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

BAKALÁŘSKÁ PRÁCE

VYŠETŘOVÁNÍ E-MAILOVÝCH PODVODŮ SE ZAMĚŘENÍM NA PRAXI POLICIE ČESKÉ REPUBLIKY

Autor práce: Jakub Král, DiS.
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: Jakub Král, DiS.
Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Vyšetřování e-mailových podvodů se zaměřením na praxi Policie České republiky

Název bakalářské práce v anglickém jazyce: Investigation of Email Fraud with a Focus on the Practice of the Police of the Czech Republic

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

Datum zadání bakalářské práce (měsíc, rok): Prosinec, 2025

Cíl bakalářské práce:

Cílem bakalářské práce je komplexně zhodnotit vyšetřovací postupy Policie České republiky při odhalování a dokumentaci e-mailových podvodů, porovnat je s charakterem používaného modus operandi pachatelů a na základě zjištěných nedostatků navrhnout kriminalisticky a procesně realizovatelná opatření ke zvýšení efektivity vyšetřování.

Student: Jakub Král, DiS.	4. 1. 2026 *datum*	*podpis*
Vedoucí práce: RNDr. Růžena Ferebauerová	7. 1. 2026 *datum*	*podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	21. 1. 2026 *datum*	*podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	21. 1. 2026 *datum*	*podpis*
Rektor: doc. Ing. Jiří Dušek, Ph.D.	21. 1. 2026 *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. Dále děkuji také jednotlivým příslušníkům SKPV PČR za poskytnuté rozhovory.

ABSTRAKT

KRÁL, J. *Vyšetřování e-mailových podvodů se zaměřením na praxi policie České republiky: bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, 2026 90 s. Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová.

Klíčová slova: kyberkriminalita, e-mailové podvody, sociální inženýrství, phishing, digitální stopa, Policie ČR.

Tato bakalářská práce se zabývá problematikou e-mailových podvodů jako specifické formy kybernetické kriminality. Teoretická část práce vymezuje základní pojmy, kategorizuje jednotlivé typy podvodů, jako jsou Scam 419, Business Email Compromise (BEC) či Romance Scams, a analyzuje psychologické mechanismy zneužívané pachateli. Praktická část je založena na kvalitativním výzkumu realizovaném formou strukturovaných rozhovorů s deseti experty z řad Policie České republiky a specialisty na kybernetickou bezpečnost. Cílem výzkumu bylo identifikovat aktuální trendy v sofistikovanosti útoků, vliv umělé inteligence na kvalitu podvodných sdělení a efektivitu procesních postupů při zajišťování digitálních stop. Práce dospívá k závěru, že klíčovým faktorem úspěšnosti útoků zůstává lidský činitel, přičemž technická opatření musí být doprovázena kontinuálním vzděláváním a úzkou spoluprací mezi veřejným a soukromým sektorem.

ABSTRACT

KRÁL, J. *Investigation of Email Fraud with a Focus on the Practice of the Policie České republiky: bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, 2026 90 s. Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová.

Keywords: cybercrime, email fraud, social engineering, phishing, digital footprint, Police of the Czech Republic.

This bachelor thesis addresses the issue of email fraud as a specific form of cybercrime. The theoretical part of the thesis defines basic concepts, categorizes various types of fraud, such as Scam 419, Business Email Compromise (BEC), and Romance Scams, and analyzes the psychological mechanisms exploited by perpetrators. The practical part is based on qualitative research conducted through structured interviews with ten experts from the Police of the Czech Republic and cybersecurity specialists. The aim of the research was to identify current trends in attack sophistication, the influence of artificial intelligence on the quality of fraudulent messages, and the efficiency of procedural methods in securing digital evidence. The thesis concludes that the human factor remains the key element in the success of attacks, emphasizing that technical measures must be accompanied by continuous education and close cooperation between the public and private sectors.

Obsah

Úvod

Kybernetický prostor se v posledním desetiletí stal integrální součástí každodenního života, a to nejen v rovině osobní komunikace a zábavy, ale především v oblasti globálního obchodu, státní správy a finančních transakcí. Tento nezvratný technologický progres však ruku v ruce přinesl i zásadní proměnu kriminálního prostředí. Tradiční formy majetkové a hospodářské kriminality se postupem času transformovaly do digitální podoby, přičemž jedním z nejrozšířenějších a zároveň nejnebezpečnějších nástrojů v rukou moderních pachatelů se stala elektronická pošta.

E-mailové podvody dnes nepředstavují pouze nahodilé pokusy o vylákání drobných finančních částek z neopatrných uživatelů. Naopak, hovoříme o vysoce organizované trestné činnosti, která využívá nejmodernější technologie anonymizace, sofistikované metody sociálního inženýrství a hlubokou znalost psychologie oběti. Fenomény jako Phishing, Business Email Compromise (BEC) nebo sofistikované schéma falešných faktur (Invoice Fraud) dnes způsobují českým firmám i jednotlivcům škody v řádech stovek milionů korun ročně. Pro Policii České republiky, a zejména pro útvary zabývající se hospodářskou a kybernetickou kriminalitou, představuje vyšetřování těchto deliktů mimořádnou výzvu, která vyžaduje specifické metodické postupy, mezinárodní součinnost a vysokou úroveň technické odbornosti.

Předkládaná bakalářská práce s názvem „Vyšetřování e-mailových podvodů se zaměřením na praxi Policie České republiky“ reaguje na tento alarmující vývoj. Volba tématu vychází z aktuální potřeby analyzovat, jakým způsobem se policie adaptuje na neustále se měnící modus operandi pachatelů. Zatímco útočníci těží z prchavosti digitálních stop a přeshraničního charakteru internetu, vyšetřovací orgány musí operovat v rámci mantinelů vymezených trestním řádem, který ne vždy dokáže v reálném čase reflektovat dynamiku kyberprostoru.

V práci bude kladen důraz na propojení teoretických východisek s praktickými poznatky z činnosti Odboru hospodářské kriminality. Bakalářská práce se pokusí odpovědět na otázku, zda jsou současné mechanismy odhalování a dokumentace e-mailových podvodů dostatečně efektivní a jaké systémové či legislativní bariéry brání úspěšnému dopadení pachatelů a zajištění výnosů z této trestné činnosti.

1 Cíl a metodika bakalářské práce

Hlavním a primárním cílem této bakalářské práce je komplexně zhodnotit vyšetřovací postupy Policie České republiky při odhalování a dokumentaci specifických forem e-mailových podvodů. Práce se zaměřuje na kritickou analýzu reálné vyšetřovací praxe, zejména v rámci Odboru hospodářské kriminality, a to s přihlédnutím k aktuálním trendům v oblasti kyberkriminality.

Pro dosažení tohoto hlavního cíle byly stanoveny následující dílčí cíle a výzkumné záměry:

- Analýza metodických postupů: Podrobně zmapovat a vyhodnotit současné vnitřní metodiky a standardní operační postupy Policie ČR při přijímání oznámení, zajišťování prvotních digitálních stop a trasování finančních toků u e-mailových podvodů.
- Komparace s modem operandi pachatelů: Porovnat zjištěné policejní postupy s reálným chováním pachatelů (např. u útoků typu BEC a Invoice Fraud). Cílem je zjistit, zda policie dokáže efektivně reagovat na sofistikované metody sociálního inženýrství a technické anonymizace (VPN, TOR[1], kryptoměny).
- Identifikace klíčových bariér: Na základě empirického šetření (rozhovorů s vyšetřovateli) pojmenovat největší nedostatky a limity, se kterými se policie v praxi potýká – ať už jde o limity legislativní, personální, technické nebo v oblasti mezinárodní právní pomoci.
- Formulace návrhů de lege ferenda a metodických doporučení: Vyvrcholením práce bude sestavení souboru konkrétních doporučení, která by mohla vést ke zvýšení efektivity vyšetřování. Tyto návrhy budou směřovat jak do oblasti úpravy vnitřních předpisů PČR, tak do oblasti preventivního působení směrem k veřejnosti a podnikatelským subjektům.

Záměrem autora je, aby tato práce nesloužila pouze jako teoretický popis dané problematiky, ale aby její závěry, podložené analýzou reálné praxe, mohly být využity jako podklad pro další diskuzi o zefektivnění boje proti kybernetické kriminalitě v podmínkách Policie ČR.

[1] JIRÁSEK, Petr. Výkladový slovník kybernetické bezpečnosti. 1. vydání. Praha: Petr Jirásek, 2021. 322 s. ISBN 978-80-908388-4-0.

2 TEORETICKÁ VÝCHODISKA

2.1 Vymezení základních pojmů

Teoretické ukotvení základních terminologických pilířů je nezbytným předpokladem pro následnou analýzu vyšetřovací praxe Policie České republiky v oblasti e-mailových podvodů. Vzhledem k vysoké dynamice technologického vývoje v kybernetickém prostoru se terminologie neustále vyvíjí, což klade zvýšené nároky na přesnost právní i kriminalistické interpretace jednotlivých pojmů. Následující pasáže se zaměřují na definování klíčových fenoménů, které tvoří rámec zkoumané problematiky, počínaje historickým exkurzem až po současné mezinárodněprávní vymezení počítačové kriminality.

Cílem této kapitoly není pouze strohý výčet definic, ale především snaha o pochopení souvislostí mezi tradičními formami podvodného jednání a jejich moderními transformacemi v digitálním prostředí. Správná interpretace těchto pojmů je totiž klíčová pro následnou právní kvalifikaci trestných činů a volbu adekvátních kriminalistických metod při zajišťování důkazního materiálu. Jak bude demonstrováno v dalších částech práce, právě nejednoznačnost nebo nesprávné pochopení některých technických aspektů e-mailové komunikace může v praxi vést k procesním pochybením při dokumentaci trestné činnosti.

2.1.1 Historický kontext a vývoj e-mailových podvodů

Při hlubší analýze e-mailových podvodů lze vysledovat, že jejich základní mechanismy nejsou produktem moderní digitální éry, nýbrž evolučním vyústěním staletí starých metod kriminálního jednání. Kriminalistická historie dokládá, že principy zneužívání lidské důvěry a manipulace s informacemi byly využívány dlouho před vznikem první počítačové sítě. Za ideového předchůdce dnešních phishingových kampaní a nigerijských dopisů je v odborné literatuře považován tzv. „podvod se španělským vězněm“ (Spanish Prisoner Scam), jehož počátky sahají až do konce 18. století. Pachatelé tehdy prostřednictvím klasické pošty oslovovali movité oběti s fiktivním příběhem o uvězněném šlechtici, k jehož osvobození byla zapotřebí finanční pomoc, za kterou byla slíbena pohádková odměna.[2]

[2] KOLOUCH, Jan. *CyberCrime*. Praha: Vyšehrad, 2016, s. 32–35. ISBN 978-80-7429-768-7.

Zásadní zlom v distribuci těchto podvodných schémat přinesla technologická revoluce v podobě dálnopisu a následně faxu v průběhu 20. století. Tato zařízení umožnila pachatelům oslovovat oběti s mnohem vyšší efektivitou a nižšími náklady na doručení. Skutečný rozmach však nastal až v 80. letech 20. století v Nigérii, kde se začal formovat fenomén známý jako „Scam 419“ (podle příslušného paragrafu nigerijského trestního zákoníku). S nástupem a komercionalizací internetu v polovině 90. let se tato trestná činnost masivně přesunula do prostředí elektronické pošty. E-mail se stal pro útočníky ideálním nástrojem díky své asynchronnosti, nízkým nákladům na provoz a možnosti globálního dosahu během několika sekund.[3]

Termín „phishing“ jako takový byl poprvé identifikován a pojmenován v polovině 90. let (uvádí se rok 1996) v rámci komunitní sítě AOL (America Online). Tehdejší útočníci začali využívat techniky sociálního inženýrství k vylákání přístupových údajů uživatelů, přičemž k tomu využívali právě e-mailové zprávy maskované za oficiální systémová upozornění. Od této doby prošly e-mailové podvody drastickou proměnou, od primitivních textových zpráv s množstvím gramatických chyb až po dnešní vysoce sofistikované útoky typu Business Email Compromise (BEC), které využívají pokročilé metody spoofingu a personifikované manipulace.[4] Moderní historie tohoto typu kriminality tak ukazuje na neustálou adaptabilitu pachatelů na nová bezpečnostní opatření, kdy technické bariéry nejsou prolamovány hrubou silou, ale skrze nejslabší článek řetězce, tedy člověka.[5]

2.1.2 Kybernetická kriminalita a Budapešťská úmluva

Pro efektivní vyšetřování e-mailových podvodů je nezbytné ukotvení problematiky v širším právním rámci kybernetické kriminality. Kyberkriminalita, jakožto globální fenomén nerespektující státní hranice, vyžaduje úzkou mezinárodní kooperaci a sjednocení legislativních standardů. Klíčovým dokumentem v této oblasti je Úmluva o počítačové kriminalitě Rady Evropy, známá pod názvem Budapešťská úmluva, která byla otevřena k podpisu 23. listopadu 2001. Pro Českou republiku vstoupila v platnost 1.

[3] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. vydání. Plzeň: Aleš Čeněk, 2022, s. 114–118. ISBN 978-80-7380-880-8.
[4] KOLOUCH, Jan. *CyberCrime*. Praha: Vyšehrad, 2016, s. 45–48. ISBN 978-80-7429-768-7.

[5] RAMEŠOVÁ, K. *Právní regulace kybernetické bezpečnosti a její meze*. Praha: C.H. Beck, 2023, s. 18. ISBN 978-80-7400-931-0.

prosince 2013 (uveřejněna pod č. 104/2012 Sb. m. s.) a stala se základním pilířem pro implementaci specifických skutkových podstat do českého trestního zákoníku.[6]

Budapešťská úmluva definuje kybernetickou kriminalitu nikoliv jako jeden konkrétní čin, ale jako soubor protiprávních jednání, která lze rozdělit do několika základních kategorií. V kontextu e-mailových podvodů jsou relevantní především ustanovení týkající se trestných činů souvisejících s počítači (např. počítačové podvody a padělání) a trestných činů proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů. Úmluva zavazuje signatářské státy k zavedení odpovídajících trestněprávních sankcí, ale také k nastavení procesních mechanismů, které umožní rychlé zajištění elektronických důkazů v reálném čase.[7]

Z pohledu vyšetřovací praxe Policie ČR je zásadní především procesní část úmluvy, která upravuje mezinárodní spolupráci. Vzhledem k tomu, že pachatelé e-mailových podvodů často využívají infrastrukturu nacházející se v jiných jurisdikcích (např. e-mailové servery v USA nebo asijských zemích), představuje Budapešťská úmluva nástroj, který umožňuje efektivnější výměnu informací mezi donucovacími orgány. Úmluva zavádí institut tzv. sítě „24/7 kontaktních míst“, která slouží k okamžité technické i právní asistenci při vyšetřování kybernetických incidentů s mezinárodním přesahem. Tento mechanismus je pro hospodářskou kriminálku klíčový zejména v případech, kdy je nutné neprodleně zajistit digitální stopu u zahraničního poskytovatele služeb dříve, než dojde k jejímu smazání nebo přepsání.[8]

Moderní pojetí kyberkriminality, jak jej definuje Úmluva, tak reflektuje skutečnost, že e-mailové podvody nejsou izolovaným deliktem, ale komplexní činností, která často naplňuje znaky vícero trestných činů současně. Budapešťská úmluva tak vytváří nezbytný právní most, bez kterého by byla úspěšná dokumentace přeshraničních e-mailových útoků v podmínkách současné Policie ČR prakticky nerealizovatelná.[9]

[6] GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Praha: Auditorium, 2015, s. 42–45. ISBN 978-80-87284-53-7.
[7] GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Praha: Auditorium, 2015, s. 58–62. ISBN 978-80-87284-53-7.
[8] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. vydání. Plzeň: Aleš Čeněk, 2022, s. 482–485. ISBN 978-80-7380-880-8
[9] GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Praha: Auditorium, 2015, s. 72–75. ISBN 978-80-87284-53-7.

2.1.3 Specifika kriminality v prostředí internetu (anonymita, přeshraniční přesah, rychlost)

Kriminalita páchaná v kyberprostoru vykazuje řadu unikátních vlastností, které ji zásadně odlišují od tradiční trestné činnosti v reálném světě. Tyto specifické rysy vytvářejí asymetrický vztah mezi pachatelem a orgány činnými v trestním řízení, neboť technologie, které slouží k legitimní komunikaci, zároveň poskytují útočníkům účinné nástroje k zakrytí jejich identity a zahlazení stop. Pro vyšetřovací praxi Policie ČR jsou v kontextu e-mailových podvodů určující především tři aspekty: anonymita, přeshraniční přesah a rychlost.[10]

Anonymita a obtížná identifikace pachatele představují primární bariéru při odhalování e-mailových útoků. V digitálním prostředí lze identitu odesílatele relativně snadno maskovat či zcela zfalšovat prostřednictvím technik, jako je e-mail spoofing. Pachatelé navíc standardně využívají anonymizační nástroje, jako jsou VPN služby, proxy servery nebo síť TOR, které efektivně skrývají jejich skutečnou IP adresu. Z hlediska kriminalistické metodiky to znamená, že digitální stopa často nevede k fyzické osobě, ale pouze k technickému uzlu, který může být zneužit bez vědomí jeho majitele.[11]

Přeshraniční přesah (transnationalita) je dalším definujícím znakem. E-mailový podvod může být iniciován z jednoho kontinentu, technicky realizován přes servery na druhém kontinentu a poškodit oběť na kontinentu třetím. Tato geografická nezávislost pachatelů staví policii před složité otázky mezinárodní jurisdikce a nutnost využívat zdlouhavé procedury mezinárodní právní pomoci. V praxi se často stává, že zatímco se český vyšetřovatel pokouší zajistit data u zahraničního poskytovatele, pachatel se již nachází v jurisdikci, která s evropskými orgány nespolupracuje.[12]

Rychlost a prchavost dat dotvářejí komplexnost problému. Realizace útoku, včetně přečerpání finančních prostředků z účtu oběti na účty tzv. bílých koní, může proběhnout v řádu sekund. Digitální stopy, které po útoku zůstávají v informačních systémech, jsou navíc extrémně prchavé. Pokud nedojde k jejich okamžitému zajištění, mohou být přepsány nebo smazány automatickými procesy správy dat. Pro Policii ČR to

[10] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. vydání. Plzeň: Aleš Čeněk, 2022, s. 42–46. ISBN 978-80-7380-880-8.
[11] KOLOUCH, Jan. *CyberCrime*. Praha: Vyšehrad, 2016, s. 124–128. ISBN 978-80-7429-768-7.
[12] HOLT, Thomas J., Adam M. BOSSALER a Kathryn C. SEIGFRIED-SPANJER. *Cybercrime and Digital Forensics: An Introduction*. 3rd ed. London: Routledge, 2022, s. 512–515. ISBN 978-0367360078.

znamená nutnost jednat v reálném čase, což je v kontrastu s administrativní náročností standardního trestního procesu.

Kombinace těchto faktorů vytváří z internetu prostředí, které maximalizuje zisk pachatele při minimálním riziku jeho dopadení. Právě pochopení těchto specifik je základním kamenem pro návrh efektivnějších metodických postupů, které se v praktické části práce pokusíme identifikovat.[13]

2.2 E-mail jako komunikační prostředek a nástroj útoku

Elektronická pošta představuje jeden z nejstarších a dodnes nejrozšířenějších pilířů digitální komunikace. Přestože se v průběhu let objevila řada modernějších platforem pro okamžitou výměnu zpráv, e-mail si zachoval své dominantní postavení, zejména v oficiální a obchodní sféře. Z pohledu kriminalistiky však právě tato všeobecná akceptace a důvěra v e-mailovou komunikaci vytváří ideální operační prostor pro pachatele trestné činnosti. E-mail v tomto kontextu nefunguje pouze jako pasivní médium pro přenos informací, ale stává se aktivním nástrojem útoku, který kombinuje technické nedostatky zastaralých protokolů s psychologickou manipulací.[14]

2.2.1 Historie a princip fungování e-mailové komunikace (protokoly SMTP, spoofing)

Pochopení e-mailových podvodů vyžaduje základní vhled do technické architektury, na které je tato služba postavena. Základy elektronické pošty byly položeny již v 70. letech 20. století, kdy byl vyvinut protokol SMTP (Simple Mail Transfer Protocol) pro odesílání zpráv. Klíčovým problémem z dnešního pohledu je fakt, že tento protokol byl navržen v prostředí uzavřených akademických a armádních sítí, kde byla prioritou funkčnost a rychlost doručení, nikoliv bezpečnost nebo ověřování identity odesílatele.

Tato historická zátěž se projevuje především v absenci nativních mechanismů pro verifikaci hlaviček e-mailu. V původní specifikaci SMTP mohl odesílatel do pole „From“ (Od) vyplnit v podstatě jakoukoliv adresu, aniž by systém kontroloval, zda mu skutečně patří. Právě tato technická nedokonalost umožnila vznik techniky známé jako e-mail

[13] CASEY, Eoghan. *Digital Evidence and Computer Crime*. 3rd ed. Academic Press, 2011, s. 25–29. ISBN 978-0123742681.
[14] HROMADA, Martin; HRŮZA, Petr; KADERKA, Josef; LUŇÁČEK, Oldřich; NEČAS, Miroslav et al. *Kybernetická bezpečnost: teorie a praxe*. Praha: Powerprint, 2015. 15 s. ISBN 978-80-87994-72-6.

spoofing (podvržení identity odesílatele), která je dodnes základním stavebním kamenem většiny e-mailových podvodů. Přestože byly v pozdějších letech vyvinuty dodatečné bezpečnostní standardy jako SPF (Sender Policy Framework) či DKIM (DomainKeys Identified Mail), jejich nasazení není univerzální a pachatelé stále nacházejí cesty, jak tyto ochrany obejít nebo zneužít jejich nesprávného nastavení na straně firemních serverů.[15]

2.2.2 Role e-mailu v moderní kriminalitě

V současné kriminální praxi plní e-mail roli „vstupní brány“ do digitálního soukromí oběti nebo do vnitřní sítě organizace. Jeho nebezpečnost spočívá v asynchronnosti, to znamená, že pachatel může zprávu odeslat kdykoliv a oběť ji přijme v prostředí, které považuje za bezpečné (v kanceláři, doma na mobilním telefonu). E-mail je pro útočníka extrémně levným a škálovatelným nástrojem, neboť náklady na odeslání milionů podvodných zpráv jsou v porovnání s potenciálním ziskem zanedbatelné.

