POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE
Fakulta bezpečnostně právní
Katedra krizového řízení

Phishing jako hrozba v oblasti kybernetické bezpečnosti

Diplomová práce

Phishing as a Threat in Cyber Security
Master thesis

VEDOUCÍ PRÁCE
Mgr. Lenka JAKUBCOVÁ Ph.D.

AUTOR PRÁCE
Bc. Jana HŮLOVÁ

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 Praze, dne 14. března 2024

Bc. Jana Hůlová

ANOTACE

Diplomová práce se zabývá problematikou phishingu jako hrozby v oblasti kybernetické bezpečnosti. Práce se skládá ze dvou hlavních částí. V teoretické části se práce zaměřuje na pojem bezpečnost, bezpečnost IT, kybernetickou bezpečnost, kybernetický prostor, data a informace. Dále zmiňuje kybernetickou bezpečnost z pohledu rozsahu, způsobu ohrožení a incidentů, s detailnějším zaměřením na phishing a jeho jednotlivé podkategorie. Následuje legislativa řešící danou problematiku a komponenty bezpečnostního systému zabývající se kybernetickou bezpečností. Poslední kapitolu tvoří případová studie se zaměřením na skupinu XDSpy užívající spearphishingové útoky. Praktická část zhodnocuje výsledky dotazníkového šetření a řízeného rozhovoru se specialistou v oboru kybernetické bezpečnosti.

KLÍČOVÁ SLOVA

kybernetická bezpečnost * phishing * hrozba * útoky * malware * osobní údaje * podvodné jednání * e-mail

ANNOTATION

The thesis deals with the issue of phishing as a threat in the field of cyber security. The thesis consists of two main parts. In the theoretical part, the thesis focuses on the concept of security, IT security, cybersecurity, cyberspace, data and information. It also mentions cybersecurity in terms of scope, threats and incidents, with a more detailed focus on phishing and its various subcategories. This is followed by legislation addressing the issue and the components of the security system dealing with cyber security. The last chapter is a case study focusing on the XDSpy group using spearphishing attacks. The practical part evaluates the results of a questionnaire survey and a guided interview with a cybersecurity specialist.

KEYWORDS

cybersecurity * phishing * threat * attacks * malware * personal data * fraudulent behavior * email

Obsah

Úvod

Téma diplomové práce bylo zvoleno z důvodu dlouhodobého studijního i profesního zájmu o problematiku kybernetické bezpečnosti. Autorka se snaží navázat na prvotní pracovní zkušenosti na pozici Trainee Security Specialist. Věnovala se oblasti krizového řízení a vzdělávání v oblasti kybernetické bezpečnosti, kde ji nejvíce oslovil phishing, který je hlavním tématem práce.

Práce se skládá ze dvou částí. Teoretickou část tvoří pět hlavních kapitol. První kapitola se věnuje vymezení základních pojmů. Druhá se zaměřuje na kybernetickou bezpečnost z pohledu rozsahu, způsobu ohrožení a incidentů. V této části je uvedena problematika hesel, včetně možnosti jejich zabezpečení, také je zde shrnuta rizikovost sociálních sítí a sledování uživatelů ve formě souborů cookies. V rámci incidentů jsou rozváděny jednotlivé kybernetické hrozby, přičemž je podrobněji věnována pozornost jednotlivým podkategoriím phishingu a současně je poukázáno na jeho nejvýznamnější nárůst v době pandemie Covid-19. Třetí kapitola je výčtem legislativy užívané v rámci kybernetické bezpečnosti. Mimo to je zde popsána nová směrnice Evropského parlamentu a Rady známá jako NIS 2, která bude v nejbližší době implementována do legislativního řádu České republiky. Čtvrtá kapitola obsahuje komponenty bezpečnostního systému České republiky zabývající se problematikou kybernetické bezpečnosti. Zahrnut je zde ústřední správní orgán, kterým je Národní úřad pro kybernetickou a informační bezpečnost společně s dalšími komponenty bezpečnostního systému České republiky. Uvedeny jsou i některé zahraniční organizace řešící danou problematiku. Poslední kapitola se zabývá případovou studií na téma XDSpy, hackerskou skupinou využívající spear phishing pro nelegální získání informací od institucí ve východní Evropě. Praktická část prezentuje metodologii a výsledky výzkumného šetření, které bylo provedeno formou dotazníkového šetření a řízeného rozhovoru se specialistou v oblasti kybernetické bezpečnosti, který se zabývá mimo jiné i vzděláváním v této oblasti. Závěrem jsou formulovány návrhy doporučení a opatření pro optimalizaci stávajícího stavu.

