VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

KYBERNETICKÁ KRIMINALITA ZAMĚŘENÁ NA BANKOVNÍ KLIENTY A MOŽNOSTI JEJÍ PREVENCE

Autor práce: Martin Dostál

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: RNDr. Růžena Ferebauerová

Katedra: Katedra právních oborů a bezpečnostních studií

2026

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 1632/5b, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

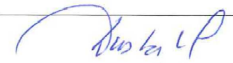
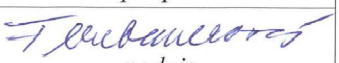
Jméno a příjmení studenta: Martin Dostál

Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: České Budějovice

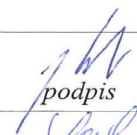
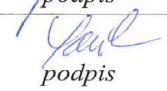
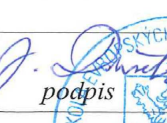
Název bakalářské práce: Kybernetická kriminalita zaměřená na bankovní klienty a možnosti její prevence
Název bakalářské práce v anglickém jazyce: Cybercrime Targeting Bank Clients and Ways to Prevent It

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, včetně titulů):
RNDr. Růžena Ferebauerová
Datum zadání bakalářské práce: duben 2025

Cíl bakalářské práce:
Hlavním cílem bakalářské práce je zhodnotit osobní zkušenosti klientů bank s preventivními opatřeními proti kybernetickým útokům a porovnat je s realně aplikovanými preventivními mechanismy ze strany bankovních institucí.
Vedlejším cílem je zhodnotit aktuální vývoj v oblasti kybernetických útoků, identifikovat jejich nejčastější formy a stanovit nejzranitelnější oblasti z pohledu kybernetické bezpečnosti bank a jejich klientů

Student: Martin Dostál	30. 4. 2025 *datum*	 *podpis*
Vedoucí práce: RNDr. Růžena Ferebauerová	27. 5. 2025 *datum*	 *podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	27. 5. 2025 *datum*	 *podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	27. 5. 2025 *datum*	 *podpis*
Rektor: doc. Ing. Jiří Dušek, Ph.D.	2. 6. 2025 *datum*	 *podpis*

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

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

.....

Děkuji vedoucí bakalářské práce, RNDr. Růženě Ferebauerové, za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

DOSTÁL, M. *Kybernetická kriminalita zaměřená na bankovní klienty a možnosti její prevence: bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, 2026. 69 s. Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová

Klíčová slova: kybernetická kriminalita, bankovní klient, sociální inženýrství, phishing, prevence, bankovní bezpečnost

Bakalářská práce zkoumá problematiku kybernetické kriminality cílené na bankovní klienty a na možnosti její prevence. Cílem práce je zhodnotit zkušenosti bankovních klientů s preventivními opatřeními proti kybernetickým útokům a porovnat je s preventivními mechanismy uplatňovanými bankovními institucemi. Teoretická část práce vychází z odborné literatury, platné právní úpravy a obecných poznatků z praxe autora a zaměřuje se na vymezení základních pojmů, nejčastější formy kybernetických útoků a jejich trestněprávní kvalifikaci. Praktická část je zpracována formou kvalitativního výzkumu, konkrétně prostřednictvím rozhovorů s osobami poškozenými kybernetickými útoky a se zástupcem vybrané bankovní instituce. Výsledkem práce je zhodnocení současného stavu prevence kybernetické kriminality a identifikace prostorů pro její zlepšení.

ABSTRACT

Dostál, M. L. *Cybercrime Targeting Bank Clients and Ways to Prevent It: Bachelor Thesis.* České Budějovice: The College of European and Regional Studies, 2026. 69 pp. RNDr. Růžena Ferebauerová

Key words: cybercrime, banking client, social engineering, phishing, prevention, banking security

This bachelor's thesis examines the issue of cybercrime targeting bank clients and the possibilities of its prevention. The aim of the thesis is to evaluate the experiences of bank clients with preventive measures against cyber attacks and to compare them with the preventive mechanisms applied by banking institutions in practice. The theoretical part of the thesis is based on professional literature, valid legal regulations and general knowledge from the author's professional practice. It focuses on the definition of basic concepts, the most common forms of cyber attacks and their legal qualification from the perspective of criminal law. The practical part is carried out in the form of qualitative research, specifically through interviews with persons who have been victims of cyber attacks and with a representative of a selected banking institution. The result of the thesis is an evaluation of the current state of cybercrime prevention and the identification of areas in which this prevention could be improved.

Obsah

Úvod

Rozvoj informačních a komunikačních technologií v posledních desetiletích zásadně proměnil způsob fungování moderní společnosti. Digitalizace finančních služeb umožnila bankovním klientům provádět většinu finančních operací prostřednictvím internetového nebo mobilního bankovnictví rychle a pohodlně bez nutnosti osobní návštěvy bankovní pobočky. Současně s těmito technologickými změnami však dochází také k rozvoji nových forem trestné činnosti, které využívají prostředí kybernetického prostoru.

Kybernetická kriminalita představuje specifickou oblast trestné činnosti, která je realizována prostřednictvím informačních technologií nebo se odehrává v prostředí počítačových sítí. Jednou z oblastí, která je těmito útoky výrazně zasažena, je bankovní sektor a zejména bankovní klienti využívající elektronické bankovní služby. Pachatelé se v těchto případech zaměřují především na získání přístupových údajů k internetovému bankovnictví nebo údajů k platebním prostředkům, přičemž často využívají metody sociálního inženýrství založené na manipulaci s lidským chováním.

Současná praxe ukazuje, že kybernetické útoky zaměřené na bankovní klienty se vyznačují kombinací technických prostředků a psychologické manipulace. Pachatelé využívají například podvodné internetové stránky, falešné e-maily, SMS zprávy nebo telefonické hovory, jejichž prostřednictvím se vydávají za pracovníky bank, přepravních společností nebo jiných institucí. Cílem těchto útoků je přimět oběť k tomu, aby sama poskytla citlivé údaje nebo provedla finanční transakci, která následně vede k neoprávněnému převodu finančních prostředků.

Problematika kybernetické kriminality zaměřené na bankovní klienty je proto v současnosti předmětem zájmu bankovních institucí, orgánů činných v trestním řízení i dalších subjektů podílejících se na prevenci kriminality. Banky zavádějí stále sofistikovanější bezpečnostní mechanismy a současně realizují preventivní kampaně zaměřené na informovanost veřejnosti. Praxe však ukazuje, že významnou roli při úspěšnosti těchto útoků hraje lidský faktor, zejména důvěřivost nebo nedostatečná informovanost uživatelů bankovních služeb.

Tato bakalářská práce se zabývá problematikou kybernetické kriminality zaměřené na bankovní klienty a možnostmi její prevence. Teoretická část práce se zaměřuje na vymezení základních pojmů, popis nejčastějších forem kybernetických útoků a jejich právní kvalifikaci z pohledu trestního práva. Praktická část práce je založena na kvalitativním výzkumu realizovaném prostřednictvím rozhovorů s osobami, které se staly obětí kybernetického podvodu, a s pracovníkem bankovní instituce zabývajícím se prevencí bankovních podvodů. Získané poznatky jsou následně analyzovány s cílem poukázat na možnosti zvyšování efektivity prevence kybernetické kriminality.

1. Cíl a metodika bakalářské práce

Cílem bakalářské práce je zhodnotit osobní zkušenosti bankovních klientů s preventivními opatřeními proti kybernetickým útokům a porovnat je s reálně aplikovanými preventivními mechanismy ze strany bankovních institucí. Vedlejším cílem práce je analyzovat aktuální vývoj kybernetické kriminality, identifikovat její nejčastější formy a vymezit nejzranitelnější oblasti z pohledu kybernetické bezpečnosti bank a jejich klientů.

Práce je rozdělena na teoretickou a praktickou část. Teoretická část je zpracována na základě odborné literatury, platné právní úpravy a dostupných odborných zdrojů a je doplněna o obecné poznatky z aplikační praxe autora v oblasti vyšetřování kybernetické trestné činnosti. Zaměřuje se na vymezení základních pojmů, typizaci nejčastějších forem kybernetických útoků a jejich právní kvalifikaci z pohledu trestního práva.

Praktická část je realizována formou kvalitativního výzkumu, konkrétně prostřednictvím polostrukturovaných rozhovorů s osobami poškozenými kybernetickými útoky a se zástupcem vybrané bankovní instituce. Cílem této části je poukázat na rozdíly mezi schopností bankovních klientů rozpoznat kybernetické hrozby a úrovní preventivních opatření, které banky uplatňují. Na základě získaných poznatků jsou v závěru práce navrhnuta doporučení směřující ke zvýšení efektivity prevence kybernetické kriminality.

Rozhovory byly realizovány v souladu se základními etickými principy kvalitativního výzkumu. Všichni účastníci byli před zahájením rozhovoru seznámeni s účelem výzkumu, způsobem zpracování získaných informací a s tím, že jejich účast je dobrovolná. Zároveň byli také informováni o anonymizaci osobních údajů a skutečnosti, že získaná data budou využita výhradně pro účely této bakalářské práce.

2. Vymezení základních pojmů

Pro správné pochopení problematiky kybernetické kriminality zaměřené na bankovní klienty je nezbytné vymezit základní pojmy, se kterými tato bakalářská práce pracuje. Oblast kybernetické kriminality v oblasti bankovního sektoru je specifická svou interdisciplinární povahou, neboť se v ní prolínají prvky trestního práva, informačních technologií, bankovnictví a prevence kriminality. Cílem této kapitoly je vytvořit terminologický rámec, který bude sloužit jako teoretický základ pro další části práce. Vymezení pojmů se zaměřuje zejména na pojmy související s kybernetickou kriminalitou, bankovními službami, platebními prostředky, sociálním inženýrstvím a prevencí kriminality, a to v rozsahu nezbytném pro naplnění cílů bakalářské práce.

2.1 Kriminalita

Kriminalita je v kriminologickém pojetí chápána jako souhrn trestných činů, které se vyskytují ve společnosti v určitém časovém a prostorovém rámci, přičemž nejde pouze o součet jednotlivých skutků, ale o komplexní společenský jev. Tento jev je výsledkem působení celé řady faktorů, které vycházejí jak z individuální roviny jednání pachatelů, tak ze širších společenských podmínek, v nichž trestná činnost vzniká a realizuje se. Kriminalita proto není izolovaným fenoménem, ale je úzce propojena s fungováním společnosti jako celku.[1]

2.2 Počítačový systém

Z technického hlediska lze počítačový systém chápat jako funkční celek složený z hardwaru, softwaru a dat, který je schopen automatizovaného zpracování informací. Tento celek může fungovat samostatně, nebo může být součástí rozsáhlejší sítě dalších systémů. V současné digitální společnosti přitom počítačové systémy nejsou omezeny pouze na klasické stolní počítače, ale zahrnují také servery, mobilní telefony, platební terminály, bankovní systémy, cloudová úložiště či další zařízení propojená prostřednictvím komunikačních sítí. [2]

[1] SCHEINOST, Miroslav. *Kriminalita očima kriminologů*. Praha: Institut pro kriminologii a sociální prevenci, 2010. s. 7-8.
[2] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. s. 57-59.

Právní vymezení pojmu počítačový systém vychází zejména z trestněprávní úpravy, která s tímto pojmem pracuje v souvislosti s trestnými činy páchanými v kyberprostoru. Trestní zákoník chápe počítačový systém jako soubor zařízení, která slouží ke zpracování dat, včetně programového vybavení a uložených informací. Toto vymezení je záměrně koncipováno tak, aby bylo schopno postihnout nejen současné technologické prostředky, ale i jejich vývoj do budoucna.[3]

V kontextu kybernetické kriminality má počítačový systém zásadní význam, neboť může vystupovat v několika rolích současně. Může být přímým cílem útoku, například při neoprávněném přístupu k bankovnímu účtu, prostředkem ke spáchání trestné činnosti, například při zneužití škodlivého softwaru, nebo prostředím, ve kterém je trestná činnost prováděna, typicky v případě online podvodů.

2.3 Kybernetický prostor

Kybernetický prostor lze chápat jako prostředí tvořené propojenými informačními a komunikačními systémy, v němž dochází k přenosu, zpracování a ukládání dat. Toto prostředí není pouze technické povahy, ale zahrnuje také uživatele a jejich interakce, čímž se stává komplexním sociálně-technickým prostorem. Kybernetický prostor je dnes nedílnou součástí fungování společnosti a jeho bezpečnost je zásadní pro ochranu informací, majetku i samotných uživatelů.[4]

Z hlediska bezpečnosti a práva je podstatné, že kybernetický prostor se vyznačuje specifickými vlastnostmi, které jej odlišují od prostředí fyzického světa. Patří mezi ně zejména vysoká míra anonymity, snadná dostupnost, rychlost šíření informací a obtížná identifikace pachatelů protiprávního jednání. Tyto charakteristiky vytvářejí příznivé podmínky pro páchání trestné činnosti, neboť pachatelé mohou využívat technologické prostředky k maskování své identity a ke komplikování procesu odhalování a dokazování.[5]

2.4 IP adresa

IP adresa (Internet Protocol address) představuje jedinečný číselný identifikátor zařízení připojeného k počítačové síti, který umožňuje vzájemnou komunikaci mezi

[3] Zákon č. 40/2009 Sb., trestní zákoník, § 136a – Počítačový systém
[4] KOLOUCH, Jan a kol. *CyberSecurity.* Praha: CZ.NIC, 2019, s. 15–20.
[5] KOLOUCH, Jan a kol. *CyberSecurity.* Praha: CZ.NIC, 2019, s. 21-25.

zařízeními v rámci internetu. Prostřednictvím IP adresy je možné směrovat datové přenosy a určit, odkud a kam jsou data odesílána. IP adresa je základním technickým prvkem síťové komunikace, avšak sama o sobě neidentifikuje konkrétní fyzickou osobu, ale pouze zařízení nebo síťové rozhraní.[6]

Z hlediska kybernetické bezpečnosti má IP adresa význam především jako jeden z identifikátorů síťové komunikace, který je využíván při monitorování přístupů k informačním systémům, detekci podezřelého chování a vyhodnocování bezpečnostních incidentů. V prostředí elektronického bankovnictví je IP adresa jedním z údajů, na jejichž základě mohou bankovní systémy posuzovat rizikovost přihlášení uživatele.[7]

2.4.1 Veřejná a soukromá IP adresa

Veřejná IP adresa je IP adresa, která je viditelná v rámci internetu a umožňuje zařízení komunikovat s jinými zařízeními mimo lokální síť. Tato adresa je obvykle přidělována poskytovatelem internetového připojení a je využívána při komunikaci se vzdálenými servery, včetně bankovních systémů. Naproti tomu soukromá IP adresa slouží k identifikaci zařízení uvnitř lokální sítě a není přímo dostupná z internetu.[8]

Rozlišení veřejné a soukromé IP adresy je důležité zejména z hlediska bezpečnosti, neboť bankovní systém obvykle zaznamenává pouze veřejnou IP adresu, ze které se uživatel připojuje. To může mít vliv na možnosti identifikace původu připojení a vyhodnocování rizikového chování.[9]

2.4.2 Statická a dynamická IP adresa

Statická IP adresa je dlouhodobě neměnná IP adresa, která je trvale přiřazena konkrétnímu zařízení nebo připojení. Tento typ adresy je typický například pro některá firemní nebo serverová připojení. Dynamická IP adresa se naopak pravidelně mění a je přidělována poskytovatelem připojení z dostupného rozsahu adres.[10]

V praxi je dynamická IP adresa běžná u domácích a mobilních připojení. Z hlediska bankovních systémů a bezpečnostního hodnocení přihlášení to znamená, že

[6] KOLOUCH, Jan a kol. *CyberSecurity.* Praha: CZ.NIC, 2019, s. 70–75.
[7] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. s. 63-64.
[8] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. s. 65-66.
[9] KOLOUCH, Jan a kol. CyberSecurity. Praha: CZ.NIC, 2019, s. 75–80.
[10] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. s. 67-68.

změna IP adresy nemusí nutně signalizovat podvodné jednání, ale může být běžným důsledkem technického nastavení připojení.[11]

2.5 VPN (virtuální privátní síť)

VPN (Virtual Private Network) je technologie, která umožňuje vytvoření šifrovaného spojení mezi uživatelem a vzdálenou sítí, kdy skutečná IP adresa uživatele je vůči cílovému systému skryta. Uživatel se při využití VPN jeví jako připojený z jiné IP adresy, často z jiné geografické lokace, než ve které se fyzicky momentálně nachází.[12]

Použití VPN má legitimní využití, například při ochraně soukromí, zabezpečení komunikace na veřejných sítích nebo při práci na dálku. Zároveň však může být VPN zneužívána k maskování skutečného původu připojení, což komplikuje identifikaci pachatele kybernetické kriminality. V prostředí elektronického bankovnictví je připojení přes VPN často vyhodnocováno jako rizikovější, zejména pokud je spojeno se zahraniční IP adresou nebo s náhlou změnou přístupových údajů.[13]

Z pohledu kybernetické bezpečnosti je VPN považována za anonymizační nástroj, který může být použit jak legitimně, tak i k páchání protiprávního jednání. Samotné použití VPN proto nelze automaticky považovat za nezákonné, avšak v kombinaci s dalšími faktory může představovat významný bezpečnostní indikátor.[14]