Z hlediska modu operandi slouží e-mail v moderní kriminalitě ke třem hlavním účelům:

1. Vektoru pro distribuci škodlivého kódu (malware): E-mailová příloha nebo odkaz slouží k infikování zařízení oběti, což následně umožňuje špionáž nebo zašifrování dat (ransomware).
2. Získání citlivých údajů (harvesting): Pomocí sociálního inženýrství jsou z oběti vylákány přístupové údaje do bankovnictví nebo firemních systémů.
3. Přímému finančnímu podvodu: Manipulace s obětí tak, aby dobrovolně provedla finanční transakci na účet pachatele, což je typické právě pro podvody typu BEC (Business Email Compromise).

E-mail se tak stal nástrojem, který v sobě koncentruje technické zranitelnosti internetu a psychologickou zranitelnost lidského faktoru, což z něj činí primární objekt zájmu pro vyšetřovatele Odborů hospodářské kriminality.[16]

[15] BREWSTER, Corey. *Business Email Compromise: The New Face of Cybercrime*. [s.l.]: Independent publ., 2020, s. 34–38. ISBN 979-8646610257.
[16] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. vydání. Plzeň: Aleš Čeněk, 2022, s. 125–129. ISBN 978-80-7380-880-8.

2.3 Typologie e-mailových podvodů

Klasifikace e-mailových podvodů je v odborné literatuře i policejní praxi neustále se vyvíjejícím procesem. Vzhledem k tomu, že pachatelé často kombinují různé metody útoku, hranice mezi jednotlivými kategoriemi mohou být někdy nejasné. Pro účely kriminalistického zkoumání a efektivního vyšetřování je však nezbytné tyto formy odlišovat, a to především na základě jejich cíle, cílové skupiny a použitého modu operandi. E-mailové podvody lze v základu dělit na masové kampaně, které sázejí na kvantitu, a vysoce sofistikované cílené útoky, které se zaměřují na konkrétní jednotlivce nebo korporátní struktury.[17]

2.3.1 Phishing a jeho varianty (plošný phishing, vishing, smishing)

Phishing (česky někdy označovaný jako „rybaření“) představuje nejrozšířenější formu e-mailového podvodu. Jeho podstata spočívá v masovém rozesílání zpráv, které budí dojem, že pocházejí od důvěryhodné instituce, nejčastěji to jsou banky, přepravní společnosti nebo státní úřad. Cílem je přimět uživatele ke kliknutí na podvodný odkaz, který jej přesměruje na falešnou webovou stránku určenou ke sběru citlivých údajů (přihlašovací údaje, čísla platebních karet).

Moderní phishing se však již neomezuje pouze na e-mailovou komunikaci. Často dochází k tzv. vícekanálovým útokům, které zvyšují důvěryhodnost podvodu:

- Vishing (Voice Phishing): Pachatel po odeslání e-mailu kontaktuje oběť telefonicky a pod legendou bankovního úředníka či policisty ji nutí k „zabezpečení“ finančních prostředků.
- Smishing (SMS Phishing): Podvodné zprávy doručované prostřednictvím SMS, které často obsahují urgentní výzvy k zaplacení celního poplatku nebo vyzvednutí zásilky.[18]

2.3.2 Spear-phishing a Whaling (cílené útoky)

Na rozdíl od plošného phishingu je spear-phishing charakteristický svým úzkým zaměřením. Pachatel si předem vybere konkrétní oběť a provede důkladný průzkum z veřejně dostupných zdrojů (sociální sítě, webové stránky firmy). E-mail je následně

[17] HOLT, Thomas J., Adam M. BOSSALER a Kathryn C. SEIGFRIED-SPANJER. *Cybercrime and Digital Forensics: An Introduction*. 3rd ed. London: Routledge, 2022, s. 165–168. ISBN 978-0367360078.
[18] KOLOUCH, Jan. *CyberCrime*. Praha: Vyšehrad, 2016, s. 132–135. ISBN 978-80-7429-768-7.

personalizován, obsahuje jméno oběti, zmínku o aktuálních projektech nebo kolezích, což dramaticky zvyšuje šanci na úspěch.

Specifickou podskupinou je pak whaling (v překladu „lov velryb“). Tento termín označuje útoky směřující na nejvyšší management společností (CEO, CFO). Úspěšný průnik do komunikace těchto osob otevírá útočníkům cestu k nejcitlivějším datům firmy nebo k autorizaci rozsáhlých finančních transferů.[19]

2.3.3 Business Email Compromise (BEC) – komplexní analýza

Fenomén Business Email Compromise (BEC), v terminologii Policie ČR někdy označovaný jako „podvodný e-mail statutárního zástupce“, představuje jeden z ekonomicky nejničivějších typů kybernetické kriminality současnosti. Na rozdíl od masových phishingových kampaní se jedná o vysoce sofistikovaný, cílený útok, který primárně nezneužívá technické zranitelnosti systémů, ale cílí na selhání lidského faktoru v rámci vnitrofiremních schvalovacích procesů. Komplexnost tohoto útoku spočívá v kombinaci precizního průzkumu (OSINT), sociálního inženýrství a technické manipulace s e-mailovou identitou.[20]

Fáze útoku a modus operandi Analýza reálných případů vyšetřovaných Odbory hospodářské kriminality ukazuje, že úspěšný BEC útok se zpravidla skládá ze čtyř kritických fází:

1. Identifikace a průzkum (Reconnaissance): Pachatelé identifikují cílovou společnost a její klíčové zaměstnance (zpravidla finanční ředitele, účetní nebo nákupčí). Využívají k tomu veřejně dostupné zdroje, jako jsou webové stránky firem, obchodní rejstřík či profesní sítě (LinkedIn), kde mapují organizační strukturu a vztahy mezi nadřízenými a podřízenými.

2. Příprava a infiltrace: Útočník si vytvoří technické zázemí. Buď zaregistruje doménu, která je vizuálně téměř k nerozeznání od domény oběti (tzv. typosquatting – např. zamění písmeno „l“ za číslici „1“), nebo se pokusí o přímý průnik do e-mailové schránky vysoce postaveného manažera pomocí dříve získaných hesel či malwaru.

[19] JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. 54-58 s. ISBN 9788024715612.
[20] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. vydání. Plzeň: Aleš Čeněk, 2022, s. 136–140. ISBN 978-80-7380-880-8.

3. Sociální inženýrství a nátlak: Toto je jádro útoku. Oběti je doručen e-mail, který budí dojem, že jej odeslal generální ředitel nebo jiný člen vedení. Zpráva je koncipována jako „přísně důvěrná“ a „extrémně urgentní“. Často operuje s legendou o akvizici nového partnera, tajném projektu nebo neodkladném vypořádání soudního sporu. Cílem je vyvolat v oběti stres a pocit důležitosti, což vede k obcházení standardních kontrolních mechanismů firmy.

4. Realizace transakce a vyvedení prostředků: Oběť pod tlakem autority provede platbu na účet uvedený v e-mailu. Tento účet je v drtivé většině případů spravován tzv. „money mule“ (bílým koněm). Jakmile peníze dorazí, jsou okamžitě řetězeny přes další účty v různých jurisdikcích nebo konvertovány do kryptoměn, aby bylo znemožněno jejich zajištění.[21]

Kategorizace BEC scénářů dle FBI a PČR:

V rámci komplexní analýzy lze rozlišit pět základních scénářů, se kterými se vyšetřovatelé nejčastěji setkávají:

- The CEO Fraud: Falešný příkaz ředitele k platbě.
- Account Compromise: Skutečné ovládnutí e-mailu zaměstnance a následná komunikace jménem oběti.
- Attorney Impersonation: Útočník se vydává za právního zástupce, který vyžaduje úhradu za právní služby nebo kauci.
- Data Theft: Útok není cílen na peníze, ale na získání citlivých údajů (např. mzdové listy, seznamy klientů), které jsou následně zpeněženy na černém trhu.
- Supply Chain Attack: Pachatel napadne dodavatelský řetězec a upravuje platební údaje u pravidelných plateb mezi obchodními partnery.

Kriminalistický význam analýzy z pohledu vyšetřování je u BEC útoků zásadní pochopit, že pachatel není pouhým „hackerem“, ale zkušeným manipulátorem, který zná firemní etiketu a mluvu daného odvětví. Dokumentace těchto případů je pro Policii ČR náročná z hlediska dokazování úmyslu a identifikace konečného příjemce výhody, neboť

[21] PORADA, Viktor. Kriminalistika: technické, forenzní a kybernetické aspekty. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o, 2016. 205-209 s. ISBN 978-80-7380-589-0.

digitální stopa bývá profesionálně zahlazena a finanční toky jsou bleskově vyvedeny mimo dosah národních orgánů. Úspěšné vyšetřování se proto neobejde bez okamžité součinnosti s bankovním sektorem a mezinárodními vyšetřovacími sítěmi.[22]

2.3.4 Invoice Fraud a Fake-invoice Schemes (podvržené faktury)

Problematika podvržených faktur představuje v kriminalistické praxi specifickou oblast, která vyžaduje precizní rozlišení mezi dvěma základními mody operandi. Ačkoliv je společným jmenovatelem neoprávněné obohacení pachatele skrze falešný platební impuls, technické a taktické provedení se v obou případech zásadně liší, což má přímý dopad na způsob následného vyšetřování a zajišťování stop.

Invoice Fraud je mimořádně nebezpečný typ útoku, který se maskuje za běžnou a legální obchodní spolupráci, což výrazně ztěžuje jeho včasné rozpoznání. Pachatel nejprve infiltruje komunikační kanál (zpravidla e-mailovou schránku) jednoho z obchodních partnerů. Následně pasivně monitoruje tok zpráv a čeká na okamžik, kdy je odesílána faktura za skutečně dodané zboží či služby. V tento moment útočník do komunikace zasáhne tak, že buď fakturu v příloze přímo upraví (změní číslo bankovního účtu), nebo e-mail zachytí a oběti jej přepošle z vizuálně identické adresy s vysvětlením, že „původní účet je z technických důvodů nedostupný“. Oběť, která platbu očekávala a zná identitu dodavatele, pak v dobré víře odešle finanční prostředky přímo na účet ovládaný pachatelem. Pro Policii ČR je v těchto případech klíčové zkoumání tzv. e-mailových hlaviček a logů serverů, aby bylo možné určit, v jakém bodě byla komunikace kompromitována.[23]

Fake-invoice Schemes (Schémata fiktivních faktur), na rozdíl od předchozího typu se zde pachatel nepokouší o průnik do existující komunikace, ale sází na kvantitu a administrativní nepozornost. Útočníci rozesílají velké množství faktur za služby, které nikdy nebyly poskytnuty, ale které působí věrohodně v kontextu běžného provozu firmy. Typicky se jedná o:

- Poplatky za registraci doménových jmen či ochranných známek.
- Zápisy do pochybných podnikatelských rejstříků a katalogů.

[22] BREWSTER, Corey. *Business Email Compromise: The New Face of Cybercrime*. [s.l.]: Independent publ., 2020, s. 85–92. ISBN 979-8646610257.
[23] PORADA, Viktor. Kriminalistika: technické, forenzní a kybernetické aspekty. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o, 2016. 212-216 s. ISBN 978-80-7380-589-0.

- Předplatné za odborný software či aktualizace databází.

Pachatelé často volí částky těsně pod hranicí, která ve vnitrofiremních směrnicích vyžaduje schválení nadřízeným, čímž maximalizují šanci, že faktura projde účtárnou jako rutinní platba. Z kriminalistického hlediska je zde zásadní analýza hromadného šíření (spamu) a trasování bankovních účtů, které jsou často vedeny na osoby v postavení tzv. bílých koní.

Rozlišení těchto dvou metod je nezbytné pro správnou právní kvalifikaci a volbu vyšetřovací verze, neboť zatímco u manipulace s fakturou jde o sofistikovaný zásah do cizího systému, u fiktivních faktur jde primárně o zneužití lidské nepozornosti a systémových mezer v kontrolních mechanismech právnických osob.[24]

2.3.5 Scam 419 a moderní variace sociálního inženýrství

Fenomén známý jako Scam 419, v českém prostředí lidově označovaný jako „nigerijské dopisy“, představuje jednu z nejtrvalejších forem e-mailového podvodu. Název je odvozen od paragrafu 419 nigerijského trestního zákoníku, který se zabývá podvody. Ačkoliv se jedná o metodu s desítky let dlouhou historií, její neustálá adaptabilita a schopnost využívat aktuální společenské dění z ní činí stále relevantní hrozbu.[25] Podstata tohoto podvodu nespočívá v technické složitosti, ale ve využití sociálního inženýrství. Jde o psychologickou manipulaci s obětí. Útočník pomocí psychologického nátlaku či manipulace přiměje oběť k tomu, aby jednala podle jeho pokynů.[26]

Klasické schéma a princip „vysokého zisku“ je základním principem Scamu 419 je příslib enormního finančního prospěchu, který je však podmíněn zaplacením relativně malého vstupního poplatku. Pachatel vystupuje v roli vysoce postaveného úředníka, právníka nebo bankéře, který potřebuje pomoc s převodem zablokovaného dědictví, vládních fondů nebo opuštěných bankovních kont po zesnulých miliardářích. Oběť je motivována vidinou provize (často ve výši 20–30 % z celkové sumy). Jakmile oběť projeví zájem, začne kolotoč požadavků na úhradu „administrativních nákladů“, „právních poplatků“, „úplatků pro úředníky“ nebo „daní z převodu“. Podvod končí v

[24] MUSIL, Jan; KONRÁD, Zdeněk a SUCHÁNEK, Jaroslav. Kriminalistika. 2., přeprac. a dopl. vyd. Beckovy mezioborové učebnice. Praha: <> Beck, 2004. 312-314 s. ISBN 8071798789.
[25] HADNAGY, Christopher. *Social Engineering: The Science of Human Hacking*. 2nd ed. Indianapolis: John Wiley & Sons, 2018, s. 142–146. ISBN 978-1119433385.
[26] ZAVRŠNIK, A. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017, s. 34. ISBN 978-80-7552-758-5.

momentě, kdy oběť buď zcela vyčerpá své finanční zdroje, nebo pochopí, že se stala obětí kriminálního jednání.[27]

Moderní variace: Romance Scams a krizové scénáře

V posledních letech se původní podvody typu „Scam 419“ transformovaly do mnohem osobnějších a nebezpečnějších forem. Tyto incidenty Policie ČR v současnosti eviduje stále častěji.

- Romance Scams (Seznamovací podvody): Pachatel buduje s obětí dlouhodobý, hluboký emocionální vztah skrze e-maily a sociální sítě. Často vystupuje pod identitou amerického vojáka na misi, lékaře v krizové oblasti nebo inženýra na ropné plošině. Poté, co získá plnou důvěru oběti, přichází s naléhavou prosbou o finanční pomoc (např. na letenku domů, léčbu zranění nebo vyplacení balíku s cennostmi ze sféry vlivu celníků). Tato forma je obzvlášť destruktivní, neboť oběti přicházejí nejen o úspory, ale čelí i těžkému psychickému traumatu.

- Charity Scams (Charitativní podvody): Útočníci zneužívají aktuální globální krize (válečné konflikty, přírodní katastrofy). Rozesílají e-maily jménem fiktivních humanitárních organizací a žádají o příspěvky, které jsou však směřovány přímo do kriminálních struktur.

- Inheritance and Lottery Scams: Moderní verze zpráv o výhrách v loteriích, kterých se oběť nikdy neúčastnila, nebo o dědictví po vzdáleném příbuzném, jehož existenci si pachatelé vykonstruovali na základě dat vytěžených z rodokmenů na internetu.[28]

Psychologický mechanismus účinku je úspěch těchto podvodů stojí na třech pilířích: vzbuzení důvěry, vyvolání silné emoce (chamtivost, soucit, láska) a následné vytvoření časového tlaku. Pachatelé jsou zručnými psychology, kteří dokážou odhadnout slabiny oběti a přizpůsobit jim svou komunikaci. Z kriminalistického hlediska je šetření těchto případů mimořádně složité, neboť finanční prostředky jsou odesílány dobrovolně

[27] KOLOUCH, Jan. *CyberCrime*. Praha: Vyšehrad, 2016, s. 138–142. ISBN 978-80-7429-768-7.
[28] KOLOUCH, Jan. *CyberCrime*. Praha: Vyšehrad, 2016, s. 145–149. ISBN 978-80-7429-768-7.

(byť v omylu) a pachatelé operují z jurisdikcí s nízkou úrovní právní pomoci, což ztěžuje jejich identifikaci i případné vydání k trestnímu stíhání.[29]

2.4 Sociální inženýrství

V kontextu kybernetické kriminality a e-mailových podvodů představuje sociální inženýrství (Social Engineering) soubor technik zaměřených na manipulaci s lidmi za účelem vylákání citlivých informací nebo přimění k určitému jednání, které je v rozporu s bezpečnostními pravidly. Zatímco klasický hacking cílí na zranitelnosti softwaru a hardwaru, sociální inženýrství se zaměřuje na „nejpřesnější“ a zároveň „nejslabší“ článek jakéhokoliv bezpečnostního systému, a to na lidský faktor. Pachatelé e-mailových podvodů nejsou pouze technicky zdatní jedinci, ale především zruční manipulátoři, kteří dokážou zneužít přirozené lidské vlastnosti, jako je důvěřivost, ochota pomoci, strach z autority nebo zvědavost.[30]

2.4.1 Psychologické aspekty a principy ovlivňování (autorita, urgence, strach)

Úspěch sociálního inženýrství v e-mailové komunikaci stojí na využití hluboce zakořeněných psychologických mechanismů. Odborná literatura v této souvislosti často odkazuje na principy Roberta Cialdiniho, které útočníci adaptují pro kriminální účely:

- Autorita: E-mail maskovaný jako příkaz nadřízeného (CEO fraud) nebo upozornění státní instituce (Policie ČR, Finanční úřad) vyvolává u oběti automatickou poslušnost. Lidé mají tendenci plnit požadavky osob, které vnímají jako legitimní autority, aniž by podrobovali jejich instrukce kritickému zkoumání.

- Naléhavost (Urgence) a nedostatek: Vytvoření časového tlaku (např. „pokud neprovedete platbu do 30 minut, váš účet bude zablokován“) vyvolává stresovou reakci. V takovém stavu dochází k omezení racionálního uvažování a oběť jedná impulzivně, což je přesně cíl pachatele.

- Reciprocita a ochota pomoci: Zejména u tzv. „romance scams“ nebo charitativních podvodů pachatelé zneužívají lidskou empatii. Vybudováním

[29] PORADA, Viktor. Kriminalistika: technické, forenzní a kybernetické aspekty. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o, 2016. 220-223 s. ISBN 978-80-7380-589-0.
[30] JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. 18-22 s. ISBN 9788024715612.

zdánlivého vztahu nebo popisem krizové situace vmanévrují oběť do pozice, kdy se cítí být morálně zavázána pomoci.

- Sociální schválení (Sociální důkaz): Pachatelé v e-mailech často uvádějí, že daný postup je „běžný“ nebo že jej již „schválili ostatní kolegové“, což v oběti rozptyluje pochybnosti o legitimitě požadavku[31].

2.4.2 Fáze útoku pomocí sociálního inženýrství (příprava, navázání vztahu, realizace, exit)

Kriminalistická analýza e-mailových podvodů ukazuje, že útoky založené na sociálním inženýrství mají zpravidla systematický průběh, který lze rozdělit do čtyř fází:

1. Informační příprava (OSINT): Sběr dat o oběti z veřejných zdrojů, sociálních sítí nebo dřívějších úniků dat. Útočník zjišťuje pracovní pozici, zájmy, používané technologie nebo obchodní partnery.

2. Navázání kontaktu a budování důvěry: Prvotní e-mailová komunikace, která nemusí být hned útočná. Cílem je získat pozornost a vybudovat zdání legitimity.

3. Vlastní realizace (Manipulace): V této fázi útočník uplatňuje výše zmíněné psychologické principy k dosažení svého cíle (např. odeslání peněz, otevření zavirované přílohy).

4. Ukončení a zahlazení stop (Exit strategy): Pachatel přeruší kontakt tak, aby u oběti co nejdéle udržel pocit, že se nic podezřelého neděje (např. poděkování za spolupráci, potvrzení o přijetí platby, která dorazí „za několik dní“).

Sociální inženýrství je v rámci e-mailových podvodů natolik efektivní, že ani nejpokročilejší technická ochrana (antiviry, firewally) nedokáže plně eliminovat riziko útoku. Pro Policii ČR je dokumentace těchto technik klíčová pro pochopení subjektivní stránky trestného činu a určení míry zavinění pachatele.[32]

[31] JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. 34-38 s. ISBN 9788024715612.
[32] HADNAGY, Christopher. *Social Engineering: The Science of Human Hacking*. 2nd ed. Indianapolis: John Wiley & Sons, 2018, s. 42–47. ISBN 978-1119433385.