Cílem diplomové práce je analyzovat hrozby v oblasti kybernetické bezpečnosti se zaměřením na phishing, a na základě zjištění povědomí uživatelů

internetu o těchto hrozbách a jejich chování na internetu koncipovat návrhy a doporučení k optimalizaci tohoto chování tak, aby byli lépe chránění před hrozbou phishingového útoku. Závěry a doporučení koncipované autorkou jsou zároveň v práci ověřeny a podpořeny vyhodnocením řízeného polostrukturovaného rozhovoru se specialistou na oblast kybernetické bezpečnosti.

1. Vymezení základních pojmů vázaných na oblast kybernetické bezpečnosti

Tato kapitola definuje elementární pojmy, jejichž vymezení je nutné pro základní orientaci v problematice kybernetické bezpečnosti.

1.1 Bezpečnost

Na bezpečnost lze nahlížet z mnoha úhlů. Podrobněji je rozveden pojem bezpečnost, bezpečnost IT a kybernetická bezpečnost. Cílem tohoto rozboru je poukázání na jednotlivé odlišnosti, které v sobě jednotlivé pojmy nesou a jak jsou prezentovány.

Bezpečnost obecně lze vyložit jako: *„Stav, kdy je systém schopen odolávat známým a předvídatelným (i nenadálým) vnějším a vnitřním hrozbám, které mohou negativně působit proti jednotlivým prvkům (případně celému systému) tak, aby byla zachována struktura systému, jeho stabilita, spolehlivost a chování v souladu s cílovostí*.“[1] Z daného pojmu je tedy patrné, že se zaměřuje na širší okruh hrozeb, které se mohou stát zdrojem rizika. Nenalezneme zde přesný výčet, který by bylo možno dále použít pro potřeby této práce.

1.2 Bezpečnost IT

Zajištění udržitelnosti informační technologie (IT) zahrnuje ochranu integrity, důvěrnosti a dosažitelnosti při zpracování, úschově, distribuci a prezentaci informací.[2] Blíže se zaměřím na významné aspekty, kterými se musí tato oblast zabývat. Důvěrnost je vlastnost informace, která vypovídá o tom, zda došlo k odhalení neoprávněným jednotlivcům, entitám nebo procesům. Integritou je myšlena jistota, že data, se kterými se operuje, nebyla neoprávněně změněna a mohou být tudíž považována za důvěryhodná. Posledním je dostupnost, která je významná z důvodu použitelnosti na žádost oprávněného okruhu subjektů.[3]

---

[1] Terminologický slovník - krizové řízení a plánování obrany státu [online]. Ministerstvo vnitra České republiky: Odbor bezpečnostní politiky a prevence kriminality, 2016. Dostupné z: https://www.mvcr.cz/clanek/terminologicky-slovnik-krizove-rizeni-a-planovani-obrany-statu.aspx. [cit. 2021-11-05]. s. 5.

[2] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6, s. 28.

[3] Terminologický slovník - krizové řízení a plánování obrany státu [online]. Ministerstvo vnitra České republiky: Odbor bezpečnostní politiky a prevence kriminality, 2016. Dostupné z:

V rámci tohoto druhu bezpečnosti se již přibližujeme k prevenci před případnými hrozbami, které by mohly nastat. Je důležité poznamenat již na počátku této práce, že tím nejcennějším jsou právě informace a data, kterými se budu také následně zabývat.

1.3 Kybernetická bezpečnost

Existuje mnoho definic, které popisují tuto problematiku, autorka zde vyzdvihuje tu, kterou popisuje Výkladový slovník kybernetické bezpečnosti: „*Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru. Zajištění důvěrnosti, integrity a dostupnosti informací v kybernetickém prostoru*.“[4] Jak je již zřejmé na první pohled, opět se zde objevují aspekty, o kterých se autorka zmiňovala výše. Jde tedy o důkaz provázanosti kybernetické bezpečnosti s bezpečností IT. Interpretaci, která je použita ve slovníku, byla považována za nejvhodnější z důvodu propojení několika odlišných kategorií s cílem hájit kybernetický prostor (zkráceně kyberprostor).

