POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra kriminální policie

Podvodné útoky v informačních a komunikačních technologiích

Bakalářská práce

Fraudulent attacks in information and communication technologies

Bachelor thesis

VEDOUCÍ PRÁCE
plk. v. v. Mgr. Vlastimil Fiedler

AUTOR PRÁCE
Magdaléna Fraňková

PRAHA
2024

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracovala samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpala, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Horoměřicích, dne 12. 3. 2024

Magdaléna Fraňková

Poděkování

Mé poděkování patří mému vedoucímu práce plk. v. v. Mgr. Vlastimilu Fiedlerovi za jeho odborné a svědomité vedení, vždy rychlou pomoc a vstřícný přístup. Dále bych chtěla poděkovat soudnímu znalci v IT Radku Benešovi MSc. a pplk. Mgr. Ondřeji Kaprovi z Policejního prezidia České republiky za poskytnutí podkladů a rozhovorů pro tuto bakalářskou práci.

ANOTACE

Tato bakalářská práce se zabývá podvodnými útoky v informačních a komunikačních technologiích, přičemž se podrobně věnuje problematice phishingových útoků. Zasazuje phishingové útoky do kontextu kybernetické kriminality a vyzdvihuje naléhavost tohoto tématu. V práci je představena řada způsobů spáchání tohoto typu útoku, včetně těch nejaktuálnějších. Phishingové útoky jsou následně zařazeny do trestněprávní roviny. Část práce je věnována policejní činnosti související s objasňováním phishingových útoků, tedy nástrojům a postupům použitým při jejich objasňování s důrazem na faktory, které objasňování znesnadňují. Závěr práce je zaměřen na prevenci těchto útoků, jak z pohledu hardwarové a softwarové ochrany, tak v oblasti lidského faktoru.

KLÍČOVÁ SLOVA

kyberprostor * kyberkriminalita * podvodné útoky v informačních a komunikačních technologiích * investiční podvody * phishingové útoky * sociální inženýrství * malware * podvod * objasňování * prevence

ANNOTATION

This bachelor thesis deals with fraudulent attacks in information and communication technologies, with a detailed focus on phishing attacks. It places phishing attacks in the context of cybercrime and highlights the urgency of this topic. The thesis presents a number of ways of perpetrating this type of attack, including the most recent ones. Phishing attacks are then placed in the criminal law context. Part of the thesis is devoted to law enforcement activities related to the clarification of phishing attacks, i.e. the tools and procedures used in their clarification, with an emphasis on the factors that make the clarification difficult. The thesis concludes with a focus on the prevention of these attacks, both in terms of hardware and software protection and the human factor.

KEYWORDS

cyberspace * cybercrime * fraudulent attacks in information and communication technologies * investment fraud * phishing attacks * social engineering * malware * fraud * detection * prevention

Obsah

Úvod

V dnešní době představují informační a komunikační technologie prvek, který se stal součástí každodenního života většiny z nás. Otevřel nám dveře do prostor, kam bychom se bez něj možná nikdy nepodívali, poskytl nám nekonečně se rozpínající množství informací, jejichž tok se neustále zrychluje, umožnil nám stát se součástí nového, virtuálního světa.

Rychle expandující virtuální prostor však přináší i nové výzvy, které zastihly společnost nepřipravenou. Stejně tak rychle, jak začal člověk těchto technologií využívat, začal tyto technologie také zneužívat. Anonymita, globálnost a dynamika virtuálního prostoru vytvořila vhodné prostředí pro páchání kriminality.

V roce 2022 tvořila kyberkriminalita v České republice (dále jen ČR) 10,2 % celkové registrované kriminality,[1] přičemž kybernetická kriminalita představuje jeden z nejvíce latentních druhů kriminality vůbec. Odhady hodnot latence zde přesahují 90 %. Celková škoda napáchaná kybernetickou kriminalitou představuje přibližně 290 miliard EUR každý rok na celém světě, což pro pachatele představuje větší zisk než celosvětové výnosy z obchodu s marihuanou, kokainem a heroinem dohromady.[2]

Současně nejrozšířenější[3] a jednou z nejefektivnějších[4] forem kyberkriminality jsou podvodné útoky v informačních a komunikačních technologiích, které neútočí pouze na technologie jako takové, ale jejich prostřednictvím i na člověka samotného. Docílí toho efektivním spojením technologií se sociálním inženýrstvím útočícím na lidskou psychiku, která tvoří ten nejslabší článek ochrany.

---

1 Vývoj registrované kriminality v roce 2022. Online. In: Policie České republiky. 2023. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx. [cit. 2023-10-31].
2 Rozvoj Policie České republiky v letech 2016-2020. Online. In: ČT 24. 2015. Dostupné z: https://ct24.ceskatelevize.cz/sites/default/files/1757756-policie-i-1.pdf. [cit. 2024-02-18].
3 Kyberkriminalita. Online. In: Policie České republiky. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx. [cit. 2023-10-22].
4 DESOLDA, Giuseppe, et al. Human factors in phishing attacks: a systematic literature review. Online. ACM Computing Surveys (CSUR). 2021, roč. 54, čís. 8. ISSN 0360-0300. Dostupné z: https://www. researchgate.net/profile/Giuseppe-Desolda/publication/361609220_Human_Factors_in_Phishing_Attacks_A_Systematic_Literature_Review/links/62bc31eaf9dee438e8cbae70/Human-Factors-in-Phishing-Attacks-A-Systematic-Literature-Review.pdf. [cit. 2024-02-06].

Cílem této práce je vytvořit ucelený přehled podvodných útoků v informačních a komunikačních technologiích, se zaměřením na ten nejrozšířenější z nich, phishing. Jejím smyslem je zdůraznit jejich důležitost a aktuálnost v kontextu současné kybernetické kriminality a představit současné hrozby tak, aby bylo možné navrhnout strategie pro jejich prevenci. Práce se zaměřuje konkrétně na analýzu nejnovějších modu operandi, zasazení těchto útoků do trestněprávní roviny a diskuzi o výzvách v oblasti objasňování tohoto druhu kybernetické kriminality.

Metodika práce je navržena tak, aby byla schopna co nejefektivněji zpracovat danou problematiku. Analyticko-syntetická metoda hraje klíčovou roli v získávání poznatků a vytváření uceleného pohledu na problematiku, kdy systematicky analyzuje různé aspekty podvodných útoků a následně tyto poznatky syntetizuje do komplexního rámce analýzy. Komparativní metoda je důležitá pro porovnání různých modus operandi phishingových útoků a identifikaci jejich podobností a rozdílů, což umožňuje odhalovat vzory a trendy v chování útočníků. V neposlední řadě je v práci využita metoda výkladu právních norem, které by mohly být užity pro trestněprávní kvalifikaci phishingových útoků, což umožňuje porozumět právním aspektům problematiky phishingu a identifikovat možnosti trestněprávního postihu těchto útoků.

Zdrojem ke sběru dat pro tuto práci byly nejen analýzy české a zahraniční literatury, ale také konzultace s odborníky na poli kybernetické bezpečnosti, včetně soudního znalce v IT Radka Beneše MSc. a pplk. Mgr. Ondřeje Kapra z Policejního prezidia České republiky, jehož odpovědi na dotazy položené v rámci rozhovoru jsou v práci citovány.

1 Úvod do terminologie informačních a komunikačních technologií

Ke správnému porozumění tématu podvodných útoků v informačních a komunikačních technologiích je zapotřebí se nejprve seznámit s terminologií informačních a komunikačních technologií samotných. V následující kapitole budou tedy představeny základní pojmy klíčové pro porozumění dané problematice a zasazení těchto podvodných útoků do kontextu kybernetické kriminality.

Problematika názvosloví je v oboru informačních a komunikačních technologií velmi různorodá, i přesto že v posledních letech panuje snaha odbornou terminologii v tomto oboru sjednotit a aplikovat do českého prostředí.[5] Z tohoto důvodu nelze v této práci postihnout tuto terminologii v plné šíři, ačkoli každý z těchto pojmů bude definován několika způsoby tak, aby byl v rámci rozsahu a pro potřebu této práce popsán co nejpřesněji.

1.1 Kyberprostor

Pojem kyberprostor je možné definovat mnoha způsoby. Kolouch vychází v jedné ze svých definic z hmotné podstaty internetu, kterou z technického hlediska definuje jako *„celosvětovou distribuovanou počítačovou síť složenou z jednotlivých menších sítí, které jsou navzájem spojeny pomocí protokolů IP a tím je umožněna komunikace, přenos dat, informací a poskytování služeb mezi subjekty navzájem.“*[6] Uvádí, že právě tímto způsobem vzniká kyberprostor, virtuální prostor vázaný na materiální podstatě.[7] Legální definici kyberprostoru je možno nalézt v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti, kde se v § 2 odst. 1, písm. a) definuje kybernetický prostor jako *„digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami*

[5] SEDLÁK, Petr; KONEČNÝ, Martin a kol. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. 1. vyd. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2. s. 12
[6] KOLOUCH, Jan. CyberCrime. 1. vyd. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7. s. 43
[7] Tamtéž

a sítěmi elektronických komunikací.“[8] Policie ČR označuje kyberprostor za „*virtuální prostředí, které nemá začátek a ani konec, nezná hranice národních států a nelze určit, jak rozsáhlý je*.“[9]

1.2 Kyberkriminalita

Ze všech výše uvedených definic kyberprostoru lze vyvodit jeho specifické znaky, tedy jeho rozpínavost, decentralizaci a globálnost.[10] Takové prostředí skýtá příznivé podmínky pro páchání kriminality. Kriminalita v kyberprostoru se nazývá kyberkriminalita, dříve také kriminalita počítačová. Tento termín však dnes dostatečně nepostihuje široké množství nových technologií, které kyberprostor vytváří a skrze které je kyberkriminalita páchána. Policie ČR definuje kyberkriminalitu jako trestnou činnost, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí.[11] Pro úplnost je třeba dodat, že za kyberkriminalitu bývá obecně považováno: a) jednání namířené proti informačním a komunikačním technologiím jako takovým a b) jednání, při němž je výraznou měrou užito informačních a komunikačních technologií jako nástroje pro spáchání trestného činu.[12]

1.2.1 Vývoj kyberkriminality

S rozvojem informačních a komunikačních technologií roste i kyberkriminalita. Je tedy zapotřebí vývoj kyberkriminality sledovat a účinně proti ní působit, jak preventivně, tak represivně. Vzhledem k povaze této práce je vhodné poukázat na vývoj kyberkriminality a vystihnout tak důležitost a naléhavost tohoto tématu. Pro účely této práce bude přitom využito výhradně statistik policejních.

---

[8] Zákon č. 181/2014 Sb., *o kybernetické bezpečnosti* v posledním znění
[9] *Kyberkriminalita*. Online. In: Policie České republiky. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx. [cit. 2023-10-22].
[10] KOLOUCH, Jan; BAŠTA, Pavel a kol. *CyberSecurity*. 1. vyd. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.s. 36
[11] *Kyberkriminalita*. Online. In: Policie České republiky. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx. [cit. 2023-10-22].
[12] KOLOUCH, Jan. *CyberCrime*. 1. vyd. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7. s. 83

Statistické vykazování kriminality páchané v kyberprostoru Policie ČR vychází z výše uvedené definice kyberkriminality. Kapr k policejním statistikám kyberkriminality v rozhovoru uvedl:

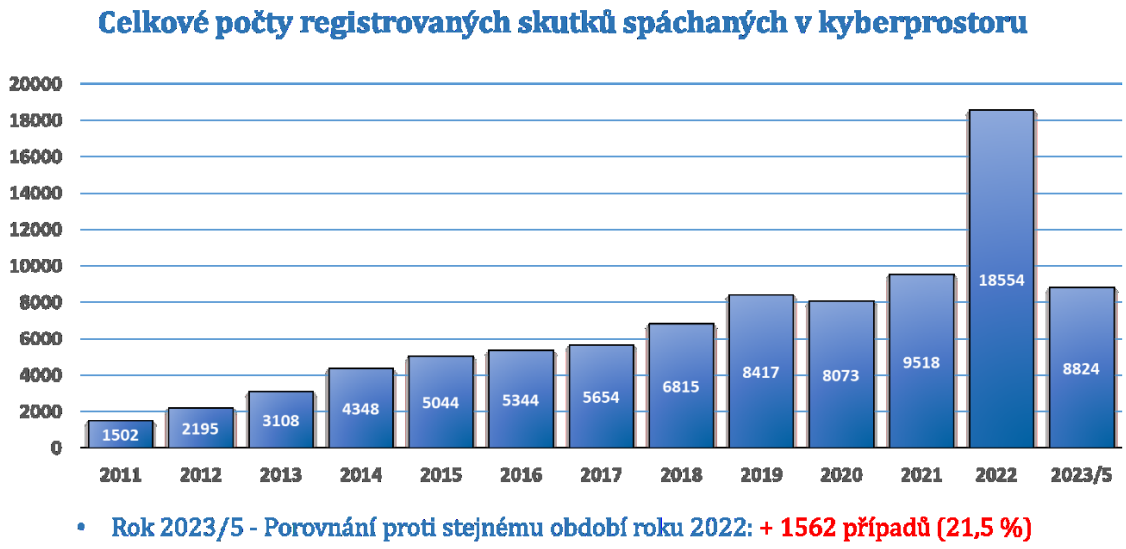
„Policie České republiky nevede přesnou statistiku zaznamenaných typů útoků. Statistiku vedeme pouze ve smyslu kategorizace do jedné skupiny, a to je sledovaná událost IT kriminalita, kam lze zařadit, jak kybernetickou kriminalitu, tak tak zvanou ostatní kriminalitu páchanou v kyberprostoru. Kybernetická kriminalita je kriminalita, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí, kdy hlavním objektem útoku je samotná oblast informačních a komunikačních technologií a v nich obsažená data. Ostatní kriminalita páchaná v kyberprostoru je kriminalita páchaná za výrazného využití informačních a komunikačních technologií, přičemž hlavním objektem útoku je zejména život, zdraví, majetek, svoboda, lidská důstojnost a mravnost. V některých případech však vedeme statistiky přesné, a to u konkrétně sledovaných detekovaných sérií.“

Počet trestných činů spáchaných v kyberprostoru sleduje Policie ČR od roku 2011, přičemž od této doby trend kriminality v kyberprostoru stále roste.[13] V roce 2011 bylo zaznamenáno 1502 trestných činů spadajících pod kriminalitu v kyberprostoru a v roce 2022 jejich počet vzrostl na 18554 viz graf 1.

Z grafu vyplývá, že je zde poměrně dlouhodobý, rostoucí trend této registrované trestné činnosti, což potvrzuje předpoklad, že se určité formy trestné činnosti začínají postupně přesouvat do kyberprostoru. V roce 2022 tvořila kyberkriminalita 10,2 % celkové registrované kriminality.[14] Tradičně nejpočetnější skupinou kriminality páchané v kyberprostoru jsou různá podvodná jednání, která tvoří zpravidla více než polovinu registrovaných skutků.[15]

---

[13] *Kyberkriminalita*. Online. In: Policie České republiky. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx. [cit. 2023-10-22].
[14] *Vývoj registrované kriminality v roce 2022*. Online. In: Policie České republiky. 2023. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx. [cit. 2023-10-31].
[15] *Kyberkriminalita*. Online. In: Policie České republiky. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx. [cit. 2023-10-22].



Graf 1 - Grafické znázornění celkového počtu registrovaných skutků spáchaných v kyberprostoru[16]

[16] Graf poskytnut Kaprem v rámci rozhovoru.