2.5 Právní aspekty a kvalifikace e-mailových podvodů

Správná právní kvalifikace e-mailových podvodů představuje pro orgány činné v trestním řízení komplexní úkol. Charakteristickým rysem této trestné činnosti je totiž fakt, že pachatelé svým jednáním často zasahují do několika chráněných zájmů současně, a to od majetkových práv oběti až po nedotknutelnost digitálních dat a soukromí. V podmínkách České republiky je stěžejním právním předpisem zákon č. 40/2009 Sb., trestní zákoník (dále jen „TrZ“), který v posledních letech prošel novelizacemi reflektujícími právě specifika kybernetické kriminality.[33]

2.5.1 Skutkové podstaty trestných činů dle TZ (§ 209, § 230, § 231, § 232)

Při vyšetřování e-mailových podvodů dochází nejčastěji k jednočinnému souběhu několika trestných činů. Dominantní roli hrají následující skutkové podstaty:

- Podvod (§ 209 TrZ): Je základním kamenem většiny případů. Pachatel uvádí oběť v omyl (např. falešnou identitou odesílatele) za účelem vlastního obohacení, čímž způsobí škodu na cizím majetku. Klíčovým znakem je zde právě příčinná souvislost mezi omylem oběti a dispozicí s majetkem.

- Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230 TrZ): K tomuto činu dochází v momentě, kdy pachatel překoná bezpečnostní opatření a vnikne do e-mailové schránky oběti. Tento paragraf chrání integritu a důvěrnost dat.

- Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému (§ 231 TrZ): Tato skutková podstata je důležitá u phishingových útoků. Trestným je již samotné získání nebo držení hesel, PIN kódů či jiných dat, která umožňují přístup k systému, pokud je účelem spáchání trestného činu.

- Neoprávněný zásah do počítačového systému nebo nosiče informací z nedbalosti (§ 232 TrZ). Ačkoliv u e-mailových podvodů převažuje úmyslné zavinění, tento paragraf může být relevantní v širším kontextu kybernetických incidentů.[34]

[33] GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Praha: Auditorium, 2015, s. 84–88. ISBN 978-80-87284-53-7.
[34] GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Praha: Auditorium, 2015, s. 92–98. ISBN 978-80-87284-53-7.

2.5.2 Problematika legalizace výnosů z trestné činnosti (§ 216 – bílí koně, kryptoměny)

E-mailový podvod nekončí v momentě, kdy oběť odešle peníze. Pro vyšetřovatele Odboru hospodářské kriminality nastává v tento okamžik nejnáročnější fáze je sledování toku finančních prostředků. Pachatelé se snaží co nejrychleji zahladit stopu k původnímu trestnému činu, čímž naplňují skutkovou podstatu Legalizace výnosů z trestné činnosti (§ 216 TrZ), v praxi známou jako „praní špinavých peněz“.

Klíčovým prvkem jsou v tomto procesu tzv. money mules (bílí koně). Jedná se o osoby, které za úplatu nebo pod vlivem manipulace (např. v rámci „romance scams“) nechávají přes své bankovní účty protékat peníze z podvodů. Tyto prostředky jsou následně:

1. Vrstveny: Přeposílány přes řetězec mnoha dalších účtů, často vedených v zahraničí, aby se ztížilo jejich trasování.

2. Integrovány: Převáděny na vysoce likvidní aktiva, jako jsou kryptoměny, dárkové karty nebo drahá elektronika, čímž se definitivně oddělí od své kriminální historie.

Z hlediska vyšetřovací praxe PČR je prokazování subjektivní stránky (úmyslu) u bílých koní velmi složité, neboť tito lidé často tvrdí, že o nelegálním původu peněz nevěděli. Nicméně v posledních letech soudní praxe stále častěji uplatňuje i formu zavinění z nedbalosti, pokud byly okolnosti transakcí prokazatelně podezřelé.[35]

2.6 Digitální stopy a důkazní materiál

V kriminalistické vědě představuje digitální stopa specifický druh věcného důkazu, který má v prostředí internetu a elektronické pošty klíčový význam pro objasnění skutkového stavu. Na rozdíl od stop materiálních (např. biologických či trasologických) vykazují digitální stopy unikátní vlastnosti, které kladou vysoké nároky na odbornost policisty při jejich vyhledávání, zajišťování a následném zkoumání. Pro vyšetřovatele e-mailových podvodů je digitální stopa často jediným pojítkem mezi virtuálním útokem a konkrétním pachatelem.[36]

[35] FIRSTOVÁ, Jana a ZÁMEK, David. *Prevence kriminality – nedílná součást systému vnitřní bezpečnosti*. Právní monografie. Praha: Wolters Kluwer, 2021. 74-79 s. ISBN 978-80-7676-057-8

[36] PORADA, Viktor. Kriminalistika: technické, forenzní a kybernetické aspekty. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o, 2016. 42-46 s. ISBN 978-80-7380-589-0.

2.6.1 Charakteristika a povaha digitální stopy (latence, křehkost)

Digitální stopy jsou definovány jako informace v digitální podobě, které jsou zapsány v paměti počítačových systémů nebo přenášeny prostřednictvím komunikačních sítí. Jejich zásadním znakem je nehmotná povaha, což znamená, že stopa existuje pouze jako sekvence binárních dat. Mezi klíčové vlastnosti, se kterými musí vyšetřovatel pracovat, patří:

- Křehkost a prchavost: Digitální data mohou být velmi snadno změněna, poškozena nebo nenávratně smazána, a to i neodbornou manipulací vyšetřovatele (např. prostým otevřením e-mailu bez použití forenzních nástrojů).
- Latence: Stopa není lidskými smysly přímo vnímatelná; k jejímu zviditelnění je zapotřebí speciální software a hardware.
- Snadná replikovatelnost: Digitální stopu lze identicky zkopírovat, což je výhodou při analýze (práce s bitovou kopií), ale komplikací při prokazování autenticity originálu.[37]

2.6.2 Klasifikace digitálních stop (metadata, hlavičky e-mailů, provozní údaje)

Při vyšetřování podvodné komunikace se Policie ČR zaměřuje především na tři typy datových nosičů informací:

1. Metadata a hlavičky e-mailů: Každý e-mail nese v tzv. „hlavičce“ (e-mail header) informaci o své cestě internetem. Obsahuje IP adresy odesílacích serverů, časy doručení a identifikační údaje klientských aplikací. Analýza hlavičky je prvním krokem k odhalení e-mail spoofingu.
2. Provozní a lokalizační údaje: Data zajišťovaná u poskytovatelů internetových služeb (ISP). Zde se vyšetřovatel dozvídá, ze které IP adresy a v jakém čase se uživatel k dané schránce přihlásil.
3. Obsahová data: Samotný text zprávy, přílohy (např. podvržené faktury) a vložené hypervazby. Přílohy mohou navíc obsahovat vlastní metadata (např. u PDF faktury lze zjistit, v jakém softwaru a kdy byla naposledy upravována).[38]

[37] PORADA, Viktor. Kriminalistika: technické, forenzní a kybernetické aspekty. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o, 2016. 48-52 s. ISBN 978-80-7380-589-0.
[38] PORADA, Viktor. Kriminalistika: technické, forenzní a kybernetické aspekty. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o, 2016. 242-246 s. ISBN 978-80-7380-589-0.

2.6.3 Proces zajištění digitální stopy v praxi PČR (hashování, integrita)

Zásadním požadavkem pro procesní použitelnost digitálního důkazu před soudem je zachování integrity dat. Policie ČR postupuje podle striktních metodických pokynů, které zahrnují použití hashovacích funkcí (např. SHA-256). Hash je unikátní digitální otisk datového souboru a jakákoliv sebemenší změna v souboru by vedla k totální změně hashe, čímž se prokazuje, že s důkazem nebylo od momentu zajištění manipulováno.

Při zajišťování důkazů u e-mailových podvodů hraje roli také čas. Vzhledem k tomu, že logy na serverech jsou často uchovávány pouze po omezenou dobu (dle zákona o elektronických komunikacích), musí vyšetřovatel jednat bezodkladně, často s využitím institutu neodkladného a neopakovatelného úkonu.[39]

2.6.4 Problémy a omezení (anonymizace, VPN, zahraniční jurisdikce)

Efektivita zajišťování a využívání digitálních stop v trestním řízení je v současnosti limitována řadou technických a legislativních faktorů. Pachatelé e-mailových podvodů si jsou vědomi procesních postupů Policie ČR a cíleně využívají nástroje, které mají za cíl přetrhnout vazbu mezi kriminálním jednáním a jejich skutečnou identitou. Tyto bariéry lze rozdělit do tří hlavních oblastí, které v kombinaci tvoří pro vyšetřovatele velmi složitý celek.

Technická anonymizace a maskování identity

Základním nástrojem útočníků je využívání služeb VPN (Virtual Private Network) a anonymizačních sítí, jako je TOR (The Onion Router). Zatímco VPN šifruje provoz a nahrazuje IP adresu uživatele adresou serveru poskytovatele (často v exotické zemi), síť TOR využívá vícevrstvé šifrování a průchod přes náhodné uzly po celém světě. Pro vyšetřovatele to znamená, že zjištěná IP adresa, ze které byl podvodný e-mail odeslán, nepatří pachateli, ale koncovému bodu anonymizační služby. Pokud poskytovatel VPN neuchovává logy o aktivitě svých uživatelů (politika „no-log“), je technická identifikace pachatele touto cestou prakticky nemožná.[40]

[39] PORADA, Viktor. Kriminalistika: technické, forenzní a kybernetické aspekty. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o, 2016. 58-62 s. ISBN 978-80-7380-589-0.
[40] HROMADA, Martin; HRŮZA, Petr; KADERKA, Josef; LUŇÁČEK, Oldřich; NEČAS, Miroslav et al. *Kybernetická bezpečnost: teorie a praxe*. Praha: Powerprint, 2015. 164 s. ISBN 978-80-87994-72-6

Zahraniční jurisdikce a cloudové služby

Dalším zásadním problémem je teritorialita práva versus bezhraničnost internetu. Většina e-mailových služeb (Gmail, Outlook) a hostingů je provozována nadnárodními korporacemi se sídlem v USA nebo jiných zemích. Získání dat o konkrétním uživateli tak vyžaduje využití nástrojů mezinárodní právní pomoci. Tento proces je však administrativně velmi náročný a časově zdlouhavý. V momentě, kdy česká policie obdrží legální cestou data ze zahraničí (např. po 6–12 měsících), jsou tyto informace často již neaktuální, neboť pachatel mezitím změnil digitální infrastrukturu i platební kanály.[41]

Šifrování a prchavost důkazů

Masivní rozšíření koncového šifrování (End-to-End Encryption) a využívání šifrovaných e-mailových klientů (např. ProtonMail) znamená, že i když se policii podaří zajistit datový přenos, jeho obsah zůstává bez dešifrovacího klíče nečitelný. Tento stav je v kriminalistické praxi označován jako „Going Dark“ je situace, kdy orgány činné v trestním řízení mají zákonnou pravomoc k odposlechu nebo domovní prohlídce, ale technicky nejsou schopny data interpretovat. V kombinaci s automatickým mazáním logů na straně poskytovatelů to vede k vysoké latenci kriminality, kdy důkazní materiál zaniká dříve, než je podvod vůbec nahlášen.[42]

Tyto překážky vytvářejí pro vyšetřovatele Odborů hospodářské kriminality extrémně nepříznivé podmínky, které vyžadují nejen vysokou technickou erudici, ale především schopnost kombinovat digitální šetření s tradičními operativně-pátracími metodami v reálném světě.

2.7 Prevence a role státních autorit

Vzhledem k technické i právní složitosti vyšetřování e-mailových podvodů se prevence stává jednou z nejúčinnějších strategií v boji proti této formě kriminality. Cílem preventivního působení je eliminovat úspěšnost útoků nikoliv na straně technické bariéry, ale na straně lidského faktoru, který je v případě sociálního inženýrství primárním cílem. Státní autority v České republice, v čele s Policií ČR a Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB), v posledních letech vyvinuly řadu

[41] KOLOUCH, Jan. *CyberCrime*. Praha: Vyšehrad, 2016, s. 188–192. ISBN 978-80-7429-768-7.
[42] HROMADA, M. et al. *Kybernetická bezpečnost: teorie a praxe*. Praha: Powerprint, 2015, **s.** 158. ISBN 978-80-87994-72-6.

projektů zaměřených na zvyšování digitální gramotnosti a ostražitosti široké veřejnosti i specifických cílových skupin.

2.7.1 Preventivní projekty Policie ČR (Volač a Klikač, projekt Kyber)

Policie České republiky realizuje preventivní aktivity, které reagují na aktuální trendy v kyberkriminalitě. Tyto kampaně jsou často postaveny na reálných kazuistikách a snaží se veřejnosti přiblížit psychologické triky pachatelů:

- Projekt „Volač a Klikač“: Jedná se o jednu z nejvýraznějších celorepublikových kampaní, která vznikla v úzké spolupráci s Českou bankovní asociací. Kampaň se zaměřuje na kombinaci vishingu (falešné volání bankovního úředníka či policisty) a phishingu (zasílání podvodných e-mailů a odkazů). Cílem je naučit občany, že banka ani policie nikdy nevyžadují citlivé přístupové údaje nebo převody peněz na „zabezpečené“ účty.

- Projekt „Kyber“: Tento dlouhodobý projekt se věnuje vzdělávání napříč generacemi. Zaměřuje se jak na rizikové chování dětí v on-line prostředí, tak na seniory, kteří jsou častým cílem podvodů typu „romance scams“ nebo falešných výher.

- Vzdělávání v korporátním sektoru: Krajská ředitelství PČR často pořádají přednášky pro zástupce firem a státní správy se zaměřením na prevenci útoků typu Business Email Compromise (BEC). Klíčovým doporučením je zavedení tzv. vícestupňového ověřování plateb, kdy je e-mailový příkaz k úhradě následně potvrzen jiným komunikačním kanálem (např. telefonicky).[43]

2.7.2 Součinnost s NÚKIB a bankovním sektorem

Kromě represivní složky (PČR) hrají v prevenci klíčovou roli i další instituce. Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) plní roli metodického a koordinačního orgánu. Vydává varování před aktuálními hrozbami, poskytuje bezplatné vzdělávací kurzy (např. kurz „Dávej kyber“) a stanovuje bezpečnostní standardy pro kritickou infrastrukturu státu.[44]

[43] KOLOUCH, Jan. *CyberCrime*. Praha: Vyšehrad, 2016, s. 204–208. ISBN 978-80-7429-768-7.
[44] HROMADA, M. et al. *Kybernetická bezpečnost: teorie a praxe*. Praha: Powerprint, 2015, s. 212. ISBN 978-80-87994-72-6.

Nezastupitelnou roli má také bankovní sektor. Komerční banky nasazují pokročilé systémy pro sledování podezřelých transakcí (AML monitoring), které dokážou v reálném čase detekovat neobvyklé pohyby na účtech, jež by mohly naznačovat probíhající podvod. Součinnost mezi bankami a policií je klíčová pro včasnou blokaci finančních prostředků dříve, než dojde k jejich vyvedení do zahraničí nebo do kryptoměn.[45]

Efektivní prevence tak nestojí pouze na aktivitě státu, ale na principu sdílené odpovědnosti, kde informovaný uživatel představuje nejpevnější článek v řetězci kybernetické bezpečnosti.

[45] FIRSTOVÁ, Jana a ZÁMEK, David. *Prevence kriminality – nedílná součást systému vnitřní bezpečnosti*. Právní monografie. Praha: Wolters Kluwer, 2021. 112-116 s. ISBN 978-80-7676-057-8

3 PRAKTICKÁ ČÁST (ANALÝZA VYŠETŘOVACÍ PRAXE)

Praktická část této bakalářské práce se zaměřuje na kritickou reflexi a hloubkovou analýzu postupů, které Policie České republiky aplikuje při vyšetřování e-mailových podvodů. Cílem této části není pouze teoretický popis ideálního stavu, ale především konfrontace zákonných a metodických požadavků s reálnou vyšetřovací praxí v podmínkách specializovaných útvarů, zejména Odboru hospodářské kriminality.

V rámci praktického šetření je kladen důraz na identifikaci procesních úskalí, technických limitů a systémových nedostatků, které v každodenní činnosti vyšetřovatelů ovlivňují efektivitu dokumentace trestné činnosti v kyberprostoru. Analýza vychází z empirických poznatků získaných prostřednictvím řízených rozhovorů s policisty, kteří se na tuto agendu specializují, a z evaluace standardních operačních postupů využívaných při zajišťování digitálních stop a trasování finančních toků.

3.1 Vyšetřování e-mailových podvodů v podmínkách Policie ČR

Vyšetřování trestné činnosti páchané prostřednictvím elektronické pošty vyžaduje specifickou organizační strukturu a vysokou míru mezioborové spolupráce. V rámci Policie ČR se na odhalování těchto deliktů podílí několik složek, přičemž klíčové postavení zaujímá Služba kriminální policie a vyšetřování (SKPV).

3.1.1 Příslušnost a specializace útvarů (OHK, SKPV, NCTEKK)

Určení věcné a místní příslušnosti je u e-mailových podvodů často komplikováno faktem, že místo spáchání činu (pachatel), místo následku (bankovní účet) a bydliště poškozeného se nacházejí v různých krajích či státech.

- Obvodní oddělení: Zpravidla slouží jako první kontaktní místo, kde dochází k přijetí trestního oznámení a prvotnímu vytěžení poškozeného.
- Odbory hospodářské kriminality (OHK): Přebírají případy s vyšší způsobenou škodou (např. BEC útoky) a podvody vykazující znaky organizovanosti. Vyšetřovatelé OHK se specializují na trasování finančních prostředků a odkrývání sítí „bílých koní“.

- Oddělení kybernetické kriminality (OKK): Poskytují vyšetřovatelům technickou podporu při analýze digitálních stop, prolamování zabezpečení nebo zajišťování dat z cloudových úložišť.

- NCTEKK: Národní centrála proti terorismu, extremismu a kybernetické kriminalitě metodicky vede nejsložitější případy s celostátním nebo mezinárodním dopadem.[46]

Tato struktura umožňuje policii reagovat jak na jednoduché phishingové podvody, tak na sofistikované útoky cílené na kritickou infrastrukturu nebo velké korporace.

3.1.2 Postup po přijetí trestního oznámení

Proces vyšetřování e-mailových podvodů je v počáteční fázi závodem s časem. Od momentu, kdy se poškozený dostaví na útvar Policie ČR k podání vysvětlení, se rozbíhá řetězec úkonů, které mají za cíl minimalizovat vzniklou škodu a zajistit digitální důkazy, které mají tendenci v čase zanikat. Standardní operační postup lze rozdělit do několika klíčových kroků:

Prvotní vytěžení poškozeného a zajištění komunikace základním úkonem je podrobné sepsání protokolu o trestním oznámení. Vyšetřovatel se nesmí spokojit pouze s popisem skutku, ale musí se zaměřit na technické detaily. Klíčové je zajistit podvodnou e-mailovou komunikaci v jejím syrovém stavu. Poškození často dělají chybu, že e-maily pouze přeposílají, čímž dochází k degradaci metadat. Policie vyžaduje uložení zprávy ve formátu .eml nebo .msg, který uchovává kompletní e-mailovou hlavičku. Tato hlavička je pro vyšetřovatele OHK zásadní, neboť obsahuje IP adresy odesílacích serverů a technické parametry cesty zprávy.

Bezodkladná součinnost s finančními institucemi, pokud tedy k oznámení dojde v krátkém časovém odstupu od provedení transakce (ideálně v řádu hodin), prioritou číslo jedna není identifikace pachatele, ale zastavení finančního toku. Vyšetřovatel využívá institutu dle § 7b trestního řádu (zajištění dat) nebo podnětu k blokaci dle zákona o některých opatřeních proti legalizaci výnosů z trestné činnosti. Dochází k okamžitému kontaktování bankovních specialistů pro kybernetickou bezpečnost. Cílem je zmrazit

[46] KOLOUCH, Jan. *CyberCrime*. Praha: Vyšehrad, 2016, s. 172–176. ISBN 978-80-7429-768-7.

finanční prostředky na účtu příjemce (často bílého koně) dříve, než dojde k jejich výběru v hotovosti nebo převodu na kryptoměnovou burzu.[47]

Zajištění digitální stopy v reálném čase souběžně s finančním šetřením musí policie zajistit provozní a lokalizační údaje. To zahrnuje:

- Vydání příkazů poskytovatelům e-mailových služeb k uchování dat (§ 7b tr. řádu).
- Zajištění logů o přístupech do schránky poškozeného, pokud došlo k jejímu napadení.
- U e-mailových podvodů typu BEC je často nutné provést ohledání počítače či mobilního telefonu oběti, aby se vyloučila přítomnost škodlivého kódu (spyware, keylogger), který mohl pachateli umožnit sledování komunikace.[48]

Kriminalistická analýza a stanovení vyšetřovacích verzí, následuje po zajištění prvotních informací dochází k vyhodnocení modu operandi. Vyšetřovatel analyzuje, zda jde o ojedinělý incident, nebo o součást rozsáhlejší kampaně. Na základě zjištěných IP adres a bankovních spojení jsou prověřovány policejní databáze a systémy mezinárodní spolupráce, aby se zjistilo, zda stejné technické parametry nefigurují i v jiných spisech v rámci celé České republiky nebo v síti Europolu.

Tento počáteční nápor na administrativu a technickou preciznost je rozhodující. Jakékoliv pochybení v této fázi, například opomenutí zajištění hlavičky e-mailu, může vést k tomu, že i když bude pachatel později odhalen, důkazní materiál bude před soudem procesně nepoužitelný.

3.1.3 Mezinárodní spolupráce (Europol, Interpol, MLAT)

Vzhledem k přeshraničnímu charakteru e-mailových podvodů představuje mezinárodní spolupráce kritický prvek vyšetřovacího procesu. Pachatelé často operují z jurisdikcí mimo Evropskou unii, využívají zahraniční hostingové služby a finanční prostředky vyvádějí do bank v zemích s nízkou úrovní právní pomoci. Policie ČR proto musí aktivně využívat široké spektrum nástrojů mezinárodní kooperace, které umožňují

[47] PORADA, Viktor. Kriminalistika: technické, forenzní a kybernetické aspekty. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o, 2016. 248-251 s. ISBN 978-80-7380-589-0.
[48] KOLOUCH, Jan. *CyberCrime*. Praha: Vyšehrad, 2016, s. 170–174. ISBN 978-80-7429-768-7.

jak rychlou operativní výměnu informací, tak formální zajišťování důkazů pro účely trestního řízení.