2.6 Geolokace IP adresy

Geolokace IP adresy představuje odhad geografické polohy zařízení nebo sítě na základě IP adresy, obvykle na úrovni státu, regionu nebo města. Tento odhad je založen na databázích spravovaných specializovanými poskytovateli a neumožňuje přesné určení fyzické polohy uživatele.[15]

V bankovním prostředí je geolokace IP adresy využívána jako nástroj pro hodnocení rizikovosti přihlášení, například při detekci přístupů ze zahraničí nebo z neobvyklých lokalit. Je však nutné zdůraznit, že geolokace IP adresy je zatížena řadou

[11] KOLOUCH, Jan a kol. *CyberSecurity*. Praha: CZ.NIC, 2019, s. 80–85.
[12] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. s. 102-104.
[13] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. s. 105-106.
[14] JIRÁSEK, Petr – NOVÁK, Luděk – POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti.* 6. doplněné a upravené elektronické vydání. Praha: Centrum kybernetické bezpečnosti, z. ú., 2025, s. 23, 122, 383.
[15] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. s. 72-74.

nepřesností, zejména v případě mobilních datových připojení, sdílených IP adres nebo použití VPN.[16]

2.7 Kybernetická kriminalita

V odborné literatuře se lze setkat s různými označeními tohoto jevu, například kyberkriminalita, kybernalita, kybernetická kriminalita nebo kybernetická trestná činnost. Tyto pojmy jsou zpravidla používány jako synonyma, přičemž jejich společným znakem je vazba na kyberprostor a informační technologie. Kolouch poukazuje na to, že kyberkriminalitu lze obecně chápat jako trestnou činnost, která se odehrává prostřednictvím počítačových sítí a informačních systémů a která zasahuje do chráněných společenských vztahů, zejména v oblasti majetku, soukromí a osobních údajů.[17]

Kybernetická kriminalita označuje takové jednání, které je v rozporu s právními předpisy nebo s obecně uznávanými morálními normami společnosti. Může být zaměřena přímo proti počítačovým systémům, jejich technickým či programovým součástem, uloženým datům nebo počítačovým sítím. Současně se však může jednat i o případy, kdy počítač nebo informační systém vystupuje pouze jako prostředek k páchání trestné činnosti, případně kdy počítačové sítě a k nim připojená zařízení tvoří prostředí, v němž k protiprávnímu jednání dochází. Specifikem kyberprostoru je skutečnost, že veškeré dění v tomto prostředí je pro člověka přímo nepozorovatelné a lze jej vnímat pouze prostřednictvím technických zařízení a nástrojů, které umožňují přístup k informačním a komunikačním technologiím.[18]

Kybernetickou kriminalitu lze také charakterizovat jako protiprávní jednání, které je pácháno prostřednictvím informačních a komunikačních technologií nebo je na tyto technologie zaměřeno. V současné době dochází k jejímu dynamickému rozvoji, který souvisí s rostoucí digitalizací společnosti a závislostí na informačních systémech. Z pohledu kybernetické bezpečnosti je přitom nutné vnímat nejen samotnou trestnou činnost, ale i zranitelnosti systémů a lidský faktor, který bývá často nejslabším článkem ochrany.[19]

[16] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. s. 75-76.
[17] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. s. 36-41.
[18] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. s. 91.
[19] KOLOUCH, Jan a kol. *CyberSecurity*. Praha: CZ.NIC, 2019, s. 35–40.

2.8 Kybernetický útok

Kybernetický útok lze obecně vymezit jako úmyslné jednání v kybernetickém prostoru, jehož cílem je narušení bezpečnosti informačních a komunikačních systémů, ohrožení dostupnosti, integrity nebo důvěrnosti informací, případně zneužití těchto systémů k dalšímu protiprávnímu jednání. Kybernetické útoky jsou charakteristické tím, že jsou realizovány prostřednictvím informačních technologií a mohou být vedeny jak proti technickým prostředkům, tak proti uživatelům těchto systémů.[20]

V kontextu této bakalářské práce je kybernetický útok chápán jako projev kybernetické kriminality, který se dotýká bankovních klientů. Kybernetické útoky představují zásadní riziko zejména v prostředí elektronického bankovnictví, kde mohou vést k neoprávněnému přístupu k účtům, zneužití platebních prostředků a tím i k finančním ztrátám.

2.9 Kybernetická bezpečnost

Obecně lze kybernetickou bezpečnost chápat jako soubor opatření založených na koordinovaném využívání lidských zdrojů, nastavených procesů a technických prostředků, jejichž cílem je předcházet kybernetickým útokům, včas je odhalovat a adekvátně na ně reagovat, zejména v případech, kdy dochází k ohrožení nebo narušení důvěrnosti, integrity či dostupnosti informací a dat v rámci informačních systémů nebo poskytovaných služeb.[21]

2.10 Prevence kriminality

Tento pojem je obecně chápán jako aktivní přístup ke kontrole kriminality, který je založen převážně na uplatňování nerepresivních nástrojů. Jejím cílem je omezování sociálně patologických jevů a současně snižování motivace i příležitostí k páchání trestné činnosti. Na realizaci preventivní politiky se kromě orgánů činných v trestním řízení, mezi něž patří justice, policie, státní zastupitelství, soudy a vězeňská služba, podílejí rovněž další subjekty, zejména nerepresivní orgány veřejné správy, zájmová sdružení, církve, podnikatelské subjekty a samotní občané. Prevence kriminality tak společně s represí tvoří nedílnou součást trestní politiky státu.[22]

[20] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. s. 33-34.
[21] PAČKA, Roman. *CSIRT: V přední linii boje proti kybernetickým hrozbám.* Brno 2019. s. 11-12.
[22] SVATOŠ, Roman. *Prevence kriminality, druhé aktualizované vydání.* VŠERS, z.ú. s. 13.

V České republice prevence kriminality představuje systematickou činnost zaměřenou na snižování výskytu trestné činnosti a jejích negativních dopadů na společnost. Nejde pouze o samotné předcházení páchání trestných činů, ale také o ovlivňování rizikových faktorů a posilování pocitu bezpečí obyvatel. Preventivní politika je v ČR realizována na více úrovních, a to jak na úrovni státu, tak krajů a obcí, přičemž důležitou roli zde sehrávají i bezpečnostní složky, zejména Policie České republiky. Dlouhodobým trendem je rovněž přesun části kriminality do kyberprostoru, na což musí preventivní opatření reagovat a přizpůsobovat se novým formám ohrožení.[23]

2.11 Bankovní klient

Bankovní klient je obecně chápán jako osoba, která má s bankou navázaný obchodní vztah, případně s bankou jedná o jeho vzniku. Tento pojem zahrnuje nejen osoby, které již využívají bankovní produkty a služby, ale také ty, které se nacházejí ve fázi jednání o jejich poskytnutí, případně osoby, které s bankou v minulosti obchodní vztah měly. Vymezení bankovního klienta je tak širší než pouhé označení držitele bankovního účtu a reflektuje skutečnost, že ochrana klienta se vztahuje i na před-smluvní a post-smluvní vztahy.[24]

2.12 Elektronické bankovnictví

Online bankovnictví lze charakterizovat jako způsob správy bankovního účtu prostřednictvím informačních technologií a připojení k internetu, kdy je uživateli umožněn vzdálený přístup k účtu a jeho ovládání pomocí počítače nebo mobilního zařízení. Mezi hlavní přínosy tohoto způsobu bankovních služeb patří časová úspora, dostupnost služeb kdykoli a kdekoli, a relativně jednoduché uživatelské ovládání. Na druhé straně však existuje riziko zneužití přístupových údajů, které může vést k neoprávněnému nakládání s finančními prostředky na účtu.[25]

[23] ČESKÁ REPUBLIKA. *Strategie prevence kriminality v České republice na léta 2022–2027*. Praha: Ministerstvo vnitra České republiky, 2022, s. 5–6, 13.

[24] ČESKÁ NÁRODNÍ BANKA. *Stanovisko k regulaci finančního trhu – výklad pojmu klient.* [online] Dostupné z WWW:https://www.cnb.cz/cs/dohled-financni-trh/legislativni-zakladna/stanoviska-k-regulaci-financniho-trhu/RS2012-09

[25] KRÁL, Mojmír. *Bezpečný internet.* Grada Publishing, a.s. 2015. s. 85

2.12.1 Platební služba a platební prostředek

Platební služba je v českém právním řádu vymezena zákonem č. 370/2017 Sb., o platebním styku, který upravuje podmínky poskytování platebních služeb, práva a povinnosti jejich poskytovatelů a uživatelů. Platební službou se dle § 3 zák. č. 370/2017 Sb. rozumí zejména činnosti spočívající ve vkladu nebo výběru peněžních prostředků na platební účet, provádění platebních transakcí, včetně převodů peněžních prostředků, a další související služby umožňující bezhotovostní platební styk.[26]

S platební službou úzce souvisí pojem platební prostředek, který představuje nástroj umožňující uživateli provést platební transakci. Platebním prostředkem mohou být například platební karty, elektronické platební aplikace, přístupové údaje k internetovému bankovnictví nebo jiné personalizované bezpečnostní prvky, jejichž použití je nezbytné k provedení platební operace, jak je uvedeno v § 2 zák. č. 370/2017 Sb.[27] Platební prostředek je zpravidla vázán na konkrétního uživatele a jeho ochrana je klíčovým prvkem bezpečnosti platebního styku.

2.12.2 Autentizace a autorizace

Autentizace představuje proces ověřování identity subjektu v informačním systému, jehož cílem je potvrdit, že daná osoba nebo entita je skutečně tím, za koho se vydává, a je tedy oprávněna vstoupit do systému nebo zahájit další interakci.[28]

Autorizace je proces, při kterém jsou subjektu na základě stanovených přístupových práv přidělena oprávnění k provádění vymezených činností v informačním systému, a to zpravidla až po úspěšném ověření jeho identity.[29]

Zatímco autentizace slouží k ověření identity uživatele, autorizace určuje rozsah jeho oprávnění k přístupu k funkcím a datům v informačním systému.

2.13 Sociální inženýrství

Podle terminologického vymezení používaného v oblasti kybernetické bezpečnosti je sociální inženýrství chápáno jako soubor technik, jejichž cílem je

[26] ČESKO. Zákon č. 370/2017 Sb., o platebním styku. In Sbírka zákonů, Česká republika. 2017, částka 129

[27] ČESKO. Zákon č. 370/2017 Sb., o platebním styku. In Sbírka zákonů, Česká republika. 2017, částka 129

[28] JIRÁSEK, Petr; NOVÁK, Luděk; POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti.* 6., doplněné a aktualizované elektronické vydání. Praha, 2025. Vydáno pod záštitou NÚKIB. s. 30

[29] JIRÁSEK, Petr; NOVÁK, Luděk; POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti.* 6., doplněné a aktualizované elektronické vydání. Praha, 2025. Vydáno pod záštitou NÚKIB. s. 32

zneužití lidského faktoru jako nejslabšího článku bezpečnostního řetězce**.** Útoky sociálního inženýrství jsou založeny na psychologických principech, jako jsou autorita, naléhavost, strach, zvědavost nebo ochota pomoci, a často se vydávají za legitimní komunikaci důvěryhodných institucí či osob.[30]

Sociální inženýrství se vyskytuje v různých podobách, mezi které patří například podvodné e-maily, telefonické hovory, falešné webové stránky nebo zprávy zasílané prostřednictvím komunikačních aplikací. Společným znakem těchto forem je snaha přimět uživatele k dobrovolnému sdělení citlivých údajů nebo k provedení určité akce, například potvrzení platební transakce nebo zadání autentizačních údajů. Tento typ útoku je často kombinován s technickými prostředky, avšak rozhodující roli vždy hraje lidský faktor.

2.13.1 Phishing

Phishing je jednou z nejrozšířenějších forem sociálního inženýrství, při níž se pachatel snaží podvodným způsobem získat citlivé informace od oběti, zejména přístupové údaje, identifikační informace nebo údaje k platebním prostředkům. Útočník se obvykle vydává za důvěryhodný subjekt, například banku, státní instituci nebo poskytovatele služeb, a komunikuje s obětí prostřednictvím elektronických kanálů, nejčastěji e-mailem nebo falešnými internetovými stránkami. Podstatou phishingu je vytvoření zdání legitimní komunikace, které má oběť přimět k dobrovolnému sdělení citlivých údajů.[31]

2.13.2 Vishing

Vishing je další formou sociálního inženýrství, která je realizována prostřednictvím hlasové komunikace, nejčastěji telefonického hovoru. Pachatel se při vishingu vydává za zaměstnance banky, technické podpory nebo jiné důvěryhodné instituce a snaží se oběť přesvědčit k poskytnutí citlivých informací nebo k provedení určitého úkonu, například autorizaci platby.[32]

[30] JIRÁSEK, Petr; NOVÁK, Luděk; POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti.* 6., doplněné a aktualizované elektronické vydání. Praha, 2025. Vydáno pod záštitou NÚKIB. s. 191.
[31] KOHOUT, Roman. *Bezpečnost v online prostředí.* Karlovy Vary, 2016. s. 29
[32] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. s. 252-254.

2.13.3 Smishing

Smishing představuje specifickou variantu phishingu, která je realizována prostřednictvím SMS zpráv nebo jiných textových zpráv zasílaných na mobilní zařízení**.** Princip útoku je obdobný jako u klasického phishingu, avšak forma komunikace je přizpůsobena mobilnímu prostředí. Útočník se snaží oběť přimět k otevření podvodného odkazu, stažení škodlivé aplikace nebo k zadání citlivých údajů.[33]

[33] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. s. 258-260.

3. Nejčastější formy útoků z praxe

Tato kapitola představuje úvod k analytické části bakalářské práce, jejímž cílem je rozbor nejčastějších forem kybernetických útoků na bankovní klienty, se kterými se lze setkat v praktické činnosti. Analytická část navazuje na teoretickou část v předchozích kapitolách a zaměřuje se na aplikaci vymezených pojmů v reálném prostředí.

Analýza vychází především z praktických zkušeností autora, získaných při řešení případů kybernetické kriminality. Tyto zkušenosti jsou v práci využity formou zobecněných poznatků a typických scénářů útoků, nikoli jako popis konkrétních kauz. Veškeré uvedené příklady jsou anonymizovány a prezentovány tak, aby nebylo možné identifikovat konkrétní osoby, bankovní instituce ani jiné subjekty, kterých se jednotlivé případy týkaly.

3.1 Phishing založený na inzertní činnosti oběti

Jednou z nejčastějších forem kybernetických útoků, se kterými se lze v praxi setkat, je phishingový útok navazující na inzertní činnost oběti. Tento typ útoku je specifický tím, že iniciátorem prvotního kontaktu není pachatel, ale samotná oběť, která zveřejní inzerát na prodej zboží prostřednictvím internetových inzertních platforem. Pachatel této situace aktivně využívá a reaguje na nově zveřejněné nabídky, přičemž oběť oslovuje pod záminkou vážného zájmu o nabízené zboží.

Z hlediska praktického průběhu lze tento typ útoku rozdělit do několika na sebe navazujících fází. V první fázi dochází k navázání kontaktu, který je veden způsobem, jenž má vzbudit důvěru a minimalizovat podezření. Pachatel zpravidla vystupuje jako běžný zájemce, používá neutrální jazyk, vyhýbá se gramatickým chybám a často komunikuje velmi zdvořile a profesionálně. V praxi se stále častěji objevují případy, kdy je komunikace vedena prostřednictvím aplikace WhatsApp nebo obdobných platforem, což přispívá k vytvoření dojmu běžné a neformální komunikace mezi dvěma uživateli.

Ve druhé fázi útoku dochází k postupnému převzetí iniciativy pachatelem. Namísto toho, aby oběť určovala podmínky prodeje, pachatel aktivně navrhuje způsob doručení i úhrady. Typicky se odkazuje na využití známých přepravních služeb a

prezentuje celý proces jako standardizovaný a bezpečný. Tento krok je z hlediska sociálního inženýrství klíčový, neboť dochází k přenesení kontroly nad transakcí z oběti na pachatele. Oběť přestává situaci aktivně řídit a postupně se dostává do role pasivního účastníka, který pouze reaguje na pokyny.

Následuje fáze, ve které pachatel zasílá odkaz na podvodnou webovou stránku. Tyto stránky jsou často velmi kvalitně zpracované a vizuálně téměř nerozeznatelné od originálních webů přepravních společností či bankovních institucí. V některých případech obsahují i funkční prvky, které simulují reálné prostředí, například načítání údajů nebo potvrzovací obrazovky. Oběť je zde vyzvána k zadání údajů k platební kartě, případně přihlašovacích údajů do internetového bankovnictví, a to pod záminkou přijetí platby za prodávané zboží.

Z pohledu pachatele je zásadní zejména poslední fáze útoku, která spočívá ve zneužití autentizačních a autorizačních mechanismů. V této fázi oběť často obdrží jednorázový kód prostřednictvím SMS zprávy nebo mobilní bankovní aplikace, který následně zadá do podvodného rozhraní. Oběť je přesvědčena, že potvrzuje příchozí platbu, ve skutečnosti však autorizuje odchozí transakci nebo přístup do svého účtu. Tento moment představuje zlomový bod celého útoku, neboť dochází k faktickému dokonání trestné činnosti.

Z praktických zkušeností lze konstatovat, že úspěšnost těchto útoků je podmíněna zejména kombinací technických prostředků a psychologické manipulace. Pachatelé cíleně využívají časového tlaku, kdy oběť motivují k rychlému jednání například tvrzením, že o zboží je velký zájem. Současně pracují s důvěrou oběti v běžně používané služby, jako jsou přepravní společnosti či bankovní instituce, čímž snižují její obezřetnost. Významnou roli hraje také fakt, že oběť očekává finanční prospěch, což může vést ke snížení kritického uvažování.