1.4 Kybernetický prostor

Jedná se o digitální prostředí, ve kterém probíhá vznik, zpracování a výměna informací tvořené informačními systémy (IS), a službami a sítěmi elektronických komunikací.[5] Kyberprostor si lze představit jako nikde nezačínající ani nekončící virtuální realitu, která je však zcela závislá na technologiích, tedy materiální podstatě. Díky distribuovanosti hmotného média, jako například počítačových systémů nebo cloudových úložišť nacházejících se v reálném světě, je umožněna existence nehmotného média, jako je právě kyberprostor. Dokáže se také adaptovat v případě poškození materiálního média, ovšem v případě

https://www.mvcr.cz/clanek/terminologicky-slovnik-krizove-rizeni-a-planovani-obrany-statu.aspx. [cit. 2021-11-05], s. 5.

[4] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6, s. 97

[5] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů v posledním znění, §2.

kompletního kolapsu dojde k nenávratnému poškození nebo dokonce zániku celého kybernetického prostoru.[6]

1.5 Data a informace

Data představují opakovaně interpretovatelnou formalizovanou podobu informace, která je náležitá pro komunikaci, vyhodnocování nebo zpracování.[7] Data vytváří základ světa informací. Podoba dat může být volná, či komprimovaná, popřípadě šifrovaná, a způsob jejich uložení může být na jakémkoliv datovém nosiči nebo formátu. Z dat se stane informace, pokud dojde k dekódování (odhalení skryté informace pomocí kódu) a interpretaci. Můžeme si to tedy představit jako změnu, díky které dojde k určité transformaci.[8]

Definovat informaci není tak zcela jednoduché, neboť z pohledu několika vědních disciplín má mnoho podob. Pro účely práce je zvolena definice z §3 odst. 3 zákona o svobodném přístupu k informacím, ve kterém se uvádí: *„Informací se pro účely tohoto zákona rozumí jakýkoliv obsah nebo jeho část v jakékoliv podobě, zaznamenaný na jakémkoliv nosiči, zejména obsah písemného záznamu na listině, záznamu uloženého v elektronické podobě nebo záznamu zvukového, obrazového nebo audiovizuálního.“* [9]

Informaci lze tedy chápat poněkud „kvalifikovaněji“ nežli data. Data jsou fakta, ale informacemi se stávají tehdy, když v kontextu nesou význam pochopitelný koncovému uživateli.[10] Informace i data mají neuvěřitelný potenciál. Obsah informací může rozhodnout o další existenci jednotlivce či firmy nebo ovlivnit vývoj společnosti.[11]

---

[6] KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7, s. 36.
[7] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Aleš Čeněk, 2022. ISBN 978-80-7380-849-5, s. 45
[8] ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5, s. 14.
[9] Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, §3 odst. 3
[10] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Aleš Čeněk, 2022. ISBN 978-80-7380-849-5, s. 51.
[11] KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7, s. 13.

2. Kybernetická bezpečnost z pohledu rozsahu, způsobu ohrožení a incidentů

Před tím, než bude popsán rozsah kybernetické bezpečnosti je nutné si uvědomit kdy a kde vše začalo. Po zrodu kybernetického prostoru se stupňovitě připojovaly samotní uživatelé, výpočetní infrastruktura, poskytovatelé služeb a konektivity. Čím více bylo připojení, tím také rapidněji stoupala potencialita jeho zneužití. Velkým lákadlem pro útočníky (které platí dodnes) je to, že kyberprostor nemá žádná pravidla a je zde obtížná obrana proti útočníkům.[12] Nesmíme tedy zapomínat, že kybernetická bezpečnost je uskutečňována nejen uvnitř nikde nezačínajícího a nekončící virtuální reality, ale také mimo ni a jsou to právě lidé, kteří se ji snaží narušit.

2.1 Rozsah kybernetické bezpečnosti

Kybernetický prostor obklopuje nás všechny. Není to však jen pouhá věta, která se hodí do tohoto tématu. Musíme si uvědomit, že v dnešní digitalizované době se můžeme my všichni stát terčem ohrožení od okamžiku připojení k internetu. Od tohoto momentu se tedy z kybernetické bezpečnosti stává také kybernetická nebezpečnost, neboť se stáváme účastníky kyberprostorových aktivit, kde neexistují pravidla. Jak již bylo zmíněno výše, žijeme v digitalizované době. Pro snazší pochopení bezpečnosti v kybernetickém prostředí je zapotřebí vymezení digitalizace, která je jeho nezbytnou součástí. Digitalizaci lze formulovat jako proces přeměny informací do počítačem čitelného formátu, kde jsou informace uspořádány do bitů.[13] Bit je základní datovou jednotkou používanou ve výpočetní technice, která může nabývat pouze dvou hodnot, kterými jsou 0 a 1.[14] Tyto dvě čísla poté znázorňují výslednou prezentaci obrazu, zvuku, dokumentu apod. Subjekty, které se pohybují na internetu, tedy vidí tyto grafiky, ovšem počítač či jiné zařízení je přijímá a zpracovává jako výše uvedená čísla. Digitalizační obklopení je v dnešní době nezbytné, už jen z pohledu digitalizace veřejné správy