Role Europolu a mezinárodních vyšetřovacích týmů

Klíčovým partnerem pro Odbory hospodářské kriminality je Europol, konkrétně jeho Evropské centrum pro boj proti kyberkriminalitě (EC3). Europol slouží jako informační uzel, který umožňuje propojovat zdánlivě nesouvisející případy napříč členskými státy EU. Pokud český vyšetřovatel zjistí, že konkrétní IP adresa nebo bankovní účet figuruje v podvodu typu BEC, skrze systém SIENA může okamžitě ověřit, zda stejné stopy neevidují kolegové v jiných zemích. V případě rozsáhlých kampaní pak dochází k vytváření společných vyšetřovacích týmů (JIT – Joint Investigation Teams), které umožňují přímou spolupráci policistů v reálném čase bez nutnosti zdlouhavého úředního postupu.[49]

Interpol a globální dosah

Zatímco Europol dominuje na evropském poli, Interpol poskytuje Policii ČR nástroje pro spolupráci se zeměmi mimo EU, což je u e-mailových podvodů (často s vazbou na Afriku či Asii) naprosto zásadní. Interpol spravuje speciální kanály pro rychlé varování a lokalizaci osob, ale také nástroje jako I-24/7, které umožňují vyšetřovatelům přístup k databázím odcizených dokladů nebo k informacím o praní špinavých peněz na globální úrovni.

Nástroje právní pomoci a MLAT

Kromě operativní spolupráce je nutné zajistit důkazy procesně čistým způsobem, aby byly použitelné před českým soudem. K tomu slouží:

- Evropský vyšetřovací příkaz (EVP): Umožňuje rychlé zajištění dat nebo výslech svědka v rámci členských států EU na základě principu vzájemného uznávání.
- MLAT (Mutual Legal Assistance Treaty): Smlouvy o vzájemné právní pomoci se státy mimo EU (např. s USA). Tento proces je sice formálně nejpřesnější, ale v praxi často nejzdlouhavější. Vyšetřovatel musí cestou Ministerstva spravedlnosti

[49] HOLT, Thomas J., Adam M. BOSSALER a Kathryn C. SEIGFRIED-SPANJER. *Cybercrime and Digital Forensics: An Introduction*. 3rd ed. London: Routledge, 2022, s. 425–430. ISBN 978-0367360078.

či Nejvyššího státního zastupitelství žádat o zajištění dat u amerických poskytovatelů (např. Google, Microsoft).[50]

Z pohledu praktického výkonu služby je mezinárodní spolupráce sisyfovskou prací, kde vyšetřovatel bojuje s různými časovými pásmy, jazykovou bariérou a odlišnými právními řády. Právě rychlost reakce skrze sítě kontaktních míst 24/7 (např. v rámci Budapešťské úmluvy) však mnohdy rozhoduje o tom, zda se podaří finanční prostředky zajistit dříve, než zmizí v nenávratnu.

3.2 Metodika výzkumného šetření

Základním stavebním kamenem praktické části této bakalářské práce je empirické šetření, jehož cílem je hloubková analýza vyšetřovací praxe v oblasti e-mailových podvodů. Vzhledem k vysoké specifičnosti tématu a nutnosti pochopit vnitřní mechanismy práce Policie ČR byl pro výzkum zvolen kvalitativní přístup. Tento přístup umožňuje, na rozdíl od kvantitativních metod, jít pod povrch statistických údajů a identifikovat reálné bariéry, se kterými se vyšetřovatelé potýkají, včetně jejich subjektivního vnímání efektivity současných metodických postupů.

3.2.1 Příprava a realizace rozhovorů

Jako hlavní výzkumný nástroj byla zvolena metoda polostrukturovaného rozhovoru (semi-structured interview). Tato volba byla motivována potřebou udržet tematickou linku výzkumu (danou seznamem připravených otázek), ale zároveň ponechat respondentům prostor pro rozvedení specifických zkušeností z jejich vlastní vyšetřovací praxe.

Příprava rozhovorů probíhala v několika fázích:

1. Konstrukce otázek: Byl sestaven soubor 20 otázek rozdělených do tematických bloků (legislativa, technické zajišťování stop, mezinárodní spolupráce, prevence).

2. Pilotní testování: Otázky byly předem konzultovány s vybraným specialistou z Odboru hospodářské kriminality, aby byla ověřena jejich srozumitelnost a relevance pro policejní praxi.

[50] KOLOUCH, Jan. *CyberCrime*. Praha: Vyšehrad, 2016, s. 188–194. ISBN 978-80-7429-768-7.

Výzkumnými otázkami této bakalářské práce jsou „Je možné zvýšit a zlepšit efektivitu boje proti kyberkriminalitě v oblasti e-mailových podvodů a zefektivnit zajišťování důkazů?“, „Jaké jsou největší bariéry při zajišťování důkazů (digitálních stop) v e-mailové komunikaci?“, „Jaké konkrétní kroky by vedly k zefektivnění zajišťování finančních prostředků vyvedených pachateli?“.

3.2.2 Charakteristika souboru respondentů

Výzkumný soubor byl sestaven metodou záměrného (účelového) výběru. Pro dosažení relevantních výsledků bylo osloveno 10 respondentů, kteří splňovali následující kritéria:

- Služební zařazení v rámci Služby kriminální policie a vyšetřování (SKPV).
- Aktivní působení na Odboru hospodářské kriminality nebo na Oddělení kybernetické kriminality.
- Minimálně tříletá praxe ve vyšetřování majetkové či hospodářské trestné činnosti s přesahem do kyberprostoru.

Tato diverzifikace souboru (kombinace vyšetřovatelů „hospodářky“ a techniků z „kyberu“) umožnila získat komplexní pohled na problematiku e-mailových podvodů, od procesně-právní roviny až po technické detaily zajišťování digitálních stop.

S ohledem na citlivost probírané agendy a ochranu informací o metodách práce PČR byla všem účastníkům zaručena plná anonymita.

3.3 Struktura otázkových bloků

Struktura rozhovoru byla rozdělena do šesti tematických celků. Každý blok otázek má za cíl rozkrýt specifickou část problematiky:

- Blok A (Fenomenologie a trendy): Má odhalit aktuální dynamiku a podíl e-mailových podvodů na celkovém nápadu trestné činnosti. Zkoumá se zde vliv AI na věrohodnost útoků.
- Blok B (Psychologie a sociální inženýrství): Tento celek je zaměřen na lidský faktor. Cílem je identifikovat, jaké psychologické mechanismy (nátlak, autorita) vedou oběť k chybnému rozhodnutí.

- Blok C (Technické a procesní zajišťování stop): Cílem je pojmenovat bariéry ve vyšetřování (šifrování, VPN) a poukázat na nejčastější chyby poškozených při zacházení s důkazním materiálem.
- Blok D (Finanční šetření a "Bílí koně"): Blok analyzuje pohyb finančních prostředků a profiluje osoby, které pomáhají s legalizací výnosů.
- Blok E (Mezinárodní spolupráce): Zkoumá efektivitu komunikace přes Europol a Interpol v reálném čase.
- Blok F (Zefektivnění vyšetřování): Prostor pro expertní reflexi legislativních nedostatků a návrhy na technologické inovace.

3.4 Vyhodnocení jednotlivých bloků rozhovorů

Blok A: Fenomenologie a trendy

Otázka č. 1: Jaký podíl tvoří e-mailové podvody na celkovém objemu kyberkriminality, kterou na vašem pracovišti řešíte?

- **Účel otázky:** Cílem bylo kvantifikovat význam zkoumaného fenoménu v rámci aktuálního nápadu trestné činnosti.
- **Analýza odpovědí:** Respondenti se shodli, že e-mailové podvody jsou „denním chlebem“. Zatímco specialisté z OKYBER odhadují podíl na **50–60 %**, vyšetřovatelé z OHK uvádějí, že e-mail je primárním nástrojem u téměř všech moderních majetkových podvodů. Shoda panuje v tom, že klasická kriminalita se z ulic definitivně přesunula na servery.

Otázka č. 2: Pozorujete v posledních dvou letech výrazný posun v sofistikovanosti útoků (např. kvalita češtiny, využití AI)?

- **Účel otázky:** Identifikovat technologický pokrok na straně pachatelů.
- **Analýza odpovědí:** Zde nastala absolutní shoda všech deseti respondentů. AI (generativní modely) zcela eliminovala dřívější poznávací znamení podvodu – špatnou gramatiku. Respondenti z OKYBER zdůrazňují, že útočníci nyní používají AI i k tvorbě personalizovaných scénářů, které znějí velmi věrohodně.

Otázka č. 3: Která z forem e-mailového podvodu je v současnosti podle vás pro oběti nejnebezpečnější a proč?

- **Účel otázky:** Prioritizace hrozeb z pohledu vyšetřovací praxe.

- **Analýza odpovědí:** Zde se objevil zajímavý rozpor daný specializací. Vyšetřovatelé OHK označili za nejnebezpečnější **Romance Scams** kvůli nevratným škodám na psychice a celoživotních úsporách jednotlivců. Naproti tomu respondenti z OKYBER akcentují **BEC podvody**, které ohrožují ekonomickou stabilitu firem a státních podniků.

Otázka č. 4: Setkáváte se s případy, kdy pachatelé využívají data vytěžená z veřejných rejstříků nebo sociálních sítí k cíleným útokům (tzv. spear-phishing)?

- **Účel otázky:** Ověřit míru využití OSINT technik pachateli.
- **Analýza odpovědí:** Všichni respondenti potvrdili, že „plošný spam“ ustupuje vysoce cíleným útokům. Pachatelé si z LinkedInu nebo obchodního rejstříku vytáhnou strukturu firmy a pak simulují e-mail od reálného nadřízeného.

Blok B: Psychologie a sociální inženýrství

Otázka č. 5: Jaké psychologické spouštěče jsou u vámi řešených případů nejčastější a nejúčinnější?

- **Účel otázky:** Pochopení mechanismu manipulace.
- **Analýza odpovědí:** Respondenti se shodují na „svaté trojici“: **autorita, strach a časový nátlak**. E-mail od „banky“ o zablokování účtu donutí oběť jednat dřív, než začne přemýšlet logicky.

Otázka č. 6: Jaká je typická profilace oběti u Romance Scams oproti útokům typu BEC na firmy?

- **Účel otázky:** Segmentace rizikových skupin pro potřeby prevence.
- **Analýza odpovědí:** U Romance Scams jsou oběťmi lidé s citovým deficitem (často ženy 45+), u BEC jde o zaměstnance v administrativě, kteří jsou pod velkým pracovním tlakem a mají přirozený respekt k hierarchii.

Otázka č. 7: Do jaké míry hraje roli v úspěšnosti podvodu "digitální negramotnost" versus momentální psychické rozpoložení oběti?

- **Účel otázky:** Rozlišení mezi technickou neznalostí a psychickou zranitelností.
- **Analýza odpovědí:** Překvapivě silná shoda (8 z 10) panuje v tom, že **psychické rozpoložení (stres, únava) je důležitější**. I technicky zdatný člověk může „v

zápalu boje“ kliknout na podvodný odkaz, pokud je útok dobře načasován na konec pracovní doby.

Blok C: Technické a procesní zajišťování stop

Otázka č. 8: Jaká je nejčastější chyba poškozených při zajišťování důkazů před nahlášením činu?

- **Účel otázky:** Identifikace chyb, které maří vyšetřování.
- **Analýza odpovědí:** Respondenti z OKYBER jednohlasně uvádějí **přeposílání e-mailu**. Tím se přemažou původní metadata odesílatele. Poškození by měli e-mail uložit jako soubor a nesahat na něj.

Otázka č. 9: Jak hodnotíte využitelnost metadat z hlaviček e-mailů při identifikaci pachatele v praxi?

- **Účel otázky:** Posouzení reálné hodnoty technických stop.
- **Analýza odpovědí:** Metadata jsou považována za nutný základ, ale v době VPN a proxy serverů málokdy vedou přímo k pachateli. Slouží spíše k určení země původu útoku.

Otázka č. 10: Jaké technické překážky jsou pro vás při zajišťování stop nejvíce limitující?

- **Účel otázky:** Definice technologických bariér policie.
- **Analýza odpovědí:** Shoda na třech faktorech: **VPN bez logování, anonymní prohlížeče (TOR) a šifrované e-mailové služby** sídlící mimo EU (např. ProtonMail).

Blok D: Finanční šetření a "Bílí koně"

Otázka č. 11: Jaké jsou nejčastější kanály pro vyvádění finančních prostředků (kryptoměny, zahraniční účty, dárkové karty)?

- **Účel otázky:** Identifikace moderních metod legalizace výnosů z trestné činnosti a mapování "únikových cest" kapitálu.
- **Analýza odpovědí:** Respondenti z obou útvarů (OHK i OKYBER) potvrzují masivní odklon od klasických bankovních převodů směrem ke kryptoměnám. Zatímco dříve dominovaly dárkové karty (Amazon, iTunes), dnes je standardem

okamžitý nákup Bitcoinu přes anonymní burzy nebo krypto-automaty. Vyšetřovatelé z OHK doplňují, že stále častěji narážejí na digitální banky (neobanky) se sídlem mimo EU, které mají velmi laxní kontrolu identity (KYC).

Otázka č. 12: Jaká je úspěšnost blokace peněz, pokud je podvod nahlášen do 24 hodin od transakce?

- **Účel otázky:** Posouzení efektivity časového faktoru a součinnosti bankovního sektoru.
- **Analýza odpovědí:** Zde panuje shoda na tom, že 24 hodin je "magická hranice". Pokud poškozený reaguje okamžitě, je šance na zajištění peněz v rámci tuzemského platebního styku poměrně vysoká (cca 50–70 %). Jakmile však transakce opustí SEPA prostor, úspěšnost drasticky klesá. Respondenti z OKYBER uvádějí, že útočníci využívají tzv. "víkendové útoky", kdy počítají s pomalejší reakcí bank i poškozených.

Otázka č. 13: Jak vnímáte roli "bílých koní"? Jde častěji o vědomé komplice, nebo o oběti manipulace?

- **Účel otázky:** Diferenciace mezi ruznými typy pachatelů/spolupachatelů pro účely trestněprávní kvalifikace.
- **Analýza odpovědí:** Tato otázka odhalila největší názorovou pestrost. Vyšetřovatelé z terénu se často setkávají s "naivními" bílými koňmi (senioři, lidé v dluzích), kteří věří, že vykonávají legální brigádu. Naproti tomu analytici z vyšších složek upozorňují na existenci profesionálních sítí, kde jsou bílí koně rekrutováni cíleně a za svou činnost pobírají fixní provizi, přičemž jsou si nezákonnosti svého počínání plně vědomi.

Blok E: Mezinárodní spolupráce

Otázka č. 14: Jak hodnotíte rychlost a efektivitu spolupráce skrze Europol (SIENA) a Interpol (I-24/7)?

- **Účel otázky:** Evaluace nástrojů mezinárodní policejní spolupráce v kontextu bezhraniční kyberkriminality.
- **Analýza odpovědí:** Platforma SIENA je hodnocena jako špičkový nástroj, který v rámci EU funguje velmi dynamicky. Respondenti z OKYBER oceňují možnost přímé komunikace se zahraničními protějšky. Interpol je vnímán jako užitečný

spíše pro dlouhodobější pátrání, nikoliv pro bleskové zajišťování digitálních stop, kde je procesní zátěž vyšší.

Otázka č. 15: Jaké jsou největší bariéry při vyřizování žádostí o právní pomoc (MLAT) do zemí mimo EU (např. USA, Nigérie)?

- **Účel otázky:** Pojmenování geopolitických a administrativních překážek, které brzdí vyšetřování.
- **Analýza odpovědí:** Hlavní bariérou je extrémní časová náročnost. Zatímco útok proběhne v sekundách, vyřízení MLAT do USA trvá měsíce a do zemí "třetího světa" (Nigérie) se často setkává s naprostou ignorancí. Respondenti shodně uvádějí, že bez ochoty cílové země spolupracovat je digitální stopa v těchto destinacích prakticky nezajistitelná.

Blok F: Zefektivnění vyšetřování

Otázka č. 16: Pokud byste mohl změnit jeden procesní nebo legislativní krok, co by nejvíce pomohlo?

- **Účel otázky:** Získání expertních doporučení de lege ferenda pro zlepšení praxe.
- **Analýza odpovědí:** Nejčastějším požadavkem je zjednodušení bankovního tajemství v prvních hodinách po činu. Vyšetřovatelé z OHK by uvítali pravomoc "zmrazit" podezřelou transakci okamžitě, bez nutnosti promptního schválení státním zástupcem, což by se dokládalo až následně.

Otázka č. 17: Existují nástroje (software/hardware), které vám aktuálně chybí nebo by zasloužily upgrade?

- **Účel otázky:** Identifikace materiálně-technických deficitů vyšetřovacích útvarů.
- **Analýza odpovědí:** Kyber-specialisté (OKYBER) volají po výkonnějších nástrojích pro blockchain analýzu a de-anonymizaci kryptoměnových peněženek. Také se objevuje požadavek na pokročilejší AI software, který by dokázal automaticky propojovat tisíce zdánlivě nesouvisejících podvodů napříč celou republikou.

Otázka č. 18: Domníváte se, že by užší integrace analytických nástrojů mezi bankami a policií mohla vést k automatickému zastavování plateb?

- **Účel otázky:** Posouzení proveditelnosti automatizované prevence v reálném čase.

- **Analýza odpovědí:** Panuje zde 100% shoda. Respondenti věří, že toto je jediná cesta k vítězství nad pachateli. Pokud by bankovní algoritmus v reálném čase porovnal odchozí platbu s policejní databází hlášených phishingových účtů, škody by se snížily o miliardy korun ročně.

Otázka č. 19: Jakou roli podle vás sehraje v blízké budoucnosti umělá inteligence?

- **Účel otázky:** Predikce budoucího vývoje hrozeb a obranných mechanismů.
- **Analýza odpovědí:** Respondenti očekávají éru "AI vs. AI". Pachatelé budou AI využívat k masivnímu generování deepfake videohovorů a hlasových zpráv (vishing), zatímco policie ji bude muset nasadit k automatické detekci těchto podvrhů. AI je vnímána jako akcelerátor obou stran konfliktu.

Otázka č. 20: Doplňující otázka (prostor pro vlastní postřehy).

- **Účel otázky:** Umožnit respondentům sdělit informace, které nebyly pokryty strukturovanou částí rozhovoru.
- **Analýza odpovědí:** Většina vyšetřovatelů zde apeluje na prevenci. Shodují se, že sebelepší represe nepomůže, pokud lidé budou stále "bezhlavě" klikat na odkazy v e-mailech. Zdůrazňují, že nejslabším článkem v řetězci kybernetické bezpečnosti zůstává a vždy bude lidský faktor.

3.5 Zhodnocení výsledků a odpovědi na výzkumné otázky

Před vyhotovením a vyhodnocením rozhovorů byly stanoveny tři výzkumné otázky:

1. „Je možné zvýšit a zlepšit efektivitu boje proti kyberkriminalitě v oblasti e-mailových podvodů a zefektivnit zajišťování důkazů?“,
2. „Jaké jsou největší bariéry při zajišťování důkazů (digitálních stop) v e-mailové komunikaci?“,
3. „Jaké konkrétní kroky by vedly k zefektivnění zajišťování finančních prostředků vyvedených pachateli?“.

První výzkumná otázka představuje samotné analytické jádro v praktické části předložené bakalářské práce, přičemž pro její komplexní zodpovězení byly klíčové především výstupy získané v rámci Bloku F, který se zaměřoval na zefektivnění vyšetřování, konkrétně pak prostřednictvím hloubkové analýzy odpovědí na otázky č. 16,

17 a 18. Na základě vzácné shody všech deseti oslovených respondentů lze jednoznačně konstatovat, že zvýšení efektivity vyšetřovacích procesů je nejen technologicky proveditelné, ale z hlediska celkové bezpečnosti digitálního prostoru v České republice naprosto nezbytné. Experti z řad oddělení hospodářské i kybernetické kriminality (OHK a OKYBER) ve svých výpovědích shodně uvádějí, že současná úroveň efektivity je značně brzděna vysokou administrativní náročností a dosavadní technologickou roztříštěností jednotlivých systémů. Z realizovaných rozhovorů dále vyplynulo, že největší potenciál pro budoucí zlepšení stavu leží v masivní automatizaci procesů, což potvrdily zejména reakce na otázku č. 18, které identifikovaly, že úzká integrace bankovních a policejních analytických nástrojů v reálném čase by dokázala radikálně změnit poměr sil mezi útočníkem a obráncem ve prospěch orgánů činných v trestním řízení. V rovině samotného zajišťování důkazů je pak podle oslovených expertů jakékoli budoucí zlepšení přímo podmíněno změnou přístupu na straně poškozených subjektů, jak bylo demonstrováno v rámci Bloku C u otázky č. 8. Lze tedy uzavřít, že pokud dojde k cílené edukaci veřejnosti v oblasti správného technického zajišťování datových zpráv, dojde k automatickému a zásadnímu zvýšení kvality důkazního materiálu, což v konečném důsledku umožní efektivnější a rychlejší průběh následného trestního řízení.