2 Podvodné útoky v informačních a komunikačních technologiích

Kybernetický útok lze dle Koloucha definovat jako „*jakékoli protiprávní jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby*.“[17] Důležitým faktorem pro posouzení (potenciálního) konkrétního kybernetického útoku je, že kybernetický útok nemusí být dokonán, nýbrž stačí, aby byl ve stadiu pokusu či přípravy. Kybernetický útok také nutně nemusí být trestným činem, důležité je, že naruší běžný způsob života útokem napadené osoby. Důvodů, proč není každý kybernetický útok trestným činem, je více. Jedním z nich je nepřiléhavost trestněprávních ustanovení na kriminalitu páchanou v kyberprostoru. Dalším může být kvalifikování takových jednání jako správněprávní či občanskoprávní delikty. V neposlední řadě nemusí být taková jednání vůbec právně postižitelná, tedy mohou být považována pouze za jednání nemorální či obecně řečeno nežádoucí. Z druhé strany je ale nutné konstatovat, že každý kybernetický trestný čin je považován za kybernetický útok.[18]

Podvod jako trestný čin je v § 209 odst. 1 zákona č. 40/2009 Sb., trestní zákoník (dále jen trestní zákoník) definován takto: „*Kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou,* …“[19] Pro účely této práce bude v definování jednotlivých druhů podvodných útoků v informačních a komunikačních využíváno této definice podvodu bez ohledu na to, jak by bylo dané jednání posuzováno v konečném výsledku na základě např. výše škody, zda by tedy bylo subsumováno pod konkrétní paragraf trestního zákoníku či by bylo kvalifikováno jako správněprávní či občanskoprávní delikt, případně nebylo jednáním protiprávním, ale pouze škodlivým. Tato definice tedy slouží pouze k charakteristice podvodného jednání jako takového. Trestněprávní rovinou

[17] KOLOUCH, Jan. *CyberCrime*. 1. vyd. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7. s. 55
[18] Tamtéž
[19] Zákon č. 40/2009 Sb., *trestní zákoník* v posledním znění

podvodných útoků v informačních a komunikačních technologiích se zaobírá samostatná kapitola.

Pokud kybernetický útok vykazuje znaky podvodu, jedná se o podvodný útok spáchaný v kyberprostoru, tedy o podvodný útok v informačních a komunikačních technologiích. Mezi takové útoky je možné zařadit např. falešné e-shopy, krádeže internetových účtů či krádeže identit a zneužívání identit na internetu. Specifickým a v poslední době hojně objevovaným útokem je tzv. investiční podvod. Patrně nejznámějším a nejrozšířenějším druhem podvodného útoku v kyberprostoru je phishingový útok.

Vzhledem k mnohosti, rozličné povaze těchto podvodných útoků a kapacitním možnostem této práce není možné obsáhnout podvodné útoky v informačních a komunikačních technologiích jako celek. Tato práce se tedy bude dále blíže zabývat pouze fenoménem podvodných investic a zejména pak útokům phishingovým.

2.1 Investiční podvody

Investiční podvody jsou sofistikované, často velmi dobře a do detailu propracované podvody v kyberprostoru. Ve své podstatě se velmi podobají útokům phishingovým, jež budou podrobně popsány v následujících kapitolách. Dalo by se říci, že od phishingových útoků se liší pouze svým rozsahem a důmyslností.

Stejně jako u phishingových útoků využívají útočníci páchající investiční podvody různé formy manipulace s cílem vylákat od uživatelů citlivé údaje za účelem přístupu do internetového nebo jiného online bankovnictví. Obvykle komunikace s takovým útočníkem začíná tak, že uživatel najde na internetu reklamu, která propaguje výhodné investice zejména do kryptoměn či akcií.[20] Aby tyto reklamy

[20] *Investiční podvody*. Online. In: Air Bank. Dostupné z: https://www.airbank.cz/co-vas-nejvic-zajima/investicni-podvody/. [cit. 2023-11-12].

byly pro uživatele zajímavější a důvěryhodnější, využívají útočníci pro své reklamy již existující známé firmy či osoby viz příloha 1.[21]

Pokud uživatel na tuto reklamu zareaguje (např. vyplněním dotazníku, zadáním kontaktních údajů), ozve se zpravidla telefonicky údajný investiční poradce.[22] Tento poradce uživatele nasměruje na investiční platformu, založí mu účet a vysvětlí, jak platforma funguje. Pod záminkou snadnější komunikace uživatele požádá, aby si stáhl do svého zařízení program pro vzdálený přístup (např. Teamviewer či Supremo). Pomocí tohoto programu útočník vidí to samé, co uživatel a může dokonce toto zařízení ovládat. Tímto způsobem se útočník dostane k citlivým údajům uživatele, a ty následně zneužije k přístupu do online bankovnictví uživatele, ze kterého odčerpá jeho finanční prostředky.[23] V některých případech útočník využije údaje dále k tomu, aby si z účtu podvedeného zažádal o úvěr či půjčku v bance, čímž způsobí uživateli další zadlužení.[24]

2.2 Phishingové útoky

Phishing lze nejčastěji označit za podvodné jednání, jehož cílem je vylákat z uživatele osobní údaje (např. přihlašovací údaje do různých domén, čísla kreditních karet).

Kolouch rozděluje phishingové útoky na ty v užším a širším slova smyslu. V užším slova smyslu se jedná o nasměrování uživatele na podvodnou webovou stránku, kde jsou vyplněny přihlašovací nebo jiné údaje, případně je uživatel pobídnut údaje vyplnit přímo (bez podvodné stránky), např. ve formě formuláře. V širším slova smyslu se jedná o jakékoli podvodné jednání, jehož cílem je vzbudit

---

[21] *Kybernetičtí podvodníci přitvrzují, proto se Komerční banka znovu zapojila do kampaně nePINdej*. Online. In: Komerční banka. 2023. Dostupné z: https://www.kb.cz/cs/o-bance/tiskove-zpravy/kyberneticti-podvodnici-pritvrzuji-proto-se-komercni-banka-znovu-zapojila-do-kampane-nepindej. [cit. 2023-11-12].

[22] *Varování před podvodnými investicemi*. Online. In: Komerční banka. 2023. Dostupné z: https://www.kb.cz/cs/o-bance/novinky/bezpecnost/varovani-pred-podvodnymi-investicemi. [cit. 2023-11-12].

[23] *Investiční podvody*. Online. In: Air Bank. Dostupné z: https://www.airbank.cz/co-vas-nejvic-zajima/investicni-podvody/. [cit. 2023-11-12].

[24] *Investiční podvody – strategická analýza*. Online. In: Finanční analytický úřad. 2021. Dostupné z: https://fau.gov.cz/files/investicni-podvody-strategicka-analyza.pdf. [cit. 2023-11-12].

v uživateli důvěru a postupovat dle scénáře připraveného útočníkem. V takovém případě nemusí údaje uživatel poskytnout sám, mohou být stahovány automaticky využitím škodlivého kódu, tzv. malwaru.[25]

2.2.1 Historie phishingových útoků

Termín phishing pravděpodobně vznikl na základě dvou připodobnění. První z nich se zakládalo na vnější podobnosti rybaření (*fishing*) a podstaty tohoto fenoménu jakožto snaze získávat co nejvíce citlivých údajů uživatelů na základě podvodného jednání, přičemž jednou ze základních charakteristik phishingu mělo být oslovení co největšího počtu uživatelů za účelem co největšího zisku.[26] Druhé z nich odkazuje na termín *phreaks*, složený ze anglických výrazů *phone* a *freaks*, který dříve označoval osoby zabývající se telefonním systémem, zejména za účelem jeho napadení.[27]

Za první mediálně známé případy phishingových útoků je považována série útoků na společnost AOL, která je poskytovatelem internetových služeb, v 90. letech minulého století. Útočníci nejprve začali krást přihlašovací údaje uživatelů, poté s pomocí algoritmu vygenerovali náhodná čísla kreditních karet. Tato data pak sloužila k zakládání nových účtů, které byly následně využívány např. k rozesílání spamu jiným uživatelům AOL. Společnost AOL proti tomu zakročila aktualizací svých bezpečnostních opatření. Útočníci však začali rozesílat falešné e-maily zákazníkům AOL, ve kterých se vydávali za zaměstnance AOL. E-maily byly pečlivě zpracovány, útočníci využívali stejné barvy a styl písma jako AOL. V těchto e-mailech žádali zákazníky, aby ověřili své AOL účty a další své osobní údaje. Společnost AOL poté začala rozesílat e-maily a zprávy, ve kterých varovala před podvodnými zprávami a e-maily a vyzývala své zákazníky, aby prostřednictvím e-mailu nebo messengeru neprozrazovali své osobní údaje.

---

[25] KOLOUCH, Jan. *CyberCrime*. 1. vyd. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7. s. 246

[26] *History of Phishing: How Phishing Attacks Evolved From Poorly Constructed Attempts To Highly Sophisticated Attacks*. Online. In: Phish Protection. Dostupné z: https://www.phishprotection.com/ resources/ history-of-phishing. [cit. 2023-11-19].

[27] *What is phishing and how training can prevent phishing attacks*. Online. Phishing Tackle. Dostupné z: https://phishingtackle.com/phishing/. [cit. 2023-11-19].

S rozvojem online obchodování se útočníci začali zaměřovat na zákazníky e-shopů a uživatele online platebních systémů.[28] První takový útok v roce 2001 na společnost E-Gold byl považován za neúspěšný. Další útoky však pokračovaly v následujících letech. Útočníci si zaregistrovali desítky domén, které vypadaly téměř identicky jako legitimní stránky, např. eBay nebo PayPal. Útočníci následně použili programy rozesílající e-mailové škodlivé kódy pro rozesílání podvodných e-mailů zákazníkům služby PayPal. V e-mailu se nacházel odkaz, který vedl na podvodnou webovou stránku, kde měl zákazník aktualizovat údaje o své platební kartě nebo jiné osobní údaje. Později následovala vlna útoků na bankovní weby a jejich zákazníky. Kolem roku 2008 se objevil Bitcoin a další kryptoměny, což otevřelo další možnosti pro útočníky, jak zaujmout potenciální oběti útoků viz např. podvodné investice, stejně tak ale umožnilo i to, že transakce využívající malware jsou nyní bezpečné a anonymní.[29]

Z uvedeného vyplývá, že podstata phishingových útoků, stejně jako některé způsoby páchání zůstávají téměř neměnné. S rozvojem informačních a komunikačních technologií se však objevují nové možnosti, jež útočníci využívají ve svůj prospěch, ať už jako prostředek, na který nalákají své potenciální oběti, či jako způsob zakrytí své ilegální činnosti.

2.2.2 Sociální inženýrství

I přes technologický rozvoj nabízející mnohé způsoby ochrany před kybernetickými útoky, jsou dnes phishingové útoky stále rozšířené a v rámci kybernetických útoků patří k těm nejvíce efektivním.[30] Phishing totiž není založen pouze na technologii, nýbrž na využití poznatků o lidském chování jakožto prostředku pro přístup k zabezpečené síti nebo systému. Takový přístup se

---

[28] *History of Phishing: How Phishing Attacks Evolved From Poorly Constructed Attempts To Highly Sophisticated Attacks*. Online. In: Phish Protection. Dostupné z: https://www.phishprotection.com/ resources/ history-of-phishing. [cit. 2023-11-19].
[29] *History of Phishing*. Online. Phishing. Dostupné z: https://www.phishing.org/history-of-phishing. [cit. 2023-11-19].
[30] DESOLDA, Giuseppe, et al. Human factors in phishing attacks: a systematic literature review. Online. *ACM Computing Surveys (CSUR)*. 2021, roč. 54, čís. 8. ISSN 0360-0300. Dostupné z: https://www.researchgate.net/profile/Giuseppe-Desolda/publication/361609220_Human_Factors_in_Phishing_Attacks_A_Systematic_Literature_Review/links/62bc31eaf9dee438e8cbae70/Human-Factors-in-Phishing-Attacks-A-Systematic-Literature-Review.pdf. [cit. 2024-02-06].

nazývá sociální inženýrství. Jeho principem je pomocí manipulace přimět uživatele učinit určitou akci či vylákat z něj osobní informace. Sociální inženýrství se však nedá považovat v každém případě za kybernetický útok jako takový, představuje spíše předpoklad pro to, aby byly kybernetické útoky úspěšné.[31]

Nejčastějšími prvky, na které útočníci při vytváření modu operandi spoléhají, je zaprvé touha člověka po rychlém uspokojení. To znamená např. nabídku rychlého výdělku při investování do podvodných investic s kryptoměnami. Dalším principem je tzv. identifikace oběti. Ta spočívá ve vyvolání pocitu, že uživatel musí pomoci konkrétní osobě v nouzi, např. je uživatel požádán o finanční podporu domnělým vojákem z Afghánistánu, který potřebuje peníze, aby uprchl z války a zabezpečil rodinu. Dalším prvkem, na který útočníci spoléhají, je potřeba uživatele zachovat dobrou pověst, ať už svojí, tak např. firemní. Uživatel je přesvědčován, že pokud peníze nepošle, bude tím jemu či firmě způsobena újma. Posledním prvkem je vyvolání strachu z nežádoucích důsledků. Takovým příkladem může být upozornění na to, že někdo brzy uživateli odcizí jeho finanční prostředky na bankovním účtu, a proto musí uživatel své prostředky převést na jiný účet, vybrat či učinit domnělé „bezpečnostní opatření“. Aby využití sociálního inženýrství bylo co nejúspěšnější, je třeba přizpůsobit metody přesvědčování a jejich témata konkrétní, nejlépe co nejobjemnější skupině uživatelů. To vyžaduje studování uživatelů, jejich chování, zájmů a potřeb.[32] Vliv na metody ovlivňování a jejich předmět nemají ale jen uživatelé, ale např. i aktuální socio-ekonomická situace, roční doba, různé trendy apod. Kapr k tomuto v rozhovoru uvedl:

„Čeho si všímáme je modifikace phishingových útoků v rámci jednotlivých částí roku, kdy například ke konci roku varujeme před tak zvaným vánočním phishingem. Pachatelé využívají zmatku kolem vánočních nákupů. Vydávají se za přepravní společnost a spoléhají na to, že při nákupech ztratíte přehled, co kde

---

[31] KOLOUCH, Jan. *CyberCrime*. 1. vyd. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7. s. 186

[32] DESOLDA, Giuseppe, et al. Human factors in phishing attacks: a systematic literature review. Online. *ACM Computing Surveys (CSUR)*. 2021, roč. 54, čís. 8. ISSN 0360-0300. Dostupné z: https://www.researchgate.net/profile/Giuseppe-Desolda/publication/361609220_Human_Factors_in_Phishing_Attacks_A_Systematic_Literature_Review/links/62bc31eaf9dee438e8cbae70/Human-Factors-in-Phishing-Attacks-A-Systematic-Literature-Review.pdf. [cit. 2024-02-06].

máte objednáno. Snaží se z vás vylákat citlivé údaje, či vás donutit k zaplacení doplatku, cla apod. V období daňového přiznání to mohou být zase legendy s daněmi.“

Ochranou před těmito útoky se zabývá samostatná kapitola. Nicméně je zde vhodné zmínit základní prvky prevence těchto útoků, které bezprostředně vyplývají z jejich podstaty jakožto podvodů v informačních a komunikačních technologiích. Prvním indikátorem, že se jedná o podvodnou zprávu, by tedy měl být apel na jeden z výše zmíněných 4 prvků, které mají u uživatele vyvolat určité emoce. Obecně se jedná o zprávy, které vyzývají k rychlé, a tím pádem nepromyšlené akci. Vždy je vhodné věnovat pozornost zprávám, jež jsou od neznámých odesílatelů, i když dnes je již možné obejít i toto pravidlo, jelikož útočníci mohou např. napodobit telefonní číslo uživateli známému člověku. Podvodné zprávy mohou být i gramaticky a pravopisně nedokonalé a způsob provedení celkově nezdařilý. To dnes již také příliš neplatí a podvodné zprávy mohou vypadat naprosto přirozeně. Dalším znakem podvodné zprávy je její obecné znění. Zprávy jsou generovány ve velkém množství a neobsahují žádné osobní údaje uživatelů. I tento prvek však byl již překonán a zprávy bývají mnohdy personalizované. Útočníci oslovují uživatele vlastními jmény a používají jejich osobní údaje (např. z uniklých databází). Posledním kritickým znakem je přítomnost podezřelých příloh a odkazů a nepravděpodobné požadavky, které by reálné společnosti nikdy po uživatelích nežádali (např. sdělit po telefonu bankéři přihlašovací údaje k internetovému bankovnictví).[33] Obecným pravidlem by tedy mělo být zejména nespěchat, vše si dobře promyslet a ověřit před kliknutím na odkazy a přílohy a zejména nikdy nesdělovat své osobní, zejména bankovní údaje žádnou formou komunikace, ani neposkytovat nikomu vzdálený přístup ke svému zařízení.