V praxi se lze setkat i s případy, kdy jsou tyto útoky realizovány ve větším měřítku prostřednictvím automatizovaných systémů, které vyhledávají nové inzeráty a generují první kontakt bez přímé účasti pachatele. Tím dochází k výraznému zvýšení efektivity a počtu oslovených obětí. Tento trend ukazuje na postupnou profesionalizaci pachatelů a jejich schopnost využívat moderní technologie k páchání trestné činnosti.

Z hlediska trestněprávního posouzení je podstatné, že i když samotné jednání vedoucí k převodu finančních prostředků provádí oběť, činí tak na základě omylu vyvolaného pachatelem. Pachatel tak naplňuje znak uvedení v omyl nebo využití omylu, přičemž poškozený v důsledku tohoto jednání sám provede finanční operaci ve prospěch pachatele. Tento mechanismus je typickým znakem podvodného jednání a v praxi představuje základní konstrukci většiny útoků tohoto typu.

Tento typ útoku je v praxi mimořádně úspěšný, neboť kombinuje technické prvky phishingu s propracovaným sociálním inženýrstvím a využívá důvěru oběti v běžně používané služby a instituce.

3.2 Vishing a sociální inženýrství založené na zneužití identity mobilního operátora

Tato forma kybernetické kriminality patří v současné praxi mezi sofistikovanější útoky, které kombinují prvky phishingu, sociálního inženýrství a zneužití ověřovacích procesů u třetích subjektů, zejména mobilních operátorů. Na rozdíl od klasického phishingu zde pachatel vystupuje aktivně a kontaktuje oběť telefonicky, čímž vytváří přímý kontakt, který působí důvěryhodněji než běžná elektronická komunikace. Pachatel se nejčastěji vydává za zaměstnance mobilního operátora a oběť oslovuje s nabídkou výhodnějšího tarifu, nových služeb nebo upozorněním na údajný technický problém, který je potřeba neodkladně řešit.

Důvěryhodnost své legendy pachatel posiluje tím, že disponuje alespoň základními osobními údaji oběti, jako je jméno, telefonní číslo nebo informace o využívaných službách. Tyto údaje bývají získány z různých úniků dat, veřejně dostupných zdrojů nebo předchozí trestné činnosti. V praxi má tento prvek zásadní význam, protože oběť má tendenci považovat volajícího za legitimního zástupce společnosti, pokud zná její osobní údaje, a snižuje tak svou přirozenou opatrnost.

V další fázi útoku dochází k využití prvků sociálního inženýrství. Pachatel oběť přesvědčí, že je nutné provést ověření totožnosti, přičemž pod touto záminkou požaduje sdělení bezpečnostního prvku, typicky PIN kódu nebo hesla určeného pro komunikaci s mobilním operátorem. Komunikace je vedena tak, aby oběť neměla prostor pro pochybnosti – pachatel často vytváří dojem časového tlaku nebo zdůrazňuje nutnost

rychlého řešení situace. Po získání těchto údajů je hovor zpravidla ukončen s tím, že požadované změny budou realizovány.

Následně pachatel kontaktuje samotného mobilního operátora a s využitím kombinace osobních údajů a získaného autentizačního prvku provede změny v zákaznickém účtu oběti. Nejčastěji se jedná o vydání nové SIM karty nebo aktivaci elektronické SIM (eSIM), čímž dojde k převzetí kontroly nad telefonním číslem oběti. Původní SIM karta oběti je tímto krokem vyřazena z provozu, což oběť zpravidla zaznamená až s určitým časovým odstupem.

Získání kontroly nad telefonním číslem představuje klíčový moment celého útoku. Telefonní číslo je totiž v současné době běžně využíváno jako prostředek pro ověřování identity při přístupu k různým službám, zejména k internetovému bankovnictví. Pachatel této skutečnosti využívá a iniciuje například změnu přístupových údajů k bankovnímu účtu. Díky tomu, že má pod kontrolou komunikační kanál, je schopen přijímat ověřovací SMS kódy a úspěšně projít bezpečnostními mechanismy.

Po získání přístupu k bankovnímu účtu pachatel zpravidla bezprostředně provádí neoprávněné platební transakce, často ve více krocích a na různé účty, aby snížil pravděpodobnost včasného odhalení. V některých případech dochází i ke změně kontaktních údajů nebo nastavení účtu tak, aby byla oběť co nejdéle odříznuta od informací o probíhajících operacích. Oběť si podvodu většinou všimne až ve chvíli, kdy zjistí, že její telefonní číslo není funkční, případně když se nemůže přihlásit do internetového bankovnictví.

Z praktických zkušeností lze uvést, že tento typ útoku je pro oběť obzvlášť nebezpečný, protože kombinuje několik faktorů, které zvyšují jeho úspěšnost. Jedná se zejména o přímý telefonický kontakt, vystupování pod autoritou známé instituce a využití důvěry v běžně používané služby. Významnou roli hraje také psychologický tlak na rychlé rozhodování, kdy oběť nemá dostatek času situaci racionálně vyhodnotit.

Z hlediska trestněprávního posouzení pachatel i v tomto případě naplňuje znak uvedení v omyl nebo využití omylu, přičemž oběť na základě tohoto omylu sama poskytne údaje nebo provede kroky, které následně vedou ke zneužití jejího bankovního účtu. Charakteristickým znakem tohoto jednání je tedy skutečnost, že klíčové úkony jsou prováděny samotnou obětí, avšak pod vlivem manipulace ze strany pachatele.

3.3 Vishing s legendou falešného bankéře

Tato forma phishingu, často označovaná jako vishing, patří z hlediska policejní praxe mezi nejzávažnější typy útoků zaměřených na bankovní klienty. Je charakteristická tím, že nedochází k technickému prolomení zabezpečení internetového bankovnictví, ale k přímému zneužití důvěry oběti a jejího vlastního jednání. Útok je založen na intenzivním využití sociálního inženýrství, práci s emocemi oběti, časovém tlaku a vytváření pocitu bezprostředního ohrožení finančních prostředků. Právě kombinace těchto prvků činí tento typ útoku mimořádně účinným.

Pachatel kontaktuje oběť telefonicky a vystupuje jako pracovník banky, případně jako specialista bezpečnostního oddělení. V některých případech je telefonní číslo upraveno tak, aby se zobrazovalo jako oficiální kontakt banky, což dále zvyšuje důvěryhodnost hovoru. Oběť je informována o údajném napadení jejího bankovního účtu, pokusu o neoprávněnou transakci nebo snaze cizí osoby sjednat na její jméno úvěr. Komunikace je vedena velmi přesvědčivě a často obsahuje i konkrétní detaily, například částky nebo typy operací, což v oběti vyvolává dojem, že se jedná o reálnou a probíhající situaci.

V této fázi pachatel pracuje především s psychologickým tlakem. Oběť je vystavena stresu a pocitu, že musí jednat okamžitě, jinak dojde ke ztrátě jejích finančních prostředků. Pachatel zároveň často zdůrazňuje, že situaci nelze řešit standardní cestou, například osobní návštěvou pobočky, protože by to bylo příliš pomalé. Tímto způsobem omezuje možnost oběti situaci ověřit a zároveň ji izoluje od jiných zdrojů informací.

V rámci hovoru je oběť instruována k provedení konkrétních kroků v internetovém bankovnictví. Jednou z častých variant je převod finančních prostředků na údajný „bezpečný účet“, který má sloužit k dočasnému ochránění peněz před útokem. Pachatel přitom tento účet prezentuje jako účet banky nebo jiného důvěryhodného subjektu, a oběť tak nemá důvod o jeho legitimitě pochybovat. V jiné variantě je oběť manipulována k tomu, aby sama sjednala úvěr, nejčastěji prostřednictvím online bankovnictví, s tvrzením, že tím zablokuje pokus pachatele o sjednání půjčky. Tento postup je z hlediska praxe obzvlášť nebezpečný, neboť oběť nejen že přijde o vlastní prostředky, ale současně se zadluží.

Pro zvýšení důvěryhodnosti útoku bývá využíváno zapojení více osob. Druhý pachatel se například vydává za policistu nebo pracovníka Policie České republiky a kontaktuje oběť s cílem potvrdit pravdivost situace. Tento krok má zásadní psychologický efekt, neboť dochází ke kombinaci dvou autorit – banky a policie. Oběť tak získává dojem, že se jedná o koordinovaný a legitimní postup, a její schopnost kritického vyhodnocení situace se výrazně snižuje.

Zásadním rysem tohoto typu útoku je skutečnost, že všechny transakce provádí oběť sama, dobrovolně a s využitím platných autentizačních a autorizačních mechanismů banky. Oběť zadává platební příkazy, potvrzuje je prostřednictvím autorizačních kódů a v některých případech i aktivně komunikuje s bankovní aplikací. Přestože z pohledu banky se jedná o standardně autorizované operace, jejich provedení je výsledkem manipulace ze strany pachatele. Pachatel tak dosahuje svého cíle bez nutnosti překonat technické zabezpečení bankovního systému.

Z pohledu praxe je důležité zmínit, že pachatelé často přizpůsobují průběh útoku konkrétní situaci oběti. Pokud oběť projeví pochybnosti, pachatel reaguje uklidňujícím způsobem a snaží se její obavy rozptýlit. Naopak pokud oběť reaguje rychle a bez většího odporu, pachatel útok urychluje, aby minimalizoval riziko odhalení. Tento dynamický přístup ukazuje na vysokou míru připravenosti pachatelů a jejich schopnost improvizace.

Oběť si zpravidla uvědomí, že se stala obětí podvodu až s časovým odstupem, nejčastěji po konzultaci s bankou nebo při zjištění, že finanční prostředky nebyly vráceny a účet, na který byly odeslány, je nedohledatelný. V některých případech dochází k odhalení až při kontrole zůstatku na účtu nebo při následném kontaktu s bankou z jiného důvodu.

Z hlediska trestněprávního posouzení pachatel i v tomto případě naplňuje znak uvedení v omyl nebo využití omylu, kdy oběť na základě tohoto omylu sama provede finanční operace ve prospěch pachatele. Charakteristické pro tento typ jednání je tedy to, že klíčové kroky provádí poškozený, avšak pod vlivem manipulace a mylné představy o skutečném stavu věci.

Z pohledu policejní praxe se jedná o případy s vysokou společenskou škodlivostí, neboť kombinují sofistikovanou manipulaci s psychikou oběti a plné

zneužití její důvěry v autority. Významným problémem je rovněž skutečnost, že oběti často jednají v dobré víře a až zpětně si uvědomují, že byly systematicky vedeny k jednání, které vedlo k jejich finanční ztrátě.

3.4 Investiční podvody

Investiční podvody představují v současné době jednu z nejzávažnějších a nejrychleji se rozvíjejících forem kybernetické kriminality zaměřené na bankovní klienty. Z pohledu policejní praxe se jedná o případy, které jsou charakteristické nejen vysokou finanční škodou, ale také dlouhodobým a systematickým působením pachatelů na poškozeného. Na rozdíl od jiných forem útoků zde pachatel neusiluje o jednorázové vylákání finančních prostředků, ale o postupné získávání důvěry oběti a opakované převody finančních částek.

Útok zpravidla začíná navázáním kontaktu prostřednictvím internetové reklamy, sociálních sítí nebo telefonického oslovení. Pachatel vystupuje jako investiční poradce nebo zástupce investiční společnosti a nabízí možnost zhodnocení finančních prostředků, často v oblasti kryptoměn, akcií nebo komodit. V této fázi pachatel využívá atraktivní prezentace, profesionálně působící webové stránky a sliby vysokého zisku při minimálním riziku. Tyto webové stránky se často tváří jako legitimní investiční platformy, avšak ve skutečnosti se jedná o podvrhy, které pouze simulují investiční prostředí.

Po navázání kontaktu je poškozený vyzván k provedení první investice, která bývá relativně nízká. Cílem tohoto kroku je získat důvěru oběti a vytvořit dojem funkčního investičního systému. Následně pachatel poškozenému zpřístupní uživatelské rozhraní, kde jsou zobrazovány fiktivní zisky a pohyby na účtu. Tyto údaje jsou však zcela smyšlené a nemají žádnou vazbu na reálné investiční operace. Poškozený je tak utvrzován v přesvědčení, že jeho investice je úspěšná, a je motivován k dalším vkladům.

V další fázi dochází k postupnému navyšování investovaných částek. Pachatel poškozeného opakovaně kontaktuje a přesvědčuje jej k dalším převodům finančních prostředků, často pod záminkou výhodné investiční příležitosti nebo nutnosti doplnění prostředků k realizaci obchodu. V praxi se lze setkat s případy, kdy poškozený provede

desítky jednotlivých plateb, a to nejen ze svého účtu, ale i prostřednictvím sjednaných úvěrů. Tento proces může probíhat v řádu dnů, ale i několika měsíců.

Z hlediska toku finančních prostředků je typické, že peníze nejsou směřovány na jeden účet, ale naopak dochází k jejich rozdělení na více různých účtů, často vedených u zahraničních bankovních institucí. V některých případech jsou finanční prostředky převáděny na účty tzv. „bílých koní“, tedy osob, které poskytly své bankovní účty k dalšímu převodu. Tyto účty slouží jako mezičlánek, přes který jsou prostředky dále přeposílány, čímž dochází ke ztížení jejich dohledání.

Specifickým prvkem těchto podvodů je rovněž využívání kryptoměn. Poškozený je vyzván k převodu finančních prostředků na kryptopeněženky, které jsou prezentovány jako investiční účty. V některých případech se jedná o reálné kryptopeněženky ovládané pachatelem, v jiných případech jsou využívány falešné platformy, které pouze zobrazují smyšlené zůstatky a pohyby. Převody do kryptoměn výrazně komplikují následné dohledání finančních prostředků a jejich případné zajištění.

Z policejní praxe je rovněž známo, že v některých případech dochází k tomu, že účet poškozeného je zneužit i k dalším převodům. Pachatel může poškozeného přesvědčit, aby přijal finanční prostředky na svůj účet a následně je odeslal na jiné účty, čímž se poškozený nevědomky zapojuje do řetězce převodů. Tento postup dále komplikuje vyšetřování, neboť dochází k prolínání role poškozeného a prostředníka.

Ve fázi, kdy poškozený požaduje výběr investovaných prostředků, dochází zpravidla k dalšímu podvodnému jednání. Pachatel podmiňuje výběr zaplacením různých poplatků, například za zpracování transakce, daň nebo „ověření účtu“. Poškozený tak může provést další platby v domnění, že se jedná o poslední krok k získání svých prostředků. Ve skutečnosti však k žádnému výběru nedochází a komunikace ze strany pachatele je následně ukončena.

Z hlediska trestněprávního posouzení je podstatné, že pachatel využívá omyl poškozeného, který je přesvědčen o reálné existenci investice a očekávaném zhodnocení. Poškozený na základě tohoto omylu opakovaně provádí finanční transakce ve prospěch pachatele. Charakteristickým znakem těchto případů je dlouhodobé působení na oběť, systematická manipulace a postupné navyšování způsobené škody.

Investiční podvody tak představují komplexní formu trestné činnosti, která kombinuje prvky psychologické manipulace, technického zajištění a organizovaného postupu pachatelů. Z pohledu policejní praxe jde o případy, které jsou náročné na dokazování i mezinárodní spolupráci, a současně mají výrazný dopad na poškozené, a to nejen po finanční, ale i psychické stránce.

4. Kvalifikace kybernetických útoků v trestněprávní rovině

Jednání popsané v předchozích kapitolách je nutné posuzovat také z hlediska trestního práva hmotného, tedy z pohledu naplnění zákonných znaků některého z trestných činů upravených v trestním zákoníku. Aby bylo možné určité jednání považovat za trestný čin, musí naplnit znaky skutkové podstaty stanovené zákonem. Skutková podstata přitom představuje soubor zákonných znaků charakterizujících určité protiprávní jednání, přičemž tyto znaky jsou vymezeny v jednotlivých ustanoveních trestního zákoníku. Jedná se zejména o objekt trestného činu, objektivní stránku, subjekt a subjektivní stránku.

Vedle formálních znaků skutkové podstaty je však nezbytné, aby jednání pachatele vykazovalo také znaky protiprávnosti, společenské škodlivosti a zavinění, které jsou podmínkou trestní odpovědnosti.[34] Teprve v případě, kdy jsou všechny tyto znaky naplněny, lze konkrétní jednání kvalifikovat jako trestný čin podle trestního zákoníku. V případě kybernetických útoků zaměřených na bankovní klienty je proto nutné vždy posuzovat konkrétní způsob jednání pachatele, použitou metodu útoku a vzniklý následek.

V souvislosti s útoky popsanými v předchozích kapitolách, které jsou založeny především na metodách sociálního inženýrství a manipulaci obětí, přichází v úvahu zejména právní kvalifikace podle § 209 zákona č. 40/2009 Sb., trestní zákoník, tedy trestný čin podvod. Trestný čin podvodu podle § 209 trestního zákoníku spočívá v tom, že pachatel uvede jiného v omyl, využije jeho omylu nebo zamlčí podstatné skutečnosti, a tím způsobí na cizím majetku škodu. V kontextu kybernetických útoků zaměřených na bankovní klienty se jedná zejména o případy, kdy je poškozený prostřednictvím metod sociálního inženýrství přiměn k provedení určitého jednání, typicky k zadání přihlašovacích údajů nebo k realizaci finanční transakce ve prospěch pachatele.