Pro adekvátní zodpovězení druhé specifické výzkumné otázky byla zásadní především data získaná v rámci Bloku C, zaměřeného na technické a procesní zajišťování stop, a Bloku E, který se věnoval problematice mezinárodní spolupráce. Z provedené analýzy vyplývá, že nejvýznamnější technologickou bariéru, kterou vyšetřovatelé z útvarů OKYBER v rámci otázky č. 10 jasně identifikovali, představuje masivní využívání sofistikovaných end-to-end šifrovaných služeb v kombinaci s využíváním VPN tunelů, které záměrně neuchovávají žádné provozní logy. Tyto technologické nástroje v praxi vytvářejí v digitální stopě pachatele značně problematická „slepá místa“, která je pro policii bez přímé a úzké součinnosti se zahraničními vládními agenturami nebo poskytovateli služeb v podstatě nemožné překonat. Vedle technologických limitů však analýza otázky č. 15 v Bloku E odhalila také kritické procesní bariéry, které se projevují zejména v mezinárodním měřítku při vyřizování žádostí o právní pomoc (MLAT) směrem do zemí mimo Evropskou unii. Respondenti shodně uvádějí, že tyto administrativní procesy trvají často celé měsíce, což je v přímém kontrastu s extrémní dynamikou kybernetického útoku, a v mnoha případech tak dochází k situaci, kdy jsou digitální stopy v době vyřízení žádosti již nenávratně smazány nebo přepsány. V neposlední řadě pak mezi experty panuje shoda v tom, že významnou bariéru tvoří i

samotný lidský faktor na straně poškozených, jak vyplynulo z otázky č. 8, neboť neodborná manipulace s podvodným e-mailem, nejčastěji v podobě jeho prostého přeposílání, nevědomky maří možnost následné technické identifikace skutečného odesílatele a znehodnocuje tak klíčová metadata hlavičky zprávy.

Odpověď na třetí specifickou výzkumnou otázku byla čerpána primárně z datové analýzy Bloku D, který se věnoval finančnímu šetření a problematice „bílých koní“, a dále z expertních návrhů obsažených v Bloku F. Jako naprosto klíčový faktor pro úspěšné zajištění prostředků byla v rámci otázky č. 12 identifikována časová bezprostřednost, neboť klíčem k úspěchu zůstává nahlášení a následná reakce v kritických prvních 24 hodinách od transakce. Z tohoto důvodu respondenti navrhují zavedení legislativní výjimky, která by policii umožnila provádět okamžitou blokaci podezřelých transakcí s tím, že potvrzení státním zástupcem by bylo dodáno až následně, což by eliminovalo současné prodlevy v komunikaci. Vzhledem k tomu, že kryptoměny v současnosti představují hlavní kanál pro únik kapitálu, jak potvrdila analýza otázky č. 11, vyšetřovatelé v rámci otázky č. 17 důrazně doporučují upgrade analytických nástrojů určených pro sledování blockchainu. Bez schopnosti efektivně sledovat pohyb v krypto-peněženkách v reálném čase totiž zůstane zajišťování financí i nadále neefektivní, protože pachatelé dokáží prostředky z bankovního systému vyvést velmi rychle. Za nejúčinnější krok k celkovému zlepšení situace pak respondenti v otázce č. 18 označili systémovou integraci s bankami skrze implementaci algoritmů, které by podezřelé platby, vycházející z typických scénářů podvodů typu Scam 419 či BEC, automaticky pozastavovaly až do momentu jejich manuální verifikace policií nebo bankovním pracovníkem.

3.6 Souhrnná diskuse a návrhy opatření

Na základě podrobné analýzy výše uvedených odpovědí na stanovené výzkumné otázky a s přihlédnutím k praktickým zkušenostem oslovených expertů lze v této části práce formulovat a navrhnout konkrétní kroky pro budoucí legislativní a procesní praxi v České republice. Prvním zásadním bodem je nezbytná legislativní úprava trestního řádu, kde je navrhováno zavedení zcela nového institutu, který lze pracovně nazvat jako „bleskové zajištění digitálních financí“. Tento nástroj by měl za cíl radikálně zkrátit stávající procesní cestu mezi bankovními institucemi a vyšetřovatelem na absolutní minimum, čímž by se eliminovaly kritické časové prodlevy, které v současnosti pachateli umožňují nenávratné vyvedení ukradených prostředků mimo dosah orgánů činných v trestním řízení. Druhým pilířem zefektivnění boje proti kyberkriminalitě by měla být

technologická standardizace, v jejímž rámci by Policie ČR měla iniciovat vznik jednotného a plně automatizovaného rozhraní pro předávání dat od tuzemských e-mailových poskytovatelů. Takový krok by v praxi výrazně urychlil aplikaci ustanovení § 7b trestního řádu a umožnil by vyšetřovatelům získávat potřebné digitální stopy v reálném čase, což je pro úspěšné trasování útočníka klíčové. Souběžně s těmito systémovými změnami je považováno za nutné spustit masivní preventivní kampaň s názvem „Ulož, neposílej“. Tato kampaň by byla primárně zaměřena na edukaci veřejnosti v oblasti správného technického zajišťování podvodných e-mailů, aby nedocházelo k ničení metadat jejich prostým přeposíláním, čímž by došlo k masivnímu zkvalitnění primárních důkazů dostupných již v momentě nahlášení trestného činu.Zcela zásadní roli v budoucím potírání tohoto druhu trestné činnosti pak autor této práce spatřuje v aktivním využívání a neustálém zdokonalování technologií založených na umělé inteligenci (AI), které jsou zde navrhovány k implementaci jako standardní součást vyšetřovacích i preventivních procesů. Lze dovozovat, že moderní AI algoritmy by měly být využívány nejen k prediktivní analýze a vyhledávání vzorců chování pachatelů napříč tisíci zdánlivě nesouvisejícími případy, ale také jako autonomní obranný val v bankovních systémech, který by dokázal podezřelé e-mailové kampaně identifikovat a blokovat dříve než stačí oslovit širší okruh obětí. Právě integrace pokročilé umělé inteligence do rukou vyšetřovatelů se jeví jako jediná efektivní cesta, jak vyrovnat technologický náskok organizovaných zločineckých skupin a zajistit, aby defenzivní schopnosti policie a bank byly vždy o krok před neustále se vyvíjejícími metodami sociálního inženýrství.

ZÁVĚR

Předložená bakalářská práce se věnovala vysoce aktuálnímu a dynamicky se rozvíjejícímu fenoménu e-mailových podvodů v kontextu moderní kriminalistické praxe Policie České republiky. Hlavním cílem práce bylo na základě teoretických východisek a následného empirického šetření analyzovat současný stav vyšetřování této specifické trestné činnosti, identifikovat klíčové bariéry, které snižují efektivitu postupu orgánů činných v trestním řízení, a následně navrhnout konkrétní opatření, jež by mohla vést ke zlepšení úspěšnosti při zajišťování důkazů i finančních prostředků.

V teoretické části práce byla pozornost věnována vymezení základních pojmů a typologii e-mailových podvodů, jako jsou Business Email Compromise (BEC), phishing či různé formy milostných podvodů (Romance Scams). Podrobný rozbor technických aspektů a metod sociálního inženýrství ukázal, že moderní kyberkriminalita se již nespoléhá pouze na technologické nedostatky systémů, ale primárně cílí na psychickou zranitelnost lidského faktoru. Současně byla v teoretické rovině zhodnocena stávající legislativní úprava a kompetence specializovaných útvarů Policie ČR, což vytvořilo nezbytný základ pro následnou praktickou část.

Praktická část práce, realizovaná formou deseti hloubkových expertních rozhovorů s vyšetřovateli z oddělení hospodářské a kybernetické kriminality, přinesla řadu zásadních zjištění, která potvrzují hypotézu o narůstající sofistikovanosti útočníků. Výzkumné šetření jednoznačně prokázalo, že masivní nasazení umělé inteligence pachateli prakticky eliminovalo dřívější rozpoznávací znaky podvodných e-mailů, jako byla špatná gramatika či stylistická neobratnost. Z analýzy výpovědí expertů vyplynulo, že největší bariéru pro úspěšné vyšetřování představuje kombinace technických překážek (šifrování, VPN), administrativní náročnosti mezinárodní spolupráce a neodborné manipulace s důkazním materiálem ze strany samotných poškozených.

Na základě stanovené hlavní výzkumné otázky bylo zjištěno, že efektivitu boje proti e-mailové kriminalitě lze výrazně zvýšit, avšak pouze za předpokladu hlubší systémové integrace. Autor práce v této souvislosti navrhuje implementaci pokročilých analytických nástrojů založených na umělé inteligenci, které by umožnily detekci podvodných schémat v reálném čase. Jako klíčový prvek se jeví návrh na legislativní úpravu, která by policii umožnila bleskové zajištění finančních prostředků na podezřelých účtech bez zbytečných procesních prodlev, které v současnosti nahrávají pachatelům při vyvádění kapitálu do nekontrolovaného prostředí kryptoměn.

Závěrem lze konstatovat, že stanovené cíle bakalářské práce byly naplněny. Provedená analýza ukázala, že boj s e-mailovými podvody není pouze otázkou technologickou, ale vyžaduje multioborový přístup zahrnující právo, psychologii i mezinárodní politiku. Předložené návrhy a opatření (de lege ferenda) mohou sloužit jako podklad pro další odbornou diskuzi o směřování kybernetické bezpečnosti v České republice. Ukazuje se, že pouze aktivní a technologicky vyspělá obhajoba digitálního prostoru, podpořená včasnou edukací veřejnosti a efektivní legislativou, dokáže v budoucnu účinně čelit neustále se vyvíjejícím hrozbám v oblasti e-mailové komunikace.

4 Seznam použitých zdrojů

Literární zdroje

1. BREWSTER, Corey. *Business Email Compromise: The New Face of Cybercrime*. [s.l.]: Independent publ., 2020. 150 s. ISBN 979-8646610257.
2. CASEY, Eoghan. *Digital Evidence and Computer Crime*. 3rd ed. Academic Press, 2011. 832 s. ISBN 978-0123742681.
3. FIRSTOVÁ, Jana a ZÁMEK, David. *Prevence kriminality – nedílná součást systému vnitřní bezpečnosti*. Právní monografie. Praha: Wolters Kluwer, 2021. 204 s. ISBN 978-80-7676-057-8.
4. GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Praha: Auditorium, 2015. 220 s. ISBN 978-80-903786-7-4.
5. HADNAGY, Christopher. *Social Engineering: The Science of Human Hacking*. 2nd ed. Indianapolis: John Wiley & Sons, 2018. 362 s. ISBN 978-1119433385.
6. HOLT, Thomas J.; BOSSLER, Adam M. a SEIGFRIED-SPELLAR, Kathryn C. *Cybercrime and digital forensics: an introduction*. Third edition. London: Routledge, Taylor & Francis Group, 2022. 812 s. ISBN 978-0367360078.
7. HROMADA, Martin; HRŮZA, Petr; KADERKA, Josef; LUŇÁČEK, Oldřich; NEČAS, Miroslav et al. *Kybernetická bezpečnost: teorie a praxe*. Praha: Powerprint, 2015. 250 s. ISBN 978-80-87994-72-6.
8. JIRÁSEK, Petr, Josef POŽÁR a Luděk NOVÁK. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. 5. doplněné a upravené vydání. Praha: Česká pobočka AFCEA; Centrum kybernetické bezpečnosti, z.ú., 2022. 352 s. ISBN 978-80-908388-4-0.
9. JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. 284 s. ISBN 9788024715612. Dostupné také z: http://krameriusndk.nkp.cz/search/handle/uuid:bb517d60-f0dd-11ea-b9b3-005056827e51.
10. KOLOUCH, Jan. *CyberCrime*. Praha: Vyšehrad, 2016. 524 s. ISBN 978-80-7429-768-7.
11. MUSIL, Jan; KONRÁD, Zdeněk a SUCHÁNEK, Jaroslav. *Kriminalistika*. 2., přeprac. a dopl. vyd. Beckovy mezioborové učebnice. Praha: <> Beck, 2004. 584 s. ISBN 8071798789.

12. PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o, 2016. 1024 s. ISBN 978-80-7380-589-0.
13. RAMEŠOVÁ, Kristina. *Právní regulace kybernetické bezpečnosti a její meze*. 1. vydání. Praha: C.H. Beck, 2023. 268 s. Právní instituty. ISBN 978-80-7400-931-0.
14. SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. 936 s. ISBN 9788073807207. Dostupné také z: http://krameriusndk.nkp.cz/search/handle/uuid:2dd74610-b1e9-11e9-8fdf-005056827e52.
15. ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer). 148 s. ISBN 978-80-7552-758-5.

5 Seznam zkratek

AI – Artificial Intelligence (Umělá inteligence)

AML – Anti-Money Laundering (Opatření proti legalizaci výnosů z trestné činnosti)

AOL – America Online

BEC – Business Email Compromise (Podvodný e-mail statutárního zástupce)

CEO – Chief Executive Officer (Generální ředitel)

CFO – Chief Financial Officer (Finanční ředitel)

DKIM – DomainKeys Identified Mail

EC3 – European Cybercrime Centre (Evropské centrum pro boj proti kyberkriminalitě)

EVP – Evropský vyšetřovací příkaz

ISP – Internet Service Provider (Poskytovatel internetových služeb)

JIT – Joint Investigation Team (Společný vyšetřovací tým)

KYC – Know Your Customer (Poznej svého klienta)

MLAT – Mutual Legal Assistance Treaty (Smlouva o vzájemné právní pomoci)

NCTEKK – Národní centrála proti terorismu, extremismu a kybernetické kriminalitě

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

OHK – Odbor hospodářské kriminality

OKK – Oddělení kybernetické kriminality

OKYBER – Oddělení kybernetické kriminality (zkrácené označení v rámci SKPV)

OSINT – Open Source Intelligence (Získávání informací z otevřených zdrojů)

PČR – Policie České republiky

SEPA – Single Euro Payments Area (Jednotná oblast pro platby v eurech)

SKPV – Služba kriminální policie a vyšetřování

SMTP – Simple Mail Transfer Protocol

SPF – Sender Policy Framework

TrZ – Trestní zákoník (Zákon č. 40/2009 Sb.)

USAR – Urban Search and Rescue (Tým pro vyhledávání a záchranu v obydlených oblastech)

VPN – Virtual Private Network (Virtuální privátní síť)

6 Přílohy

Sepsaný rozhovor – kriminalista 1

1. **Jaký podíl tvoří e-mailové podvody (Scam 419, BEC, Romance Scams) na celkovém objemu kyberkriminality, kterou na vašem pracovišti řešíte?**
   - Je to dominantní složka naší práce. Odhaduji, že podvody spojené s elektronickou poštou tvoří tak 50 % až 60 % veškeré kybernetické agendy, kterou u nás na oddělení řešíme.
2. **Pozorujete v posledních dvou letech výrazný posun v sofistikovanosti útoků (např. kvalita češtiny, využití AI)?**
   - Ten posun je neuvěřitelný. Díky zapojení umělé inteligence a pokročilých překladačů úplně zmizela dřívější lámaná čeština. Útoky jsou teď mnohem věrohodnější a hůře rozpoznatelné i pro zkušené uživatele.
3. **Která z forem e-mailového podvodu je v současnosti podle vás pro oběti nejnebezpečnější a proč?**
   - Z hlediska finančních dopadů jsou to rozhodně BEC podvody na firmy, kde škody jdou do milionů. Z hlediska lidské tragédie jsou ale nejhorší Romance Scams, tam ty oběti přicházejí o všechno, o peníze i o psychické zdraví.
4. **Setkáváte se s případy, kdy pachatelé využívají data vytěžená z veřejných rejstříků nebo sociálních sítí k cíleným útokům (tzv. spear-phishing)?**
   - Ano, v podstatě u každého většího firemního podvodu. Pachatelé si z LinkedInu nebo rejstříků přesně zjistí, kdo je účetní a kdo ředitel, a pak ten útok ušijí přesně na míru.
5. **Jaké psychologické spouštěče (strach, autorita, časový tlak) jsou u vámi řešených případů nejčastější a nejúčinnější?**
   - Je to ta známá kombinace autority a tlaku. Pachatel vystupuje jako šéf nebo banka a vytvoří pocit, že se věc musí vyřešit hned teď, jinak bude zle. V tom stresu lidé dělají chyby.
6. **Jaká je typická profilace oběti u Romance Scams oproti útokům typu BEC na firmy?**
   - U Romance Scams jsou to často osamělí lidé, kteří hledají porozumění. U BEC podvodů to nejsou typické oběti, ale spíše loajální zaměstnanci firem, kteří prostě jen chtějí rychle splnit úkol od „nadřízeného“.
7. **Do jaké míry hraje roli v úspěšnosti podvodu "digitální negramotnost" versus momentální psychické rozpoložení oběti?**

- Digitální gramotnost sice pomáhá, ale psychika je silnější. Máme případy, kdy i IT odborník naletěl na phishing, protože byl unavený, měl před dovolenou a prostě na ten odkaz kliknul bez přemýšlení.

8. **Jaká je nejčastější chyba poškozených při zajišťování důkazů před nahlášením činu (např. přeposílání e-mailů)?**
   - To je klasika, lidé nám ten podvodný e-mail jen přepošlou. Tím ale přepíšou metadata a my ztratíme stopu k odesílateli. Potřebujeme vždy e-mail uložený jako soubor se všemi hlavičkami, nebo se k zajišťování e-mailů používá také elektronické zajištění e-mailů, a to v originální podobě, v souladu s metodikou kpt. Mgr. Jana Bačkovského, OKK NCOZ.
9. **Jak hodnotíte využitelnost metadat z hlaviček e-mailů při identifikaci pachatele v praxi?**
   - Je to pro nás základní odrazový můstek. Pokud není hlavička zničená, zjistíme z ní aspoň to, přes jaké servery zpráva šla a kde začít trasovat IP adresy.
10. **Jaké technické překážky (VPN, TOR, šifrovaní typu ProtonMail) jsou pro vás při zajišťování stop nejvíce limitující?**
    - Všechno, co jste vyjmenoval, je problém. Pokud pachatel použije VPN bez logování nebo šifrovaný ProtonMail, tak nám ta stopa končí ve slepé uličce. Bez spolupráce se zahraničím se pak nepohneme.
11. **Jak efektivní je v praxi využívání institutu podle § 7b trestního řádu u tuzemských poskytovatelů?**
    - U nás v Česku to funguje docela dobře a rychle. Problém je, že většina útoků jde přes zahraniční servery jako Gmail.
12. **Jaké jsou nejčastější kanály pro vyvádění finančních prostředků (kryptoměny, zahraniční účty, dárkové karty)?**
    - Dneska vedou kryptoměny. Peníze jdou z účtu oběti na účet bílého koně a odtud okamžitě do krypto-automatu nebo na burzu. Pak už je trasování extrémně složité.
13. **Jaká je úspěšnost blokace peněz, pokud je podvod nahlášen do 24 hodin od transakce?**
    - Těch 24 hodin je kritických. Pokud se to stihne, šance na zajištění peněz je poměrně vysoká, třeba kolem 70 %. Jakmile to trvá déle, ty peníze už jsou dávno „vyprané“ v cizině nebo v bitcoinu.

14. **Jak vnímáte roli "bílých koní"? Jde častěji o vědomé komplice, nebo o oběti manipulace?**
    - Často jsou to lidé v exekucích, co si chtějí přivydělat a „neptají se“. Ale u Romance Scams jsou to často sami poškození, které pachatel přiměje, aby přes jejich účet prošly peníze od dalších obětí.
15. **Jak hodnotíte rychlost a efektivitu spolupráce skrze Europol (SIENA) a Interpol (I-24/7)?**
    - SIENA v rámci Evropy funguje skvěle, tam ta výměna informací běží rychle. Interpol je dobrý na celosvětové pátrání, ale u digitálních stop, kde jde o vteřiny, je to někdy moc administrativně náročné.
16. **Jaké jsou největší bariéry při vyřizování žádostí o právní pomoc (MLAT) do zemí mimo EU (např. USA, Nigérie)?**
    - Ta největší bariéra je čas. Vyřízení žádosti trvá měsíce, i rok. V digitálním světě je rok celá věčnost, logy jsou smazané a pachatel má deset jiných identit.
17. **Pokud byste mohl změnit jeden procesní nebo legislativní krok, co by nejvíce pomohlo zvýšit efektivitu vyšetřování kyberpodvodů?**
    - Potřebujeme pravomoc okamžitě „stopnout“ podezřelou platbu v bance i bez soudního příkazu v prvních hodinách. To papírování nás hrozně brzdí a dává pachateli náskok.
18. **Existují nástroje (software/hardware) pro vyhledávání a analýzu digitálních stop, které vám aktuálně chybí nebo by zasloužily upgrade?**
    - Chybí nám hlavně lepší analytické nástroje na trasování kryptoměn v reálném čase. Taky by pomohl systém s podporou AI, který by sám propojoval hlavičky e-mailů z tisíců různých spisů dohromady.
19. **Domníváte se, že by užší integrace analytických nástrojů mezi bankami a policií mohla vést k automatickému zastavování podezřelých plateb v reálném čase?**
    - Jednoznačně ano. Pokud by bankovní systémy automaticky porovnávaly platby s naší databází nahlášených podvodů, škody by klesly o miliardy. Je to jediná cesta, jak útočníky předběhnout.
20. **Jakou roli podle vás sehraje v blízké budoucnosti umělá inteligence – bude více pomáhat pachatelům při tvorbě podvodů, nebo policii při jejich odhalování?**

- Bude to boj „AI proti AI“. Pachatelé ji teď využívají k masové výrobě útoků, my ji musíme začít využívat k jejich masové detekci. Pokud zaspíme v technologiích, tak to bude opravdu problém.