[12] SEDLÁK, Petr a KONEČNÝ, Martin a kol. *Kybernetická (ne)bezpečnost*. Brno: CERM akademické nakladatelství, 2021. ISBN 978-80-7623-068-2, s. 34.
[13] SEDLÁK, Petr a KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost*. Brno: CERM akademické nakladatelství, 2021. ISBN 978-80-7623-068-2, s. 16.
[14] CZ.NIC, Z. S. P. O. *Úvod do problematiky dat*. Online. 2023. Dostupné z: https://www.jaknainternet.cz/page/2596/uvod-do-problematiky-dat/. [cit. 2023-11-26].

a ukládání papírové dokumentace do elektronické podoby (skenování, archivace). Kromě této modernizace veřejné správy se také zvyšuje počet využívání informačních a komunikačních technologií (ICT) v domácnostech a mezi jednotlivci. Pro potvrzení této teorie níže demonstruji ukazatele využívání ICT, které provedl Český statistický úřad. Údaje pochází z šetření uskutečněného v řádu několika let, poslední z nich probíhalo dle nařízení Evropského parlamentu a Rady Evropské unie 2019/1700 ze dne 10. října 2019. Probíhalo prostřednictvím dotazníku, na který odpovědělo 6779 lidí ve věku od 16 let. Otázek bylo celkem 144, 7 z nich bylo zaměřeno na domácnosti a zbylé na jednotlivce.[15] Pro potřeby práce jsem vybrala pouze dva ukazatele, které nejvíce souvisely s kybernetickou bezpečností a digitalizací.

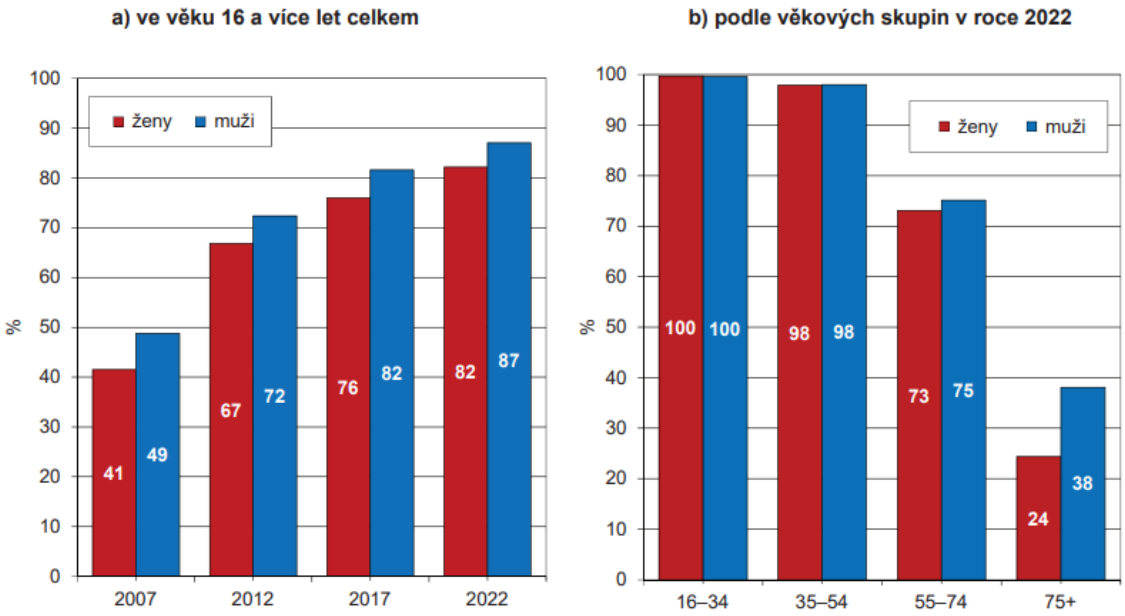
Tabulka č. 1: Procentuální ukazatel osob ve věku 16 a více let používající internet