[33] *Ochrana před útoky phishing*. Online. In: Microsoft. Dostupné z: https://support.microsoft.com/cs-cz/windows/ochrana-p%C5%99ed-%C3%BAtoky-phishing-0c7ea947-ba98-3bd9-7184430e1f860a44. [cit. 2024-02-17].

2.2.3 Druhy phishingových útoků

Phishing skrze e-mail

E-mailový phishing je nejstarší a zároveň patrně stále nejrozšířenější formou phishingu. Tento druh phishingu je možné rozdělit do dvou skupin. První jsou phishingové e-maily obsahující odkaz na podvodnou webovou stránku, druhou jsou ty, které neobsahují odkaz, nýbrž přílohu, která obsahuje určitý druh malwaru.

Oba dva typy zahrnují prvky sociálního inženýrství, vydávají se za konkrétní osobu či instituci, vyvolávají u uživatele různé emoce, které přinutí uživatele jednat pod tlakem a tím přehlédnout jisté nedokonalosti a nelogičnosti příchozí zprávy.[34]

U prvního typu se nebezpečí skrývá u podvodné stránky, na kterou e-mail odkazuje. Podvodná stránka může napodobovat např. banku, platební bránu apod. Jejím cílem je, aby uživatel zadal své údaje právě prostřednictvím této stránky. Podvodná webová stránka může na první pohled působit nerozeznatelně od té pravé, nicméně není možné, aby útočník vytvořil totožnou stránku s tou, která již existuje. Musí se tedy lišit v délce nebo znění domény. Nutno zmínit, že na takové podvodné stránky se lze dostat i přes běžný vyhledavač vlastní činností. Opatrnost by tedy měla být na místě vždy, kdy uživatel zadává citlivé informace na webových stránkách, nikoli pouze po přesměrování odkazem.[35] Odkaz v e-mailu slouží pouze pro to, aby na existující stránky přivedl pozornost a přilákal tím více uživatelů, příkladmo viz příloha 2.

V druhém případě, tedy u e-mailu s přílohou viz příloha 3, představuje nebezpečí právě ona příloha. Poté, co uživatel otevře přílohu, aktivuje se skript, jenž stáhne malware, který útočníkovi zprostředkuje vzdálený přístup k zařízení. To v praxi

---

[34] KOLOUCH, Jan. *CyberCrime*. 1. vyd. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7. s. 186

[35] *Nový druh internetového podvodu*. Online. In: Policie České republiky. 2022. Dostupné z: https://www.policie.cz/clanek/sprava-jihoceskeho-kraje-zpravodajstvi-novy-druh-internetoveho-podvodu.aspx. [cit. 2023-11-27].

znamená, že útočník může např. nahrávat videa pomocí webkamery, pořizovat snímky obrazovky nebo sbírat citlivé údaje uživatele.[36]

Phishing skrze sociální sítě

Phishing skrze sociální sítě se příliš neliší od phishingu e-mailového. Kromě toho, že se podvodná zpráva nachází nikoli na e-mailu, nýbrž na sociálních sítích, je možné spatřovat rozdílnost v tom, že v případě sociálních sítí těží útočníci z toho, že se vydávají za konkrétní, uživateli známé osoby, zpravidla známé či přátele uživatelů. Toho docílí tak, že odcizí či věrohodně napodobí účet uživatele na sociální síti. Nic netušící uživatel pak může poskytnout útočníkovi citlivé údaje v domnění, že je poskytuje svému známému či kamarádovi. Útočník používá fráze jako „Jsi to ty ve videu?“ viz příloha 4 či „Ahoj, můžeš mi poslat své telefonní číslo?“ V takových případech se může jednat o tzv. podvod s m-platbou, kdy útočník požádá uživatele o telefonní číslo, aby si na jeho mobilní telefon mohl zaslat kód pro svou potřebu pod záminkou, že nemá mobilní telefon u sebe. Pokud mu uživatel vyhoví, přijde mu na mobilní telefon zpráva s kódem, který má následně útočníkovi nadiktovat. Pokud tak učiní, potvrdí nechtěně platbu a z jeho účtu odejde potvrzovaná částka.[37]

Reverzní inzertní podvody

Reverzní inzertní podvody představují typ bazarového podvodu, kdy podvedenou osobou není nakupující, nýbrž prodávající. Tyto podvody jsou uskutečňovány na základě nabídek prodeje v internetových bazarech (Bazoš, Vinted, Sbazar či např. Marketplace na Facebooku), přičemž komunikační platformou, skrze kterou samotné podvodné jednání probíhá, je zpravidla Messenger či WhatsApp, tedy sociální sítě různého druhu. Z tohoto pohledu by bylo možné podřadit reverzní inzertní podvody pod phishing skrze sociální sítě. Nicméně díky své specifičnosti

---

[36] *Phishing: Pozor na nebezpečné přílohy OneNote*. Online. In: HP market. 2023. Dostupné z: https://www.hpmarket.cz/document.asp?dc=onenote-phishing. [cit. 2023-11-27].
[37] *Sociální sítě, nová platforma pro útoky sociálních inženýrů*. Online. In: Hacking Lab. 2019. Dostupné z: https://hackinglab.cz/cs/blog/socialni-site-nova-platforma-pro-utoky-socialnich-inzenyru/. [cit. 2023-12-03].

a využití jiných platforem k prodeji zboží je vhodné tento druh phishingu popsat samostatně.

Vše začíná podáním nabídky prodeje uživatelem. Útočník na základě inzerátu uživatele kontaktuje přes sociální sítě či jiný komunikační prostředek se záměrem zájmu o nabízené zboží. Zpravidla pak navrhuje uživateli předání zboží přes přepravce jako je DPD, GLS či např. Zásilkovna s tím, že dopravu uhradí. Následně zašle uživateli odkaz na platební bránu, kde má uživatel po potvrzení a vyplnění určitých údajů získat finanční prostředky za prodávané zboží viz příloha 5. Odkaz však ve skutečnosti vede na podvrženou webovou stránku útočníka, kde je uživatel vyzván k vyplnění osobních údajů, včetně bankovních údajů. Útočník poté kradené bankovní údaje využije k přístupu do internetového či mobilního bankovnictví, případně zneužije údaje uvedené na kreditní kartě a připraví uživatele o finanční prostředky.[38]

Společnost ESET provedla ve spolupráci s Policií ČR průzkum o zkušenostech uživatelů s podvodným jednáním na internetových bazarech. Sběr dat byl uskutečňován ve dnech 17. a 18. 5. 2022 na reprezentativním vzorku 1100 respondentů v České republice agenturou Ipsos. Výsledkem průzkumu jest, že 31 % z dotázaných respondentů se osobně setkalo s podvodem na internetovém bazaru, přičemž věkově nejpočetnější skupinu z těchto tvořili osoby ve věku 30-40 let. Dále bylo zjištěno, že nejčastěji byli uživatelé kontaktování útočníky přes aplikaci Messenger (12,27 %), e-mail (10,82 %) či aplikaci WhatsApp (7,18 %). Respondenti byli dále tázáni na vznik škody, přičemž 20,64 % respondentů uvedlo, že se jim podařilo podvod včas rozpoznat a k žádné škodě tedy nedošlo, 9,36 % respondentům vznikla škoda do 1 000 Kč a 5 % respondentů přišlo o finanční prostředky v hodnotě do 5 000 Kč. Zajímavým poznatkem dále bylo, že vzhledem k datům z průzkumu nahlásilo podvod bezprostředně (do 24 hodin) na Policii ČR pouze 4,09 % dotázaných uživatelů, přičemž 7 % respondentů nejprve zkusilo s útočníky komunikovat samo, a teprve později se obrátilo na

[38] *Podvody na Bazoši a Sbazaru: Jak prodávat na internetu bezpečně?* Online. In: Dvojklik. 2022. Dostupné z: https://www.dvojklik.cz/podvody-na-bazosi-a-sbazaru-jak-prodavat-na-internetu-bezpecne/. [cit. 2024-01-15].

Policii ČR. Z uvedeného vyplývá, že 20,82 % dotázaných uživatelů se na Policii ČR neobrátilo vůbec.[39]

Smishing

Smishing představuje obdobu klasického phishingového e-mailu, kde prostředkem, který využívá útočník k podvodnému jednání není e-mail, ale SMS zpráva. Název smishing tedy vznikl složením slov SMS a phishing. Od phishingového e-mailu se liší především tím, že neobsahuje přílohu. Veškeré nebezpečí tedy představuje odkaz viz příloha 6, který po kliknutí na něj buďto zavede uživatele na podvržené webové stránky, kde je uživatel vyzván k vyplnění osobních údajů či spustí malware, po jehož instalaci do zařízení je útočník schopen požadované osobní údaje získat sám.[40]

V minulém roce útočníci rozesílali např. podvodné SMS zprávy, jejichž znění bylo takovéto: „*ČSSZ, na vašem účtu je k dispozici výplata…*“ Ve zprávě byl přítomen i odkaz na podvržené webové stránky České zprávy sociálního zabezpečení, které vypadaly téměř k nerozeznání od těch pravých. Pan X z Třeboně tento odkaz otevřel a na podvržených stránkách se přihlásil pomocí své bankovní identity. Stránka se poté dlouze načítala a pan X se domníval, že jde pouze o výpadek. Později pan X zjistil, že přišel o 150 000 Kč.[41]

Kapr k tomuto v rozhovoru uvedl:

„Co se týče smishingu, tak se v poslední době setkáváme hlavně s SMS zprávami s legendou státní finanční pomoci. Pachatelé zneužili situace a toho, že velké množství lidí čekalo nějakou pomoc od státu a najednou vám přijde SMS zpráva, která se tváří, jako od Ministerstva práce a sociálních věcí, kde máte kliknout na

---

[39] *Průzkum ESET: Třetina lidí se stala cílem podvodu na internetových bazarech*. Online. In: Eset. 2022. Dostupné z: https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/pruzkum-eset-tretina-lidi-se-stala-cilem-podvodu-na-internetovychbazarech/#_ga=2.77191125.1973274478.1705308083-786498258.1702148979. [cit. 2024-01-15].

[40] *Co je smishing*. Online. In: Moneta. Dostupné z: https://www.moneta.cz/slovnik-pojmu/detail/smishing. [cit. 2024-01-15].

[41] *Podvodná zpráva informovala o výplatě. Muž přišel o 150 tisíc.* Online. In: Jindřichohradecký deník. 2023. Dostupné z: https://jindrichohradecky .denik.cz/zlociny-a-soudy/podvodna-zprava-informovala-o-vyplate-muz-prisel-o-150-tisic-20230731.html. [cit. 2024-02-17].

odkaz. Dostanete se na spoofovanou stránku, která je prakticky k nerozeznání od originální. Zde pod dojmem, že vyplňujete požadované údaje do bankovní identity, nevědomky tyto údaje zasíláte pachateli, a ještě a přístup mu dále ještě svou neopatrností odsouhlasíte. Pachatel následně provádí převody na připravené bankovní účty založené legalizátory. Nebezpečí je zde zejména u cílených útoků, kde se vaše jméno může objevit přímo v textu SMS zprávy. Jméno mohou vyčíst z uniklých databází.“

Vishing

Vishing je typ phishingu, kde k podvodnému jednání útočníka dochází nikoli skrze psanou komunikaci s uživatelem prostřednictvím e-mailu, SMS zpráv či sociálních sítí, nýbrž skrze hlasový, telefonní hovor. Pojem vishing vznikl složením anglických výrazů *voice* (hlas) a phishing.

Vishingový útok začíná telefonátem, přičemž telefonní číslo zobrazující se v mobilním zařízení uživatele může být spoofované, tedy nereálné, pouze napodobené. Útočník může pomocí metody spoofingu napodobit kterékoli telefonní číslo a přesvědčit tak uživatele o své věrohodnosti. Vishingové útoky jsou prováděny buďto přímo útočníkem, tedy jeho vlastním hlasem či jsou pomocně využívány technologie automatického převodu textu na řeč, které uživatele na útočníka později přesměrují. Díky možnostem využití strojového učení pro tvorbu syntetických hlasů se stává vishing vysoce přesvědčivou metodou podvodného jednání, jelikož útočník s jeho pomocí dokáže napodobit hlas uživateli známé osoby. Jakmile získá útočník alespoň částečnou důvěru uživatele, snaží se ho přimět k vydání osobních údajů potřebných k převodu peněz, typicky přihlašovací údaje do mobilního či internetového bankovnictví nebo platební údaje. V opačném případě přiměje uživatele pod falešnou záminkou své finanční prostředky dobrovolně odeslat či předat.[42] K tomu, aby útočník k takovémuto jednání uživatele přesvědčil, využívá různé legendy. Kapr v rozhovoru k problematice vishingu uvedl následující:

[42] *Vishing*. Online. In: Eset. Dostupné z: https://www.eset.com/cz/vishing/. [cit. 2024-01-17].

„S tímto typem útoku se ve větší míře setkáváme hlavně v posledních dvou letech, a to hlavně s legendou „Falešný bankéř“, kdy se pachatel v telefonátu vydává za pracovníka banky, který vás vystraší s tím, že někdo zneužil vaše doklady a je potřeba zachránit peníze na vašem bankovním účtu. Pachatelé se v těchto případech vydávají v telefonátech i za policisty. Na displeji mobilního telefonu se vám dokonce objeví policejní tel. číslo 974…, či přímo nápis konkrétní součásti policie. Falešný policista podpoří legendu pachatele, a navíc vás ještě vystraší povinností mlčenlivosti a eventuálnímu trestnímu stíhání při nespolupráci. Pachatelé v podvodných telefonátech využívají i další legendy. Například legenda VNUK. Falešná technická podpora. Podvodná investice a další.“

Deepfake phishing

Deepfake phishing je typ phishingu, kde prostředek klamání či iluze představuje podvržený typicky audio, video záznam či fotografie. Název deepfake vznikl složením anglických výrazů *deep learning* a *fake.* Výraz *deep learning* odkazuje na schopnost tzv. „hloubkového učení“, které realizuje umělá inteligence pomocí svých algoritmů. Výraz *fake* vyjadřuje, že obsah vytvořený pomocí metody „hloubkového učení“ není pravý, totiž nezobrazuje skutečnost, ale pouze obraz skutečnosti se podobající.[43] Deepfake je možno definovat jako umělou tvorbu či manipulaci audio, video záznamů či jiných forem digitálního obsahu za účelem přesvědčení uživatele, že se určitá osoba chovala či vypadala jinak, případně že se určitá situace stala či stala jinak.[44] Deepfake phishing pak představuje deepfake vytvořený za účelem vylákání finančních prostředků uživatele.

Jak bylo zmíněno výše, deepfake vychází z technologie tzv. „hloubkového učení“, které realizuje umělá inteligence. Podvržené audio, video či jiné záznamy tedy vytváří umělá inteligence za využití různých technik, např. GAN (*Generative Adversarial Networks*) na základě velkého množství vzorků (audio, video

[43] *Social Engineering 2.0: The Rise of Deepfake Phishing*. Online. In: Secure World. 2023. Dostupné z: https://www.secureworld.io/industry-news/ social-engineering-deepfake-phishing. [cit. 2024-01-22].
[44] PATIL, Kundan, et al. Deepfake detection using biological features: a survey. Online. In: *ArXiv preprint arXiv:2301.05819*. 2023. Dostupné z: https://arxiv.org/abs/2301.05819. [cit. 2024-01-22].

záznamů, obrázků apod.). Dnes je díky běžně dostupným webovým stránkám a aplikacím (FaceApp apod.) možné vytvořit pomocí umělé inteligence deepfake obrázek nebo video i s velmi malými znalostmi strojového učení a programování.[45] To představuje nebezpečí poměrně snadného zneužití umělé inteligence k páchání podvodných a jiných útoků.