Sepsaný rozhovor – kriminalista 2

1. **Jaký podíl tvoří e-mailové podvody (Scam 419, BEC, Romance Scams) na celkovém objemu kyberkriminality, kterou na vašem pracovišti řešíte?**
    - Řekl bys, že je to víc než polovina. E-mail zůstává nejjednodušší vstupní branou. Pokud vezmu čistě majetkovou trestnou činnost v kyberprostoru, tak tyhle typy podvodů tvoří odhadem 65 % všech našich spisů.
2. **Pozorujete v posledních dvou letech výrazný posun v sofistikovanosti útoků (např. kvalita češtiny, využití AI)?**
    - Ten rozdíl je markantní. Už neplatí, že podvodníka poznáte podle špatného skloňování. Útočníci dnes používají pokročilé jazykové modely, takže texty jsou stylisticky na úrovni oficiální korporátní komunikace. Je to mnohem nebezpečnější.
3. **Která z forem e-mailového podvodu je v současnosti podle vás pro oběti nejnebezpečnější a proč?**
    - Finančně nejvíc bolí Business Email Compromise, protože tam se hraje o miliony z firemních rozpočtů. Ale lidsky jsou nejvíce devastující Romance Scams, ty oběti často skončí s obrovskými dluhy a v hlubokých depresích, protože ztratily i iluzi vztahu.
4. **Setkáváte se s případy, kdy pachatelé využívají data vytěžená z veřejných rejstříků nebo sociálních sítí k cíleným útokům (tzv. spear-phishing)?**
    - Naprosto běžně. Pachatelé si dělají důkladný průzkum (OSINT). Zjistí si strukturu firmy z LinkedInu, jména účetních z webu a pak pošlou e-mail, který působí, že ho píše skutečný kolega z vedlejší kanceláře.
5. **Jaké psychologické spouštěče (strach, autorita, časový tlak) jsou u vámi řešených případů nejčastější a nejúčinnější?**
    - Je to hlavně uměle vytvořený stres. Pachatel vás dostane do situace, kdy „musíte“ hned jednat, jinak hrozí sankce nebo ztráta zakázky. Pod tímto tlakem člověk přestane přemýšlet racionálně a podlehne autoritě falešného ředitele.

6. **Jaká je typická profilace oběti u Romance Scams oproti útokům typu BEC na firmy?**

    - U milostných podvodů jsou to lidé, kteří jsou v určité životní krizi nebo izolaci. U BEC jsou to naopak lidé velmi výkonní a loajální, kteří prostě jen chtějí vyhovět požadavku svého nadřízeného, aniž by tušili, že je falešný.

7. **Do jaké míry hraje roli v úspěšnosti podvodu "digitální negramotnost" versus momentální psychické rozpoložení oběti?**

    - Můžete být IT expert, ale když vám zavolají ve dvě ráno nebo vás zastihnou v osobní krizi, chybujete. Psychické rozpoložení a únava hrají mnohem větší roli než to, jestli umíte ovládat počítač.

8. **Jaká je nejčastější chyba poškozených při zajišťování důkazů před nahlášením činu (např. přeposílání e-mailů)?**

    - Bohužel je to právě to přeposílání e-mailu místo jeho uložení ve formátu .eml nebo .msg. Tím zničíme důležité trasovací údaje v hlavičce. Vždycky říkáme, že je potřeba s tím e-mailem pracovat jako s fyzickou stopou – ideálně na něj nesahat a nechat to na odborné elektronické zajištění podle Bačkovského metodiky.

9. **Jak hodnotíte využitelnost metadat z hlaviček e-mailů při identifikaci pachatele v praxi?**

    - Je to klíčový důkaz. Z hlavičky vyčteme IP adresy, časová razítka a servery, přes které zpráva putovala. Bez těchto metadat se vyšetřovatel v podstatě nemá čeho chytit.

10. **Jaké technické překážky (VPN, TOR, šifrovaní typu ProtonMail) jsou pro vás při zajišťování stop nejvíce limitující?**

    - Největší problém jsou anonymizační služby, které neuchovávají logy. Jakmile stopa skončí u VPN providera v zemi, která nespolupracuje, jsme v podstatě v koncích. To samé platí pro šifrovanou komunikaci.

11. **Jak efektivní je v praxi využívání institutu podle § 7b trestního řádu u tuzemských poskytovatelů?**

- V Česku to funguje skvěle. Pokud potřebujeme „zmrazit“ data u Seznamu nebo místních operátorů, reakce je rychlá. Problém nastává, když jsou data u Googlu nebo Microsoftu, kde musíme jít cestou mezinárodní pomoci.

12. **Jaké jsou nejčastější kanály pro vyvádění finančních prostředků (kryptoměny, zahraniční účty, dárkové karty)?**

    - Dneska je to jednoznačně cesta přes kryptoměny. Peníze se bleskově protočí přes účty bílých koní a skončí v Bitcoinu. Trasovat takový řetězec je pak nesmírně náročné na čas i techniku.

13. **Jaká je úspěšnost blokace peněz, pokud je podvod nahlášen do 24 hodin od transakce?**

    - Prvních 24 hodin je rozhodujících. Pokud poškozený zareaguje hned, máme šanci ty peníze v bankovním systému stopnout. Úspěšnost je pak docela vysoká. Jakmile to trvá déle, peníze zmizí v zahraničí nebo v kryptu.

14. **Jak vnímáte roli "bílých koní"? Jde častěji o vědomé komplice, nebo o oběti manipulace?**

    - Je to různé. Máme tu lidi, co do toho jdou vědomě pro provizi, ale i spoustu nešťastníků, kteří věří, že dělají legální brigádu. U Romance Scams se bílým koněm stává často sama oběť, která nevědomky pere peníze pro svého „partnera“.

15. **Jak hodnotíte rychlost a efektivitu spolupráce skrze Europol (SIENA) a Interpol (I-24/7)?**

    - Europol a jejich SIENA je pro nás v Evropě neocenitelný nástroj, je to rychlé a efektivní. Interpol je spíš pro ty globální věci, ale tam už ta administrativa vyšetřování někdy brzdí.

16. **Jaké jsou největší bariéry při vyřizování žádostí o právní pomoc (MLAT) do zemí mimo EU (např. USA, Nigérie)?**

    - Hlavně ta šílená délka procesu. Než se žádost vyřídí, data na serverech už dávno nejsou. V digitálním prostředí prostě nemůžeme čekat měsíce na odpověď.

17. **Pokud byste mohl změnit jeden procesní nebo legislativní krok, co by nejvíce pomohlo zvýšit efektivitu vyšetřování kyberpodvodů?**

    - Určitě by pomohlo zrychlení mechanismu pro blokaci finančních toků. Potřebovali bychom mít možnost zastavit platbu operativně, abychom neztráceli drahocenný čas čekáním na formální příkazy.

18. **Existují nástroje (software/hardware) pro vyhledávání a analýzu digitálních stop, které vám aktuálně chybí nebo by zasloužily upgrade?**

    - Vždycky je co zlepšovat v oblasti krypto-analýzy. Taky by nám pomohly pokročilé systémy pro korelaci dat, které by dokázaly samy najít shody mezi tisíci různými případy podvodů.

19. **Domníváte se, že by užší integrace analytických nástrojů mezi bankami a policií mohla vést k automatickému zastavování podezřelých plateb v reálném čase?**

    - Bezesporu. Kdyby banky dokázaly okamžitě reagovat na vzorce chování, které vykazují podvodné transakce, a propojily to s našimi poznatky, ušetřili bychom lidem obrovské jmění.

20. **Jakou roli podle vás sehraje v blízké budoucnosti umělá inteligence – bude více pomáhat pachatelům při tvorbě podvodů, nebo policii při jejich odhalování?**

    - Zatím mají náskok útočníci, kteří AI používají k automatizaci útoků. My musíme odpovědět stejnou silou.

Sepsaný rozhovor – kriminalista 3

1. **Jaký podíl tvoří e-mailové podvody (Scam 419, BEC, Romance Scams) na celkovém objemu kyberkriminality, kterou na vašem pracovišti řešíte?**

    - Je to naprostý základ naší každodenní agendy. Kdybych to měl kvantifikovat, tak podvody založené na sociálním inženýrství přes e-mail tvoří minimálně 60 % živých spisů. Je to zkrátka nejefektivnější cesta k zisku pro útočníky.

2. **Pozorujete v posledních dvou letech výrazný posun v sofistikovanosti útoků (např. kvalita češtiny, využití AI)?**

    - Ten progres je skokový. Doba, kdy jsme lidem říkali, ať hledají chyby v pravopisu, je pryč. Generativní modely AI umožňují útočníkům tvořit perfektní texty, které jsou stylisticky neodlišitelné od běžné obchodní korespondence.

3. **Která z forem e-mailového podvodu je v současnosti podle vás pro oběti nejnebezpečnější a proč?**

    - Z hlediska systémového ohrožení firem je to BEC, tam ty částky likvidují podnikání. Z pohledu individuální oběti jsou to Romance Scams, protože tam dochází k totálnímu odčerpání celoživotních úspor a totální psychické destrukci člověka.

4. **Setkáváte se s případy, kdy pachatelé využívají data vytěžená z veřejných rejstříků nebo sociálních sítí k cíleným útokům (tzv. spear-phishing)?**

    - Prakticky u každého sofistikovanějšího útoku. Pachatelé si dělají důkladný profil oběti. Vědí, kdo ve firmě schvaluje platby, kdo je na dovolené, a využívají tyto informace k tomu, aby útok působil maximálně autenticky.

5. **Jaké psychologické spouštěče (strach, autorita, časový tlak) jsou u vámi řešených případů nejčastější a nejúčinnější?**

    - Funguje hlavně falešný pocit naléhavosti. Útočník oběť vmanipuluje do stavu, kdy má pocit, že musí jednat okamžitě, jinak způsobí škodu. V

kombinaci s imitací autority (např. generálního ředitele) to funguje v 9 z 10 případů.

6. **Jaká je typická profilace oběti u Romance Scams oproti útokům typu BEC na firmy?**

    - U Romance Scams jde o lidi v určité sociální izolaci, kteří hledají oporu. U BEC útoků jsou oběťmi často velmi kompetentní a pracovití lidé, kteří se jen snaží vyjít vstříc požadavku, o kterém si myslí, že je legitimní.

7. **Do jaké míry hraje roli v úspěšnosti podvodu "digitální negramotnost" versus momentální psychické rozpoložení oběti?**

    - Negramotnost je sekundární faktor. Klíčová je psychika. Útoky jsou designované tak, aby obešly logické uvažování. I člověk, který se v IT vyzná, může v momentě únavy nebo stresu fatálně selhat.

8. **Jaká je nejčastější chyba poškozených při zajišťování důkazů před nahlášením činu (např. přeposílání e-mailů)?**

    - Rozhodně to, že nám přepošlou e-mail jako běžnou zprávu. Tím dojde k nevratné modifikaci hlaviček. Vždy vyžadujeme uložení e-mailu jako datového souboru v originálním formátu (.eml), aby bylo možné provést regulérní elektronické zajištění dle metodiky kpt. Bačkovského z OKK NCOZ.

9. **Jak hodnotíte využitelnost metadat z hlaviček e-mailů při identifikaci pachatele v praxi?**

    - metadata jsou alfou a omegou technického šetření. Pokud máme k dispozici nepoškozenou hlavičku, můžeme identifikovat trasu zprávy, odesílací servery a v ideálním případě i zdrojovou IP adresu pachatele.

10. **Jaké technické překážky (VPN, TOR, šifrovaní typu ProtonMail) jsou pro vás při zajišťování stop nejvíce limitující?**

    - Největší bariérou jsou služby, které ze své podstaty neukládají logy o aktivitě uživatelů. Jakmile stopa skončí u offshore VPN providera nebo v síti TOR, šance na přímou identifikaci pachatele se blíží nule.

11. **Jak efektivní je v praxi využívání institutu podle § 7b trestního řádu u tuzemských poskytovatelů?**

    - V rámci ČR je tento nástroj velmi účinný. Tuzemští provideři reagují na výzvy k uchování dat korektně a rychle. Problémem zůstává, že většina kriminální infrastruktury leží mimo jurisdikci ČR.

12. **Jaké jsou nejčastější kanály pro vyvádění finančních prostředků (kryptoměny, zahraniční účty, dárkové karty)?**

    - Aktuálně dominují kryptoměny v kombinaci s bleskovými převody mezi účty bílých koní. Pachatelé využívají rychlost digitálních plateb k tomu, aby peníze vyvedli z dosahu bankovního dohledu během minut.

13. **Jaká je úspěšnost blokace peněz, pokud je podvod nahlášen do 24 hodin od transakce?**

    - Šance je poměrně vysoká, pokud se jedná o tuzemský platební styk nebo prostor SEPA. Těch 24 hodin je skutečně limitní hranice pro efektivní zásah banky. Jakmile peníze odejdou na krypto-burzu, je konec.

14. **Jak vnímáte roli "bílých koní"? Jde častěji o vědomé komplice, nebo o oběti manipulace?**

    - Je to široké spektrum. Od profesionálních „praček“, které to dělají pro zisk, až po naivní lidi, kteří si myslí, že jen přeposílají peníze v rámci legálního zaměstnání. U podvodů na seniory se bílým koněm stává oběť nevědomky.

15. **Jak hodnotíte rychlost a efektivitu spolupráce skrze Europol (SIENA) a Interpol (I-24/7)?**

    - Kanál SIENA je pro nás v evropském kontextu zásadní a velmi rychlý. Interpol je užitečný pro globální koordinaci, ale administrativní náročnost je u něj citelně vyšší.

16. **Jaké jsou největší bariéry při vyřizování žádostí o právní pomoc (MLAT) do zemí mimo EU (např. USA, Nigérie)?**

    - Jednoznačně časový faktor. Procesování žádostí přes ministerstva spravedlnosti trvá měsíce. V digitálním světě, kde se stopy mažou po

dnech, je tento systém v podstatě nepoužitelný pro zajištění aktuálních logů.

17. **Pokud byste mohl změnit jeden procesní nebo legislativní krok, co by nejvíce pomohlo zvýšit efektivitu vyšetřování kyberpodvodů?**

    - Rozhodně zavedení možnosti bleskové operativní blokace bankovních účtů policií bez nutnosti okamžitého schválení státním zástupcem v kritických prvních hodinách po činu.

18. **Existují nástroje (software/hardware) pro vyhledávání a analýzu digitálních stop, které vám aktuálně chybí nebo by zasloužily upgrade?**

    - Potřebovali bychom pokročilejší nástroje pro křížovou analýzu dat napříč různými kriminálními případy a modernější software pro trasování transakcí v decentralizovaných financích (DeFi).

19. **Domníváte se, že by užší integrace analytických nástrojů mezi bankami a policií mohla vést k automatickému zastavování podezřelých plateb v reálném čase?**

    - Je to v podstatě jediná cesta k reálnému snížení škod. Banky mají algoritmy na detekci anomálií a my máme data o pachateli. Jejich propojení by bylo revoluční.

20. **Jakou roli podle vás sehraje v blízké budoucnosti umělá inteligence – bude více pomáhat pachatelům při tvorbě podvodů, nebo policii při jejich odhalování?**

    - AI bude hlavním motorem obou stran. Pachatelé ji využijí k masové automatizaci podvodů, my ji musíme integrovat do procesů vyšetřování k detekci vzorců, které lidské oko neuvidí. Bez technologického upgradu budeme tahat za kratší konec.

Sepsaný rozhovor – kriminalista 4

1. **Jaký podíl tvoří e-mailové podvody (Scam 419, BEC, Romance Scams) na celkovém objemu kyberkriminality, kterou na vašem pracovišti řešíte?**

    - Je to naprostá většina. Pokud se podívám na to, co nám denně přistává na stole, tak tyhle e-mailové věci tvoří dobrých 70 %. Ostatní věci, jako jsou útoky na servery, jsou proti tomu v menšině.

2. **Pozorujete v posledních dvou letech výrazný posun v sofistikovanosti útoků (např. kvalita češtiny, využití AI)?**

    - Ten rozdíl je děsivý. Dřív jste podvodníka poznali podle toho, že psal jako tatar. Dneska, s těmi AI nástroji, vám přijde e-mail, který vypadá líp než ten od vašeho právníka. Ta čeština je už v podstatě bezchybná.

3. **Která z forem e-mailového podvodu je v současnosti podle vás pro oběti nejnebezpečnější a proč?**

    - Za mě jsou to ty milostné podvody (Romance Scams). U BEC jde „jen“ o peníze firmy, ale u těch citovek ti lidé přicházejí o všechno. O důstojnost, o rodinu a často i o střechu nad hlavou, protože se kvůli pachateli zadluží až po uši.

4. **Setkáváte se s případy, kdy pachatelé využívají data vytěžená z veřejných rejstříků nebo sociálních sítí k cíleným útokům (tzv. spear-phishing)?**

    - Pořád. Pachatelé nejsou hloupí, udělají si domácí úkol. Zjistí si z obchodního rejstříku, kdo firmu zastupuje, na Facebooku si najdou, co ty lidi zajímá, a pak na ně udeří s informacemi, které působí hrozně důvěryhodně.

5. **Jaké psychologické spouštěče (strach, autorita, časový tlak) jsou u vámi řešených případů nejčastější a nejúčinnější?**

    - Kombinace strachu a spěchu. Pachatel vám nakecá, že se něco hrozného stane, když hned teď nepošlete peníze. Lidé v panice vypnou mozek a dělají věci, kterým by se za normálních okolností vysmáli.

6. **Jaká je typická profilace oběti u Romance Scams oproti útokům typu BEC na firmy?**

- Romance Scams cílí na lidi, co jsou sami a chtějí trochu pozornosti. BEC je o něčem jiném, tam jsou oběťmi poctiví zaměstnanci, co chtějí jen dobře odvést svou práci a vyhovět požadavku, o kterém si myslí, že jde z vedení.

7. **Do jaké míry hraje roli v úspěšnosti podvodu "digitální negramotnost" versus momentální psychické rozpoložení oběti?**

    - Digitální znalosti vás nespasí, když jste v háji psychicky. Viděl jsem lidi z IT, co naletěli, protože byli unavení nebo měli zrovna osobní trable. Pachatelé jsou mistři v tom, jak vás vystihnout v oslabení.

8. **Jaká je nejčastější chyba poškozených při zajišťování důkazů před nahlášením činu (např. přeposílání e-mailů)?**

    - Lidé to prostě jen přepošlou dál, jako by to byla fotka z dovolené. Tím ten důkaz v podstatě poškodí. My pro to elektronické zajištění podle metodiky kpt. Bačkovského potřebujeme ten původní e-mail v té podobě, v jaké přišel, jako soubor se vším všudy, co je „pod kapotou“.

9. **Jak hodnotíte využitelnost metadat z hlaviček e-mailů při identifikaci pachatele v praxi?**

    - Bez toho jsme v koncích. Hlavička je pro nás mapa. Pokud je v pořádku, můžeme začít rozmotávat, odkud to přišlo a přes koho to letělo. Bez metadat je to jako hledat jehlu v kupce sena po tmě.

10. **Jaké technické překážky (VPN, TOR, šifrovaní typu ProtonMail) jsou pro vás při zajišťování stop nejvíce limitující?**

    - Šifrované služby typu ProtonMail jsou pro nás noční můra. Jakmile tam stopa skočí, tak bez spolupráce s jejich centrálou, která je často v cizině a moc s námi nemluví, končíme u zavřených dveří.

11. **Jak efektivní je v praxi využívání institutu podle § 7b trestního řádu u tuzemských poskytovatelů?**

    - Čeští provideři vědí, že když voláme, tak to hoří, a ta data nám bleskově „zakonzervují“. Problém je, že zločinci často jedou přes servery, co v Česku vůbec nejsou.

12. **Jaké jsou nejčastější kanály pro vyvádění finančních prostředků (kryptoměny, zahraniční účty, dárkové karty)?**

    - Dneska je to hlavně krypto. Je to hrozně rychlé a anonymní. Pachatel ty peníze přes bílé koně prožene do nějaké pochybné burzy v zahraničí a my už pak vidíme jen prázdné účty.

13. **Jaká je úspěšnost blokace peněz, pokud je podvod nahlášen do 24 hodin od transakce?**

    - Těch 24 hodin je svatý grál. Když to lidé nahlásí hned, banky to stihnou stopnout. Jakmile to trvá déle, ty prachy už jsou v bitcoinu a nikdo je neuvidí. Čas je náš největší nepřítel.

14. **Jak vnímáte roli "bílých koní"? Jde častěji o vědomé komplice, nebo o oběti manipulace?**

    - Je to tak půl na půl. Máme tu „profesionály“, co si tím přivydělávají, ale taky spoustu chudáků, co si mysleli, že mají skvělou brigádu z domova. U těch milostných podvodů do toho pachatelé často uvrtají i samotné oběti.

15. **Jak hodnotíte rychlost a efektivitu spolupráce skrze Europol (SIENA) a Interpol (I-24/7)?**

    - SIENA je v Evropě pecka, to funguje skoro online. Interpol je taky dobrý, ale tam už do toho kecá víc byrokracie a trvá to déle, což u digitálních stop není zrovna ideální.

16. **Jaké jsou největší bariéry při vyřizování žádostí o právní pomoc (MLAT) do zemí mimo EU (např. USA, Nigérie)?**

    - Ta šílená čekací doba. Než se to vyřídí, logy na serverech se pětkrát přemažou. Tenhle systém právní pomoci je v digitální době prostě strašně pomalý.

17. **Pokud byste mohl změnit jeden procesní nebo legislativní krok, co by nejvíce pomohlo zvýšit efektivitu vyšetřování kyberpodvodů?**

- Chtěl bych, abychom mohli v bance zablokovat podezřelý účet okamžitě, ne až po tom, co oběháme všechna razítka. Když jde o minuty, legislativa nás hrozně brzdí.

18. **Existují nástroje (software/hardware) pro vyhledávání a analýzu digitálních stop, které vám aktuálně chybí nebo by zasloužily upgrade?**

    - Určitě by se hodily lepší programy na sledování kryptotransakcí. A taky něco, co by samo propojovalo různé případy dohromady, abychom viděli, že ten samý šmejd podvádí lidi po celé republice.

19. **Domníváte se, že by užší integrace analytických nástrojů mezi bankami a policií mohla vedst k automatickému zastavování podezřelých plateb v reálném čase?**

    - Stoprocentně. Banky ty systémy mají, my máme ty „černé listiny“. Kdyby se to spojilo, ušetřilo by to lidem neskutečné prachy. Je to jediná rozumná cesta do budoucna.

