF THE COMPTROLLER OF THE CURRENCY. *Cybersecurity: A Self-Assessment Resource for Banks and Financial Institutions.* Online. Washington, D.C.: U.S. Department of the Treasury, 2022. Dostupné z: <https://www.occ.gov/publications-and-resources/publications/cybersecurity-and-financial-system-resilience/files/pub-2022-cybersecurity-report.pdf>. [cit. 2025-03-26].

OTTIS, Rain. *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.* Online. Tallinn: Cooperative Cyber Defence Centre of Excellence, 2008. Dostupné z: https://www.ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf [cit. 2025-03-29].

PORADA, Viktor a RAIS, Karel. Právní, kriminalistické a kybernetické aspekty kybernetické kriminality a bezpečnosti: pocta Vladimíru Smejkalovi. Brno: Akademické nakladatelství CERM, 2021. ISBN 978-80-7623-065-1.

ROHMEYER, Paul a BAYUK, Jennifer L. *Financial Cybersecurity Risk Management: Leadership Perspectives and Guidance for Systems and Institutions.* New York: Apress, 2018. ISBN 987-1-4842-4193-6.

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

SEMENYUTA, O. G. a SHAPIRO, I. E. Risks of banking transformation in digitalization. In: MAKARENKO, E. N., VOVCHENKO, N. G. a TISHCHENKO, E. N., eds. *Technological trends in the AI economy. Smart Innovation, Systems and Technologies.* Vol. 625. Singapore: Springer, 2023. ISBN 978-981-19-7411-3. Dostupné z: https://doi.org/10.1007/978-981-19-7411-3_38. [cit. 2025-01-23].

SOCIÉTÉ GÉNÉRALE. *Komerční banka startuje Novou éru bankovníctví.* Online. 2023. Dostupné z: <https://www.societegenerale.com/en/news/newsroom/kb-change-2025>. [cit. 2025-01-23].

ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

TANKER. *End-to-end encryption is the future of GDPR compliance*. Online. 2018. Dostupné z: <https://medium.com/tanker-blog/end-to-end-encryption-is-the-future-of-gdpr-compliance-7700022257e4>. [cit. 2025-03-26].

TUYTEL, Paul. *What is invoice fraud?* Online. BILL Learning Center, 2023. Dostupné z: <https://www.bill.com/learn/fraud/what-is-invoice-fraud>. [cit. 2025-03-31].

VIPIN, C., RAJARAJESWARI, P., HARSHIT, S., KUMAR, K. S., KRISHNADEV, G. a GAFTANDZHIEVA, S. An in-depth examination of man-in-the-middle attacks and their impact on cybersecurity. In: KIN SHUN WONG, Thomas a KAPPALA, Venkata Kiran, eds. *6G Communications Networking and Signal Processing. SGCNSP 2023*. Lecture Notes in Electrical Engineering, vol. 1270. Singapore: Springer, 2025. Dostupné z: https://doi.org/10.1007/978-981-97-7876-8_25. [cit. 2025-01-23].

Vláda České republiky. *Kybernetická bezpečnost*. Online. 2021. Dostupné z: https://vlada.gov.cz/cz/evropske-zalezitosti/umela-inteligence/kyberneticka_bezpecnost/kyberneticka-bezpecnost-192766/#. [cit. 2025-04-19].

WILSON, Tracy V. *How phishing works*. Online. Dostupné z: <https://computer.howstuffworks.com/worst-computer-viruses.htm>. [cit. 2025-04-02].

SEZNAM OBRÁZKŮ

Obrázek 1 - Četnost podvodů dle typu v letech 2018-2024 (KB, interní zdroj, 2025).....	55
Obrázek 2 – Směřování podvodných transakcí v roce 2020 (KB, interní zdroj, 2025).....	56
Obrázek 3 - Směřování podvodných transakcí v roce 2021 (KB, interní zdroj, 2025)	57
Obrázek 4 - Četnost věkových kategorií (KB, interní zdroj, 2025)	57
Obrázek 5 - Počty podvodů v jednotlivých krajích (KB, interní zdroj, 2025).....	58
Obrázek 6 – Schéma procesu zpracování podezřelé platby (KB, interní zdroj, 2025)	59
Obrázek 7 - BTL komunikace bezpečnostních prvků (E-mailová komunikace KB zaslaná klientům, 2022)	63
Obrázek 8 – Zkušenost respondentů s kyberpodvody (KB, interní zdroj, 2025).....	66
Obrázek 9 – Preferovaný zdroj informací (KB, interní zdroj, 2025)	68
Obrázek 10 - Příklad phishingu (vlastní zdroj)	72
Obrázek 11 – Příklad fake invoice (vlastní zdroj)	75
Obrázek 12 – Článek o oběti romance scamu (Novinky.cz, 2024, online).....	80
Obrázek 13 - Příklad smishing útoku (vlastní zdroj)	83

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AI	Artificial Intelligence
APT	Advanced Persistent Threat
APT	Advanced Pesistent Thread
ATL	Above The Line
BIS	Bank for International Settlements
BTL	Below The Line
C&C	Command and Control
CASP	Crypto-Asset Service Provider
CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CSP	Customer Security Programme
ČBA	Česká bankovní asociace
DDoS	Distributed Denial of Service
DDoS	Distributed Denial of Service
DLP	Data Loss Prevention
DNS	Domain Name Systém
DORA	Digital Operational Resilience Act
EBA	European Banking Authority
EDR	Endpoint Detection and Response
ENISA	European Union Agendy for Cybersecurity
ESCB	European System of Central Banks
ESD	Electronic Software Distribution
ESMA	European Securities and Markets Authority
EU	Evropská unie
FDS	Fraud Detection Systém

FS-ISAC	Financial Services Information Sharing and Analysis Center
ICMP	Internet Control Message Protocol
ICP/IP	Internet Communication Protocol/Internet Protocol
ICT	Information and Communication Technologies
IRP	Incident Response Plan
IT	Information Technology
KB	Komerční banka, a. s.
KII	Kritické informační infrastruktury
MFA	Multi-Factor Authentication
MiCA	Markets in Crypto-Assets Regulation
MitM	Man-in-the-Middle
MVP	Minimum Viable Product
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
P2P	Peer-to-peer
PCI-DSS	Payment Card Industry Data Security Standard
PČR	Policie České republiky
PSD2	Payment Services Directive 2
SG	Société Générale
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SMS	Short Message Service
SOC	Security Operations Center
SWIFT	Society for Worldwide Interbank Financial Telecommunication

TIP	Threat Intelligence Platformy
TLPT	Threat-Led Penetration Testing
TLS/SSL	Transport Layer Security/Secure Sockets Layer
USA	United States of America
VOIP	Voiceover Internet Protocol