Existuje mnoho způsobů, jak zneužít deepfake k podvodnému útoku. Jeden z nich, vishing, je již popsán výše. Podvodná audio nahrávka např. bankovního úředníka, policisty, zaměstnavatele či známého v nouzi vyvolá v uživateli emoce a ten pod jejich nátlakem vydá útočníkovi své finanční prostředky v dojmu, že je posílá skutečné osobě, kterou zná či které důvěřuje. Jelikož je ale toto jednání již kategorizováno jako vishing, bude se tato kapitola nadále zabývat pouze podvodnými video záznamy. Princip tohoto podvodného jednání je však téměř totožný. Liší se pouze tím, že místo audio záznamu je uživateli předložen video záznam. Může se jednat jak o záznam někoho uživateli známého, např. zaměstnavatele, kolegu, kamaráda apod., tak o záznam někoho, s kým se uživatel nezná, např. veřejně známé osobnosti. Záminka pro zaslání finančních prostředků uživatelem je tedy různá od převedení firemních finančních prostředků na pokyn domnělého nadřízeného po napodobeniny veřejně známých osobností využívaných jako reklamy na podvodné investiční platformy.[46]

Stejně tak jako je pomocí umělé inteligence možno vytvořit deepfake, je možno vytvořit i systém, který deepfake detekuje, tedy je schopen rozeznat deepfake od skutečného záznamu. Děje se tak na základě různých kritérií. Jedním z nich mohou být např. biologické znaky a faktory jako je obočí, mrkání oka, pohyb oka, pohyb uší a úst či detekce srdečního rytmu.[47]

---

[45] PATIL, Kundan, et al. Deepfake detection using biological features: a survey. Online. In: *ArXiv preprint arXiv:2301.05819*. 2023. Dostupné z: https://arxiv.org/abs/2301.05819. [cit. 2024-01-22].
[46] *Šéf vygenerovaný počítačem: Jak fungují deepfakes?* Online. In: Eset. 2023. Dostupné z: https://digitalsecurityguide.eset.com/cz/sef-vy generovany-pocitacem-jak-funguji-deepfakes. [cit. 2024-01-22].
[47] PATIL, Kundan, et al. Deepfake detection using biological features: a survey. Online. In: *ArXiv preprint arXiv:2301.05819*. 2023. Dostupné z: https://arxiv.org/abs/2301.05819. [cit. 2024-01-22].

Quishing

Quishing je zvláštní druh phishingu, kde je podvodný útok realizován prostřednictvím QR kódu. Název quishing tedy vznikl složením výrazů QR kód a phishing. QR kódy jsou dvourozměrné čárové kódy, které mají v sobě zakódovány určité množství dat. Je možné je skenovat pomocí mobilního telefonu nebo čtečky QR kódů. Po naskenování QR kódu je uživatel přesměrován k zakódovanému zdroji informací, např. na webovou stránku. QR kódy dnes představují i jednu z variant jak jednofázového, tak dvoufázového ověření při přihlašování do různých účtů a aplikací, včetně těch bankovních.

QR kódy lze dělit do dvou skupin, a to na statické a dynamické. Jakmile statický QR kód vznikne, data zakódovaná v nich není možné měnit. Oproti tomu data zakódovaná v dynamických QR kódech je možné měnit, aniž by se zároveň s tím změnil vzhled QR kódu. To umožňuje útočníkům příležitost k manipulaci s legitimními QR kódy, tedy změně jejich původního zdroje na škodlivý.

Obdobně jako u phishingu skrze e-mail má útočník několik možností, jak pomocí QR kódu získat citlivé údaje uživatele. Po naskenování QR kódu je uživatel buďto přesměrován na podvrženou webovou stránku, kde je vyzván k vyplnění osobních, nejčastěji bankovních údajů či je uživatel vyzván ke stažení skrytého malwaru, případně se tento stáhne sám, aniž by o tom uživatel věděl. Pomocí malwaru útočník získá osobní údaje sám.[48] V případě jednorázového či dvoufázového ověřování QR kódem může dojít ke krádeži osobních údajů pouhým naskenováním kódu v případě, že se útočník vydává za provozovatele např. sociální sítě a podstrčí uživateli podvržený QR kód. Dalším způsobem, který útočníci využívají, je pozměnění dat v QR kódech vytvořených ke QR platbám. Místo na účet původního příjemce jsou pak finanční prostředky doručeny na

[48] *Quishing*. Online. In: So Safe. Dostupné z: https://sosafe-awareness.com/glossary/quishing/. [cit. 2024-01-18].

bankovní účet útočníka či legalizátora. Stejně tak mohou vytvářet falešné QR kódy s požadavky na inkaso.[49]

QR kódy mohou být součástí e-mailů, zpráv na sociálních sítích, webových stránek či aplikací, ale je možné se s nimi setkat i na veřejně přístupných místech, na ulicích, v restauračních zařízeních apod. Nebezpečí quishingu spočívá prvně v tom, že mobilní zařízení, která je skenují, nejsou zpravidla tak dobře zabezpečená proti napadení jako počítače a jim podobná zařízení. Druhý faktor výrazně ovlivňující bezpečnost se projevuje zejména u e-mailů obsahujících závadný QR kód. Detektory škodlivých kódů a další e-mailové filtry označí e-mail za potenciálně závadový pouze pokud obsahuje podezřelé adresy URL nebo přílohy. QR kódy se však vkládají do e-mailů pouze jako obrázky či jsou vkládány do přiložených dokumentů s nepodezřelou příponou. V neposlední řadě představují podvodné QR kódy nebezpečí právě díky nemožnosti rozpoznat jejich zakódovaný obsah pouhým okem, apelují tedy na přirozenou lidskou zvědavost.

2.2.4 Trestně právní úprava phishingových útoků

Phishingový útok lze nejčastěji trestně právně kvalifikovat jako podvod dle § 209 trestního zákoníku.[50] Trestní zákoník definuje trestný čin podvodu v odst. 1 takto:

„*Kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci*.“[51]

Další právní kvalifikace se liší na základě konkrétních skutků, které byly spáchány. V úvahu připadá § 230 trestního zákoníku, tedy neoprávněný přístup

---

[49] *Útočník si najde cestu i přes QR kód. Jak skenovat bezpečně?* Online. In: Dvojklik. 2022. Dostupné z: https://www.dvojklik.cz/utocnik-si-najde-cestu-i-pres-qr-kod-jak-skenovat-bezpecne/. [cit. 2024-01-18].

[50] JONÁŠOVÁ, Eliška. Aktuální kybernetické hrozby a odpovídající právní úprava v Evropské unii a v Kanadě. Online. *Bezpečnostní teorie a praxe*. 2018, roč. 18, čís. 3. ISSN 1801-8211. Dostupné z: https://veda.polac.cz/wp-content/uploads/2019/04/032018_Aktu%C3 %A1 ln%C3%AD-kybernetick%C3%A9-hrozby-a-odpov%C3%ADdaj%C3%ADc%C3%AD-pr%C3%A1vn%C3%AD -%C3%BAprava-v-Evropsk%C3%A9-u nii-a-v-Kanad%C4%9B.pdf. [cit. 2024-01-23].

[51] Zákon č. 40/2009 Sb., *trestní zákoník* v posledním znění

k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací, dále § 231, tedy opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat a v neposlední řadě také § 234, tedy neoprávněné opatření, padělání a pozměnění platebního prostředku.[52]

Vzhledem k charakteru této práce bude pro rozbor těchto skutkových podstat patrně nejvhodnější rozdělit phishingové útoky na ty, které jsou provedeny bez využití malwaru a na ty, které malware využívají.

Phishingové útoky bez využití malwaru

Phishingové útoky, které nevyužívají malware jsou útoky, které přesvědčí uživatele, aby své osobní, nejčastěji bankovní údaje poskytl útočníkovi sám. Typicky jsou to tedy phishingové e-maily s odkazem.[53]

Trestným činem neoprávněného přístupu k počítačovému systému dle § 230 odst. 1 trestního zákoníku, se rozumí:

„*Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci*.“[54]

Z uvedeného vyplývá, že k naplnění skutkové podstaty dojde po překonání bezpečnostního opatření, čímž útočník neoprávněně získá přístup k počítačovému systému nebo jeho části. Z definice phishingového útoku bez využití malwaru je však patrné, že uživatel své údaje poskytne sám, útočník tedy nepřekonává žádná bezpečnostní opatření. § 230 odst. 1 trestního zákoníku je tímto pro phishingový útok bez malwaru nepoužitelný.[55]

---

[52] KRUPIČKA, Jiří. Kybernetická kriminalita. Online. *Acta Universitatis Carolinae*. 2012, roč. 58, čís. 4. ISSN 0323-0619. Dostupné z: https://www.prf.cuni.cz/dokumenty-download/1404048928/. [cit. 2.9. 2018].
[53] KOLOUCH, Jan. *CyberCrime*. 1. vyd. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7. s. 186
[54] Zákon č. 40/2009 Sb., *trestní zákoník* v posledním znění
[55] KRUPIČKA, Jiří. Kybernetická kriminalita. Online. *Acta Universitatis Carolinae*. 2012, roč. 58, čís. 4. ISSN 0323-0619. Dostupné z: https://www.prf.cuni.cz/dokumenty-download/1404048928/. [cit. 2.9. 2018].

Trestným činem neoprávněného přístupu k počítačovému systému dle § 230 odst. 2 trestního zákoníku, se rozumí:

„*Kdo zasáhne do počítačového systému nebo nosiče informací tím, že… bude potrestán odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci.*“[56]

Tento odstavec se však obdobně jako odstavec výše nevztahuje na situaci, kdy útočníkovi sdělí potřebné údaje uživatel sám, a proto se pro kvalifikování phishingového útoku bez malwaru nehodí.[57]

Trestným činem opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle § 231 odst. 1 trestního zákoníku, se rozumí:

„*Kdo vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechová a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části nebo k neoprávněnému zásahu do počítačového systému nebo nosiče informací, nebo b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části, v úmyslu, aby jej bylo užito ke spáchání trestného činu porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b) nebo c) nebo trestného činu neoprávněného přístupu k počítačovému systému a neoprávněného zásahu do počítačového systému nebo nosiče informací podle § 230 odst. 1 nebo 2, bude potrestán odnětím svobody až na dvě léta, propadnutím věci nebo zákazem činnosti.“*[58]

---

[56] Zákon č. 40/2009 Sb., *trestní zákoník* v posledním znění
[57] KRUPIČKA, Jiří. Kybernetická kriminalita. Online. *Acta Universitatis Carolinae*. 2012, roč. 58, čís. 4. ISSN 0323-0619. Dostupné z: https://www.prf.cuni.cz/dokumenty-download/1404048928/. [cit. 2.9. 2018].
[58] Zákon č. 40/2009 Sb., *trestní zákoník* v posledním znění

V tomto odstavci je sice postihnuto samotné opatření či přechování přístupových dat, nicméně pouze za účelem porušení tajemství dopravovaných zpráv či neoprávněného přístupu k počítačovému systému a neoprávněného zásahu do počítačového systému nebo nosiče informací. Ani pod tento odstavec tedy není možné phishingový útok bez malwaru subsumovat.[59]

Trestným činem neoprávněného opatření, padělání a pozměnění platebního prostředku dle § 234 odst. 1 se rozumí:

„*Kdo sobě nebo jinému bez souhlasu oprávněného uživatele opatří, zpřístupní, přijme nebo přechovává platební prostředek, který umožňuje výběr hotovosti nebo převod peněžních prostředků anebo virtuálních aktiv používaných namísto peněžních prostředků (dále jen „platební prostředek“) a který náleží jinému, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.*“[60]

V § 234 odst. 1 trestního zákoníku se dále píše o opatření, zpřístupnění, přijetí a přechovávání platebního prostředku, které náleží jinému, bez souhlasu oprávněného uživatele, což by mohlo odpovídat jednání, které koresponduje s některými typy phishingových útoků. Sporný je zde však samotný pojem platební prostředek. Otázkou je, zda se dají bankovní a platební údaje považovat za platební prostředek či nikoli.[61] Zde je třeba si definovat platební prostředek. Jeho legální definice je obsažena v § 2 odst. 1 písm. d) zákona č. 370/2017 Sb., o platebním styku (dále jen zákon o platebním styku). Zde je uvedeno, že pro účely tohoto zákona se platebním prostředkem rozumí:

„*zařízení nebo soubor postupů dohodnutých mezi poskytovatelem a uživatelem, které jsou vztaženy k osobě uživatele a kterými uživatel dává platební příkaz“.*[62]

---

[59] KRUPIČKA, Jiří. Kybernetická kriminalita. Online. *Acta Universitatis Carolinae*. 2012, roč. 58, čís. 4. ISSN 0323-0619. Dostupné z: https://www.prf.cuni.cz/dokumenty-download/1404048928/. [cit. 2.9. 2018].
[60] Zákon č. 40/2009 Sb., *trestní zákoník* v posledním znění
[61] KRUPIČKA, Jiří. Kybernetická kriminalita. Online. *Acta Universitatis Carolinae*. 2012, roč. 58, čís. 4. ISSN 0323-0619. Dostupné z: https://www.prf.cuni.cz/dokumenty-download/1404048928/. [cit. 2.9. 2018].
[62] Zákon č. 370/2017 Sb., *o platebním styku* v posledním znění

Pro srovnání je vhodné přiložit i legální definici jedinečného identifikátoru dle § 2 odst. 3 písm. g), zákona o platebním styku. Jedinečným identifikátorem se rozumí:

„kombinace písmen, číslic nebo symbolů, kterými se podle určení poskytovatele identifikuje uživatel nebo jeho účet při provádění platebních transakcí“[63]

Krupička se zde domnívá, že v případě bankovních a platebních údajů získaných phishingovým útokem se nejedná o platební prostředek, nýbrž právě o jedinečný identifikátor, a proto nelze § 234 odst. 1 v případě phishingového útoku bez malwaru použít.

Útočník se však dopustí trestného činu neoprávněného opatření, padělání a pozměnění platebního prostředku, pokud naplní skutkovou podstatu uvedenou v § 234 odst. 3 alinea druhá trestního zákoníku, tedy:[64]

„*kdo padělaný nebo pozměněný platební prostředek použije jako pravý nebo platný, bude potrestán odnětím svobody na tři léta až osm let*.“[65]

Tohoto trestného činu se útočník dopustí, tedy ho dokoná, pokud podvodně získané bankovní či platební údaje využije k zadání elektronického příkazu. V tomto případě se tedy útočník dopustí trestného činu neoprávněného opatření, padělání a pozměnění platebního prostředku (§ 234 odst. 3 alinea druhá trestního zákoníku) v jednočinném souběhu s dokonaným trestným činem podvodu dle § 209 trestního zákoníku či jeho pokusem. Pokud útočník bankovní či platební údaje nevyužije, je trestně odpovědný pouze za pokus trestného činu neoprávněného opatření, padělání a pozměnění platebního prostředku a trestného činu podvodu.[66]

Z výše uvedeného vyplývá, že útočník, jenž spáchal phishingový útok bez využití malwaru, může být za splnění podmínek stanovených trestním zákoníkem

---

[63] Zákon č. 370/2017 Sb., *o platebním styku* v posledním znění
[64] KRUPIČKA, Jiří. Kybernetická kriminalita. Online. *Acta Universitatis Carolinae*. 2012, roč. 58, čís. 4. ISSN 0323-0619. Dostupné z: https://www.prf.cuni.cz/dokumenty-download/1404048928/. [cit. 2.9. 2018].
[65] Zákon č. 40/2009 Sb., *trestní zákoník* v posledním znění
[66] KRUPIČKA, Jiří. Kybernetická kriminalita. Online. *Acta Universitatis Carolinae*. 2012, roč. 58, čís. 4. ISSN 0323-0619. Dostupné z: https://www.prf.cuni.cz/dokumenty-download/1404048928/. [cit. 2.9. 2018].

a v závislosti na konkrétním skutku trestně odpovědný za trestný čin podvodu dle § 209 trestního zákoníku, případně za trestný čin neoprávněného opatření, padělání a pozměnění platebního prostředku dle § 234 odst. 1 či odst. 3 alinea druhá trestního zákoníku.