20. **Jakou roli podle vás sehraje v blízké budoucnosti umělá inteligence – bude více pomáhat pachatelům při tvorbě podvodů, nebo policii při jejich odhalování?**

    - AI bude pomáhat oběma. Pachatelé s ní budou podvádět ve velkém, my ji musíme mít k tomu, abychom ty tisíce podvodů stíhali zpracovávat. Je to technologický závod ve zbrojení.

Sepsaný rozhovor – kriminalista 5

1. **Jaký podíl tvoří e-mailové podvody (Scam 419, BEC, Romance Scams) na celkovém objemu kyberkriminality, kterou na vašem pracovišti řešíte?**
    - Pokud se bavíme o majetkové trestné činnosti páchané v digitálu, tak tyhle podvody tvoří dobrou polovinu veškerého našeho nápadu. Je to v podstatě náš denní chleba, tyhle případy se nám na stole vrší nejrychleji.
2. **Pozorujete v posledních dvou letech výrazný posun v sofistikovanosti útoků (např. kvalita češtiny, využití AI)?**
    - Ten skok je obrovský. Dřív ty maily o dědictví z Nigérie vypadaly jako z Google Translatoru z roku 2010. Dneska, s těmi novými modely AI, vám přijde e-mail, který stylisticky a gramaticky sedí na 100 %. Je to čím dál těžší poznat i pro lidi, co se v tom pohybují.
3. **Která z forem e-mailového podvodu je v současnosti podle vás pro oběti nejnebezpečnější a proč?**
    - Z pohledu vyšetřovatele je nejhorší BEC podvod, protože tam firmy přicházejí o likviditu během pár minut a ty částky jsou astronomické. Lidsky jsou ale nejvíc zničující Romance Scams – ty oběti často ztratí všechno a stydí se to vůbec nahlásit, dokud není pozdě.
4. **Setkáváte se s případy, kdy pachatelé využívají data vytěžená z veřejných rejstříků nebo sociálních sítí k cíleným útokům (tzv. spear-phishing)?**
    - Ano, v podstatě u každého většího útoku na firmy. Pachatelé si zmapují LinkedIn, firemní weby a rejstříky. Pak přesně vědí, kdo je zástupce ředitele a kdo má v účtárně přístup k bankovnictví. Je to precizně připravený lov.
5. **Jaké psychologické spouštěče (strach, autorita, časový tlak) jsou u vámi řešených případů nejčastější a nejúčinnější?**
    - Časový pres. Pachatel vytvoří iluzi, že se musí okamžitě zaplatit nějaká smyšlená faktura nebo potvrdit údaje, jinak hrozí obrovská škoda. Lidé v tom spěchu přestanou prověřovat fakta a prostě vyhoví "autoritě".
6. **Jaká je typická profilace oběti u Romance Scams oproti útokům typu BEC na firmy?**
    - U těch milostných podvodů jsou to často lidé, kteří jsou sami a hledají porozumění. U BEC podvodů jsou to naopak velmi zodpovědní

zaměstnanci, kteří jen chtějí vyhovět pokynu svého šéfa a nechtějí brzdit chod firmy.

7. **Do jaké míry hraje roli v úspěšnosti podvodu "digitální negramotnost" versus momentální psychické rozpoložení oběti?**
    - Psychika je podle mě důležitější faktor než technické znalosti. Máme případy, kdy naletěli lidé s vysokoškolským vzděláním, protože je pachatel zastihl v momentě slabosti, únavy nebo velkého stresu.
8. **Jaká je nejčastější chyba poškozených při zajišťování důkazů před nahlášením činu (např. přeposílání e-mailů)?**
    - Že nám ty maily jen přepošlou jako běžnou poštu. Tím se úplně znehodnotí metadata. Pro naše elektronické zajištění podle metodiky kpt. Bačkovského (OKK NCOZ) musíme mít originální soubor s hlavičkou, abychom mohli trasovat cestu té zprávy.
9. **Jak hodnotíte využitelnost metadat z hlaviček e-mailů při identifikaci pachatele v praxi?**
    - Je to naprostý základ. Pokud máme k dispozici originální hlavičku a ta není zmanipulovaná, je to pro nás digitální stopa, která nám ukáže, přes jaké servery a IP adresy se k nám ten podvod dostal.
10. **Jaké technické překážky (VPN, TOR, šifrovaní typu ProtonMail) jsou pro vás při zajišťování stop nejvíce limitující?**
    - Hlavně anonymizační služby bez ukládání logů. Když stopa skončí u VPN providera někde na Seychelách nebo v síti TOR, tak bez mezinárodní spolupráce s těmi poskytovateli prostě končíme u zdi.
11. **Jak efektivní je v praxi využívání institutu podle § 7b trestního řádu u tuzemských poskytovatelů?**
    - S českými poskytovateli se spolupracuje dobře. Jsou naučení, že když pošleme výzvu k uchování dat, tak ty logy zmrazí a počkají na náš další postup. Problém je, že většina podvodů jde ze zahraničí.
12. **Jaké jsou nejčastější kanály pro vyvádění finančních prostředků (kryptoměny, zahraniční účty, dárkové karty)?**
    - Dneska je to jednoznačně cesta přes kryptoměny. Peníze se bleskově proženou přes účty bílých koní a pak hned na krypto-burzu. Jakmile se ty peníze "umyjí" v bitcoinu, je šance na jejich dohledání minimální.

13. **Jaká je úspěšnost blokace peněz, pokud je podvod nahlášen do 24 hodin od transakce?**
    - Do 24 hodin je ta šance relativně vysoká. Banky mají určité mechanismy, jak to v systému stopnout. Jakmile to trvá déle než den, ty prostředky jsou většinou už dávno v zahraničí nebo vybrané v hotovosti.
14. **Jak vnímáte roli "bílých koní"? Jde častěji o vědomé komplice, nebo o oběti manipulace?**
    - Je to mix. Máme tu lidi, co to dělají pro provizi a vědí, že to není čisté. Ale u těch citových podvodů jsou bílými koňmi často sami poškození, které pachatel vmanipuluje do role "zprostředkovatele".
15. **Jak hodnotíte rychlost a efektivitu spolupráce skrze Europol (SIENA) a Interpol (I-24/7)?**
    - SIENA v rámci Evropy funguje skvěle, tam je ta komunikace rychlá. Interpol je taky užitečný, ale tam už do toho vstupuje víc administrativy a trvá to déle, což u digitálních stop hraje proti nám.
16. **Jaké jsou největší bariéry při vyřizování žádostí o právní pomoc (MLAT) do zemí mimo EU (např. USA, Nigérie)?**
    - Ta hrozná délka vyřizování. Než se přes ministerstva dočkáme odpovědi, tak logy na serverech v cizině jsou dávno smazané. V digitálním světě je rok čekání na odpověď prostě nepoužitelný systém.
17. **Pokud byste mohl změnit jeden procesní nebo legislativní krok, co by nejvíce pomohlo zvýšit efektivitu vyšetřování kyberpodvodů?**
    - Určitě blesková možnost blokace účtů policií bez zbytečného papírování v prvních hodinách. Ta časová ztráta při čekání na formální souhlasy je to, co dává pachateli náskok.
18. **Existují nástroje (software/hardware) pro vyhledávání a analýzu digitálních stop, které vám aktuálně chybí nebo by zasloužily upgrade?**
    - Chybí nám hlavně lepší analytické nástroje na trasování kryptoměn v reálném čase. A taky software, který by dokázal automaticky propojovat různé případy napříč kraji na základě společných prvků.
19. **Domníváte se, že by užší integrace analytických nástrojů mezi bankami a policií mohla vést k automatickému zastavování podezřelých plateb v reálném čase?**

- Bezesporu. Banky ty systémy mají a kdyby se to propojilo s našimi databázemi, ušetřilo by to lidem miliardy korun. Je to jediná cesta k reálnému snížení škod.

20. **Jakou roli podle vás sehraje v blízké budoucnosti umělá inteligence – bude více pomáhat pachatelům při tvorbě podvodů, nebo policii při jejich odhalování?**
    - Zatím vede pachatel, protože AI používá k masovému generování útoků. My musíme odpovědět stejnou mincí – nasadit AI na detekci a třídění dat, abychom ty tisíce podvodů stíhali vůbec zpracovávat.

Sepsaný rozhovor – kriminalista 6

1. **Jaký podíl tvoří e-mailové podvody (Scam 419, BEC, Romance Scams) na celkovém objemu kyberkriminality, kterou na vašem pracovišti řešíte?**
    - Pokud se podívám na nápad trestné činnosti u nás na kraji, tak podvody využívající e-mailovou komunikaci tvoří přibližně 55 % až 60 % agendy. Je to masová záležitost, která se na nás valí ve vlnách.
2. **Pozorujete v posledních dvou letech výrazný posun v sofistikovanosti útoků (např. kvalita češtiny, využití AI)?**
    - Ten posun je brutální. Dřívější „lámaná“ čeština je minulostí. Pachatelé teď používají LLM modely (jako ChatGPT), takže ty e-maily jsou stylisticky vybroušené, bez gramatických chyb a působí naprosto profesionálně. Rozpoznat podvod jen podle textu je dneska skoro nemožné.
3. **Která z forem e-mailového podvodu je v současnosti podle vás pro oběti nejnebezpečnější a proč?**
    - Z hlediska objemu škod je to BEC. Tam útočníci cílí na statisíce eur. Ale z pohledu společenské nebezpečnosti a dopadu na jednotlivce jsou to Romance Scams. Ty oběti jsou emočně zmanipulované natolik, že pachateli věří víc než vlastní rodině nebo policii.
4. **Setkáváte se s případy, kdy pachatelé využívají data vytěžená z veřejných rejstříků nebo sociálních sítí k cíleným útokům (tzv. spear-phishing)?**
    - Ano, je to standardní součást přípravy útoku. Útočníci si z LinkedInu nebo obchodního rejstříku vytáhnou organizační strukturu firmy, jména kompetentních osob a pak útok ušijí přesně na míru danému prostředí.
5. **Jaké psychologické spouštěče (strach, autorita, časový tlak) jsou u vámi řešených případů nejčastější a nejúčinnější?**
    - Nejlépe funguje kombinace autority a falešné urgence. Když e-mail vypadá, že ho píše CEO a spěchá to, zaměstnanci mají tendenci obcházet standardní kontrolní mechanismy, jen aby vyhověli.
6. **Jaká je typická profilace oběti u Romance Scams oproti útokům typu BEC na firmy?**
    - U milostných podvodů jsou to často lidé ve středním a vyšším věku, kteří jsou v izolaci. U BEC jsou oběťmi loajální a svědomití pracovníci

středního managementu nebo účtáren, kteří se prostě jen snaží dobře dělat svoji práci.

7. **Do jaké míry hraje roli v úspěšnosti podvodu "digitální negramotnost" versus momentální psychické rozpoložení oběti?**
    - Gramotnost sice pomůže, ale psychika je rozhodující. Máme případy, kdy naletěli vysokoškoláci i technici, protože byli v tu chvíli unavení, pod stresem nebo v euforii. Pachatelé cílí na emoce, ne na znalost Windows.
8. **Jaká je nejčastější chyba poškozených při zajišťování důkazů před nahlášením činu (např. přeposílání e-mailů)?**
    - Klasickou chybou je pouhé přeposlání e-mailu. Tím se modifikují technické parametry zprávy. My potřebujeme originální soubor (.eml nebo .msg), abychom mohli provést elektronické zajištění podle metodiky kpt. Bačkovského a analyzovat hlavičky.
9. **Jak hodnotíte využitelnost metadat z hlaviček e-mailů při identifikaci pachatele v praxi?**
    - Metadata z hlaviček jsou pro nás základní technickou stopou. Pokud je e-mail správně zajištěn, můžeme z nich vyčíst IP adresy odesílajících serverů a trasovat cestu zprávy až k prvnímu uzlu.
10. **Jaké technické překážky (VPN, TOR, šifrovaní typu ProtonMail) jsou pro vás při zajišťování stop nejvíce limitující?**
    - Šifrované služby jako ProtonMail a užívání VPN bez logování jsou pro nás velké zdi. Pokud stopa skončí u providera v jurisdikci, která nespolupracuje, tak se bez mezinárodní asistence dál nedostaneme.
11. **Jak efektivní je v praxi využívání institutu podle § 7b trestního řádu u tuzemských poskytovatelů?**
    - U nás v Česku to funguje výborně. Tuzemští provideři reagují na výzvy k uchování dat pružně a v zákonných lhůtách. Problémem je spíš to, že infrastruktura útočníků je většinou v zahraničí.
12. **Jaké jsou nejčastější kanály pro vyvádění finančních prostředků (kryptoměny, zahraniční účty, dárkové karty)?**
    - V současnosti dominují bleskové převody na účty bílých koní a následná konverze do kryptoměn. Peníze se v bankovním systému „vypaří“ během pár minut po jejich odeslání obětí.

13. **Jaká je úspěšnost blokace peněz, pokud je podvod nahlášen do 24 hodin od transakce?**
    - Těch prvních 24 hodin je kritický časový rámec. Pokud se to stihne, šance na zajištění peněz v rámci SEPA prostoru je poměrně slušná. Jakmile to trvá déle, ty peníze jsou už v kryptu a šance se limitně blíží nule.
14. **Jak vnímáte roli "bílých koní"? Jde častěji o vědomé komplice, nebo o oběti manipulace?**
    - Máme lidi, kteří to dělají pro rychlý zisk a vědí, že perou špinavé peníze. Ale u Romance Scams se bílým koněm stává často sama oběť, která věří, že jen pomáhá svému „virtuálnímu partnerovi“.
15. **Jak hodnotíte rychlost a efektivitu spolupráce skrze Europol (SIENA) a Interpol (I-24/7)?**
    - SIENA je v rámci Evropy špičkový nástroj pro rychlou výměnu informací. Interpol je taky fajn, ale u digitálních stop, kde jde o vteřiny, je ten systém někdy až příliš administrativně těžkopádný.
16. **Jaké jsou největší bariéry při vyřizování žádostí o právní pomoc (MLAT) do zemí mimo EU (např. USA, Nigérie)?**
    - Jednoznačně čas. Vyřízení žádosti o data trvá měsíce. Než přijde odpověď z USA nebo Afriky, logy na serverech jsou dávno přemazané a pachatel má deset jiných identit.
17. **Pokud byste mohl změnit jeden procesní nebo legislativní krok, co by nejvíce pomohlo zvýšit efektivitu vyšetřování kyberpodvodů?**
    - Potřebovali bychom legislativní pravomoc k operativní blokaci účtů v prvních hodinách po nahlášení, abychom neztráceli čas čekáním na formální schválení, zatímco peníze odtékají do ciziny.
18. **Existují nástroje (software/hardware) pro vyhledávání a analýzu digitálních stop, které vám aktuálně chybí nebo by zasloužily upgrade?**
    - Určitě analytické systémy pro trasování kryptoměn v reálném čase a pokročilé AI nástroje, které by dokázaly propojovat různé kauzy na základě technických podobností e-mailů.
19. **Domníváte se, že by užší integrace analytických nástrojů mezi bankami a policií mohla vedst k automatickému zastavování podezřelých plateb v reálném čase?**

- Jednoznačně ano. Banky mají algoritmy na detekci anomálií a my máme data o pachateli. Propojení těchto světů by dokázalo zachránit miliardy korun ročně.

20. **Jakou roli podle vás sehraje v blízké budoucnosti umělá inteligence – bude více pomáhat pachatelům při tvorbě podvodů, nebo policii při jejich odhalování?**
    - Bude to technologický závod. Pachatelé teď vedou díky automatizaci útoků, my musíme odpovědět nasazením AI do analýzy a detekce. Pokud v tomto technologickém rozvoji zaspíme, bude to velký problém.

Sepsaný rozhovor – kriminalista 7

1. **Jaký podíl tvoří e-mailové podvody (Scam 419, BEC, Romance Scams) na celkovém objemu kyberkriminality, kterou na vašem pracovišti řešíte?**
    - Hele, kdybych to měl říct od boku, tak e-mailový podvody nám dělají klidně třetinu až polovinu všech případů kyberkriminality. Záleží na období, ale je to prostě masovka.
2. **Pozorujete v posledních dvou letech výrazný posun v sofistikovanosti útoků (např. kvalita češtiny, využití AI)?**
    - Jo, a dost brutální posun. Dřív jsi poznal podvod podle lámaný češtiny na první dobrou. Dneska? Texty jak od rodilého mluvčího, někdy i lepší než od reálných lidí. AI tomu hodně pomohla.
3. **Která z forem e-mailového podvodu je v současnosti podle vás pro oběti nejnebezpečnější a proč?**
    - Největší průšvih je teď BEC. Tam lítají miliony, protože pachatel trefí firmu v citlivým momentu a přesvědčí účetní, že má poslat prachy „šéfovi“ nebo „dodavateli“.
4. **Setkáváte se s případy, kdy pachatelé využívají data vytěžená z veřejných rejstříků nebo sociálních sítí k cíleným útokům (tzv. spear-phishing)?**
    - Jo, spear-phishing je dneska standard. Pachatel si tě prolustruje na LinkedInu, Facebooku, z rejstříků, pak ti napíše mail, co sedí jak ***** na hrnec.
5. **Jaké psychologické spouštěče (strach, autorita, časový tlak) jsou u vámi řešených případů nejčastější a nejúčinnější?**
    - Nejvíc funguje kombinace: strach + časovej tlak + autorita. Typicky „okamžitě zaplať, jinak průser“. Lidi pak nepřemýšlí.
6. **Jaká je typická profilace oběti u Romance Scams oproti útokům typu BEC na firmy?**
    - Romance scam? Často osamělí lidi, někdy starší, někdy prostě někdo, kdo hledá vztah. BEC? Tam je to spíš o roli, účetní, finanční manažeři, lidi, co mají přístup k penězům.
7. **Do jaké míry hraje roli v úspěšnosti podvodu "digitální negramotnost" versus momentální psychické rozpoložení oběti?**
    - Není to jen o „digitální negramotnosti“. Upřímně – nachytají se i chytrý lidi. Hodně dělá momentální stav – stres, únava, tlak v práci.

8. **Jaká je nejčastější chyba poškozených při zajišťování důkazů před nahlášením činu (např. přeposílání e-mailů)?**
    - Největší klasika? Přepošlou mail špatně, místo jako přílohu ho pošlou dál normálně a zničí hlavičky. Nebo smažou komunikaci.
9. **Jak hodnotíte využitelnost metadat z hlaviček e-mailů při identifikaci pachatele v praxi?**
    - Hlavičky jsou fajn, ale v praxi často slepá ulička. Pachatel jede přes několik serverů, VPN, spoofing, spíš vodítko než důkaz.
10. **Jaké technické překážky (VPN, TOR, šifrovaní typu ProtonMail) jsou pro vás při zajišťování stop nejvíce limitující?**
    - VPN, TOR, šifrovaný služby typu ProtonMail, to je pro nás peklo. Bez spolupráce ze zahraničí jsme často nahraný.
11. **Jak efektivní je v praxi využívání institutu podle § 7b trestního řádu u tuzemských poskytovatelů?**
    - U českých poskytovatelů to funguje docela dobře a rychle. Problém je, že většina těch služeb je mimo ČR.
12. **Jaké jsou nejčastější kanály pro vyvádění finančních prostředků (kryptoměny, zahraniční účty, dárkové karty)?**
    - Nejčastěji jsou to zahraniční účty, pak rychlý přeposílání přes několik účtů, a čím dál víc krypto. Dárkový karty už míň, ale furt jsou.
13. **Jaká je úspěšnost blokace peněz, pokud je podvod nahlášen do 24 hodin od transakce?**
    - Když to někdo nahlásí do 24 hodin, tak máme šanci, řekněme klidně 30–50 %, že něco zachráníme. Po pár dnech už je to skoro pryč.
14. **Jak vnímáte roli "bílých koní"? Jde častěji o vědomé komplice, nebo o oběti manipulace?**
    - Půl na půl. Někteří ví přesně, do čeho jdou. Jiní jsou zmanipulovaný – třeba „práce z domova“, a ani netuší, že perou prachy.
15. **Jak hodnotíte rychlost a efektivitu spolupráce skrze Europol (SIENA) a Interpol (I-24/7)?**
    - Europol (SIENA) funguje celkem svižně. Interpol taky, ale záleží na zemi. Někde odpoví rychle, jinde čekáš věčnost.
16. **Jaké jsou největší bariéry při vyřizování žádostí o právní pomoc (MLAT) do zemí mimo EU (např. USA, Nigérie)?**

- MLAT do zemí mimo EU? To je běh na dlouhou trať. Měsíce, někdy roky. A často dostaneš odpověď, když už je to stejně k ničemu.

17. **Pokud byste mohl změnit jeden procesní nebo legislativní krok, co by nejvíce pomohlo zvýšit efektivitu vyšetřování kyberpodvodů?**
    - Kdybych mohl něco změnit? Rychlejší přístup k datům od zahraničních providerů. To by nám zvedlo úspěšnost o desítky procent.
18. **Existují nástroje (software/hardware) pro vyhledávání a analýzu digitálních stop, které vám aktuálně chybí nebo by zasloužily upgrade?**
    - Nástroje máme, ale vždycky je co zlepšovat, hlavně automatizace analýzy dat a lepší propojení databází.
19. **Domníváte se, že by užší integrace analytických nástrojů mezi bankami a policií mohla vést k automatickému zastavování podezřelých plateb v reálném čase?**
    - Jo, tohle by byl gamechanger. Kdyby banky a policie jely víc v reálným čase, spousta plateb by se dala stopnout dřív, než zmizí.
20. **Jakou roli podle vás sehraje v blízké budoucnosti umělá inteligence – bude více pomáhat pachatelům při tvorbě podvodů, nebo policii při jejich odhalování?**
    - Upřímně obě strany. Pachatelé ji už využívají teď. Ale zároveň nám může dost pomoct s analýzou dat a odhalováním vzorců. Bude to takový závod, kdo ji využije líp.