Specifikem těchto útoků je skutečnost, že samotné jednání směřující k převodu finančních prostředků provádí poškozený, avšak na základě omylu vyvolaného pachatelem. Pachatel tak využívá psychologické manipulace a důvěry oběti, čímž

[34] ŠÁMAL, Pavel a kol. *Trestní zákoník I. Komentář. 2. vydání*. Praha: C. H. Beck, 2012, s. 146.

dochází k naplnění znaku uvedení v omyl nebo využití omylu ve smyslu trestního zákoníku.[35]

Právě uvedení oběti v omyl je typickým znakem velké části kybernetických útoků zaměřených na bankovní klienty. Pachatelé v těchto případech vystupují například jako pracovníci banky, zaměstnanci technické podpory, pracovníci přepravních společností nebo dokonce jako policisté. Oběť je následně přesvědčena, že komunikuje s důvěryhodnou osobou, a na základě této mýlky provádí další kroky, například poskytne přístupové údaje k internetovému bankovnictví, zadá údaje k platební kartě nebo sama provede finanční transakci. Právě tato manipulace s obětí, která vede k majetkové dispozici, představuje základní znak trestného činu podvodu.

Dalším relevantním trestným činem v souvislosti s kybernetickými útoky na bankovní klienty je neoprávněné opatření, padělání a pozměnění platebního prostředku podle § 234 trestního zákoníku. Tento trestný čin postihuje jednání spočívající zejména v neoprávněném opatření si platebního prostředku nebo jeho údajů, jakož i jeho následnému zneužití.

V prostředí elektronického bankovnictví může být platebním prostředkem nejen fyzická platební karta, ale také údaje, které umožňují provedení platební transakce. Typicky se může jednat o údaje k platební kartě, přihlašovací údaje do internetového bankovnictví nebo jiné personalizované bezpečnostní prvky. V praxi tak může dojít například k situaci, kdy oběť zadá údaje ke své platební kartě na podvodné internetové stránce, která se tváří jako legitimní platební brána, a pachatel tyto údaje následně využije k provedení neoprávněné platební transakce.

Další variantou může být situace, kdy pachatel prostřednictvím sociálního inženýrství získá přístup k internetovému bankovnictví oběti a následně sám provádí platební operace z jejího účtu. V těchto případech může být jednání pachatele kvalifikováno právě podle § 234 trestního zákoníku, neboť dochází k neoprávněnému použití platebního prostředku nebo údajů, které umožňují provedení platební transakce. Judikatura Nejvyššího soudu dovodila, že za platební prostředek ve smyslu § 234 trestního zákoníku lze považovat i elektronický platební příkaz realizovaný prostřednictvím internetového bankovnictví. Pokud pachatel neoprávněně získá

[35] ŠÁMAL, Pavel a kol. *Trestní zákoník II. Komentář. 2. vydání.* Praha: C. H. Beck, 2012, s. 2053–2060.

přístupové údaje k účtu a následně zadá platební příkaz, jedná se o padělání a užití platebního prostředku, neboť se pachatel vydává za oprávněného uživatele účtu a využívá bankovní systém k převodu finančních prostředků.[36]

Vedle výše uvedených ustanovení může v úvahu připadat také právní kvalifikace podle § 230 trestního zákoníku – neoprávněný přístup k počítačovému systému a nosiči informací. Tento trestný čin postihuje jednání, při němž pachatel neoprávněně pronikne do počítačového systému nebo jiným způsobem obejde jeho zabezpečení. Typicky se může jednat například o prolomení hesla, zneužití bezpečnostní zranitelnosti nebo instalaci škodlivého softwaru.

V případech popsaných v této bakalářské práci však zpravidla nedochází k naplnění skutkové podstaty tohoto trestného činu, neboť pachatelé se do bankovního systému nedostávají vlastním technickým jednáním, ale prostřednictvím manipulace s obětí. Klient je v důsledku sociálního inženýrství přiměn k tomu, aby sám poskytl přístupové údaje nebo provedl určité operace v internetovém bankovnictví. Pachatel tak fakticky využívá legitimní přístupové oprávnění klienta, aniž by musel technicky překonávat zabezpečení bankovního systému. Z tohoto důvodu bývá v praxi jednání pachatelů kvalifikováno především jako trestný čin podvod, případně jako neoprávněné opatření a použití platebního prostředku. Správné právní posouzení situace je proto vždy výsledkem komplexního hodnocení všech okolností konkrétního případu.

4.1 Vyšetřování kybernetické kriminality

Počítačová kriminalita se vyznačuje vysokou mírou rozmanitosti a specifickými rysy, které spočívají zejména v absenci fyzicky zjistitelných stop po trestné činnosti. Z tohoto důvodu není při jejím objasňování možné spoléhat výhradně na tradiční kriminalistické metody obecné povahy, neboť jejich samostatné použití by bylo časově náročné a v konečném důsledku málo efektivní. Tento druh kriminality je zároveň charakteristický rychlým vývojem a značnou mírou latence, která podstatně komplikuje její odhalování. Orgány činné v trestním řízení se tak často potýkají s obtížemi při snaze držet krok s pachateli, jejichž činnost se odehrává v technologicky složitém prostředí informačních systémů. Efektivní vyšetřování proto vyžaduje, aby policisté disponovali odpovídajícími znalostmi z oblasti informačních technologií. Pachatelé počítačové

[36] Usnesení Nejvyššího soudu ČR ze dne 16. 5. 2018, sp. zn. 4 Tdo 456/2018; srov. též usnesení Nejvyššího soudu ČR sp. zn. 4 Tdo 1115/2022.

kriminality bývají zpravidla vysoce erudovaní a systematicky se snaží minimalizovat či zcela eliminovat stopy své činnosti, přičemž poškození mnohdy neprojevují výrazný zájem na oznámení nebo objasnění trestného činu.[37]

Na uvedené teoretické vymezení navazují praktické zkušenosti z vyšetřování kybernetické kriminality, které potvrzují, že objasňování tohoto typu trestné činnosti je mimořádně komplexní a zatížené řadou překážek. V případech kybernetické kriminality zaměřené na bankovní klienty se výrazně projevuje vysoká míra latence, kdy poškození často trestnou činnost vůbec neoznámí. Důvodem může být například stud, obava z přiznání vlastní chyby, nízká důvěra v policii a na obecně známou nízkou šanci úspěšného objasnění skutku. Tím dochází k významné časové prodlevě, která má zásadní negativní dopad na možnosti efektivního vyšetřování. Další komplikací je omezený přístup orgánů činných v trestním řízení k informacím nezbytným pro objasnění skutku. V případě napadení internetového bankovnictví jde zejména o údaje chráněné bankovním tajemstvím, jejichž poskytnutí je podmíněno souhlasem majitele účtu, případně procesními úkony v trestním řízení. I v případech, kdy je souhlas udělen, dochází k časovým prodlevám v řádu týdnů, ne-li měsíců, než banka poskytne požadované podklady. Typicky jde o výpisy systémových logů z internetového bankovnictví. Tyto záznamy obsahují časový a věcný přehled provedených operací, včetně výpisu IP adres, z nichž je často patrné využití automatizovaných nástrojů schopných provádět velké množství úkonů v krátkém časovém úseku, čehož není člověk schopen. Současně je z IP adres zřejmé využívání anonymizačních služeb jako VPN, a připojení prostřednictvím poskytovatelů internetového připojení a mobilních operátorů z různých částí světa.

Obdobně problematické je získávání údajů o telekomunikačním provozu, které podléhá zákonným omezením a vyžaduje splnění procesních podmínek pro prolomení zákonné ochrany těchto dat. Mobilní operátoři navíc uchovávají provozní údaje pouze po omezenou dobu a v řadě případů se komunikace uskutečňuje prostřednictvím zahraničních operátorů nebo neregistrovaných SIM karet, což další postup výrazně komplikuje. V kombinaci s časovými prodlevami tak dochází k situacím, kdy jsou klíčové stopy nenávratně ztraceny ještě před jejich zajištěním.

[37] GŘIVNA, Tomáš; POLČÁK, Radim. *Kyberkriminalita a právo.* Praha: Auditorium, 2008, s. 87.

V případech bankovních podvodů je navíc nutné zjišťovat informace o cílových účtech, na které byly finanční prostředky převedeny, což je možné pouze se souhlasem státního zástupce. Následné prověřování vlastníků těchto účtů a finančních toků je často komplikováno skutečností, že peníze bývají obratem převáděny na další účty, vybírány prostřednictvím bankomatů nebo použity k online platbám, nejčastěji u zahraničních obchodníků. Tyto skutečnosti v praxi výrazně snižují šanci na ztotožnění konkrétního pachatele a názorně ilustrují, že u kybernetické kriminality zaměřené na bankovní klienty je čas klíčový faktor a reálné vyšetřování často trvá v řádu týdnů až měsíců.

5. Prevence kybernetických útoků na bankovní klienty

5.1 Prevence kybernetické kriminality ze strany bank

Bankovní instituce představují klíčový prvek systému prevence kybernetické kriminality zaměřené na bankovní klienty. Vzhledem k rostoucímu významu elektronických plateb a internetového bankovnictví jsou banky nuceny zavádět komplexní bezpečnostní opatření, jejichž cílem je minimalizovat riziko podvodného jednání a posílit důvěru klientů v bezhotovostní platební styk. Prevence v bankovním sektoru je přitom založena na kombinaci technických nástrojů, organizačních opatření a postupů řízení rizik, které reagují na identifikovaná bezpečnostní ohrožení v oblasti elektronických plateb.[38]

Jedním ze základních preventivních nástrojů používaných bankami jsou systémy pro detekci podvodných transakcí (Fraud Detection Systems). Tyto systémy průběžně analyzují platební operace klientů a vyhodnocují, zda se nejedná o nestandardní nebo podezřelou transakci. V případě identifikace rizikového chování mohou banky například dočasně zablokovat transakci, požadovat dodatečné ověření identity klienta nebo klienta kontaktovat s cílem ověřit oprávněnost prováděné operace. Takové systémy umožňují bankám reagovat na pokusy o podvod v reálném čase a minimalizovat možné finanční ztráty.[39]

Dalším významným preventivním opatřením je monitoring transakcí a analýza chování klienta. Banky sledují například neobvyklé platební vzorce, změny zařízení používaného pro přístup k internetovému bankovnictví, přihlášení z netypických geografických lokalit nebo neobvyklé objemy finančních operací. Pokud systém vyhodnotí určitou transakci jako rizikovou, může dojít k jejímu pozastavení nebo k provedení dalších bezpečnostních kontrol. Monitoring transakcí a průběžné

[38] EVROPSKÁ CENTRÁLNÍ BANKA. Doporučení pro bezpečnost internetových plateb. Frankfurt: Evropská centrální banka, 2013, s. 6–7. [online]. [cit. 2026-03-17]. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/dohled-financni-trh/.galleries/legislativni_zakladna/banky_a_zalozny/download/ecb_doporuceni_pro_bezpecnost_internetovych_plateb.pdf

[39] ČESKÁ NÁRODNÍ BANKA. Phishing: věrohodně se tvářící podvod. ČNB Blog [online]. [cit. 2026-03-17]. Dostupné z: https://www.cnb.cz/cs/o_cnb/cnblog/Phishing-verohodne-se-tvarici-podvod/

vyhodnocování rizik představují základní součást systému řízení bezpečnosti elektronických plateb a patří mezi klíčové mechanismy prevence finančních podvodů.[40]

Velmi důležitým bezpečnostním prvkem v oblasti elektronického bankovnictví je také silné ověření uživatele, často označované jako dvoufaktorová nebo multifaktorová autentizace. Tento mechanismus vyžaduje, aby uživatel při přihlášení do internetového bankovnictví nebo při potvrzení platební transakce použil alespoň dva různé autentizační faktory, například kombinaci hesla a jednorázového kódu zaslaného prostřednictvím SMS nebo mobilní aplikace. Povinnost používat silné ověření uživatele při provádění elektronických plateb vyplývá z právní úpravy platebního styku a jejím cílem je výrazně snížit riziko neoprávněného přístupu k bankovnímu účtu. [41]

Dalším preventivním opatřením uplatňovaným bankami jsou limity platebních transakcí a řízení oprávnění klienta. Banky nastavují maximální částky pro jednotlivé typy plateb nebo omezují možnost provádění některých operací bez dodatečného ověření. Tyto limity mohou být stanoveny jak na úrovni banky, tak individuálně klientem. V případě nestandardní nebo vysoké transakce tak dochází k dodatečné kontrole, která může zabránit neoprávněnému převodu finančních prostředků.[42]

Významnou roli v prevenci kybernetických útoků hraje rovněž zabezpečení komunikace mezi klientem a bankou, které je realizováno prostřednictvím šifrování dat a využívání bezpečnostních protokolů. Banky využívají například protokoly HTTPS, certifikáty a další technologie, které zajišťují důvěrnost a integritu přenášených informací. Cílem těchto opatření je zabránit odposlechu komunikace nebo neoprávněnému zásahu do přenášených dat.[43]

---

[40] EVROPSKÁ CENTRÁLNÍ BANKA. Doporučení pro bezpečnost internetových plateb. Frankfurt: Evropská centrální banka, 2013, s. 7–8. [online]. [cit. 2026-03-17]. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/dohled-financni-trh/.galleries/legislativni_zakladna/banky_a_zalozny/download/ecb_doporuceni_pro_bezpecnost_internetovych_plateb.pdf

[41] EVROPSKÝ PARLAMENT A RADA EU. Směrnice (EU) 2015/2366 o platebních službách na vnitřním trhu (PSD2). Úřední věstník EU, 2015. [online]. [cit. 2026-03-17]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32015L2366

[42] EVROPSKÁ CENTRÁLNÍ BANKA. Doporučení pro bezpečnost internetových plateb. Frankfurt: ECB, 2013, s. 10–11. [online]. [cit. 2026-03-17]. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/dohled-financni-trh/.galleries/legislativni_zakladna/banky_a_zalozny/download/ecb_doporuceni_pro_bezpecnost_internetovych_plateb.pdf

[43] EVROPSKÁ CENTRÁLNÍ BANKA. Doporučení pro bezpečnost internetových plateb. Frankfurt: ECB, 2013, s. 6–7. [online]. [cit. 2026-03-17]. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/dohled-financni-trh/.galleries/legislativni_zakladna/banky_a_zalozny/download/ecb_doporuceni_pro_bezpecnost_internetovych_plateb.pdf

Vedle technických opatření je nedílnou součástí prevence také informování a edukace klientů. Banky pravidelně upozorňují na aktuální formy podvodného jednání, například phishing, vishing nebo smishing, a poskytují klientům doporučení, jak se v těchto situacích chovat. Informace jsou šířeny prostřednictvím internetového bankovnictví, mobilních aplikací, e-mailů nebo veřejných kampaní. Cílem těchto aktivit je zvýšit povědomí klientů o rizicích a posílit jejich schopnost rozpoznat podvodné jednání.[44]

V posledních letech lze v bankovním sektoru pozorovat také rostoucí využívání pokročilých analytických nástrojů založených na principech strojového učení a umělé inteligence. Tyto systémy umožňují bankám lépe identifikovat neobvyklé vzorce chování klientů a v reálném čase vyhodnocovat rizikovost jednotlivých transakcí. Na rozdíl od tradičních systémů jsou schopny adaptace na nové typy podvodného jednání, což je zásadní zejména v oblasti kybernetické kriminality, kde pachatelé své postupy neustále mění a přizpůsobují aktuálním bezpečnostním opatřením. Bankovní instituce v rámci své činnosti věnují významnou pozornost řízení rizik a kontrole finančních operací, což představuje základní předpoklad pro prevenci podvodného jednání v oblasti elektronických plateb.[45]

Dalším významným prvkem prevence je spolupráce bank mezi sebou a s dalšími institucemi, zejména s orgány činnými v trestním řízení a regulátory finančního trhu. Banky si v rámci této spolupráce předávají informace o aktuálních hrozbách, podezřelých účtech a způsobech páchání trestné činnosti. Tato koordinace umožňuje rychlejší reakci na nové formy útoků a zvyšuje pravděpodobnost odhalení pachatelů. V praxi se lze setkat s případy, kdy včasné sdílení informací mezi bankami vedlo k zablokování finančních prostředků ještě před jejich dalším převodem do zahraničí.

Z pohledu praxe je rovněž významná schopnost bank rychle reagovat na oznámení klienta o podezřelé transakci. V případě včasného nahlášení může banka provést okamžité kroky směřující k zablokování účtu nebo zastavení platební operace. Tento postup je však časově omezený a jeho úspěšnost závisí na rychlosti reakce klienta

[44] ČESKÁ NÁRODNÍ BANKA. Phishing: věrohodně se tvářící podvod. *ČNB Blog* [online]. [cit. 2026-03-17]. Dostupné z: https://www.cnb.cz/cs/o_cnb/cnblog/Phishing-verohodne-se-tvarici-podvod/

[45] MEJSTŘÍK, Michal; PEČENÁ, Magda; TEPLÝ, Petr. *Bankovnictví v teorii a praxi*. 1. vydání. Praha: Karolinum, 2014, s. 88-90.

i banky. Z tohoto důvodu banky klienty opakovaně upozorňují na nutnost bezodkladného kontaktování banky při jakémkoli podezření na podvodné jednání.