Phishingové útoky s využitím malwaru

Phishingové útoky, ke kterým je využit malware, jsou útoky, kde součástí phishingové zprávy je příloha obsahující malware. Uživatel v tomto případě své osobní, zpravidla bankovní údaje neposkytuje útočníkovi sám, nýbrž útočník se jich zmocňuje za pomoci malwaru skrytého v příloze, kterou uživatel otevřel či stáhl. Typicky jsou to tedy phishingové e-maily s přílohou.[67]

Útok, který je spáchán pomocí malwaru, je trestný dle výše zmíněného § 230 trestního zákoníku, jedná se tedy o trestný čin neoprávněného přístupu k počítačovému systému a neoprávněného zásahu do počítačového systému nebo nosiče informací. Opatřování a přechovávání malwaru je trestné dle výše zmíněného § 231 trestního zákoníku, jedná se tedy o trestný čin opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat. Ovšem pouze za předpokladu, že je tak činěno s úmyslem spáchat trestný čin dle § 182 odst. 1, písm. b), c) trestního zákoníku, tedy porušení tajemství dopravovaných zpráv či trestný čin dle § 230 odst. 1 a 2 trestního zákoníku, tedy neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací.[68]

Z výše uvedeného lze vyvodit, že útočník, jenž se dopustil phishingového útoku s využitím malwaru, může být za podmínek stanovených trestním zákoníkem a v závislosti na konkrétním skutku trestně odpovědný za trestný čin podvodu dle § 209, případně trestný čin neoprávněného opatření, padělání a pozměnění

---

[67] KOLOUCH, Jan. *CyberCrime*. 1. vyd. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7. s. 186

[68] JONÁŠOVÁ, Eliška. Aktuální kybernetické hrozby a odpovídající právní úprava v Evropské unii a v Kanadě. Online. *Bezpečnostní teorie a praxe*. 2018, roč. 18, čís. 3. ISSN 1801-8211. Dostupné z: https://veda.polac.cz/wp-content/uploads/2019/04/032018_Aktu%C3%A1ln%C3%AD-kybernetick%C3%A9-hrozby-a-odpov%C3%ADdaj%C3%ADc%C3%AD-pr%C3%A1vn%C3%AD-%C3%BAprava-v-Evropsk%C3%A9-u nii-a-v-Kanad%C4%9B.pdf. [cit. 2024-01-23].

platebního prostředku dle § 234 odst. 1 a odst. 3 alinea druhá trestního zákoníku, dále trestný čin neoprávněného přístupu k počítačovému systému a neoprávněného zásahu do počítačového systému nebo nosiče informací dle § 230 odst. 1 a 2 trestního zákoníku a trestný čin opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle § 231 trestního zákoníku, za podmínky, že takto jednal s úmyslem spáchat trestný čin neoprávněného přístupu k počítačovému systému a neoprávněného zásahu do počítačového systému nebo nosiče informací dle § 230 odst. 1 a 2 trestního zákoníku.

2.2.5 Objasňování podvodných útoků v informačních a komunikačních technologiích

Přestože se podvodný útok v informačních a komunikačních technologiích nejčastěji trestně právně kvalifikuje jako trestný čin podvodu dle § 209 trestního zákoníku, z hlediska jeho objasňování je zásadní právě to, že byl spáchán v kyberprostoru. Je tomu tak, jelikož kyberprostor je natolik specifické prostředí, že vyžaduje v určitých směrech zvláštní přístup. Z definic kyberprostoru, které jsou již popsány v předchozí kapitole, vyplývají jeho specifické vlastnosti, kterými jsou především jeho globálnost, dynamičnost a anonymita. Přitom platí, že právě díky těmto jeho vlastnostem se kyberprostor stává relativně příznivým prostředím pro páchání kriminality, což dokládá fakt, že v roce 2022 tvořila kyberkriminalita 10,2 % celkové registrované kriminality.[69]

Odezvou na mj. kritický nárůst kyberkriminality byl vznik nového samostatného útvaru s celostátní působností, Národní centrály proti terorismu, extremismu a kybernetické kriminalitě (dále jen NCTEKK) Služby kriminální policie a vyšetřování (dále jen SKPV), která vznikla ke dni 1. 1. 2023 vyčleněním sekcí terorismu, extremismu a kybernetické kriminality z Národní centrály proti

[69] *Vývoj registrované kriminality v roce 2022*. Online. In: Policie České republiky. 2023. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx. [cit. 2023-10-31].

organizovanému zločinu SKPV.[70] NCTEKK SKPV se zabývá objasňováním těch nejzávažnějších forem kriminality. Dále se objasňováním kybernetické kriminality zabývají specializovaná oddělení, která vznikla zhruba před sedmi lety v každém kraji v rámci krajských ředitelství Policie ČR.[71] Méně závažné formy kybernetické kriminality pak objasňují útvary zřízené krajskými ředitelstvími Policie ČR.

2.2.6 Typické právní nástroje využívané při objasňování phishingových útoků

Policie ČR využívá k objasňování phishingových útoků různé právní nástroje. Policejní orgán, který byl pověřen příslušným ministrem, je oprávněn v řízení o úmyslném trestném činu a za splnění dalších podmínek stanovených v § 158 b zákona č. 141/1961 Sb., o trestním řízení soudním (dále jen trestní řád) využívat operativně pátrací prostředky, přičemž operativně pátracími prostředky se rozumí předstíraný převod, sledování osob a věcí a použití agenta. Dále je využíván institut odposlechu a záznamu telekomunikačního provozu dle trestního řádu a další ustanovení trestního řádu.[72] Využívány jsou i podpůrné operativně pátrací prostředky upravené v zákoně č. 273/2008 Sb., o Policii ČR, jimiž jsou informátor, krycí prostředky, zabezpečovací technika a zvláštní finanční prostředky.[73]

2.2.7 Typické postupy při objasňování phishingových útoků

Postup objasňování phishingových útoků se v mnohém podobá postupu objasňování jiných druhů kriminality. Jak již však bylo řečeno výše, vzhledem k tomu, že je phishingový útok ze své podstaty podřazen pod kybernetickou kriminalitu, vyžaduje jeho objasňování v mnohém zvláštní přístup. Za charakteristické lze považovat existenci digitálních stop, jejich vyhledávání, zajišťování a vyhodnocování, potřebu spolupráce s odborníky na informační

---

[70] *Národní centrála proti terorismu, extremismu a kybernetické kriminalitě SKPV*. Online. In: Policie České republiky. Dostupné z: https://www.policie.cz/clanek/narodni-centrala-proti-terorismu-extremismu-a-kyberneticke-kriminalite.aspx. [cit. 2023-12-09].
[71] *Napadená zařízení okamžitě odpojte od internetu, říká major Valiček*. Online. In: O2 CyberNews. 2023. Dostupné z: https://o2cybernews.cz /clanky/prevence-je-zaklad-obrany-proti-kyberutokum-rika-policista. [cit. 2024-02-03].
[72] Zákon č. 141/1961 Sb., *o trestním řízení soudním* v posledním znění
[73] Zákon č. 273/2008 Sb., *o Policii ČR* v posledním znění

a komunikační technologie, bankovním sektorem, provozovateli telekomunikačních a internetových služeb a mezinárodní spolupráci. V této kapitole bude naznačen postup Policie ČR při objasňování phishingových útoků tak, jak v rozhovoru popsal Kapr a bude doplňován o poznatky jiných odborníků.

Kapr se v rozhovoru k následující problematice vyjádřil takto:

„Vše začíná příjmem oznámení. Následovat by mělo ohledání virtuálního prostoru, kdy dojde k zajištění digitálních důkazů. Vždy je potřeba pečlivě vyslechnout oběť s cílem zjistit, kde všude se mohl pachatel pohybovat. Pak už je to hodně individuální. Zpravidla se zjišťují možné IP logy pachatele.“

Zde je důležité dodat, že pro objasňování kybernetické kriminality je vždy klíčové zajištění co největšího počtu digitálních stop. Ty se nachází na každém technologickém zařízení získávajícím, zpracovávajícím a uchovávajícím data. Tyto stopy mají specifické vlastnosti, z nichž patrně nejpodstatnější je jejich nízká životnost. Je proto důležité všechny tyto stopy co nejdříve zajistit, případně zabránit jejich smazání či jejich smazání obnovit.[74] Aby mohla být práce Policie ČR co nejefektivnější, je žádoucí, aby uživatel tyto stopy zachytil, pokud možno zanechal v původním stavu a kontaktoval Policii ČR v co nejkratším čase. K tomu dodává vedoucí odboru analytiky a kybernetické kriminality na Krajském ředitelství Středočeského kraje Valiček v rozhovoru pro O2 CyberNews toto:

„*Rozhodně by neměl napadaný subjekt jakkoli manipulovat s daty – není dobrý nápad přeinstalovat počítač, nebo třeba resetovat napadený mobilní telefon do továrního nastavení.*“[75]

Policie ČR po podání trestního oznámení následně provede ohledání místa činu či věci (počítače, notebooku, mobilního telefonu…), přičemž je zařízení, které je důkazním prostředkem, ohledáno buďto přímo na místě činu či na služebně, kde bylo trestní oznámení podáno. Následně může být dle § 78 či § 113 trestního řádu

---

[74] PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty.* 2. dopl. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-741-2. s. 967 srov. s. 972

[75] *Napadená zařízení okamžitě odpojte od internetu, říká major Valiček*. Online. In: O2 CyberNews. 2023. Dostupné z: https://o2cybernews.cz /clanky/prevence-je-zaklad-obrany-proti-kyberutokum-rika-policista. [cit. 2024-02-03].

Policii ČR vydáno k dalšímu zkoumání.[76] V další fázi objasňování je pak klíčová spolupráce se znalci v oboru informačních a komunikačních technologií, ale i s provozovateli telekomunikačních a internetových služeb. Jelikož spáchaným phishingovým útokem uživateli pravděpodobně vznikla finanční újma, a to odčerpáním finančních prostředků z bankovního účtu uživatele, je při objasňování phishingových útoků důležitá i spolupráce s bankovním sektorem. Kapr v rozhovoru k této spolupráci dodal:

„*V případě, že dojde k finanční újmě, tak se snažíme zachránit finanční prostředky, a to ve spolupráci s bankovním sektorem a FAÚ. Případně se snažíme trasovat cestu finančních toků. Často se setkáváme s osobami legalizatorů, které je potřeba řádně vyslechnout a zjistit všechny důležité okolnosti případu. Může se jednat o legalizaci výnosů z trestné činnosti. I legalizace z nedbalosti může být trestná.*“

Pokud dojde k finanční újmě, měl by tedy uživatel, ať už ve spolupráci s Policií ČR či sám, v co nejkratší době kontaktovat svoji banku, jelikož existuje šance, že s její pomocí bude moci své finanční prostředky získat zpět, přičemž platí, že čím dříve uživatel banku kontaktuje, tím větší je šance na jejich navrácení. Nevoralová, tisková mluvčí Komerční banky uvedla v rozhovoru pro Seznam zprávy toto:

„*Klient by měl kontaktovat svoji banku a popsat přesně, co se stalo, zda klient předal informace pouze k přihlášení do svého internetového, mobilního bankovnictví, nebo i ke kreditní kartě, aby zaměstnanci banky věděli, co vše je zapotřebí zablokovat, a pak také popsat, jak podvod probíhal.*“[77]

V závěru je třeba dodat, že jelikož kybernetická kriminalita často přesahuje hranice jednotlivých států, je žádoucí i spolupráce na úrovni mezinárodní. K tomu Kapr v rozhovoru ČR uvedl:

---

[76] *Přístup k datům z mobilních telefonů*. Online. In: Policie České republiky. 2021. Dostupné z: https://www.policie.cz/clanek/pristup-k-datum-z-mobilnich-telefonu.aspx. [cit. 2024-02-05].
[77] *Falešná SMS může stát tisíce korun. Co dělat, když jste naletěli?* Online. In: Seznam Zprávy. 2023. Dostupné z: https://www.seznamzpravy.cz/ clanek/tech-technologie-falesna-sms-muze-stat-tisice-korun-co-delat-když-jste-naleteli-225927. [cit. 2024-02-03].

„V některých případech spolupracujeme i na mezinárodní úrovni. A to při vyžadování údajů od zahraničních subjektů. Dále jsou v některých případech tvořeny mezinárodní vyšetřovací týmy, a to v případech, kdy konkrétní skupina pachatelů páchá trestnou činnost na území více států. Některé získané poznatky předáváme i do Europolu EC3, kde se snažíme získat poznatky, zda nebyla obdobná trestná činnost se stejnými atributy řešena i policejními orgány v jiných evropských státech. S kolegy z jiných států spolupracujeme, a to v rámci jednotlivých sérií i obecně. Snažíme se navzájem varovat před novými hrozbami a předáváme si poznatky o možnostech prověřování.“

2.2.8 Problémy v objasňování phishingových útoků

První komplikací v objasňování phishingových útoků je specifičnost typických stop. Dalo by se říci, že klíčovou roli zde představují stopy digitální, jež však nemají dlouhou životnost a mohou být manipulovatelné útočníkem.[78] Při ohledání zařízení, jež je důkazním prostředkem, je nejprve třeba zjistit, zda byl phishingový útok spáchán za pomoci malware a pokud ano, znemožnit útočníkovi pomocí malwaru páchat další škodu. Otázkou zde zůstává, zda zkoumané zařízení odpojit od sítě či nikoli. Za předpokladu, že se neodpojí, může být uživateli napáchána další škoda. Odpojení se tedy jeví jako lepší varianta, avšak určitý druh malwaru pozná, že je odpojen od sítě a nadále se neprojevuje, jeho přítomnost tedy není zjistitelná. Dále je třeba rozhodnout, jakým způsobem budou data získána, přičemž by se mělo vždy postupovat co nejrychleji a s co nejmenším škodami.

Vždy by se měla zvážit přítomnost odborníka na informační a komunikační technologie na místě ohledání, ať už by se jednalo o firemní IT oddělení, CSIRT tým či forenzní analytiky.[79]

---

[78] PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty*. 2. dopl. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-741-2. s. 967 srov. s. 972

[79] ČERMÁK, Miroslav. Úskalí zajišťování digitálních stop v případě podezření na trestný čin neoprávněného přístupu k počítačovému systému. Online. *Bezpečnostní teorie a praxe*. 2019, roč. 19, čís. 3. ISSN 1801-8211. Dostupné z: https://veda.polac.cz/wp-content/uploads/2020/01/%C3%9Askal%C3%AD-zaji%C5%A1%C5%A5ov%C3%A1n%C3%AD-digit%C3%A1ln%C3%ADch-stop-v-p%C5%99%C3%ADpad%C4%9B-podez%C5%99en%C3%AD-na-trestn%C3%BD-%C4%8Din-neopr%C3%A1vn%C4%9Bn%C3%A9ho-p%C5%99%C3%ADstupu-k-po%C4%8D%C3%ADta%C4%8Dov%C3%A9mu-syst%C3%A9mu.pdf. [cit. 2024-02-06].

Druhý problém vychází z faktu, že phishingové útoky často překračují hranice jednotlivých států. Je tedy třeba při jejich objasňování spolupracovat s jinými státy. Mezinárodní spolupráce komplikují jak rozdílnosti v trestním právu hmotném, tak v trestním právu procesním. Za problematickou je zde považována zejména časová náročnost procesních postupů při spolupráci s jinými státy, jelikož procesní úkon, který by dle našeho trestního řádu trval několik dní, může ve spolupráci s jinými státy trvat i několik měsíců z důvodu neexistence lhůt, jejich rozdílné délky či neochoty spolupracovat. To je značně neefektivní vzhledem k faktu, že digitální stopy mají krátkou životnost a potřebují být tedy zajištěny v co nejkratším čase. Rozdílnosti v trestním právu hmotném v oblasti kyberkriminality mají sjednotit mezinárodní, regionální a dvoustranné úmluvy, vzorové právo či směrnice v rámci Evropské unie. Patrně nejvýznamnější z nich je Úmluva o počítačové kriminalitě Rady Evropy, kterou ČR ratifikovala v roce 2013. Úmluva mimo hmotněprávní úpravu zahrnuje i úpravu procesní. Trestně procesní mezistátní úpravu umožňuje kromě výše zmíněné úmluvy např. směrnice o evropském vyšetřovacím příkazu,[80] která upravuje proces dokazování v rámci Evropské unie od 22. 5. 2017.[81] Dále je klíčová spolupráce prostřednictvím mezinárodních organizací, příkladmo Europol a Interpol a také kyberbezpečnostními orgány a CSIRT týmy jednotlivých států.[82]

Právě díky podstatě digitálních stop, jejich rychlému zániku a možnosti s nimi manipulovat v kombinaci s faktem, že většina phishingových útoků je páchána mezistátně, je patrně největším problémem při objasňování právě nedostatek důkazů, které by vedly k dopadení pachatele. To bohužel způsobuje nedůvěru

[80] STUPKA, Václav. *Kyberkriminalita jako mezinárodní problém*. Online. In: Masarykova univerzita. 2021. Dostupné z: https://is.muni.cz/el/law/ jaro2021/LI301Zk/109981614/kyberkiminalita_jako_mezinarodni_problem_xcgtwfeu.pdf. [cit. 2024-02-06].