Sepsaný rozhovor – kriminalista 8

1. **Jaký podíl tvoří e-mailové podvody (Scam 419, BEC, Romance Scams) na celkovém objemu kyberkriminality, kterou na vašem pracovišti řešíte?**
    - Pokud vyfiltrujeme čistě útoky na integritu dat, tak sociální inženýrství realizované skrze mailovou komunikaci dominuje. V našem nápadu to představuje stabilně přes 60 % případů. Je to zkrátka vektor útoku s nejlepším poměrem cena/výkon.
2. **Pozorujete v posledních dvou letech výrazný posun v sofistikovanosti útoků (např. kvalita češtiny, využití AI)?**

- Ten technologický skok je nepopíratelný. Integrace LLM (velkých jazykových modelů) do útočných kitů prakticky eliminovala lingvistické bariéry. Dnešní phishingové kampaně mají syntaxi i lexiku na úrovni rodilého mluvčího, což výrazně zvyšuje úspěšnost konverze u obětí.

3. **Která z forem e-mailového podvodu je v současnosti podle vás pro oběti nejnebezpečnější a proč?**
    - Z hlediska systémového rizika pro korporátní sféru je to jednoznačně BEC, kde dochází k masivním transferům kapitálu. Nicméně v rovině individuálního dopadu jsou nejvíce destruktivní Romance Scams, protože tam dochází k dlouhodobé emoční exploataci a totální finanční likvidaci fyzické osoby.
4. **Setkáváte se s případy, kdy pachatelé využívají data vytěžená z veřejných rejstříků nebo sociálních sítí k cíleným útokům (tzv. spear-phishing)?**
    - Naprosto standardně. Fáze rekognoskace (průzkumu) je u BEC útoků klíčová. Útočníci korelují data z LinkedInu, výročních zpráv a registru plátců DPH, aby vytvořili dokonale cílený scénář pro konkrétního zaměstnance.
5. **Jaké psychologické spouštěče (strach, autorita, časový tlak) jsou u vámi řešených případů nejčastější a nejúčinnější?**
    - Je to klasická exploatace časové tísně a hierarchického uspořádání. Pachatel simuluje krizovou situaci, která vyžaduje okamžitou akci, čímž u oběti vyřadí racionální kontrolní mechanismy a vynutí si reaktivní chování.
6. **Jaká je typická profilace oběti u Romance Scams oproti útokům typu BEC na firmy?**
    - U Romance Scams cílí predátoři na osoby v sociální deprivaci. U BEC jsou cílem "high-performers" – lidé orientovaní na výkon a plnění úkolů, kteří v dobré víře akceptují pokyn domnělé autority, aby nezdržovali provoz.
7. **Do jaké míry hraje roli v úspěšnosti podvodu "digitální negramotnost" versus momentální psychické rozpoložení oběti?**
    - Technické znalosti jsou v těchto scénářích podružné. Útoky jsou navrženy tak, aby bypassovaly kognitivní filtry. Pokud je subjekt v

afektu nebo pod extrémní únavou, i zkušený administrátor může provést neautorizovanou operaci nebo kliknout na infikované URL.

8. **Jaká je nejčastější chyba poškozených při zajišťování důkazů před nahlášením činu (např. přeposílání e-mailů)?**
    - Kritickou chybou je neprofesionální manipulace s daty, konkrétně prosté přeposlání zprávy (Forward). Tím dochází k destrukci hlaviček a ztrátě kontinuity digitální stopy. Pro validní forenzní analýzu a zajištění dle metodiky kpt. Bačkovského (NCOZ) je nutné exportovat zprávu v nativním formátu včetně všech SMTP hlaviček.
9. **Jak hodnotíte využitelnost metadat z hlaviček e-mailů při identifikaci pachatele v praxi?**
    - Je to pro nás primární datový zdroj. Pokud je hlavička autentická, poskytuje nám informace o odesílacích MX serverech, X-originačních IP adresách a časových razítkách, což je nezbytný podklad pro následné trasování.
10. **Jaké technické překážky (VPN, TOR, šifrovaní typu ProtonMail) jsou pro vás při zajišťování stop nejvíce limitující?**
    - Největší bariérou jsou "no-log" politiky zahraničních VPN providerů a end-to-end šifrování platforem typu Proton. Pokud proces skončí v jurisdikci, která nereflektuje žádosti o součinnost, stává se stopa fakticky nesledovatelnou.
11. **Jak efektivní je v praxi využívání institutu podle § 7b trestního řádu u tuzemských poskytovatelů?**
    - Vnitrostátní kooperace je na velmi vysoké úrovni. § 7b je efektivní nástroj pro retenci dat u českých subjektů. Limitace nastává v momentě, kdy je infrastruktura hostována u globálních hráčů mimo dosah českých procesních norem.
12. **Jaké jsou nejčastější kanály pro vyvádění finančních prostředků (kryptoměny, zahraniční účty, dárkové karty)?**
    - Trendem je blesková konverze FIAT měny na kryptoaktivita. Prostřednictvím sítě bílých koní se prostředky fragmentují a následně "perou" skrze mixery nebo burzy bez KYC politiky, což extrémně komplikuje asset recovery.

13. **Jaká je úspěšnost blokace peněz, pokud je podvod nahlášen do 24 hodin od transakce?**
    - Ten limit 24 hodin je naprosto zásadní. V rámci tohoto okna je pravděpodobnost úspěšné intervence a zajištění prostředků v bankovním sektoru relativně vysoká. Po uplynutí této doby se šance na reálné zajištění blíží nule.
14. **Jak vnímáte roli "bílých koní"? Jde častěji o vědomé komplice, nebo o oběti manipulace?**
    - Spektrum je široké. Od vědomých aktérů v kriminálním řetězci až po "money mules" rekrutované pod záminkou legálního home-office. U Romance Scams dochází k tragickému paradoxu, kdy se primární oběť stává nevědomým bílým koněm pro další útoky.
15. **Jak hodnotíte rychlost a efektivitu spolupráce skrze Europol (SIENA) a Interpol (I-24/7)?**
    - Platforma SIENA představuje standard pro bezpečnou a relativně rychlou operativní komunikaci v EU. Interpol plní roli spíše v globálním měřítku, ale jeho procesy jsou pro dynamiku kyberprostoru často příliš rigidní.
16. **Jaké jsou největší bariéry při vyřizování žádostí o právní pomoc (MLAT) do zemí mimo EU (např. USA, Nigérie)?**
    - Největší překážkou je temporální diskrepance – doba vyřízení žádosti neodpovídá době expirace digitálních záznamů (logů). Než dojde k vyřízení právní pomoci, relevantní data u poskytovatele často již neexistují.
17. **Pokud byste mohl změnit jeden procesní nebo legislativní krok, co by nejvíce pomohlo zvýšit efektivitu vyšetřování kyberpodvodů?**
    - Implementace institutu okamžitého zmrazení finančních operací ze strany policie bez nutnosti předchozího soudního schválení v urgentních případech, kdy hrozí bezprostřední odliv prostředků do zahraničí.
18. **Existují nástroje (software/hardware) pro vyhledávání a analýzu digitálních stop, které vám aktuálně chybí nebo by zasloužily upgrade?**
    - Potřebujeme robustnější analytické platformy pro automatizovanou korelaci Big Data a pokročilé nástroje pro forenzní analýzu blockchainových transakcí v reálném čase.

19. **Domníváte se, že by užší integrace analytických nástrojů mezi bankami a policií mohla vést k automatickému zastavování podezřelých plateb v reálném čase?**
    - Jednoznačně. Synergie mezi detekčními systémy bank a policejními databázemi je jediný způsob, jak efektivně eliminovat škody v době, kdy útoky probíhají v řádech milisekund.
20. **Jakou roli podle vás sehraje v blízké budoucnosti umělá inteligence – bude více pomáhat pachatelům při tvorbě podvodů, nebo policii při jejich odhalování?**
    - AI bude asymetrickou zbraní. V rukou útočníků slouží k automatizaci a personalizaci útoků. Naší jedinou šancí je integrace AI do defenzivních mechanismů a analytiky, aby bylo možné včas detekovat vzorce chování útočníků v globálním měřítku.

Sepsaný rozhovor – kriminalista 9

1. **Jaký podíl tvoří e-mailové podvody (Scam 419, BEC, Romance Scams) na celkovém objemu kyberkriminality, kterou na vašem pracovišti řešíte?**
    - Pokud se podíváme na přeshraniční kriminalitu, tak tyhle typy podvodů dominují. Odhadem tvoří kolem 65 % naší agendy. E-mail je pro pachatele z druhého konce světa pořád ta nejlevnější vstupenka k cizím penězům.
2. **Pozorujete v posledních dvou letech výrazný posun v sofistikovanosti útoků (např. kvalita češtiny, využití AI)?**
    - Je to neuvěřitelný skok. Dřív jsme se těm překladům smáli, dneska už není čemu. Útočníci masivně využívají automatizované nástroje pro úpravu textu, takže ty zprávy jsou gramaticky čisté a stylisticky naprosto přirozené. Bariéra jazyka padla.
3. **Která z forem e-mailového podvodu je v současnosti podle vás pro oběti nejnebezpečnější a proč?**
    - Z pohledu celkového objemu odcizených peněz je to BEC, tam ty rány bolí ekonomiku nejvíc. Ale lidsky jsou nejtragičtější Romance Scams. Ty oběti jsou v takovém emociálním zajetí, že s námi často odmítají spolupracovat, protože věří té iluzi víc než realitě.
4. **Setkáváte se s případy, kdy pachatelé využívají data vytěžená z veřejných rejstříků nebo sociálních sítí k cíleným útokům (tzv. spear-phishing)?**
    - Prakticky neustále. OSINT (průzkum z otevřených zdrojů) je pro ně klíčový. Vytěží LinkedIn, aby znali jména, a obchodní rejstřík, aby věděli, kdo podepisuje smlouvy. Pak posílají maily, které vypadají jako legitimní vnitrofiremní komunikace.
5. **Jaké psychologické spouštěče (strach, autorita, časový tlak) jsou u vámi řešených případů nejčastější a nejúčinnější?**
    - Je to ta klasická smyčka, uměle vytvořený stres a autoritativní vystupování. Když vám napíše "ředitel", že je potřeba zaplatit fakturu hned, jinak padne kontrakt, většina lidí prostě vypne kritické myšlení a jedná reaktivně.
6. **Jaká je typická profilace oběti u Romance Scams oproti útokům typu BEC na firmy?**
    - U těch vztahových věcí jsou to většinou lidé v citovém vakuu, kteří hledají uznání. U firemních podvodů jsou oběťmi svědomití lidé, kteří se

prostě jen snaží vyjít vstříc svému nadřízenému a nezdržovat procesy ve firmě.

7. **Do jaké míry hraje roli v úspěšnosti podvodu "digitální negramotnost" versus momentální psychické rozpoložení oběti?**
    - Technické znalosti jsou v těchto případech druhořadé. Útočníci cílí na emoce. Máme případy, kdy naletěli vysokoškolští profesoři, protože je pachatel zastihl v momentě velké únavy nebo osobního neštěstí. Emoce vždycky přebijí logiku.
8. **Jaká je nejčastější chyba poškozených při zajišťování důkazů před nahlášením činu (např. přeposílání e-mailů)?**
    - Bohužel je to to laické přeposlání zprávy. Tím se nevratně přepíše celá řada technických údajů. My pro řádné elektronické zajištění podle metodiky kpt. Bačkovského z NCOZ potřebujeme ten e-mail v jeho surové podobě jako soubor, abychom mohli analyzovat originální hlavičky.
9. **Jak hodnotíte využitelnost metadat z hlaviček e-mailů při identifikaci pachatele v praxi?**
    - Bez metadat jsme v podstatě slepí. Jsou to digitální otisky, které nám ukazují trasu zprávy přes poštovní servery. Pokud je máme, můžeme začít legálně žádat o informace o IP adresách v zahraničí.
10. **Jaké technické překážky (VPN, TOR, šifrovaní typu ProtonMail) jsou pro vás při zajišťování stop nejvíce limitující?**
    - Nejhorší jsou služby v jurisdikcích, které absolutně nereagují na mezinárodní dožádání. Jakmile stopa skončí u šifrovaného mailu nebo VPN providera v zemi bez právní pomoci, šance na odhalení identity pachatele se blíží nule.
11. **Jak efektivní je v praxi využívání institutu podle § 7b trestního řádu u tuzemských poskytovatelů?**
    - V rámci Česka to funguje velmi pružně. Tuzemští poskytovatelé jsou na tyto postupy zvyklí a data "zmrazí" na výzvu rychle. Problémem je ale fakt, že většina infrastruktury podvodníků leží mimo naše území.
12. **Jaké jsou nejčastější kanály pro vyvádění finančních prostředků (kryptoměny, zahraniční účty, dárkové karty)?**

- Momentálně hrají prim kryptoměny. Peníze se bleskově proženou přes řetězec účtů bílých koní a skončí v Bitcoinu. Trasování takových toků přes anonymní burzy v zahraničí je pak extrémně komplikované.

13. **Jaká je úspěšnost blokace peněz, pokud je podvod nahlášen do 24 hodin od transakce?**
    - Prvních 24 hodin je kritický limit. Pokud poškozený zareaguje okamžitě, šance na stopnutí platby v bankovním systému je poměrně vysoká. Po uplynutí této doby peníze většinou nenávratně zmizí v cizině nebo v kryptu.
14. **Jak vnímáte roli "bílých koní"? Jde častěji o vědomé komplice, nebo o oběti manipulace?**
    - Je to různorodé. Máme tu lidi, co to dělají vědomě pro provizi, ale i spoustu nešťastníků, kteří věří, že dělají legální práci pro zahraniční firmu. U Romance Scams je tragické, když pachatel do role bílého koně vmanévruje samotnou oběť.
15. **Jak hodnotíte rychlost a efektivitu spolupráce skrze Europol (SIENA) a Interpol (I-24/7)?**
    - Europol a jejich kanál SIENA je v rámci Evropy špičkový a velmi rychlý. Interpol je užitečný pro globální zatykače, ale u digitálních stop, kde rozhodují hodiny, je ten systém někdy až příliš byrokratický.
16. **Jaké jsou největší bariéry při vyřizování žádostí o právní pomoc (MLAT) do zemí mimo EU (např. USA, Nigérie)?**
    - Rozhodně časový faktor. Vyřízení dožádání mimo EU trvá měsíce, někdy i roky. V digitálním prostředí je to nepoužitelný systém – než přijde odpověď, data na serverech jsou dávno přemazaná.
17. **Pokud byste mohl změnit jeden procesní nebo legislativní krok, co by nejvíce pomohlo zvýšit efektivitu vyšetřování kyberpodvodů?**
    - Rozhodně možnost operativního zmrazení bankovních transakcí policií bez nutnosti čekat na formální souhlasy v prvních hodinách po nahlášení. Časová prodleva hraje pachateli do karet.
18. **Existují nástroje (software/hardware) pro vyhledávání a analýzu digitálních stop, které vám aktuálně chybí nebo by zasloužily upgrade?**

- Potřebovali bychom lepší analytické nástroje na korelaci mezinárodních dat a modernější software pro trasování transakcí v oblasti kryptoměn v reálném čase.

19. **Domníváte se, že by užší integrace analytických nástrojů mezi bankami a policií mohla vést k automatickému zastavování podezřelých plateb v reálném čase?**
    - Jednoznačně. Propojení bankovních algoritmů s našimi informacemi o nahlášených útocích je jedinou cestou, jak ty miliony zachránit ještě předtím, než odtečou do ciziny.
20. **Jakou roli podle vás sehraje v blízké budoucnosti umělá inteligence – bude více pomáhat pachatelům při tvorbě podvodů, nebo policii při jejich odhalování?**
    - Bude to technologický souboj. Pachatelé AI využívají k automatizaci útoků, my ji musíme začít využívat k jejich masové analýze a propojování jednotlivých případů. Kdo zaspí, ten prohraje.

Sepsaný rozhovor – kriminalista 10

1. **Jaký podíl tvoří e-mailové podvody (Scam 419, BEC, Romance Scams) na celkovém objemu kyberkriminality, kterou na vašem pracovišti řešíte?**
    - Když to vezmu podle našich spisů, tak e-mailový podvody jsou tak čtvrtina až třetina. Není to všechno, ale rozhodně to zabírá dost kapacity.
2. **Pozorujete v posledních dvou letech výrazný posun v sofistikovanosti útoků (např. kvalita češtiny, využití AI)?**
    - Posun tam je, ale neřekl bych, že všude. Pořád chodí i úplně primitivní věci. Ale když narazíš na „lepší kus“, tak to fakt vypadá věrohodně – hlavně ty cílený útoky.
3. **Která z forem e-mailového podvodu je v současnosti podle vás pro oběti nejnebezpečnější a proč?**
    - Za mě romance scam. Ne kvůli částkám, ale kvůli dopadu na lidi. Ty lidi přijdou nejen o peníze, ale často i o iluze a psychicky je to semele.
4. **Setkáváte se s případy, kdy pachatelé využívají data vytěžená z veřejných rejstříků nebo sociálních sítí k cíleným útokům (tzv. spear-phishing)?**
    - Jo, a čím dál víc. Dřív to byl spíš náhodný rozstřel, dneska si tě vytipujou. Někdy ví o oběti víc než vlastní kolegové.
5. **Jaké psychologické spouštěče (strach, autorita, časový tlak) jsou u vámi řešených případů nejčastější a nejúčinnější?**
    - Nejvíc zabírá důvěra. Oni si ji vybudujou, a pak stačí malej impuls. Strach a tlak tam jsou, ale bez tý důvěry by to nefungovalo.
6. **Jaká je typická profilace oběti u Romance Scams oproti útokům typu BEC na firmy?**
    - Romance scam, jsou to často lidi, co jsou v nějaký životní fázi, kdy hledají blízkost. BEC? Tam je to spíš o systému, kdy někdo jen udělá chybu v procesu.
7. **Do jaké míry hraje roli v úspěšnosti podvodu "digitální negramotnost" versus momentální psychické rozpoložení oběti?**
    - Digitální negramotnost hraje roli, ale není to rozhodující. Viděl jsem vysokoškoláky, co naletěli. Spíš jde o to, jestli člověk zrovna „vypne“.
8. **Jaká je nejčastější chyba poškozených při zajišťování důkazů před nahlášením činu (např. přeposílání e-mailů)?**

- Lidi často začnou sami „vyšetřovat“. Klikají na odkazy, odepisují, snaží se něco zjistit a tím to ještě zhorší.

9. **Jak hodnotíte využitelnost metadat z hlaviček e-mailů při identifikaci pachatele v praxi?**
    - Upřímně asi tak v 90 % případů nic moc. Použitelný to je spíš u amatérů.
10. **Jaké technické překážky (VPN, TOR, šifrovaní typu ProtonMail) jsou pro vás při zajišťování stop nejvíce limitující?**
    - Největší problém je kombinace všeho, při spojení anonymizační služby + zahraničí. Jedna věc by se dala řešit, ale dohromady je to problém.
11. **Jak efektivní je v praxi využívání institutu podle § 7b trestního řádu u tuzemských poskytovatelů?**
    - U nás to jde, ale jsme limitovaný hranicema. Jakmile to jde ven, zpomalí se to.
12. **Jaké jsou nejčastější kanály pro vyvádění finančních prostředků (kryptoměny, zahraniční účty, dárkové karty)?**
    - Pořád jedou klasický bankovní převody. Krypto roste, ale není to ve všech případech. Pachatelé používají to, co je zrovna nejjednodušší.
13. **Jaká je úspěšnost blokace peněz, pokud je podvod nahlášen do 24 hodin od transakce?**
    - Do 24 hodin je to ideální, ale realita? Lidi přijdou třeba až za tři dny. Když přijdou včas, šance je slušná, ale nikdy jistota.
14. **Jak vnímáte roli "bílých koní"? Jde častěji o vědomé komplice, nebo o oběti manipulace?**
    - Spíš oběti než komplici. Často si myslí, že dělají normální práci. Ale samozřejmě jsou i tací, co to dělají vědomě.
15. **Jak hodnotíte rychlost a efektivitu spolupráce skrze Europol (SIENA) a Interpol (I-24/7)?**
    - Europol je fajn, tam to má nějakou úroveň. Ale pořád to není tak rychlý, jak bychom potřebovali.
16. **Jaké jsou největší bariéry při vyřizování žádostí o právní pomoc (MLAT) do zemí mimo EU (např. USA, Nigérie)?**
    - Největší problém je legislativa a rozdílný přístupy. Každá země to řeší jinak a my se tomu musíme přizpůsobit.

17. **Pokud byste mohl změnit jeden procesní nebo legislativní krok, co by nejvíce pomohlo zvýšit efektivitu vyšetřování kyberpodvodů?**
    - Méně papírování, víc operativy. Někdy nás víc brzdí administrativa než samotný pachatel.
18. **Existují nástroje (software/hardware) pro vyhledávání a analýzu digitálních stop, které vám aktuálně chybí nebo by zasloužily upgrade?**
    - Ne že by něco úplně chybělo, ale spíš bych uvítal lepší školení a víc lidí, co s tím umí dělat.
19. **Domníváte se, že by užší integrace analytických nástrojů mezi bankami a policií mohla vést k automatickému zastavování podezřelých plateb v reálném čase?**
    - Určitě by to pomohlo, ale musí se to udělat citlivě. Jakmile do toho zatáhneš automatiku, nese to i riziko chyb.
20. **Jakou roli podle vás sehraje v blízké budoucnosti umělá inteligence – bude více pomáhat pachatelům při tvorbě podvodů, nebo policii při jejich odhalování?**
    - AI bude nástroj. Nic víc. Kdo ji bude umět líp použít, ten bude mít navrch a zatím mi přijde, že pachatelé jsou v tomhle docela napřed.