Významnou oblastí prevence je také vnitřní bezpečnost bankovních institucí a školení zaměstnanců. Zaměstnanci bank jsou pravidelně vzděláváni v oblasti rozpoznávání podvodného jednání a postupů při řešení bezpečnostních incidentů. V některých případech dochází i k simulovaným útokům, jejichž cílem je ověřit připravenost zaměstnanců reagovat na pokusy o sociální inženýrství. Tato opatření přispívají k minimalizaci rizika selhání lidského faktoru na straně banky.

Z hlediska současných trendů je rovněž patrný přesun části prevence směrem k samotným uživatelům, a to prostřednictvím technologických nástrojů integrovaných přímo do bankovních aplikací. Jedná se například o upozornění na rizikové chování, varování před podezřelými transakcemi nebo edukativní prvky, které klienta upozorňují na možné podvodné scénáře. Tyto nástroje mají za cíl aktivně zapojit klienta do procesu ochrany jeho finančních prostředků.

Přestože banky disponují širokou škálou preventivních opatření, praxe ukazuje, že jejich účinnost je do značné míry limitována lidským faktorem. Pachatelé se stále častěji zaměřují právě na obcházení technických zabezpečení prostřednictvím manipulace s klientem. Z tohoto důvodu nelze prevenci vnímat pouze jako soubor technických opatření, ale jako komplexní proces, který zahrnuje jak technologickou ochranu, tak i zvyšování povědomí a odpovědného chování uživatelů.

5.2 Prevence ze strany bankovních klientů

Vedle preventivních opatření realizovaných bankovními institucemi hraje zásadní roli v oblasti kybernetické bezpečnosti také samotné chování bankovních klientů. Praxe ukazuje, že značná část kybernetických útoků zaměřených na bankovní klienty je založena na metodách sociálního inženýrství, kdy pachatel nevyužívá technické zranitelnosti systému, ale manipuluje samotného uživatele. Z tohoto důvodu je prevence ze strany klientů založena především na dodržování základních bezpečnostních zásad při používání internetového bankovnictví, elektronických platebních prostředků a základních zásad bezpečného chování v internetové síti jako takových.

Základním preventivním opatřením je ochrana přístupových údajů k internetovému bankovnictví a platebním prostředkům. Klienti by nikdy neměli sdělovat své přihlašovací údaje, autorizační kódy ani údaje z platební karty třetím osobám, a to ani v případě, že se osoba vydává za pracovníka banky nebo jiné důvěryhodné instituce. Bankovní instituce přitom opakovaně upozorňují, že tyto údaje po klientech nikdy nepožadují prostřednictvím e-mailu, SMS zprávy ani telefonicky.[46]

Dalším důležitým prvkem prevence je schopnost klienta rozpoznat podvodné jednání, zejména phishingové, smishingové nebo vishingové útoky. Tyto útoky jsou často realizovány prostřednictvím e-mailových zpráv, SMS nebo telefonních hovorů, které se snaží vyvolat dojem naléhavé situace, například údajného ohrožení bankovního účtu nebo nutnosti potvrzení platby. Typickým znakem těchto útoků je snaha pachatele vyvolat časový tlak a přimět oběť k rychlému jednání bez dostatečného ověření informací.[47]

Významným preventivním opatřením je také bezpečné používání internetového bankovnictví a digitálních zařízení. Klienti by měli využívat pouze zabezpečená zařízení, pravidelně aktualizovat operační systém a bezpečnostní software a vyhýbat se přihlašování do internetového bankovnictví prostřednictvím veřejných nebo nezabezpečených sítí. Současně je vhodné věnovat zvýšenou pozornost internetovým stránkám, na které klient zadává své citlivé údaje, a ověřovat jejich důvěryhodnost.[48]

Další oblastí prevence je kontrola prováděných finančních operací a aktivní přístup klienta k zabezpečení účtu. Klienti by měli pravidelně kontrolovat pohyby na svém účtu, nastavovat si notifikace o provedených transakcích a v případě podezřelé operace neprodleně kontaktovat svou banku. Včasná reakce může v řadě případů zabránit vzniku větší finanční škody nebo umožnit zablokování neoprávněné transakce.[49]

---

[46] ČESKÁ NÁRODNÍ BANKA. Phishing: věrohodně se tvářící podvod. ČNB Blog [online]. [cit. 2026-03-17]. Dostupné z: https://www.cnb.cz/cs/o_cnb/cnblog/Phishing-verohodne-se-tvarici-podvod/

[47] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Prevence v kyber! [online]. [cit. 2026-03-17]. Dostupné z: https://nukib.gov.cz/download/vzdelavani/kurzy/Prevence-v-kyber.pdf

[48] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Základy kybernetické bezpečnosti [online]. [cit. 2026-03-17]. Dostupné z: https://nukib.gov.cz/download/vzdelavani/kurzy/Zaklady-kyberneticke-bezpecnosti.pdf

[49] EVROPSKÁ CENTRÁLNÍ BANKA. Doporučení pro bezpečnost internetových plateb. Frankfurt: ECB, 2013, s. 9. [online]. [cit. 2026-03-17]. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/dohled-financni-

Z pohledu praxe je vhodné upozornit také na problematiku instalace a využívání aplikací třetích stran, zejména v souvislosti s investičními podvody nebo technickou podporou. Pachatelé často přesvědčí oběť k instalaci aplikací umožňujících vzdálený přístup k zařízení, například pod záminkou pomoci při provedení investice nebo řešení technického problému. Tímto způsobem získávají přímou kontrolu nad zařízením oběti a mohou sledovat její činnost, včetně zadávání přihlašovacích údajů do internetového bankovnictví. Prevence v této oblasti spočívá především v neinstalování neznámých aplikací a neposkytování vzdáleného přístupu neověřeným osobám.[50]

Dalším významným rizikovým faktorem je nedostatečné oddělení osobních a pracovních aktivit v online prostředí. V praxi se lze setkat s případy, kdy klient používá stejné zařízení a stejné přihlašovací údaje pro více služeb, což zvyšuje pravděpodobnost jejich zneužití v případě úniku dat. Doporučovaným preventivním opatřením je používání unikátních hesel pro jednotlivé služby, případně využívání správců hesel, které umožňují bezpečné ukládání a správu přístupových údajů.[51]

Z hlediska současných trendů je rovněž důležité zmínit narůstající míru personalizace útoků. Pachatelé stále častěji využívají informace dostupné na sociálních sítích nebo z veřejných zdrojů, aby své útoky přizpůsobili konkrétní oběti. Klient by si měl být vědom toho, jaké informace o sobě zveřejňuje, a měl by omezit sdílení citlivých údajů, které by mohly být zneužity k vytvoření důvěryhodného podvodného scénáře.

Z pohledu prevence je rovněž zásadní schopnost klienta správně reagovat v okamžiku, kdy má podezření na podvodné jednání. V takové situaci je nezbytné neprodleně ukončit komunikaci s pachatelem, neprovádět žádné další finanční operace a kontaktovat bankovní instituci. Současně je vhodné změnit přístupové údaje a v případě podezření na zneužití zařízení provést jeho kontrolu bezpečnostním softwarem. Včasná reakce může významně omezit rozsah vzniklé škody.

Specifickou oblastí prevence je také práce s psychologickými aspekty rozhodování. Pachatelé často využívají stres, strach nebo naopak vidinu rychlého zisku, aby ovlivnili jednání oběti. Klient by si měl být vědom toho, jaké informace o sobě

---

trh/.galleries/legislativni_zakladna/banky_a_zalozny/download/ecb_doporuceni_pro_bezpecnost_internetovych_plateb.pdf

[50] MITNICK, Kevin; SIMON, William. *The Art of Deception: Controlling the Human Element of Security*. Indianapolis: Wiley, 2002, s. 80-90.

[51] MITNICK, Kevin; SIMON, William. *The Art of Deception: Controlling the Human Element of Security*. Indianapolis: Wiley, 2002, s. 30-40.

zveřejňuje, neboť právě jejich kombinace může být zneužita k vytvoření důvěryhodného podvodného scénáře.[52] Schopnost zachovat klid, ověřit si informace z nezávislého zdroje a nepodléhat časovému tlaku představuje jeden z nejúčinnějších nástrojů prevence.

Z provedené analýzy vyplývá, že prevence kybernetické kriminality ze strany bankovních klientů je založena především na informovanosti, obezřetnosti a dodržování základních bezpečnostních zásad. Přestože banky zavádějí stále sofistikovanější technická opatření, lidský faktor zůstává jedním z nejvýznamnějších rizikových prvků. Schopnost klienta rozpoznat podvodné jednání a správně reagovat na podezřelé situace tak představuje klíčový předpoklad pro efektivní ochranu finančních prostředků v prostředí elektronického bankovnictví.

5.3 Institucionální prevence kybernetické kriminality v České republice

Prevence kybernetické kriminality zaměřené na bankovní klienty není pouze záležitostí bankovních institucí a samotných uživatelů, ale významnou roli v této oblasti sehrávají také státní orgány a další instituce působící v oblasti bezpečnosti a ochrany kybernetického prostoru. V České republice je systém prevence kybernetické kriminality založen na spolupráci více subjektů, mezi které patří zejména Policie České republiky, Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), Česká národní banka a Česká bankovní asociace.

Jedním z klíčových subjektů v oblasti prevence a odhalování kybernetické kriminality je Policie České republiky, která se podílí nejen na vyšetřování jednotlivých případů, ale také na preventivní činnosti zaměřené na informování veřejnosti. Policie ČR pravidelně upozorňuje na aktuální formy podvodného jednání, zejména prostřednictvím médií a preventivních kampaní, a poskytuje veřejnosti doporučení, jak se v případě podezřelých situací zachovat. Současně spolupracuje s bankovními institucemi a dalšími subjekty při řešení konkrétních případů kybernetických útoků.[53]

[52] SCHNEIER, Bruce. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: W. W. Norton & Company, 2015, s.4-6.

[53] POLICIE ČESKÉ REPUBLIKY. Kyberkriminalita [online]. [cit. 2026-03-17]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

Významnou roli v oblasti prevence kybernetických hrozeb plní také Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), který je ústředním správním úřadem pro oblast kybernetické bezpečnosti v České republice. NÚKIB se zaměřuje zejména na prevenci kybernetických incidentů, vydávání metodických doporučení a vzdělávání veřejnosti v oblasti bezpečného chování v kybernetickém prostoru. Součástí jeho činnosti jsou rovněž vzdělávací projekty a osvětové kampaně zaměřené na rozpoznání kybernetických hrozeb, včetně podvodů souvisejících s elektronickým bankovnictvím.[54]

Dalším významným subjektem je Česká národní banka, která vykonává dohled nad finančním trhem a podílí se na zajištění stability a bezpečnosti bankovního sektoru. V oblasti prevence kybernetické kriminality se ČNB zaměřuje zejména na regulaci a kontrolu bezpečnostních standardů bank, vydávání doporučení a informování veřejnosti o aktuálních rizicích. Prostřednictvím svých informačních kanálů upozorňuje například na aktuální formy phishingových útoků a poskytuje doporučení pro bezpečné využívání finančních služeb.[55]

V oblasti prevence kybernetické kriminality hraje důležitou roli také Česká bankovní asociace (ČBA), která sdružuje bankovní instituce působící na území České republiky. ČBA se podílí na realizaci společných preventivních kampaní zaměřených na ochranu klientů před podvodným jednáním, například prostřednictvím kampaní upozorňujících na rizika spojená s phishingem nebo telefonickými podvody. Tyto kampaně mají za cíl zvýšit povědomí veřejnosti o aktuálních hrozbách a posílit bezpečné chování uživatelů bankovních služeb.[56]

Z uvedeného vyplývá, že prevence kybernetické kriminality v České republice je založena na spolupráci státních institucí, institucí vykonávající dohled a soukromého sektoru. Tato spolupráce je nezbytná vzhledem k dynamickému vývoji kybernetických hrozeb a jejich přesahu do zahraničí. Účinná prevence je proto založena nejen na technických opatřeních a legislativním rámci, ale také na systematické výchově veřejnosti a sdílení informací mezi jednotlivými subjekty.

[54] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Prevence v kyber! [online]. [cit. 2026-03-17]. Dostupné z: https://nukib.gov.cz/download/vzdelavani/kurzy/Prevence-v-kyber.pdf

[55] ČESKÁ NÁRODNÍ BANKA. Phishing: věrohodně se tvářící podvod. ČNB Blog [online]. [cit. 2026-03-17]. Dostupné z: https://www.cnb.cz/cs/o_cnb/cnblog/Phishing-verohodne-se-tvarici-podvod/

[56] ČESKÁ BANKOVNÍ ASOCIACE. Kybernetická bezpečnost [online]. [cit. 2026-03-17]. Dostupné z: https://www.cbaonline.cz/stranky/kyberneticka-bezpecnost

5.4 Prevence ze strany Policie České republiky

Prevence kybernetické kriminality ze strany Policie České republiky představuje důležitou součást systému ochrany bankovních klientů před podvodným jednáním v kybernetickém prostoru. Policie ČR v této oblasti neplní pouze represivní funkci spočívající v odhalování a vyšetřování trestné činnosti, ale současně se aktivně podílí na preventivních aktivitách zaměřených na snižování rizika vzniku této kriminality. Preventivní činnost policie je přitom realizována jak na celostátní úrovni, tak i na úrovni jednotlivých krajských ředitelství a územních odborů.

Z pohledu praxe lze uvést, že jedním ze základních nástrojů prevence je informování veřejnosti o aktuálních formách kybernetické kriminality. Policie ČR pravidelně zveřejňuje varování před konkrétními typy podvodů, zejména prostřednictvím médií, sociálních sítí a oficiálních webových stránek. Tato varování reagují na aktuální trendy, jako jsou phishingové útoky, vishing, investiční podvody nebo zneužití bankovních účtů. Cílem těchto aktivit je upozornit veřejnost na konkrétní scénáře podvodného jednání a poskytnout základní doporučení, jak se v takových situacích zachovat.

Dalším významným prvkem prevence je přímá komunikace s veřejností prostřednictvím preventivních akcí a vzdělávacích aktivit. Policie ČR se podílí na organizaci besed, seminářů a preventivních kampaní, které jsou zaměřeny na různé skupiny obyvatel, včetně seniorů, kteří patří mezi nejohroženější skupiny. Tyto aktivity mají za cíl zvýšit povědomí o kybernetických hrozbách a posílit schopnost jednotlivců rozpoznat podvodné jednání.

Z pohledu policejní praxe je však zásadní také fáze po oznámení trestného činu. V případě, že poškozený nahlásí podezřelou transakci nebo podvodné jednání včas, může policie ve spolupráci s bankovními institucemi přispět k omezení následků trestné činnosti. V praxi dochází například k neprodlenému kontaktování banky s cílem zablokovat finanční prostředky na účtu příjemce nebo zabránit dalším převodům. Úspěšnost těchto opatření je však výrazně ovlivněna časovým faktorem, neboť pachatelé často převádějí finanční prostředky v krátkém časovém úseku na další účty, mnohdy vedené v zahraničí.

V praxi se lze velmi často setkat s případy, kdy poškození oznámí podvodné jednání až s časovým odstupem, kdy již došlo k převedení finančních prostředků na více účtů nebo do prostředí kryptoměn. V těchto případech je možnost jejich zajištění výrazně omezená. Typickým znakem těchto útoků je řetězení převodů, kdy jsou finanční prostředky rozděleny na menší částky a postupně přeposílány přes více účtů, často i přes účty tzv. „bílých koní“. Tento postup výrazně komplikuje jejich dohledání a následné zajištění.

Důležitou součástí prevence je také spolupráce Policie ČR s dalšími subjekty. Policie úzce spolupracuje s bankovními institucemi, mobilními operátory a dalšími organizacemi, které mohou přispět k identifikaci pachatelů nebo k omezení škod způsobených trestnou činností.

Z pohledu praxe je však nutné zdůraznit i limity preventivní činnosti Policie ČR. Jedním z hlavních problémů je rychlost, s jakou dochází k převodům finančních prostředků, a skutečnost, že pachatelé často využívají zahraniční účty nebo anonymizované prostředí kryptoměn. Dalším limitem je lidský faktor na straně poškozených, kteří i přes opakovaná varování často podléhají manipulaci a sami provádějí úkony vedoucí ke vzniku škody.

Z uvedeného vyplývá, že prevence kybernetické kriminality ze strany Policie České republiky je založena na kombinaci informování veřejnosti, spolupráce s dalšími subjekty a operativní reakce na vzniklé incidenty. Přestože tyto aktivity přispívají ke snižování rizika podvodného jednání, jejich účinnost je do značné míry závislá na spolupráci samotných bankovních klientů a jejich schopnosti rozpoznat podvodné jednání a včas na něj reagovat.

6. Praktická část

Teoretické poznatky uvedené v předchozích kapitolách této práce poskytují základní rámec pro pochopení problematiky kybernetické kriminality zaměřené na bankovní klienty. Byly zde vymezeny klíčové pojmy související s kybernetickým prostorem, internetovým bankovnictvím, sociálním inženýrstvím a preventivními opatřeními v oblasti kybernetické bezpečnosti. Současně byly na základě zkušeností z praxe popsány typické scénáře kybernetických útoků, se kterými se lze při řešení této trestné činnosti setkat.