[81] PIKNA, Bohumil. Evropský vyšetřovací příkaz, nový unijní nástroj justiční spolupráce. Online. *Bezpečnostní teorie a praxe*. 2017, roč. 17, čís. 3. ISSN 1801-8211. Dostupné z: https://veda.polac.cz/wp-content/uploads/2018/11/032017Evropsk%C3%BD-vy%C5%A1et%C5%9 9ovac%C3%AD-p%C5%99%C3%ADkaz-nov%C3%BD-unijn%C3%AD-n%C3%A1stroj-justi%C4%8Dn%C3%AD-spolupr%C3%A1ce.pdf. [cit. 2024-02-06].

[82] STUPKA, Václav. *Kyberkriminalita jako mezinárodní problém*. Online. In: Masarykova univerzita. 2021. Dostupné z: https://is.muni.cz/el/law/ jaro2021/LI301Zk/109981614/kyberkiminalita_jako_mezinarodni_problem_xcgtwfeu.pdf. [cit. 2024-02-06].

občanů a institucí k objasnění případu. Mnoho útoků proto není Policii ČR ani nahlášeno a velká část kybernetické kriminality tak zůstává latentní.[83]

2.3 Ochrana před podvodnými útoky v informačních a komunikačních technologiích

Phishing a jiné jemu podobné podvodné útoky se řadí mezi nejefektivnější kybernetické útoky. Je tomu tak proto, že díky metodám sociálního inženýrství neútočí pouze na informační a komunikační technologie jako takové, ale i na osobu uživatele. Systém prevence tedy není závislý pouze na softwarovém a hardwarovém vybavení elektrotechnických zařízení, ale i na lidském faktoru, přičemž právě ten představuje nejslabší článek ochrany. V této kapitole budou stručně představeny prostředky ochrany před těmito útoky, s důrazem na ty, které jsou závislé na lidském faktoru.

2.3.1 Softwarové zabezpečení

Mezi základní nástroj ochrany elektrotechnických zařízení lze považovat hardwarové a softwarové zabezpečení. Vzhledem k povaze této práce se tato kapitola bude dále zaměřovat pouze na zabezpečení pomocí softwaru. Mezi jeho nejzákladnější varianty lze zařadit firewall a antivirový program. Firewall je bezpečnostní systém, který slouží ke kontrolování a omezování síťového provozu na základě předdefinovaných kritérií. Firewall může být jak hardwarový (modem), tak softwarový, jenž bývá součástí operačních systémů (Microsoft Windows apod.).[84] Jeho účelem je chránit zařízení připojené k síti tedy před škodlivými vlivy zvenčí. Odlišnou funkci představuje tzv. virtuální privátní síť (dále jen VPN), jejímž cílem je chránit data, která jsou odesílána a přijímána přes síť. Data, která jsou uživatelem odesílána, procházejí serverem VPN, který poskytuje uživateli novou IP adresu, jež skrývá jeho skutečnou polohu a identitu. Toho využívají i útočníci

[83] KUCHTA, Josef. Aktuální problémy počítačové kriminality včetně její prevence. Online. *Časopis pro právní vědu a praxi*. 2016, roč. 24, čís. 1. ISSN 1805-2789. Dostupné z: https://journals.muni.cz/cpvp/article/ view/5260/4344. [cit. 2024-02-06].

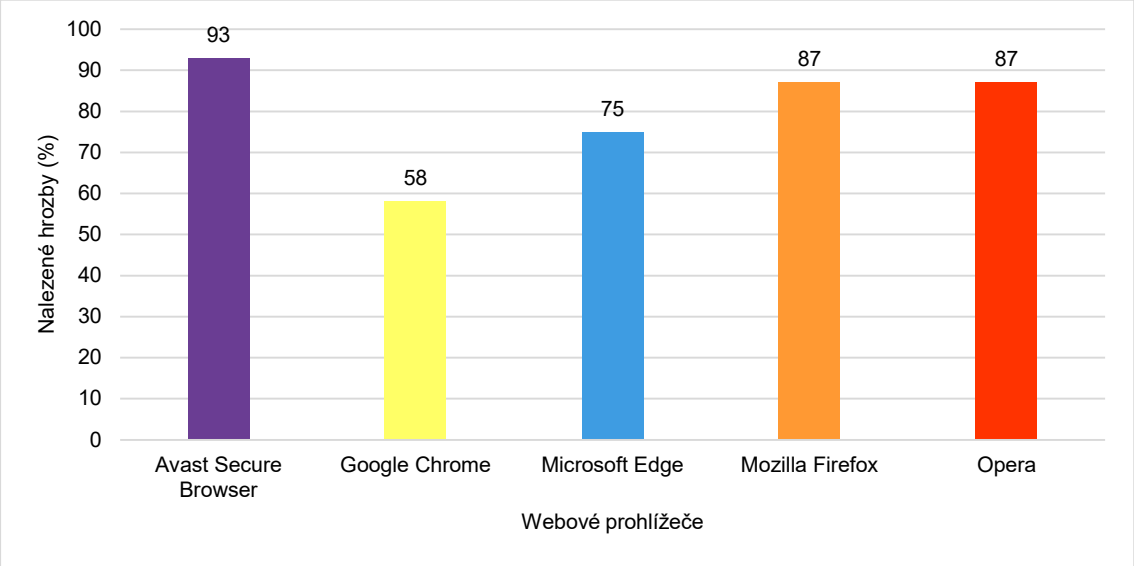
[84] *Co je brána Firewall?* Online. In: Microsoft. Dostupné z: https://support.microsoft.com/cs-cz/office/co-je-br%C3%A1na-firewall-6870c88d-69b6-4db4-9cb1-0e4afa7a8603. [cit. 2024-02-09].

při páchání kybernetických útoků. Vytvoření VPN umožňuje také bezpečné připojení na veřejných sítích, bezpečný přenos dat či vzdálený přístup k privátním sítím.[85] Antivirový program je bezpečnostní systém, jehož úkolem je identifikovat a eliminovat škodlivý software. Dříve tento systém fungoval na základě detekce charakteristických řetězců, tzv. signatury viru, tedy na základě předdefinovaných kritérií. Dnes antivirový systém využívá strojového učení spolu s využitím dalších metod, které s sebou přináší nové technologie jako je emulace kódu, heuristika a analýza chování. Tyto technologie umožňují antivirovému programu nejen detekovat hrozby dle předdefinovaných kritérií, nýbrž i rozpoznat hrozby nové, dosud neznámé. Moderní antivirové programy s více vrstvami pokročilých technologií jsou schopné identifikovat a eliminovat ransomware, spyware, spam, a dokonce i phishing a jemu podobné podvodné útoky.[86]

Neméně důležitou roli v zabezpečení před phishingovými útoky představuje webový prohlížeč. Každý webový prohlížeč disponuje vlastními, odlišnými bezpečnostními opatřeními proti různým kybernetickým hrozbám, včetně phishingových útoků. Společnost AV-Comparatives provedla v dubnu 2023 nezávislé testování webových prohlížečů v závislosti na jejich zabezpečení proti phishingovým útokům. Na testování bylo použito 250 phishingových URL adres a 250 bezpečných URL adres. Testovány byly tyto webové prohlížeče: Avast Secure Browser, Google Chrome, Microsoft Edge, Mozilla Firefox a Opera. Nejlépe se umístil Avast Secure Browser, který rozpoznal a zablokoval 93 % testovaných hrozeb. Nejhůře se umístil Google Chrome, jenž detekoval a zablokoval pouze 53 % testovaných hrozeb.[87] Zde je na místě dodat, že Google

[85] *Co to je VPN a proč si ji pořídit?* Online. In: Eset. Dostupné z: https://www.eset.com/cz/vpn/. [cit. 2024-02-09].
[86] *Antivirus*. Online. In: Eset. Dostupné z: https://www.eset.com/cz/antivirus-software/. [cit. 2024-02-10].
[87] *Independent Tests of Anti-Virus Software*. Online. In: AV-Comparatives. 2023. Dostupné z: https://www.av-comparatives.org/wp-content/uploads/2023/05/gen_phishing_04-2023.pdf. [cit. 2024-02-11].

Chrome je dlouhodobě nejužívanějším prohlížečem na světě. K lednu 2024 ho využívalo 64 % uživatelů.[88]



Graf 2 - Grafické znázornění webových prohlížečů v závislosti na procentuálním vyjádření nalezených a zablokovaných hrozeb[89]

Vývoj webových prohlížečů je velmi dynamický a výsledky výzkumu mohou být ke dni jeho citování již zastaralé. Některé z nich poskytují navíc zdarma nadstandartní zabezpečení náročnějším uživatelům. Příkladmo webový prohlížeč Google Chrome v roce 2020 zavedl nové bezpečnostní opatření, tzv. vylepšené bezpečné prohlížení, jež umožňuje poskytování kontroly zabezpečení v reálném čase. Tato možnost výrazně urychluje proces detekování hrozeb. V základní bezpečnostní verzi je seznam nebezpečných URL adres hostován lokálně a při kontrole obsahuje pouze adresy zde dostupné po poslední aktualizaci. Phishingové stránky však velice rychle vznikají a zanikají, a proto tento způsob není příliš efektivní. Princip vylepšeného bezpečnostního prohlížení je založen na

[88] *Browser Market Share Worldwide*. Online. In: Statcounter. Dostupné z: https://gs.statcounter.com/. [cit. 2024-02-11].
[89] *Independent Tests of Anti-Virus Software*. Online. In: AV-Comparatives. 2023. Dostupné z: https://www.av-comparatives.org/wp-content/uploads/2023/05/gen_phishing_04-2023.pdf. [cit. 2024-02-11].

kontrole cloudové databáze Google v reálném čase, tedy bez časové prodlevy. To umožňuje srovnávat reálnou situaci vždy s těmi nejaktuálnějšími daty.[90]

Možností, jak se chránit pomocí softwaru před phishingovými útoky, je ještě mnoho, přestože zejména v poslední době je v rámci efektivnosti tendence k tomu co nejvíce bezpečnostních prvků obsáhnout do jednoho programu, např. antivirového. Pokrok v informačních a komunikačních technologiích a zejména v útocích na ně si však vyžaduje pořád nové formy softwarové ochrany reagující na nové, konkrétní hrozby. Kromě výše vyjmenovaných softwarových bezpečnostních opatření tedy existuje mnoho dalších, jež nejsou tak komplexní jako firewall či antivirový program, nicméně fungují na obdobných principech a plní podobné funkce. Mnohdy se hranice mezi nimi stírají a jeden obsahuje zároveň druhý. Takovým příkladem může být např. spam filtr, jehož úkolem je identifikovat e-maily, které by mohly obsahovat malware, tedy mj. phishingové e-maily s přílohou. Spam filtr obyčejně tvoří součást bezpečnostních prvků většiny poskytovatelů e-mailových služeb, stejně tak může být součástí rozsáhlého antivirového programu či fungovat jako samostatný softwarový program. I proti jiným formám phishingových útoků dnes existuje řada zajímavých bezpečnostních prvků, příkladem mohou být aplikace do mobilního telefonu na skenování QR kódů, které umožňují např. náhled cílové adresy URL, což může uživatele ochránit před stažením malwaru. I tyto aplikace však mohou být užity jako prostředek pro útočníky ke stažení malwaru do zařízení uživatele.[91]

Klíčová je i problematika hesel a jejich ověřování. Nejbezpečnější variantou ověřování hesel je tzv. multifaktorová autentizace, jež spočívá v ověření identity člověka pomocí dvou či více na sobě nezávislých informací, ať už jde o hesla, informace z předmětů, které uživatel vlastní (doklady apod.) či biometrické údaje.[92]

---

[90] *Prohlížeč Chrome spustí ochranu proti phishingu v reálném čase pro všechny*. Online. In: Chip. 2023. Dostupné z: https://www.chip.cz/prohlizec-chrome-spusti-ochranu-proti-phishingu-v-realnem-case-pro-vsechny. [cit. 2024-02-11].

[91] *Quishing*. Online. In: So Safe. Dostupné z: https://sosafe-awareness.com/glossary/quishing/. [cit. 2024-01-18].

[92] *Dvoufaktorová autentizace*. In: Forensee [online]. [cit. 2024-02-12]. Dostupné z: https://www.forensee.cz/2020/11/18/dvoufaktorova-autentizace/

2.3.2 Lidský faktor

Existuje mnoho možností, jak pomocí technologií zabezpečit své elektrotechnické zařízení před kybernetickými hrozbami. Podvodné útoky však necílí pouze na elektrotechnické zařízení jako takové, jako spíše na člověka, který ho ovládá. Softwarové programy sice mohou do určité míry rozpoznat přítomnost malwaru, podvodnou webovou stránku či jiné varovné náznaky a tím člověka ochránit ještě před prvním setkáním s podvodnou stránkou či malwarem napadeným souborem, nicméně je třeba si uvědomit dvě skutečnosti. Prvně i ten nejlepší softwarový program může selhat a zadruhé je v drtivé většině phishingový útok spáchán za nechtěné spoluúčasti člověka (zadáním údajů do podvržené webové stránky apod.). Jinými slovy technologická ochrana pomůže zpravidla zabránit jakési prvé fázi útoku, zatímco druhá fáze spočívá ve správném vyhodnocení situace člověkem. V mnoha případech, typicky při vishingových útocích či u deepfake phishingu, tedy zjednodušeně řečeno u útoků s hojným využitím umělé inteligence, zatím neexistuje hojně rozšířený systém technologické prevence. Dalo by se tedy říci, že jediným bezpečnostním prvkem je zde člověk sám. Důležitost problematiky lidského faktoru začíná v posledních letech vnímat i odborná veřejnost. Např. Desolda a kol. provedli rozsáhlý výzkum a analýzu celkem 52 odborných publikací vydaných mezi lety 2001 a 2019 na téma lidského faktoru v souvislosti s phishingovými útoky, z nějž plynou mj. některé následující poznatky.

Za nejzranitelnější oblast lidského faktoru je v první řadě považován fakt, že uživatelé si nejsou vědomi hrozeb, které se v kyberprostoru objevují, a proto jsou spokojeni s úrovní svých znalostí a svého zabezpečení tak, jak jsou. V takové situaci je nasnadě, že zájem být informován o dané problematice není dostatečný. Do vzdělávání v dané problematice je navíc třeba věnovat určitou část časových, finančních i informačních zdrojů, což mnoho uživatelů i firem odradí. Nedostatek

znalostí v této oblasti přitom může způsobit značné škody, jimž by mohl vzdělaný uživatel předejít.[93]

Zde se vybízí otázka, jak co nejefektivněji rozšiřovat povědomí o hrozbách spojených s podvodnými útoky v kyberprostoru, tak aby byli uživatelé motivováni se v dané problematice dále vzdělávat. Policie ČR participuje na řadě kampaní, jak na mezinárodní (#BuySafePaySafe, #CyberScams aj.) tak na vnitrostátní úrovni (nePINdej! či Nebuď labuť! apod.). Vnitrostátní kampaně bývají často výsledkem spolupráce Policie ČR s bankovním sektorem. Právě bankovní sektor nabízí celou řadu vzdělávacích materiálů, přičemž jejich největší výhodou je jejich aktuálnost a nenáročnost, co se časových a finančních zdrojů týče. Uživatel si snadno může přečíst přímo na webových stránkách své banky, v e-mailu, v internetovém či mobilním bankovnictvím ty nejaktuálnější hrozby. Obdobné informace poskytují i média, která informují nejen o hrozbách v kyberprostoru včetně statistik, ale i o jejich obětech a pachatelích. V dnešní době se však stále více objevují i videa a reportáže, které velice kvalitně popisují danou problematiku a zároveň reagují na potřebu společnosti vzdělávat novou formou. Kromě vzdělávání pasivní formou existuje i mnoho kurzů a testovacích programů, ať už v rámci firem, tak i pro jednotlivce, kde se uživatel může na příkladech aktivně učit. Ty však už vyžadují od uživatele či firmy větší časovou a zpravidla i finanční náročnost.

Dalo by se tedy říci, že uživatelé mají poměrně snadný přístup ke kvalitním informacím a do určité míry i ke vzdělávacím kurzům. Podvody v informačních a komunikačních technologiích jsou však stále úspěšné a je tedy třeba se nespokojit s aktuálním stavem, nýbrž se tématu prevence dále věnovat, přičemž je důležité veřejnost o těchto hrozbách správně informovat. Nejvhodnější by bylo ukázat důležitost a aktuálnost této problematiky na statistických přehledech, nejlépe i s údajem o škodách. Tyto statistiky by měly být zveřejňovány pravidelně

[93] DESOLDA, Giuseppe, et al. Human factors in phishing attacks: a systematic literature review. Online. *ACM Computing Surveys (CSUR)*. 2021, roč. 54, čís. 8. ISSN 0360-0300. Dostupné z: https://www.researchgate.net/profile/Giuseppe-Desolda/publication/361609220_Human_Factors_in_Phishing_Attacks_A_Systematic_Literature_Review/links/62bc31eaf9dee438e8cbae70/Human-Factors-in-Phishing-Attacks-A-Systematic-Literature-Review.pdf. [cit. 2024-02-06].

důvěryhodným zdrojem. V oblasti vzdělávání se jako vhodné se nabízí zařadit např. povinné preventivní programy pro děti do škol, stejně jako pořádat programy pro seniory, např. v rámci univerzit třetího věku. Možnost zlepšení na poli přibližování se uživatelovým potřebám může být i úprava stávajících bezpečnostních programů, např. změna provedení indikátorů v zabezpečovacích systémech. Výzkumy ukázaly, že varovná hlášení implementovaná v prohlížečích, které upozorňují uživatele na hrozby související s phishingem, by mohla být výrazně vylepšena. Varovná hlášení často obsahují příliš odborný jazyk, kterému běžný uživatel nemusí rozumět, a navíc se jejich vzhled nemění, uživatel si na ně tedy brzy zvykne a je pravděpodobné, že příště varovný indikátor přeskočí a vystaví se tím nebezpečí. Zajímavou metodou, jak vzdělávat uživatele, jsou různé hry a interaktivní programy, jako je PhishGuru, What.Hack, nebo školící systémy, např. Anti-Phishing Phil.[94] Další efektivní možností, jak vzdělávat uživatele např. ve firmách je rozesílání cvičných e-mailů. Všechny tyto e-maily jsou bezpečné, nicméně některé z nich imitují podvodné e-maily. Uživatel tedy není v reálném nebezpečí, pouze podezřelé e-maily označí jako hrozbu. Následně je mu podána zpětná vazba, zda e-mail označil správně či ne. Uživatel je tedy udržován pořád ve střehu a zároveň je nenásilně seznamován s novými hrozbami. Zároveň tato metoda podává zpětnou vazbu zaměstnavateli, který je lépe obeznámen s bezpečnostní situací na svém pracovišti a může následně vhodně volit kroky k jejímu zlepšení.

Nástrojů, jak zlepšit prevenci před phishingovými útoky ve vztahu k lidskému faktoru je ještě mnoho a na tomto poli je třeba ještě mnohé prozkoumat. Stejně tak jako se útočník snaží pochopit, jak lidé přemýšlí a jak se rozhodují, aby jeho útoky byly co nejefektivnější, je třeba, aby byl při vytváření preventivních opatření kladen důraz na porozumění lidem, jak uvažují a jak se rozhodují a naučit se je efektivně motivovat.

---

[94] DESOLDA, Giuseppe, et al. Human factors in phishing attacks: a systematic literature review. Online. *ACM Computing Surveys (CSUR)*. 2021, roč. 54, čís. 8. ISSN 0360-0300. Dostupné z: https://www.researchgate.net/profile/Giuseppe-Desolda/publication/361609220_Human_Factors_in_Phishing_Attacks_A_Systematic_Literature_Review/links/62bc31eaf9dee438e8cbae70/Human-Factors-in-Phishing-Attacks-A-Systematic-Literature-Review.pdf. [cit. 2024-02-06].

Závěr

Cílem této práce bylo vytvořit komplexní pohled na fenomén podvodných útoků v informačních a komunikačních technologiích se zaměřením na phishing, v současné době nejrozšířenější z nich. Smyslem práce bylo zařadit tyto útoky do kontextu kybernetické kriminality, postihnout jejich aktuálnost a důležitost v dnešním virtuálním světě. Práce se zaměřila i na phishing z pohledu jeho trestněprávní úpravy a problematiky jeho objasňování. V neposlední řadě poskytla kritický pohled na možnosti prevence proti těmto podvodným útokům.

Phishingové útoky představují specifický úsek kybernetické kriminality, jelikož se jedná o podvodné útoky, které se od těch klasických liší pouze svou formou. Odehrávají se v prostředí informačních a komunikačních technologií, tedy v nově, avšak rychle se vyvíjejícím kyberprostoru. Vyskytují se tedy na pomyslném pomezí mezi světem reálným a virtuálním. Tento jejich specifický znak je problematický v mnoha ohledech, počínaje statistickým vykazováním, přes jejich trestněprávní kvalifikaci a objasňování, prevencí konče.

Z práce vyplývá, že prostoru k lepšímu porozumění a uzpůsobení stávajících metod a prostředků je ještě mnoho, jak z pohledu trestně-právního, tak i v oblasti objasňování. Budoucí výzkumy na poli právním by mohly být zaměřeny na aktualizaci norem tuzemského práva trestního za účelem přiléhavější kvalifikace phishingového útoku, stejně tak na normy práva mezinárodního, ve prospěch sjednocení právního pohledu na phishingové útoky a urychlení procesních opatření vedoucích k dopadení pachatelů těchto útoků.

Je však zřejmé, že i navzdory snaze odborníků v oblasti práva či policejních orgánů co nejvíce zlepšit a zefektivnit prostředky pro boj proti tomuto druhu kybernetické kriminality, phishing bude stále v dnešní společnosti hojně zastoupen a jeho objasňování vždy ztížené. Je proto třeba zaměřit se předně na prevenci před těmito útoky. Větší pozornost by tedy měla být věnována lidskému faktoru jakožto nejslabšímu článku ochrany proti těmto podvodným útokům. Co platí o phishingových útocích dnes, nemusí platit zítra. Společnost tedy musí být stále ve střehu, připravena čelit novým hrozbám. Je proto žádoucí, aby se odborná

veřejnost touto problematikou dále zaobírala, přicházela s novými nápady a udržela společnost motivovanou k dalšímu vzdělávání v této problematice. Útočník bude sice vždy o krok napřed, nicméně my jako společnost můžeme tyto kroky předvídat a na boj proti těmto podvodným útokům se adekvátně připravit.

SEZNAM POUŽITÝCH ZDROJŮ

Monografie

1. DONÁT, Josef; TOMÍŠEK, Jan. *Právo v síti: průvodce právem na internetu*. 1. vyd. Praha: C.H. Beck, 2016. ISBN 978-80-7400-610-4.
2. KOLOUCH, Jan; BAŠTA, Pavel a kol. *CyberSecurity*. 1. vyd. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.
3. KOLOUCH, Jan. *CyberCrime*. 1. vyd. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7.
4. PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty.* 2. dopl. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-741-2.
5. SEDLÁK, Petr; KONEČNÝ, Martin a kol. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. 1. vyd. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

Zákonná úprava

1. Zákon č. 141/1961 Sb., *o trestním řízení soudním* v posledním znění
2. Zákon č. 181/2014 Sb., *o kybernetické bezpečnosti* v posledním znění
3. Zákon č. 273/2008 Sb., o *Policii ČR* v posledním znění
4. Zákon č. 370/2017 Sb., *o platebním styku* v posledním znění
5. Zákon č. 40/2009 Sb., *trestní zákoník* v posledním znění

Elektronické zdroje

1. ČERMÁK, Miroslav. Úskalí zajišťování digitálních stop v případě podezření na trestný čin neoprávněného přístupu k počítačovému systému. Online. *Bezpečnostní teorie a praxe*. 2019, roč. 19, čís. 3. ISSN 1801-8211. Dostupné z: https://veda.polac.cz/wpcontent/uploads/2020/01/%C3%9Askal%C3%AD-zaji%C5%A1%C5%A5ov%C3%A1n%C3%AD-digit%C3%A1ln%C3%ADch-stop-v-p%C5%99%C3%ADpad%C4%9B-podez%C5%99en%C3%AD-na-trestn%C3%BD-%C4%8Din-neopr%C3%A1vn%C4%9Bn%C3%A9ho-p%C5%99%C3%ADstupu-k-po%C4%8D%C3%ADta%C4%8Dov%C3%A9mu-syst%C3%A9mu.pdf. [cit. 2024-02-06].

2. DESOLDA, Giuseppe, et al. Human factors in phishing attacks: a systematic literature review. Online. *ACM Computing Surveys (CSUR).* 2021, roč. 54, čís. 8. ISSN 0360-0300. Dostupné z: https://www.researchgate.net/profile/Giuseppe-Desolda/publication/361609220_Human_Factors_in_Phishing_Attacks_A_Systematic_Literature_Review/links/62bc31eaf9dee438e8cbae70/Human-Factors-in-Phishing-Attacks-A-Systematic-Literature-Review.pdf. [cit. 2024-02-06].
3. JONÁŠOVÁ, Eliška. Aktuální kybernetické hrozby a odpovídající právní úprava v Evropské unii a v Kanadě. Online. *Bezpečnostní teorie a praxe*. 2018, roč. 18, čís. 3. ISSN 1801-8211. Dostupné z: https://veda.polac.cz/wp-content/uploads/2019/04/032018_Aktu%C3%A1ln%C3%AD-kybernetick%C3%A9-hrozby-a-odpov%C3%ADdaj%C3%ADc%C3%AD-pr%C3%A1vn%C3%AD-%C3%BApravа-v-Evropsk%C3%A9-unii-a-v-Kanad%C4%9B.pdf. [cit. 2024-01-23].
4. KRUPIČKA, Jiří. Kybernetická kriminalita. Online. *Acta Universitatis Carolinae.* 2012, roč. 58, čís. 4. ISSN 0323-0619. Dostupné z: https://www.prf.cuni.cz/dokumenty-download/1404048928/. [cit. 2.9. 2018].
5. KUCHTA, Josef. Aktuální problémy počítačové kriminality včetně její prevence. Online. *Časopis pro právní vědu a praxi*. 2016, roč. 24, čís. 1. ISSN 1805-2789. Dostupné z: https://journals.muni.cz/cpvp/article/view/5260/4344. [cit. 2024-02-06].
6. PATIL, Kundan, et al. *Deepfake detection using biological features: a survey.* Online. In: ArXiv preprint arXiv:2301.05819. 2023. Dostupné z: https://arxiv.org/abs/2301.05819. [cit. 2024-01-22].
7. PIKNA, Bohumil. Evropský vyšetřovací příkaz, nový unijní nástroj justiční spolupráce. Online. *Bezpečnostní teorie a praxe*. 2017, roč. 17, čís. 3. ISSN 1801-8211. Dostupné z: https://veda.polac.cz/wp-content/uploads/2018/11/032017Evropsk%C3%BD-vy%C5%A1et%C5%99ovac%C3%AD-p%C5%99%C3%ADkaz-nov%C3%BD-unijn%C3%AD-n%C3%A1stroj-justi%C4%8Dn%C3%AD-spolupr%C3%A1ce.pdf. [cit. 2024-02-06].

8. STUPKA, Václav. *Kyberkriminalita jako mezinárodní problém*. Online. In: Masarykova univerzita. 2021. Dostupné z: https://is.muni.cz/el/law/jaro2021/LI301Zk/109981614/kyberkiminalita_jako_mezinarodni_problem_xcgtwfeu.pdf. [cit. 2024-02-06].

Webové stránky

1. *Antivirus*. Online. In: Eset. Dostupné z: https://www.eset.com/cz/antivirus-software/. [cit. 2024-02-10].
2. *Browser Market Share Worldwide*. Online. In: Statcounter. Dostupné z: https://gs.statcounter.com/. [cit. 2024-02-11].
3. *Co je brána Firewall?* Online. In: Microsoft. Dostupné z: https://support.microsoft.com/cs-cz/office/co-je-br%C3%A1na-firewall-6870c88d-69b6-4db4-9cb1-0e4afa7a8603. [cit. 2024-02-09].
4. *Co je smishing*. Online. In: Moneta. Dostupné z: https://www.moneta.cz/slovnik-pojmu/detail/smishing. [cit. 2024-01-15].
5. *Co to je VPN a proč si ji pořídit?* Online. In: Eset. Dostupné z: https://www.eset.com/cz/vpn/. [cit. 2024-02-09].
6. *Deepfake detection*. Online. In: European Data Protection Supervisor. Dostupné z: https://edps.europa.eu/data-protection/technology-monitoring/techsonar/deepfake-detection_en?etrans=cs. [cit. 2024-01-22].
7. *Falešná SMS může stát tisíce korun. Co dělat, když jste naletěli?* Online. In: Seznam Zprávy. 2023. Dostupné z: https://www.seznamzpravy.cz/clanek/tech-technologie-falesna-sms-muze-stat-tisice-korun-co-delat-když-jste-naleteli-225927. [cit. 2024-02-03].
8. *History of Phishing*. Online. Phishing. Dostupné z: https://www.phishing.org/history-of-phishing. [cit. 2023-11-19].
9. *History of Phishing: How Phishing Attacks Evolved From Poorly Constructed Attempts To Highly Sophisticated Attacks*. Online. In: Phish Protection. Dostupné z: https://www.phishprotection.com/resources/history-of-phishing. [cit. 2023-11-19].

10. *Independent Tests of Anti-Virus Software*. Online. In: AV-Comparatives. 2023. Dostupné z: https://www.av-comparatives.org/wp-content/uploads/2023/05/gen_phishing_04-2023.pdf. [cit. 2024-02-11].
11. *Internetem se opět šíří podvodné reklamy na investice do akcií ČEZu.* Online. In: Fakticky.cz. Dostupné z: https://fakticky.cz/internetem-se-opet-siri-podvodne-reklamy-na-investice-do-akcii-cezu/. [cit. 2024-03-10].
12. *Investiční podvody – strategická analýza*. Online. In: Finanční analytický úřad. 2021. Dostupné z: https://fau.gov.cz/files/investicni-podvody-strategicka-analyza.pdf. [cit. 2023-11-12].
13. *Investiční podvody*. Online. In: Air Bank. Dostupné z: https://www.airbank.cz/co-vas-nejvic-zajima/investicni-podvody/. [cit. 2023-11-12].
14. *Kyberkriminalita*. Online. In: Policie České republiky. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx. [cit. 2023-10-22].
15. *Kybernetičtí podvodníci přitvrzují, proto se Komerční banka znovu zapojila do kampaně nePINdej*. Online. In: Komerční banka. 2023. Dostupné z: https://www.kb.cz/cs/o-bance/tiskove-zpravy/kyberneticti-podvodnici-pritvrzuji-proto-se-komercni-banka-znovu-zapojila-do-kampane-nepindej. [cit. 2023-11-12].
16. *Napadená zařízení okamžitě odpojte od internetu, říká major Valíček*. Online. In: O2 CyberNews. 2023. Dostupné z: https://o2cybernews.cz/clanky/prevence-je-zaklad-obrany-proti-kyberutokum-rika-policista. [cit. 2024-02-03].
17. *Národní centrála proti terorismu, extremismu a kybernetické kriminalitě SKPV*. Online. In: Policie České republiky. Dostupné z: https://www.policie.cz/clanek/narodni-centrala-proti-terorismu-extremismu-a-kyberneticke-kriminalite.aspx. [cit. 2023-12-09].
18. *Nový druh internetového podvodu.* Online. In: Policie České republiky. 2022. Dostupné z: https://www.policie.cz/clanek/sprava-jihoceskeho-kraje-zpravodajstvi-novy-druh-internetoveho-podvodu.aspx. [cit. 2023-11-27].
19. *Ochrana před útoky phishing.* Online. In: Microsoft. Dostupné z: https://support.microsoft.com/cs-cz/windows/ochrana-p%C5%99ed-%C3%BAtoky-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44. [cit. 2024-02-17].