Na tuto teoretickou část navazuje praktická část bakalářské práce, jejímž cílem je porovnat fungování preventivních mechanismů bankovních institucí s reálnou zkušeností bankovních klientů, kteří se stali obětmi kybernetické kriminality. Zatímco bankovní instituce zavádějí stále sofistikovanější technická i organizační opatření k ochraně finančních prostředků klientů, samotná účinnost těchto opatření je do značné míry ovlivněna lidským faktorem, zejména schopností klientů rozpoznat podvodné jednání a adekvátně na něj reagovat.

Za tímto účelem byl proveden kvalitativní výzkum založený na rozhovorech s vybranými respondenty. Do výzkumu byli zařazeni celkem čtyři respondenti. Pracovník bankovní instituce, který se ve své profesní činnosti zabývá problematikou detekce a prevence bankovních podvodů, a dále osoby, které mají osobní zkušenost s kybernetickým útokem zaměřeným na jejich bankovní účet. Získané poznatky jsou následně analyzovány a porovnány s teoretickými východisky uvedenými v předchozích kapitolách práce.

Cílem této části práce je identifikovat hlavní faktory, které mohou přispívat k úspěšnosti kybernetických útoků na bankovní klienty, a na základě těchto zjištění formulovat doporučení směřující ke zvýšení efektivity preventivních opatření v oblasti kybernetické bezpečnosti.

6.1 Metodika výzkumu

Pro potřeby praktické části bakalářské práce byla zvolena metoda kvalitativního výzkumu, konkrétně forma polostrukturovaných rozhovorů. Tato metoda byla vybrána s ohledem na charakter zkoumané problematiky, která je výrazně ovlivněna

individuálními zkušenostmi a subjektivním vnímáním jednotlivých účastníků kybernetických incidentů. Kybernetické podvody v oblasti bankovnictví jsou často založeny na sociálním inženýrství a psychologické manipulaci, a proto je pro jejich pochopení důležité zohlednit nejen technické okolnosti incidentu, ale také lidský faktor, tedy způsob uvažování a rozhodování samotných klientů.

Metoda rozhovoru umožňuje získat podrobnější a komplexnější informace, než jaké by bylo možné získat například prostřednictvím standardizovaného dotazníkového šetření. Respondenti mají při rozhovoru větší prostor popsat průběh incidentu vlastními slovy, doplnit své osobní zkušenosti a vyjádřit své názory na fungování preventivních opatření bankovních institucí. Současně tato metoda umožňuje flexibilně reagovat na odpovědi respondentů a v případě potřeby upřesnit některé skutečnosti, které mohou být pro výzkum relevantní.

Pro všechny respondenty byl připraven soubor předem definovaných otázek. Tyto otázky byly zaměřeny zejména na zkušenosti respondentů s kybernetickým incidentem, jejich informovanost o preventivních opatřeních bank a na průběh řešení situace po zjištění podvodu. Polostrukturovaná forma rozhovoru umožnila zachovat jednotný tematický rámec výzkumu a zároveň poskytla respondentům prostor pro doplnění dalších informací, které považovali za důležité.

Zařazení respondentů do dvou skupin bylo zvoleno záměrně, aby bylo možné porovnat pohled bankovní instituce na problematiku prevence kybernetické kriminality s reálnou zkušeností klientů, kteří byli těmito útoky přímo zasaženi. Zatímco rozhovor s pracovníkem banky poskytuje informace o technických a organizačních opatřeních využívaných bankou k ochraně klientů, rozhovory s poškozenými osobami umožňují lépe pochopit průběh samotných incidentů a způsob, jakým klienti vnímají preventivní opatření bankovních institucí.

Všichni respondenti byli před zahájením rozhovoru seznámeni s účelem výzkumu a s tím, že jejich účast je dobrovolná. Současně byli informováni o anonymizaci získaných údajů a o skutečnosti, že poskytnuté informace budou využity výhradně pro účely této bakalářské práce. Z tohoto důvodu nejsou v práci uváděny žádné identifikační údaje, které by umožňovaly ztotožnění konkrétních osob nebo bankovní instituce. Pro přehlednost a zachování autenticity jsou přepisy těchto rozhovorů uvedeny v přílohách této práce.

6.2 Analýza rozhovoru s pracovníkem bankovní instituce

Rozhovor s pracovníkem bankovní instituce poskytuje důležitý pohled na problematiku kybernetické kriminality zaměřené na bankovní klienty z perspektivy finanční instituce, která se s těmito incidenty setkává v každodenní praxi. Respondent působí v oblasti prevence a detekce bankovních podvodů a ve své pracovní činnosti se podílí na monitorování podezřelých transakcí, vyhodnocování rizikového chování klientů v internetovém bankovnictví a na nastavování bezpečnostních mechanismů banky. Z jeho odpovědí vyplývá, že kybernetická kriminalita představuje pro bankovní sektor dlouhodobý a rostoucí problém, který vyžaduje neustálé přizpůsobování bezpečnostních opatření.

Z rozhovoru vyplývá, že banky se s pokusy o kybernetické podvody setkávají prakticky na denní bázi. Podle respondenta patří mezi nejčastější typy útoků zejména phishing, vishing, podvodné investiční platformy nebo útoky založené na sociálním inženýrství, které mají za cíl přimět klienta k dobrovolnému provedení finanční transakce nebo ke sdělení citlivých údajů. Tento poznatek koresponduje s teoretickými východisky uvedenými v předchozích kapitolách práce, podle nichž jsou útoky založené na sociálním inženýrství v současnosti jednou z nejrozšířenějších forem kybernetické kriminality zaměřené na bankovní klienty.

Významnou součástí ochrany klientů jsou podle respondenta preventivní aktivity banky. Ty zahrnují především informování klientů o aktuálních hrozbách prostřednictvím různých komunikačních kanálů, například prostřednictvím internetového bankovnictví, mobilní aplikace, elektronické pošty nebo informačních kampaní realizovaných ve spolupráci s profesními organizacemi bankovního sektoru. Tyto aktivity mají za cíl zvýšit povědomí klientů o možných formách podvodného jednání a upozornit je na rizika spojená s poskytováním citlivých údajů třetím osobám.

Respondent však současně upozorňuje na skutečnost, že účinnost těchto preventivních aktivit je obtížné přesně vyhodnotit. I přes dlouhodobé informační kampaně a dostupnost bezpečnostních doporučení existuje skupina klientů, která podobným upozorněním nevěnuje dostatečnou pozornost. Tento poznatek potvrzuje váhu lidského faktoru v oblasti kybernetické bezpečnosti, kdy technické zabezpečení systémů může být velmi pokročilé, avšak kamenem úrazu bývá často jednání samotného klienta.

Vedle preventivních aktivit zaměřených na edukaci klientů banky využívají také řadu technických nástrojů určených k detekci podezřelého chování v internetovém bankovnictví. Podle respondenta se jedná zejména o monitorování neobvyklých transakcí, sledování změn zařízení nebo přístupových údajů, vyhodnocování přihlášení z rizikových IP adres či geografických lokalit a využívání různých typů seznamů rizikových zařízení nebo účtů. Tyto informace jsou následně vyhodnocovány prostřednictvím interních bezpečnostních systémů, které kombinují více faktorů a na jejich základě stanovují míru rizikovosti konkrétní operace.

V současnosti banky stále více využívají také prvky behaviorální analýzy, tedy sledování způsobu, jakým klient s bankovním rozhraním pracuje. Může jít například o rychlost zadávání údajů, pohyb kurzoru nebo neobvyklou rychlost provádění jednotlivých operací. Tyto parametry mohou napovědět, zda se jedná o běžné chování klienta, nebo o automatizovaný či podvodný přístup k účtu. Výsledkem těchto analýz je zpravidla stanovení určitého rizikového skóre, podle kterého systém rozhoduje o dalším postupu.

Pokud bankovní systémy vyhodnotí určité chování jako rizikové, mohou být podle respondenta okamžitě aktivována různá bezpečnostní opatření. V některých případech dochází k dodatečnému ověření identity klienta, v jiných situacích může být dočasně omezen přístup k bankovnímu účtu nebo pozastavena konkrétní transakce. Současně může být klient kontaktován pracovníkem banky, který s ním situaci ověří. Podle respondenta probíhají automatizované reakce bankovních systémů často v řádu sekund, zatímco manuální vyhodnocení situace a následný kontakt s klientem může trvat déle v závislosti na konkrétních okolnostech.

Z rozhovoru rovněž vyplývá, že banky průběžně vyhodnocují zkušenosti z již řešených incidentů a využívají je k dalšímu zlepšování preventivních opatření. Získané poznatky se promítají například do úprav detekčních pravidel, aktualizace varovných upozornění nebo zavádění nových technologických řešení do bezpečnostních systémů banky. Tento proces ukazuje, že ochrana bankovních klientů je dynamickou oblastí, která se neustále vyvíjí v reakci na nové formy kybernetických útoků.

Za největší slabinu současného systému ochrany bankovních klientů považuje respondent především lidský faktor. Podvodníci podle něj často využívají psychologickou manipulaci, časový tlak a důvěru klientů v autoritu banky nebo jiných

institucí. Tímto způsobem jsou schopni přimět klienty k provedení transakcí nebo k poskytnutí citlivých údajů, aniž by museli technicky překonávat zabezpečení bankovních systémů. Tento závěr potvrzuje skutečnost, že velká část úspěšných útoků je založena právě na metodách sociálního inženýrství.

Z pohledu prevence považuje respondent za nejúčinnější kombinaci technologických opatření a systematické edukace klientů. Vedle zdokonalování detekčních systémů bank je podle něj důležité zaměřit se také na srozumitelnou a prakticky orientovanou informovanost klientů, která by měla být přizpůsobena různým skupinám uživatelů bankovních služeb. Právě propojení technických nástrojů banky s informovaností a obezřetností klientů může podle respondenta významně přispět ke snížení počtu úspěšných kybernetických útoků.

6.3 Analýza rozhovorů s oběťmi kybernetických podvodů

Druhou skupinu respondentů tvořily osoby, které se v minulosti staly obětí kybernetického podvodu souvisejícího s využíváním internetového bankovnictví. Rozhovory s těmito respondenty poskytují důležitý pohled na problematiku kybernetické kriminality z perspektivy samotných poškozených osob a umožňují lépe pochopit, za jakých okolností k jednotlivým incidentům došlo. Současně přinášejí informace o tom, jak klienti bank vnímají preventivní opatření bankovních institucí a jaké zkušenosti mají s řešením podvodného jednání po jeho odhalení.

Z odpovědí respondentů vyplývá, že všichni dlouhodobě využívají internetové bankovnictví a běžně jej používají při každodenních finančních operacích. Internetové bankovnictví je pro ně standardním nástrojem pro správu financí, který využívají několik let a používají jej pravidelně. Tato skutečnost ukazuje, že obětí kybernetických podvodů se nemusí stát pouze osoby bez zkušeností s digitálními technologiemi, ale také běžní uživatelé bankovních služeb, kteří jsou na využívání online bankovnictví dlouhodobě zvyklí.

Pokud jde o samotný průběh incidentů, odpovědi respondentů potvrzují význam sociálního inženýrství jako jednoho z hlavních nástrojů pachatelů kybernetické kriminality. V jednom z případů došlo k podvodu v souvislosti s prodejem zboží prostřednictvím internetového inzertního portálu, kdy oběť klikla na podvodný odkaz týkající se údajného doručení zásilky a následně byla kontaktována osobou vydávající

se za pracovníka banky. V jiném případě byl útok realizován prostřednictvím podvodného e-mailu vydávajícího se za zprávu od České pošty. Další respondent popsal situaci obecně jako chybu v úsudku a uvěření podvodné komunikaci, kdy se jednalo o příslib výhodných investic a následné zpřístupnění vlastního zařízení, respektive i bankovní aplikace. Přestože se jednotlivé scénáře liší, společným prvkem všech případů je využití důvěry oběti a manipulace s jejím rozhodováním.

Významným zjištěním je rovněž skutečnost, že respondenti si často nebyli vědomi konkrétních preventivních upozornění ze strany banky před samotným incidentem. Jeden z respondentů uvedl, že si žádných preventivních informací před incidentem nebyl vědom a s podobnými informacemi se setkal až dodatečně po vyřešení situace. Naopak jiný respondent uvedl, že banka sice preventivní informace poskytovala prostřednictvím různých komunikačních kanálů, avšak těmto upozorněním nevěnoval dostatečnou pozornost. Tyto odpovědi naznačují, že preventivní komunikace bank může být sice dostupná, avšak její účinnost závisí také na míře pozornosti a obezřetnosti samotných klientů.

Z rozhovorů dále vyplývá, že ve většině případů iniciovali řešení vzniklé situace samotní klienti, kteří kontaktovali banku po zjištění podvodu. Pouze v jednom případě respondent uvedl, že byl bankou kontaktován přímo v souvislosti s podezřelou transakcí, avšak v době, kdy již bylo na zásah pozdě. Tyto zkušenosti ukazují, že reakce banky může být do určité míry závislá na okolnostech konkrétního incidentu a na tom, zda bankovní systémy vyhodnotí danou transakci jako podezřelou.

Zajímavým zjištěním je také skutečnost, že respondenti po této zkušenosti změnili své chování při používání internetového bankovnictví. Všichni uvedli, že se po incidentu snaží být opatrnější, více kontrolují prováděné transakce nebo se snaží ověřovat důvěryhodnost internetových služeb. Někteří respondenti také uvedli, že si po incidentu sjednali pojištění proti kybernetickým podvodům nebo začali využívat další bezpečnostní opatření. Tato skutečnost potvrzuje, že osobní zkušenost s kybernetickým podvodem často vede k výraznému zvýšení opatrnosti při používání digitálních bankovních služeb.

Pokud jde o hodnocení preventivních opatření bank, respondenti se shodují především na tom, že by přivítali výraznější a srozumitelnější upozornění na rizikové situace. Jeden z respondentů například uvedl, že by bylo vhodné zavést výraznější

upozornění při provádění větších finančních transakcí nebo při nestandardních. Další respondent navrhl například delší časový odstup při provádění některých typů plateb, zejména v případě zahraničních transakcí. Tyto návrhy ukazují, že klienti často očekávají aktivnější roli banky při prevenci podvodného jednání. Současně však z odpovědí respondentů vyplývá, že významnou roli hraje také osobní odpovědnost klientů. Někteří respondenti sami přiznávají, že podcenili riziko nebo nevěnovali dostatečnou pozornost preventivním informacím, které byly dostupné. Tento poznatek potvrzuje závěry uvedené v předchozí kapitole, podle nichž je lidský faktor často nejslabším článkem v systému ochrany bankovních klientů.

Z provedené analýzy rozhovorů lze tedy konstatovat, že kybernetické podvody zaměřené na bankovní klienty jsou ve značné míře založeny na psychologické manipulaci a využívání důvěry obětí. Přestože banky zavádějí stále sofistikovanější bezpečnostní mechanismy, jejich účinnost je do značné míry ovlivněna schopností klientů rozpoznat podvodné jednání a adekvátně na něj reagovat. Výsledky rozhovorů zároveň naznačují, že vedle technických opatření bank je pro zvýšení bezpečnosti bankovních klientů klíčová také systematická a srozumitelná edukace uživatelů digitálních bankovních služeb.

7. Komparace výsledků rozhovorů a návrhy preventivních opatření

Analýza rozhovorů s pracovníkem bankovní instituce a s osobami, které se staly obětí kybernetického podvodu, umožňuje porovnat dva odlišné pohledy na problematiku kybernetické kriminality zaměřené na bankovní klienty. Zatímco bankovní instituce přistupují k ochraně klientů především prostřednictvím technických a organizačních bezpečnostních opatření, zkušenosti poškozených osob poukazují na praktické situace, ve kterých tato opatření nemusí být dostatečně účinná. Porovnání těchto dvou perspektiv tak umožňuje identifikovat hlavní faktory, které ovlivňují úspěšnost kybernetických útoků, a současně formulovat možné směry dalšího zlepšení preventivních opatření.

Z rozhovoru s pracovníkem bankovní instituce vyplývá, že banky věnují problematice kybernetické bezpečnosti značnou pozornost a využívají širokou škálu technických nástrojů pro detekci podvodného jednání. Mezi tyto nástroje patří zejména monitoring neobvyklých transakcí, sledování změn zařízení nebo přístupových údajů, vyhodnocování přihlášení z rizikových IP adres či geografických lokalit a využívání behaviorální analýzy uživatelského chování. Tyto mechanismy umožňují bankám v řadě případů odhalit podezřelé operace a reagovat na ně prostřednictvím blokace transakce, dodatečného ověření identity klienta nebo kontaktování klienta bankou.

Na druhé straně rozhovory s oběťmi kybernetických podvodů ukazují, že i přes existenci těchto bezpečnostních opatření dochází v praxi k situacím, kdy jsou klienti manipulováni k provedení transakcí, které následně vedou ke krádeži jejich finančních prostředků. Společným znakem analyzovaných případů je skutečnost, že pachatelé využívají zejména metody sociálního inženýrství, tedy psychologickou manipulaci, vytváření časového tlaku a zneužití důvěry obětí v autoritu institucí. V takových případech klient často provádí jednotlivé kroky sám a využívá přitom legitimní autentizační a autorizační mechanismy bankovního systému.

Porovnání odpovědí obou skupin respondentů rovněž ukazuje určitou rozdílnost ve vnímání preventivních opatření. Z pohledu banky jsou preventivní informace klientům předávány prostřednictvím různých komunikačních kanálů, například prostřednictvím internetového bankovnictví, mobilních aplikací, e-mailových

upozornění nebo informačních kampaní. Naopak část klientů uvádí, že si těchto upozornění před incidentem nebyla vědoma, případně jim nevěnovala dostatečnou pozornost. Tento rozdíl naznačuje, že samotná existence preventivních informací nemusí automaticky znamenat jejich efektivní využití ze strany klientů.