20. *Phishing není jen o e-mailové komunikaci. Týká se i sociálních sítích!* Online. In: Praha 11. 2023. Dostupné z: https://www.praha11.cz/cs/mestska-cast/bezpecnost/prevence/phishing-neni-jen-o-e-mailove-komunikaci-tyka-se-i-socialnich-sitich.html. [cit. 2023-12-03].
21. *Phishing: Pozor na nebezpečné přílohy OneNote*. Online. In: HP market. 2023. Dostupné z: https://www.hpmarket.cz/document.asp?dc=onenote-phishing. [cit. 2023-11-27].
22. *Podvodná zpráva informovala o výplatě. Muž přišel o 150 tisíc*. Online. In: Jindřichohradecký deník. 2023. Dostupné z: https://jindrichohradecky.denik.cz/zlociny-a-soudy/podvodna-zprava-informovala-o-vyplate-muz-prisel-o-150-tisic-20230731.html. [cit. 2024-02-17].
23. *Podvody na Bazoši a Sbazaru: Jak prodávat na internetu bezpečně?* Online. In: Dvojklik. 2022. Dostupné z: https://www.dvojklik.cz/podvody-na-bazosi-a-sbazaru-jak-prodavat-na-internetu-bezpecne/. [cit. 2024-01-15].
24. *Prohlížeč Chrome spustí ochranu proti phishingu v reálném čase pro všechny.* Online. In: Chip. 2023. Dostupné z: https://www.chip.cz/prohlizec-chrome-spusti-ochranu-proti-phishingu-v-realnem-case-pro-vsechny. [cit. 2024-02-11].
25. *Průzkum ESET: Třetina lidí se stala cílem podvodu na internetových bazarech.* Online. In: Eset. 2022. Dostupné z: https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/pruzkum-eset-tretina-lidi-se-stala-cilem-podvodu-na-internetovych-bazarech/#_ga=2.77191125.1973274478.1705308083-786498258.1702148979. [cit. 2024-01-15].
26. *Příklad phishingového útoku v podobě SMS zprávy.* Online. In: Forensee. 2021. Dostupné z: https://www.forensee.cz/2021/05/03/priklad-phishingoveho-utoku-v-podobe-sms-zpravy/. [cit. 2024-01-15].
27. *Přístup k datům z mobilních telefonů.* Online. In: Policie České republiky. 2021. Dostupné z: https://www.policie.cz/clanek/pristup-k-datum-z-mobilnich-telefonu.aspx. [cit. 2024-02-05].
28. *Quishing*. Online. In: So Safe. Dostupné z: https://sosafe-awareness.com/glossary/quishing/. [cit. 2024-01-18].

29. *Rozvoj Policie České republiky v letech 2016-2020*. Online. In: ČT 24. 2015. Dostupné z: https://ct24.ceskatelevize.cz/sites/default/files/1757756-policie-i-1.pdf. [cit. 2024-02-18].
30. *Social Engineering 2.0: The Rise of Deepfake Phishing*. Online. In: Secure World. 2023. Dostupné z: https://www.secureworld.io/industry-news/social-engineering-deepfake-phishing. [cit. 2024-01-22].
31. *Sociální sítě, nová platforma pro útoky sociálních inženýrů.* Online. In: Hacking Lab. 2019. Dostupné z: https://hackinglab.cz/cs/blog/socialni-site-nova-platforma-pro-utoky-socialnich-inzenyru/. [cit. 2023-12-03].
32. *Šéf vygenerovaný počítačem: Jak fungují deepfakes?* Online. In: Eset. 2023. Dostupné z: https://digitalsecurityguide.eset.com/cz/sef-vygenerovany-pocitacem-jak-funguji-deepfakes. [cit. 2024-01-22].
33. *Upozornění na podvodné e-maily Phishing*. Online. In: Komerční banka. 2023. Dostupné z: https://www.kb.cz/cs/o-bance/novinky/bezpecnost/upozorneni-na-podvodne-e-maily-phishing-13-7-2023. [cit. 2023-11-27].
34. *Útočník si najde cestu i přes QR kód. Jak skenovat bezpečně?* Online. In: Dvojklik. 2022. Dostupné z: https://www.dvojklik.cz/utocnik-si-najde-cestu-i-pres-qr-kod-jak-skenovat-bezpecne/. [cit. 2024-01-18].
35. *Varování před podvodnými investicemi.* Online. In: Komerční banka. 2023. Dostupné z: https://www.kb.cz/cs/o-bance/novinky/bezpecnost/varovani-pred-podvodnymi-investicemi. [cit. 2023-11-12].
36. *Vishing.* Online. In: Eset. Dostupné z: https://www.eset.com/cz/vishing/. [cit. 2024-01-17].
37. *Vývoj registrované kriminality v roce 2022*. Online. In: Policie České republiky. 2023. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx. [cit. 2023-10-31].
38. *What is phishing and how training can prevent phishing attacks.* Online. Phishing Tackle. Dostupné z: https://phishingtackle.com/phishing/. [cit. 2023-11-19].

SEZNAM GRAFŮ

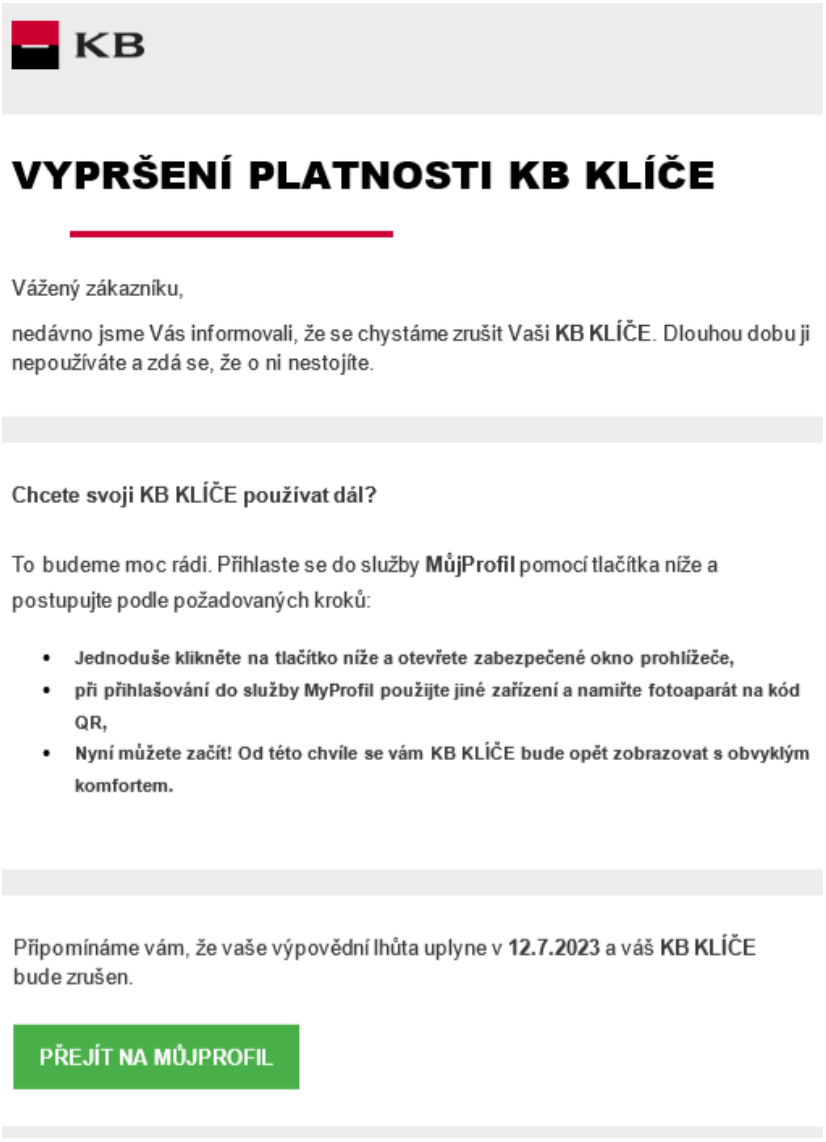
SEZNAM PŘÍLOH

PŘÍLOHY

Příloha 1 – Podvodný inzerát[95]

[95] Internetem se opět šíří podvodné reklamy na investice do akcií ČEZu. Online. In: Fakticky.cz. Dostupné z: https://fakticky.cz/internetem-se-opet-siri-podvodne-reklamy-na-investice-do-akcii-cezu/. [cit. 2024-03-10].

Příloha 2 - Phishing skrze e-mail s odkazem[96]



KB

VYPRŠENÍ PLATNOSTI KB KLÍČE

Vážený zákazníku,

nedávno jsme Vás informovali, že se chystáme zrušit Vaši **KB KLÍČE**. Dlouhou dobu ji nepoužíváte a zdá se, že o ni nestojíte.

Chcete svoji KB KLÍČE používat dál?

To budeme moc rádi. Přihlaste se do služby **MůjProfil** pomocí tlačítka níže a postupujte podle požadovaných kroků:

- **Jednoduše klikněte na tlačítko níže a otevřete zabezpečené okno prohlížeče,**
- **při přihlašování do služby MyProfil použijte jiné zařízení a namiřte fotoaparát na kód QR,**
- **Nyní můžete začít! Od této chvíle se vám KB KLÍČE bude opět zobrazovat s obvyklým komfortem.**

Připomínáme vám, že vaše výpovědní lhůta uplyne v **12.7.2023** a váš **KB KLÍČE** bude zrušen.

PŘEJÍT NA MŮJPROFIL

[96] *Upozornění na podvodné e-maily Phishing*. Online. In: Komerční banka. 2023. Dostupné z: https://www.kb.cz/cs/o-bance/novinky/bezpecnost/ upozorneni-na-podvodne-e-maily-phishing-13-7-2023. [cit. 2023-11-27].

Příloha 3 - Phishing skrze e-mail s přílohou[97]


st 13.01.2021 4:56

Fakturace a platba <daniel.chitu@primariatecuci.ro>

Potvrzení platebního příkazu

Komu undisclosed-recipients:

Vážený pane / paní

Jsme rádi, že vás můžeme informovat, že váš klient pověřil Komercní Banku správou platby faktur podrobně popsanou v přiloženém dokumentu.

S pozdravem,
Fakturace a platba

Platební příkaz.pdf

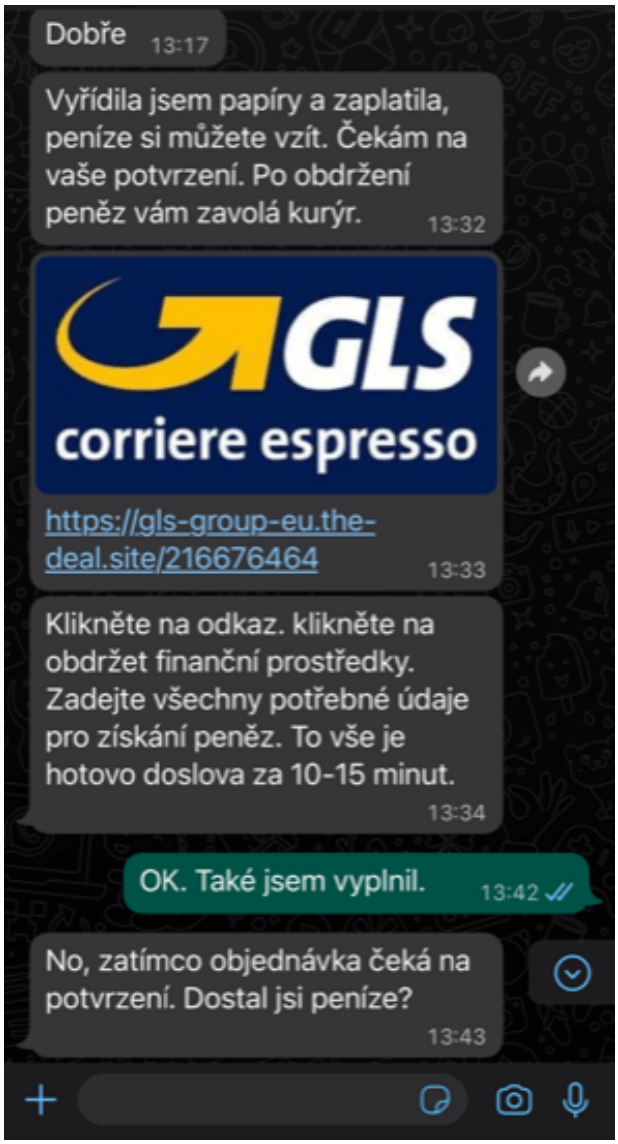
--
This message has been scanned for viruses and dangerous content by MailScanner, and is believed to be clean.

Příloha 4 - Phishing skrze sociální sítě[98]

[97] *Upozornění na podvodné e-maily Phishing*. Online. In: Komerční banka. 2023. Dostupné z: https://www.kb.cz/cs/o-bance/novinky/bezpecnost/ upozorneni-na-podvodne-e-maily-phishing-13-7-2023. [cit. 2023-11-27].

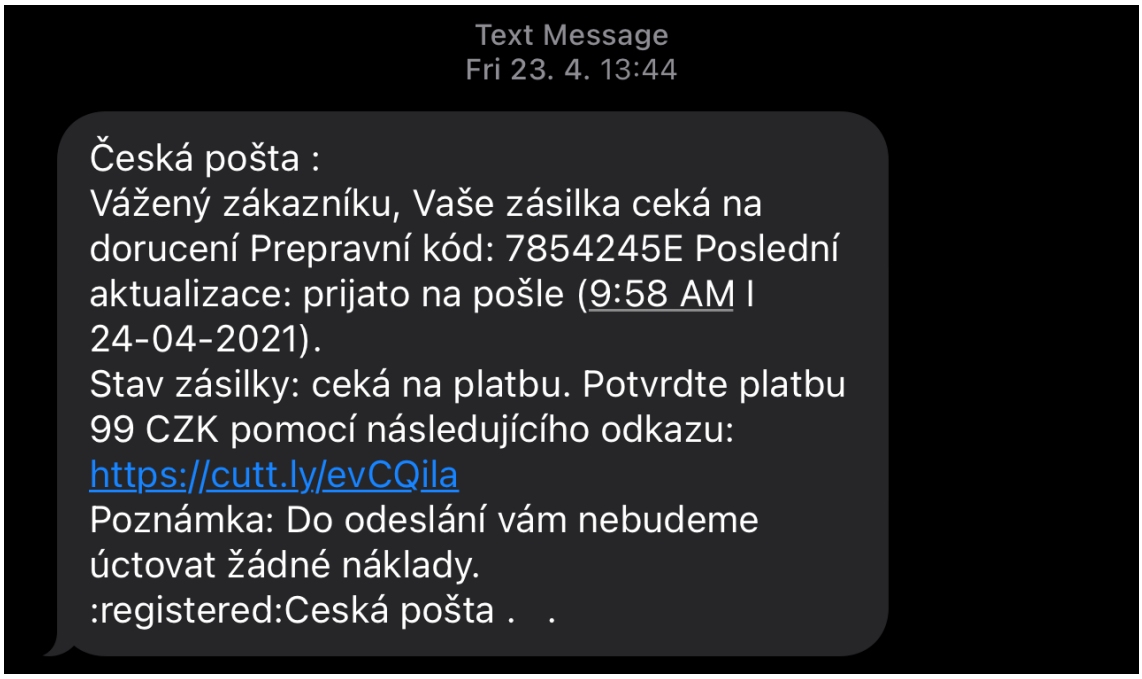
[98] *Phishing není jen o e-mailové komunikaci. Týká se i sociálních sítích!* Online. In: Praha 11. 2023. Dostupné z: https://www.praha11.cz/cs/mestska-cast/bezpecnost/prevence/phishing-neni-jen-o-e-mailove-komunikaci-tyka-se-i-socialnich-sitich.html. [cit. 2023-12-03].

Příloha 5 - Reverzní inzertní podvod[99]



[99] *Podvody na Bazoši a Sbazaru: Jak prodávat na internetu bezpečně?* Online. In: Dvojklik. 2022. Dostupné z: https://www.dvojklik.cz/podvody-na-bazosi-a-sbazaru-jak-prodavat-na-internetu-bezpecne/. [cit. 2024-01-15].

Příloha 6 - Smishing[100]



[100] *Příklad phishingového útoku v podobě SMS zprávy*. Online. In: Forensee. 2021. Dostupné z: https://www.forensee.cz/2021/05/03/priklad-phishingoveho-utoku-v-podobe-sms-zpravy/. [cit. 2024-01-15].