Dalším významným zjištěním je skutečnost, že reakce banky na podezřelé operace může být v některých případech omezená tím, že klient transakci sám autorizuje. V takové situaci je pro banku obtížné rozlišit, zda se jedná o legitimní operaci, nebo o jednání provedené pod vlivem podvodného jednání třetí osoby. Tato skutečnost potvrzuje, že v oblasti kybernetické bezpečnosti bankovních služeb nelze spoléhat pouze na technické zabezpečení systémů, ale je nutné věnovat značnou pozornost také informovanosti a obezřetnosti samotných klientů.

Na základě provedené analýzy lze identifikovat několik oblastí, ve kterých by bylo možné posílit preventivní opatření zaměřená na ochranu bankovních klientů před kybernetickými útoky.

První oblastí je zvýšení srozumitelnosti a praktičnosti preventivní komunikace směrem ke klientům. Informace o kybernetických hrozbách by měly být prezentovány způsobem, který je pro běžné uživatele snadno pochopitelný a který zdůrazňuje konkrétní rizikové situace, se kterými se mohou klienti setkat. Vhodným nástrojem mohou být například krátká a jasná upozornění přímo v prostředí internetového bankovnictví nebo mobilní aplikace, která klienta upozorní na možná rizika v okamžiku provádění konkrétní operace. Vhodné by byly také krátké praktické příklady, kterým porozumí většina klientů.

Druhou oblastí je další rozvoj technických nástrojů pro detekci nestandardního chování klienta. V současnosti již banky využívají různé formy behaviorální analýzy a vyhodnocování rizikových scénářů, nicméně další rozvoj těchto systémů může přispět k rychlejší identifikaci potenciálně podvodných operací. V praxi by to mohlo znamenat například důslednější vyhodnocování neobvyklých platebních vzorců nebo zavedení dodatečných bezpečnostních kontrol v situacích, kdy klient provádí nestandardní finanční operace nebo větší množství úkonů v krátkém časovém úseku, což neodpovídá lidským možnostem.

Třetí oblastí je systematická edukace klientů v oblasti kybernetické bezpečnosti. Výsledky rozhovorů ukazují, že mnoho klientů si plně uvědomí rizika spojená s kybernetickými podvody až poté, co se sami stanou jejich obětí. Preventivní aktivity by proto měly být zaměřeny na dlouhodobé zvyšování povědomí o kybernetických hrozbách a na posilování základních bezpečnostních návyků při používání digitálních bankovních služeb, k čemuž je v digitální době paradoxně vhodnější osobní jednání s klientem než „anonymní“ informační zprávy formou emailu, sms zpráv nebo zpráv v bankovní aplikaci, které klient bez větší pozornosti přejde, takzvaně „odklikne“. Dobrým příkladem by bylo povinné vyhrazení času na tuto edukaci při osobním kontaktu s klientem, kteří jsou často pravidelně zváni do banky k aktualizaci služeb, které banka klientovi poskytuje.

Na základě provedené analýzy lze konstatovat, že ochrana bankovních klientů před kybernetickou kriminalitou je výsledkem kombinace několika faktorů. Vedle technických bezpečnostních opatření bank hraje zásadní roli také lidský faktor, tedy schopnost klientů rozpoznat podvodné jednání a adekvátně na něj reagovat. Účinná prevence proto vyžaduje propojení technologických nástrojů bank s dostatečnou informovaností a obezřetností uživatelů bankovních služeb.

Výsledky provedeného výzkumu zároveň potvrzují stanovený cíl této bakalářské práce, kterým bylo zhodnotit zkušenosti bankovních klientů s preventivními opatřeními proti kybernetickým útokům a porovnat je s preventivními mechanismy využívanými bankovními institucemi. Provedená analýza ukazuje, že mezi těmito dvěma pohledy existuje určitý rozdíl, zejména v oblasti vnímání preventivních informací a v roli lidského faktoru při realizaci kybernetických útoků. Z těchto poznatků lze vyvodit, že další rozvoj prevence kybernetické kriminality by měl být zaměřen nejen na technické zabezpečení bankovních systémů, ale také na efektivnější komunikaci a vzdělávání bankovních klientů v oblasti bezpečného používání elektronického bankovnictví.

Závěr

Kybernetická kriminalita představuje v současné digitální společnosti významný bezpečnostní problém, který se stále častěji dotýká také běžných uživatelů bankovních služeb. Rozvoj informačních technologií a rostoucí využívání elektronického bankovnictví přináší řadu výhod v podobě dostupnosti a rychlosti finančních operací, současně však vytváří nové příležitosti pro páchání trestné činnosti v kybernetickém prostoru. Pachatelé kybernetických útoků přitom stále častěji využívají sofistikované metody sociálního inženýrství, které jsou zaměřeny především na manipulaci s lidským chováním a zneužití důvěry bankovních klientů.

Cílem této bakalářské práce bylo zhodnotit zkušenosti bankovních klientů s preventivními opatřeními proti kybernetickým útokům a porovnat je s preventivními mechanismy uplatňovanými bankovními institucemi. Teoretická část práce se zaměřila na vymezení základních pojmů souvisejících s kybernetickou kriminalitou, kybernetickou bezpečností a bankovními službami. Současně byly popsány nejčastější formy kybernetických útoků zaměřených na bankovní klienty a základní specifika vyšetřování této trestné činnosti.

Na teoretickou část navázala praktická část práce, která byla realizována formou kvalitativního výzkumu založeného na polostrukturovaných rozhovorech. Do výzkumu byl zahrnut pracovník bankovní instituce, který se profesně zabývá prevencí a detekcí bankovních podvodů, a dále osoby, které se v minulosti staly obětí kybernetického podvodu souvisejícího s využíváním internetového bankovnictví. Cílem této části bylo získat konkrétní poznatky z praxe a porovnat pohled bankovních institucí na prevenci kybernetické kriminality se zkušenostmi samotných klientů.

Z provedené analýzy vyplynulo, že bankovní instituce využívají celou řadu technických a organizačních opatření zaměřených na ochranu klientů před kybernetickými útoky. Mezi tato opatření patří zejména monitoring neobvyklých transakcí, sledování změn přístupových zařízení nebo IP adres, využívání behaviorální analýzy uživatelského chování a další nástroje pro vyhodnocování rizikových operací. Tyto mechanismy umožňují bankám v řadě případů identifikovat podezřelé aktivity a reagovat na ně prostřednictvím blokace transakcí, dodatečného ověření identity klienta nebo přímého kontaktování klienta bankou.

Současně však rozhovory s oběťmi kybernetických podvodů ukázaly, že značná část útoků je založena především na metodách sociálního inženýrství. Pachatelé využívají psychologickou manipulaci, vytvářejí časový tlak a zneužívají důvěru obětí v bankovní instituce nebo jiné autority. V těchto situacích klient často provádí jednotlivé operace sám a využívá přitom legitimní autentizační a autorizační mechanismy bankovního systému. Z pohledu banky se tak může jednat o autorizovanou transakci, přestože byla provedena na základě podvodného jednání.

Výsledky výzkumu rovněž naznačují, že mezi bankovními institucemi a klienty může existovat určitý rozdíl ve vnímání preventivních opatření. Zatímco banky poskytují klientům informace o kybernetických hrozbách prostřednictvím různých komunikačních kanálů, část klientů těmto informacím nevěnuje dostatečnou pozornost nebo si jejich existenci neuvědomuje. To potvrzuje, že vedle technických bezpečnostních opatření hraje významnou roli také lidský faktor, zejména informovanost a obezřetnost uživatelů bankovních služeb.

Na základě provedené analýzy lze konstatovat, že účinná prevence kybernetické kriminality zaměřené na bankovní klienty musí být založena na kombinaci několika vzájemně se doplňujících způsobů. Vedle dalšího rozvoje technických nástrojů pro detekci podvodného jednání je důležité zaměřit se také na srozumitelnou a systematickou edukaci klientů v oblasti kybernetické bezpečnosti. Preventivní opatření by měla být klientům prezentována způsobem, který je pro běžné uživatele snadno pochopitelný a který zdůrazňuje konkrétní rizikové situace, se kterými se mohou při využívání elektronického bankovnictví setkat.

Přínosem této bakalářské práce je zejména propojení teoretických poznatků s praktickými zkušenostmi z oblasti prevence a řešení kybernetických podvodů. Výsledky provedené analýzy potvrzují význam lidského faktoru v oblasti kybernetické bezpečnosti a poukazují na potřebu kombinovat technická bezpečnostní opatření bank s efektivní komunikací a vzděláváním klientů. Tyto poznatky mohou přispět k lepšímu pochopení problematiky kybernetické kriminality zaměřené na bankovní klienty a současně mohou být využity při dalším rozvoji preventivních aktivit v oblasti ochrany bankovních služeb.

Seznam použitých zdrojů

Literární zdroje

1. ČESKÁ REPUBLIKA. *Strategie prevence kriminality v České republice na léta 2022–2027*. Praha: Ministerstvo vnitra České republiky, 2022. 36 s.
2. GŘIVNA, T, POLČÁK R. *Kyberkriminalita a právo*. Praha: Auditorium, 2008. 220 s. ISBN 978-80-903786-7-4.
3. HOLAS, Jakub. *Bezpečí, kriminalita a prevence*. Praha: Institut pro kriminologii a sociální prevenci, 2019. 119 s. ISBN 978-80-7338-185-1.
4. JIRÁSEK, Petr – NOVÁK, Luděk – POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti. 6. doplněné a upravené elektronické vydání*. Praha: NÚKIB, 2025. 396 s. ISBN 978-80-908388-9-5.
5. JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. 284 s. ISBN 978-80-247-1561-2.
6. KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z.s.p.o, 2016. 552 s. ISBN 978-80-88168-15-7.
7. KOLOUCH, J. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o, 2019. 556 s. ISBN 978-80- 88168-31-7.
8. MEJSTŘÍK, Michal; PEČENÁ, Magda; TEPLÝ, Petr. *Bankovnictví v teorii a praxi*. 1. vydání. Praha: Karolinum, 2014. 853 s. ISBN 978-80-246-2870-7.
9. SCHEINOST, Miroslav. *Kriminalita očima kriminologů*. 1. vydání. Praha: Institut pro kriminologii a sociální prevenci, 2010. 238 s. ISBN 978-80-7338-096-0.
10. SMEJKAL, V. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. 1166 s. ISBN 978-80-7380-849-5.
11. ŠÁMAL, Pavel a kol. *Trestní zákoník I. Komentář.* 2. vydání. Praha: C. H. Beck, 2012. 1450 s. ISBN 978-80-7400-428-5.
12. ŠÁMAL, Pavel a kol. *Trestní zákoník II. Komentář*. 2. vydání. Praha: C. H. Beck, 2012. 1451-3586 s. ISBN 978-80-7400-429-2.
13. ZEMAN, Petr a kol. *Bezpečí, kriminalita a prevence*. Praha: Institut pro kriminologii a sociální prevenci, 2011. ISBN 978-80-7338-107-3.

14. MITNICK, Kevin; SIMON, William. *The Art of Deception: Controlling the Human Element of Security*. Indianapolis: Wiley, 2002. 352 s. ISBN 978-0-7645-4280-0.
15. SCHNEIER, Bruce. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: W. W. Norton & Company, 2015. 383 s. ISBN 978-0-393-35217-7.

Elektronické zdroje

1. ČESKÁ BANKOVNÍ ASOCIACE. Bezpečnost klientů [online]. [cit. 2026-03-17]. Dostupné z: https://www.cbaonline.cz/bezpecnost
2. ČESKÁ NÁRODNÍ BANKA. Bezpečnost platebního styku [online]. [cit. 2026-03-17]. Dostupné z: https://www.cnb.cz
3. ČESKÁ NÁRODNÍ BANKA. Phishing: věrohodně se tvářící podvod [online]. [cit. 2026-03-17]. Dostupné z: https://www.cnb.cz/cs/o_cnb/cnblog/phishing-verohodne-se-tvarici-podvod/
4. EVROPSKÁ CENTRÁLNÍ BANKA. Doporučení pro bezpečnost internetových plateb [online]. [cit. 2026-03-17]. Frankfurt: ECB, 2013. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/platebni-styk/.galleries/download/Doporuceni_pro_bezpecnost_internetovych_plateb.pdf
5. EVROPSKÝ PARLAMENT A RADA EU. Směrnice (EU) 2015/2366 (PSD2) o platebních službách [online]. [cit. 2026-03-17]. Dostupné z: https://eur-lex.europa.eu
6. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Kybernetická bezpečnost [online]. [cit. 2026-03-17]. Dostupné z: https://nukib.gov.cz
7. POLICIE ČESKÉ REPUBLIKY. Kyberkriminalita [online]. [cit. 2026-03-17]. Dostupné z: https://www.policie.cz
8. VLÁDA ČESKÉ REPUBLIKY. Strategie prevence kriminality v České republice na léta 2022–2027 [online]. [cit. 2026-03-17]. Dostupné z: https://www.mvcr.cz

Legislativní dokumenty

1. ČESKO. Zákon č. 40/2009 Sb., trestní zákoník.
2. ČESKO. Zákon č. 370/2017 Sb., o platebním styku.

Judikatura

1. NEJVYŠŠÍ SOUD ČR. Usnesení ze dne 16. 5. 2018, sp. zn. 4 Tdo 456/2018.
2. NEJVYŠŠÍ SOUD ČR. Usnesení sp. zn. 4 Tdo 1115/2022.

Seznam zkratek

1. **ČBA** – Česká bankovní asociace
2. **ČNB** – Česká národní banka
3. **ČR** – Česká republika
4. **eSIM** – embedded SIM (elektronická SIM karta)
5. **IP** – Internet Protocol
6. **NÚKIB** – Národní úřad pro kybernetickou a informační bezpečnost
7. **PIN** – Personal Identification Number
8. **SMS** – Short Message Service
9. **VPN** – Virtual Private Network

Seznam příloh

Přílohy

Příloha č. 1 – Rozhovor s pracovníkem banky

Forma rozhovoru: polostrukturovaný rozhovor
Charakteristika respondenta: pracovník bankovní instituce (manažer týmu Fraud Management, anonymizováno)

Otázka 1: Jaká je Vaše pracovní pozice a jakým způsobem se ve své práci setkáváte s problematikou bezpečnosti bankovních klientů?
Odpověď: Pracuji jako manažer v týmu Fraud Managementu UniCredit Bank CZ/SK. V rámci své pracovní činnosti se denně zabývám prevencí a detekcí podvodného jednání zaměřeného na klienty banky. Sleduji podezřelé transakce, vyhodnocuji rizikové chování klientů v internetovém bankovnictví a podílím se na nastavování bezpečnostních pravidel a preventivních procesů. Současně poskytujeme součinnost orgánům činným v trestním řízení při vyšetřování podvodných jednání.

Otázka 2: Jak často se banka setkává s případy kybernetické kriminality v oblasti internetového bankovnictví?
Odpověď: Případy kybernetické kriminality jsou v praxi banky každodenní záležitostí. Nejčastěji se jedná o falešné investiční platformy, vishing, phishing, podvodné vzdálené přístupy a další formy sociálního inženýrství, které se neustále vyvíjejí. Objem těchto incidentů je vysoký a dlouhodobě vykazuje rostoucí trend.

Otázka 3: Jaké preventivní programy či kampaně banka aktuálně využívá?
Odpověď: Banka využívá kombinaci více přístupů. Patří sem zejména průběžné vzdělávání klientů prostřednictvím článků na webových stránkách banky a sociálních sítích, dále varovné kampaně při nárůstu určitého typu útoků, které jsou realizovány například formou notifikací v mobilní aplikaci nebo e-mailem. Součástí prevence jsou také bezpečnostní upozornění přímo v internetovém bankovnictví a mobilní aplikaci. Banka se rovněž podílí na společných kampaních s Českou bankovní asociací, například #nePINdej. Důležitou součástí jsou také interní blokační mechanismy, které se aktivují při splnění definovaných rizikových kritérií a vedou k následnému kontaktu klienta.

Otázka 4: Jak se preventivní informace klientům předávají?
Odpověď: Preventivní informace jsou klientům předávány prostřednictvím více komunikačních kanálů současně. Jedná se zejména o webové stránky banky, mobilní a internetové bankovnictví, push notifikace a e-mailovou komunikaci, ale také sociální sítě, například LinkedIn.

Otázka 5: Považujete tyto preventivní aktivity za dostatečné z hlediska jejich srozumitelnosti a dosahu? Jaká forma prevence se podle Vaší zkušenosti ukazuje jako nejúčinnější?
Odpověď: Účinnost preventivních aktivit je obtížně měřitelná a lze konstatovat, že osvěty a vzdělávání klientů není nikdy dostatek. Stále existuje skupina klientů, která těmto aktivitám nevěnuje pozornost nebo je ignoruje. Navzdory preventivním kampaním navíc počet podvodných útoků dlouhodobě roste. Z hlediska efektivity se jako nej-

účinnější ukazuje kombinace technických opatření, zejména analýzy chování klienta, a možnosti včasné blokace finančních prostředků v případě podezření na podvod.

Otázka 6: Jaká technická preventivní opatření banka využívá k detekci podezřelého chování?
Odpověď: Mezi hlavní technická opatření patří monitoring neobvyklých transakcí a aktivit klienta, využívání blacklistů a watchlistů klientů, IP adres nebo zařízení, omezení přihlášení z rizikových IP adres či geografických lokalit a sledování změn zařízení. Banka rovněž detekuje anomální vzorce chování při přihlašování a transakcích a identifikuje možné známky kompromitace zařízení, například přítomnost škodlivého softwaru.

Otázka 7: Sleduje banka změny chování klienta (např. IP adresu, zařízení nebo počet operací)?
Odpověď: Ano, sledování změn chování klienta je standardní součástí systémů pro detekci podvodů. Sledují se například přihlášení z neobvyklých nebo rizikových IP adres, změna zařízení, operačního systému nebo prohlížeče, změny geografické polohy v krátkém časovém úseku a také abnormální transakční chování. Tyto informace jsou následně kombinovány do rizikových scénářů.

Otázka 8: Jakým způsobem banka vyhodnocuje situace, které mohou naznačovat automatizovaný nebo podvodný přístup k účtu?
Odpověď: Banka využívá kombinaci behaviorální analýzy a předem nastavených pravidel. Sleduje například pohyb myši, rychlost zadávání přihlašovacích údajů nebo nestandardně rychlé interakce v systému. Na základě těchto dat je vytvářeno rizikové skóre, které slouží jako podklad pro další rozhodování o postupu vůči dané transakci nebo účtu.

Otázka 9: Jak banka reaguje v okamžiku, kdy vyhodnotí chování klienta jako rizikové?
Odpověď: Reakce banky závisí na míře vyhodnoceného rizika. Může dojít ke zpřísnění ověřovacích mechanismů, například vyžádání dodatečného potvrzení transakce, dočasnému omezení přístupu k bankovním službám, manuální kontrole analytikem nebo kontaktování klienta za účelem ověření situace.

Otázka 10: Dochází ke kontaktování klienta nebo omezení funkcí účtu?
Odpověď: Ano, obvykle dochází ke kombinaci těchto opatření. Klient je kontaktován telefonicky za účelem ověření situace a v případě podezření může dojít k dočasné blokaci transakce, účtu nebo přístupu do internetového bankovnictví.

Otázka 11: Jaká je časová náročnost takové reakce z pohledu banky?
Odpověď: Technická reakce systému, například blokace transakce, probíhá v řádu sekund, protože systémy jsou plně automatizované. V případě manuálního vyhodnocení a kontaktování klienta závisí časová náročnost na dostupnosti klienta, obvykle se pohybuje v řádu desítek minut až hodin, výjimečně i dní.

Otázka 12: Jakou zpětnou vazbu banka získává od klientů v souvislosti s preventivními opatřeními?
Odpověď: Systematická zpětná vazba od klientů není v této oblasti k dispozici.

Otázka 13: Setkáváte se s tím, že klienti preventivní upozornění podceňují nebo ignorují?

Odpověď: Ano, lze předpokládat, že část klientů preventivní upozornění podceňuje nebo je ignoruje.

Otázka 14: Jak banka vyhodnocuje zkušenosti z již řešených incidentů a promítá je do další prevence?
Odpověď: Zkušenosti z řešených incidentů jsou systematicky využívány k dalšímu zlepšování bezpečnostních opatření. Dochází k úpravám detekčních pravidel a modelů, aktualizaci varovných sdělení pro klienty, zpřísnění procesů a limitů a sdílení poznatků mezi jednotlivými odděleními, například v oblasti fraud managementu, risku a AML. Současně dochází k zavádění nových technologií.

Otázka 15: Kde vidíte hlavní slabinu v ochraně bankovních klientů před kybernetickou kriminalitou?
Odpověď: Za nejslabší článek lze považovat lidský faktor, zejména důvěřivost klientů, jejich náchylnost k psychologické manipulaci a nedostatečnou obezřetnost. Technická opatření se neustále zdokonalují, avšak sociální inženýrství dokáže tato opatření v řadě případů obejít.

Otázka 16: Jaké opatření by podle Vás mělo největší potenciál snížit počet úspěšných útoků?
Odpověď: Největší potenciál má kombinace technických opatření a edukace klientů. V oblasti technických opatření se jedná například o pokročilejší behaviorální analýzu, varování klienta přímo při rizikové akci, automatické blokace vysoce rizikových transakcí nebo využití umělé inteligence při detekci podvodů. V oblasti edukace je důležité zaměřit se na jednoduchou, srozumitelnou a cílenou komunikaci, například prostřednictvím krátkých a vizuálně přehledných upozornění nebo edukativních prvků při aktivaci bankovních služeb.

Příloha č. 2 – Rozhovor s respondentem č. 1

Forma rozhovoru: polostrukturovaný rozhovor
Charakteristika respondenta: osoba poškozená kybernetickým útokem (anonymizováno)

Otázka 1: Jak dlouho využíváte internetové bankovnictví a jak často jej používáte?
Odpověď: Internetové bankovnictví využívám minimálně pět let, spíše však déle. Používám jej pravidelně, zpravidla několikrát týdně při běžné správě svých finančních prostředků.

Otázka 2: Jakým způsobem došlo k situaci, kdy jste se stala obětí kybernetické kriminality?
Odpověď: K incidentu došlo v souvislosti s prodejem věcí prostřednictvím inzertního portálu Bazoš. Při komunikaci ohledně dopravy jsem bez dostatečného ověření klikla na zaslaný odkaz, který působil důvěryhodně. Následně mě kontaktoval údajný bankéř, který ve skutečnosti vystupoval pod falešnou identitou.

Otázka 3: Setkala jste se před incidentem s preventivními informacemi ze strany banky týkajícími se kybernetické bezpečnosti?

Odpověď: Před samotným incidentem jsem si žádných preventivních informací ze strany banky vědoma nebyla. Stejně tak mi předtím nebylo nabídnuto ani pojištění proti obdobným podvodům.

Otázka 4: Pokud ano, jakou formou Vám byly tyto informace předány?
Odpověď: S určitými informacemi a upozorněními jsem se setkala až dodatečně, tedy až po samotném incidentu.

Otázka 5: Považovala jste tyto informace za srozumitelné a užitečné?
Odpověď: Ve chvíli, kdy se ke mně tyto informace dostaly, jsem je již vnímala jako užitečné. Zároveň jsem však měla pocit, že přišly pozdě, protože před samotným útokem jsem obdobná varování nezaregistrovala.

Otázka 6: Jak banka reagovala poté, co došlo k narušení bezpečnosti nebo k podezřelé transakci?
Odpověď: Ihned po zjištění problému jsem sama kontaktovala banku. Bylo mi doporučeno obrátit se na Policii České republiky a následně řešit situaci znovu s bankou, zejména ve vztahu ke změně přístupových údajů a zabezpečení účtu.

Otázka 7: Kontaktovala Vás banka sama, nebo jste musela iniciovat řešení Vy?
Odpověď: Řešení situace jsem iniciovala sama a věnovala jsem tomu značné úsilí. Banka mě v první fázi sama nekontaktovala.

Otázka 8: Zaznamenala jste během incidentu nebo po něm omezení funkcí účtu, dodatečné ověřování nebo jiné bezpečnostní kroky?
Odpověď: Ze strany banky jsem bezprostředně po incidentu nezaznamenala výraznější omezení funkcí účtu. Sama jsem si však nechala nastavit nová hesla a zároveň jsem si sjednala pojištění proti obdobným podvodům, a to i u druhé banky, kde mám veden účet.

Otázka 9: Změnila jste po této zkušenosti své chování při používání internetového bankovnictví?
Odpověď: Ano, tato zkušenost moje chování výrazně změnila. Dnes si více kontroluji převody, věnuji větší pozornost tomu, kam zadávám své údaje, a při nákupech nebo platbách využívám pouze ověřené internetové obchody a důvěryhodné služby.

Otázka 10: Vnímáte nyní preventivní opatření banky jinak než před incidentem?
Odpověď: Ano, po této zkušenosti je vnímám odlišně. Po určité době mě banka znovu kontaktovala a společně jsme zkontrolovali nastavení účtu, možnosti pojištění proti podvodům a další bezpečnostní prvky. Po aktualizaci účtu mi také začalo chodit více informačních e-mailů a upozornění na možné podvodné situace. Před samotným incidentem jsem nic takového nevnímala a zároveň jsem si tehdy tuto hrozbu příliš nepřipouštěla.

Otázka 11: Co Vám podle Vašeho názoru v prevenci chybělo nebo nebylo dostatečné?
Odpověď: Chyběly mi především výraznější informace o možných hrozbách přímo v aplikaci nebo internetovém bankovnictví. Za užitečné bych považovala také větší omezení možností nebo výraznější upozornění a dodatečné ověření při okamžitém převodu vyšší částky peněz.

Otázka 12: Co by podle Vás mohla banka udělat lépe, aby podobným situacím předcházela?
Odpověď: Domnívám se, že by banka mohla klienty aktivněji oslovovat například v souvislosti s aktualizací účtu nebo nabídkou pojištění. Takový krok by mohl současně sloužit i jako upozornění na aktuální rizika a hrozby. V mém případě jsem byla bankou aktivně oslovena až následně. Pozitivně vnímám také to, že na podobné podvody upozorňují média a televize, nicméně reklama zaměřená na podvodného bankéře se objevila až poté, co jsem se sama stala obětí podvodu.

Otázka 13: Jaké doporučení byste dala ostatním klientům na základě své zkušenosti?
Odpověď: Ostatním klientům bych doporučila především to, aby nevěřili automaticky všemu, co se na první pohled tváří důvěryhodně, ale aby si informace vždy ověřovali. Důležité je nejednat unáhleně, zastavit se a celou situaci si promyslet. Já sama jsem si dříve myslela, že mě se něco takového nemůže stát, což se ukázalo jako omyl. Za vhodné považuji také rozdělení finančních prostředků na více účtů a sjednání pojištění proti podvodům.

Příloha č. 3 – Rozhovor s respondentem č. 2

Forma rozhovoru: polostrukturovaný rozhovor
Charakteristika respondenta: osoba poškozená kybernetickým útokem (anonymizováno)

Otázka 1: Jak dlouho využíváte internetové bankovnictví a jak často jej používáte?
Odpověď: Internetové bankovnictví využívám přibližně od roku 2015. Používám jej pravidelně, zhruba třikrát týdně, zejména pro běžnou správu financí a provádění plateb.

Otázka 2: Jakým způsobem došlo k situaci, kdy jste se stal obětí kybernetické kriminality?
Odpověď: Obdržel jsem podvodný e-mail, který se tvářil jako zpráva od České pošty. Zpráva působila věrohodně a obsahovala výzvu k provedení určité akce, na kterou jsem následně reagoval.

Otázka 3: Setkal jste se před incidentem s preventivními informacemi ze strany banky týkajícími se kybernetické bezpečnosti?
Odpověď: Ano, banka o těchto hrozbách pravidelně informuje, a to prostřednictvím různých komunikačních kanálů.

Otázka 4: Pokud ano, jakou formou Vám byly tyto informace předávány?
Odpověď: Informace jsem zaznamenal především prostřednictvím mobilní aplikace banky, e-mailové komunikace a SMS zpráv.

Otázka 5: Považoval jste tyto informace za srozumitelné a užitečné?
Odpověď: Ano, tyto informace jsem vnímal jako srozumitelné a užitečné. Přesto jsem jim v dané chvíli nevěnoval dostatečnou pozornost.

Otázka 6: Jak banka reagovala poté, co došlo k narušení bezpečnosti nebo k podezřelé transakci?

Odpověď: Po kontaktování banky mi bylo doporučeno obrátit se na Policii České republiky a dále situaci řešit v součinnosti s bankou.

Otázka 7: Kontaktovala Vás banka sama, nebo jste musel iniciovat řešení Vy?
Odpověď: Banku jsem kontaktoval sám poté, co jsem si uvědomil, že se mohlo jednat o podvodné jednání.

Otázka 8: Zaznamenal jste během incidentu nebo po něm omezení funkcí účtu, dodatečné ověřování nebo jiné bezpečnostní kroky?
Odpověď: Nezaznamenal jsem žádné výrazné omezení funkcí účtu ani další bezpečnostní opatření ze strany banky.

Otázka 9: Změnil jste po této zkušenosti své chování při používání internetového bankovnictví?
Odpověď: Ano, své chování jsem změnil. Snažím se být obezřetnější a věnovat větší pozornost tomu, s jakými zprávami a odkazy pracuji. Do určité míry mě v tomto směru kontroluje i manželka, což přispívá k větší opatrnosti.

Otázka 10: Vnímáte nyní preventivní opatření banky jinak než před incidentem?
Odpověď: Ano, po této zkušenosti se snažím být obecně více obezřetný a preventivní opatření banky vnímám vážněji než dříve.

Otázka 11: Co Vám podle Vašeho názoru v prevenci chybělo nebo nebylo dostatečné?
Odpověď: Domnívám se, že hlavním problémem bylo to, že jsem preventivním informacím nevěnoval dostatečnou pozornost. Informace byly k dispozici, ale nepovažoval jsem je za natolik důležité, abych se jimi řídil.

Otázka 12: Co by podle Vás mohla banka udělat lépe, aby podobným situacím předcházela?
Odpověď: Domnívám se, že u některých typů transakcí, například u zahraničních plateb, by mohl být nastaven delší časový odstup mezi zadáním a realizací platby, což by klientovi poskytlo více času na případné přehodnocení situace.

Otázka 13: Jaké doporučení byste dal ostatním klientům na základě své zkušenosti?
Odpověď: Ostatním klientům bych doporučil především opatrnost a sledování aktuálních informací o kybernetických hrozbách. Důležité je nepodceňovat preventivní upozornění a věnovat jim náležitou pozornost.

Příloha č. 4 – Rozhovor s respondentem č. 3

Forma rozhovoru: polostrukturovaný rozhovor
Charakteristika respondenta: osoba poškozená kybernetickým útokem (anonymizováno)

Otázka 1: Jak dlouho využíváte internetové bankovnictví a jak často jej používáte?
Odpověď: Internetové bankovnictví využívám přibližně deset let a používám jej téměř každý den, zejména pro běžnou správu financí a provádění plateb.

Otázka 2: Jakým způsobem došlo k situaci, kdy jste se stal/a obětí kybernetické kriminality?
Odpověď: K incidentu došlo v důsledku chybného úsudku a uvěření podvodnému jednání. Situace působila důvěryhodně, což vedlo k tomu, že jsem podvod nerozpoznal/a včas.

Otázka 3: Setkal/a jste se před incidentem s preventivními informacemi ze strany banky týkajícími se kybernetické bezpečnosti?
Odpověď: S těmito informacemi jsem se setkával/a spíše zřídka. Po incidentu však vnímám, že je banka poskytuje častěji a intenzivněji.

Otázka 4: Pokud ano, jakou formou Vám byly tyto informace předávány?
Odpověď: Informace byly poskytovány především prostřednictvím mobilní aplikace banky a webových stránek.

Otázka 5: Považoval/a jste tyto informace za srozumitelné a užitečné?
Odpověď: Ano, informace jsem vnímal/a jako srozumitelné a užitečné, nicméně jsem jim před incidentem nepřikládal/a dostatečný význam.

Otázka 6: Jak banka reagovala poté, co došlo k narušení bezpečnosti nebo k podezřelé transakci?
Odpověď: Banka mě kontaktovala bezprostředně po zjištění podezřelé aktivity. Reakce byla rychlá, avšak v daném okamžiku již bylo pozdě zabránit vzniku škody.

Otázka 7: Kontaktovala Vás banka sama, nebo jste musel/a iniciovat řešení Vy?
Odpověď: V tomto případě mě kontaktovala banka jako první, což považuji za pozitivní.

Otázka 8: Zaznamenal/a jste během incidentu nebo po něm omezení funkcí účtu, dodatečné ověřování nebo jiné bezpečnostní kroky?
Odpověď: Ano, po incidentu došlo k zavedení dodatečných bezpečnostních opatření, která měla zabránit dalšímu neoprávněnému přístupu k účtu.

Otázka 9: Změnil/a jste po této zkušenosti své chování při používání internetového bankovnictví?
Odpověď: Ano, tato zkušenost vedla ke změně mého chování. Snažím se být obezřetnější a věnovat větší pozornost bezpečnosti při používání internetového bankovnictví.

Otázka 10: Vnímáte nyní preventivní opatření banky jinak než před incidentem?
Odpověď: Ano, po této zkušenosti vnímám preventivní opatření banky jako důležitější a věnuji jim větší pozornost.

Otázka 11: Co Vám podle Vašeho názoru v prevenci chybělo nebo nebylo dostatečné?
Odpověď: Domnívám se, že zásadním problémem bylo podcenění rizika a přesvědčení, že se podobná situace nemůže stát právě mně. Tento postoj vedl k nižší míře obezřetnosti.

Otázka 12: Co by podle Vás mohla banka udělat lépe, aby podobným situacím předcházela?
Odpověď: Banka by mohla zavést ještě důslednější kontrolu podezřelých transakcí a případně častěji upozorňovat klienty na rizikové operace.

Otázka 13: Jaké doporučení byste dal/a ostatním klientům na základě své zkušenosti?
Odpověď: Doporučil/a bych ostatním klientům, aby si veškeré informace vždy ověřovali, ideálně přímo u banky nebo na pobočce, a aby nepodceňovali možné hrozby v oblasti kybernetické kriminality.