Ukazatel	2010		2015		2019		2020		2021		2022	
	ženy	muži	ženy	muži	ženy	muži	ženy	muži	ženy	muži	ženy	muži
Celkem	**58,1**	**65,8**	**73,5**	**77,9**	**78,3**	**83,6**	**79,7**	**83,0**	**81,1**	**84,4**	**82,2**	**87,0**
Věková skupina												
16–34 let	86,7	87,2	95,9	96,2	97,3	98,1	98,7	97,7	99,3	98,4	99,7	99,6
35–54 let	72,1	74,4	91,1	90,4	96,1	95,5	96,8	96,5	97,6	96,8	97,9	98,0
55–74 let	29,0	38,6	52,0	59,1	63,0	70,9	65,8	68,8	68,9	70,9	73,1	75,1
75+ let	2,5	9,1	5,6	17,6	12,9	26,5	15,0	26,2	17,3	30,0	24,3	38,1
Vzdělání (25-64 let)												
střední bez maturity a nižší	41,7	55,3	70,5	76,2	82,8	86,2	85,3	86,9	87,6	88,5	89,7	91,5
střední s maturitou	83,1	84,3	94,0	96,2	97,7	97,9	97,5	98,3	98,5	97,9	98,4	98,7
vysokoškolské	94,6	96,8	99,2	99,6	99,6	99,7	99,5	99,0	99,8	99,5	100,0	99,8
Ekonomická aktivita												
zaměstnaní	77,1	78,3	91,9	91,5	96,7	96,1	96,7	95,8	97,4	96,7	97,9	97,2
mateřská / rodičovská dovolená	84,8	.	94,2	.	96,0	.	97,9	.	98,3	.	99,0	.
studenti	97,6	97,4	99,7	98,3	98,1	99,5	100,0	100,0	100,0	100,0	100,0	100,0
starobní důchodci	14,8	19,3	29,5	37,2	37,1	45,9	40,8	44,4	44,0	47,7	46,7	53,5

Zdroj: Český statistický úřad, Roční výběrové šetření o ICT v domácnostech

[15] MANA, Martin. ŽENY, MUŽI A DIGITALIZACE. Online. *Český statistický úřad*. 2023, č. CSU-007576/2023-63, article 062053-23, s. 1-41. ISSN 978-80-250-3417-0. Dostupné z: Odbor statistik rozvoje bezpečnosti, https://www.czso.cz/documents/10180/215504666/06205323.pdf/0cf505ab-bbdd-4005-bf25-98d5691b5576?version=1.1. [cit. 2023-11-26], s. 5-10.

Graf č. 1: Procentuální ukazatel žen a mužů používajících internet



Zdroj: Český statistický úřad

Jak je možné vidět, v řádu let se stupňuje počet uživatelů internetu. Tito uživatelé mohou využívat sociální sítě, nákupy na internetu nebo internetové bankovnictví. Všechny tyto aktivity jsou také předmětem kybernetické bezpečnosti. Při užívání internetu je zapotřebí mít na paměti také prosazování kybernetické bezpečnosti pomocí principů, které jsou nazývány triády. Některé zdroje je uvádějí jako CIA triády, kde C znamená Confidentiality neboli důvěrnost, I jako Integrity čili celistvost a poslední A jako Availability, v překladu dostupnost. Pod důvěrnost nepochybně spadá, že k informaci mají přístup pouze oprávněné osoby, vylučuje tak zneužití informace. Celistvost představuje informaci, která byla doručena uživateli bez nežádoucích úprav či změn. Jedná se tedy o zajištění neporušitelnosti, správnosti a úplnosti informací v informačních systémech. Dostupnost znamená, že v případě potřeby může oprávněný uživatel získat data ze systému. Cílem kybernetické bezpečnosti je tedy ochrana těchto principů, aby byla zachována veškerá data a informace, a nedošlo k jejich změně, zneužití nebo ztrátě.[16] Cílem útočníků, kteří páchají kybernetickou kriminalitu, je dosažení opaku této triády, neboli nabytí DAD triády. Ta je v složena z Disclosure – odhalení, Alteration – modifikace a Destruction – zničení. Následky této triády mohou být

[16] APTIEN.COM. *Co je CIA triáda informační bezpečnosti*. Online. 2023. Dostupné z: https://aptien.com/cs/kb/articles/what-is-cia-triad. [cit. 2023-11-26].

katastrofální. Může dojít k únikům dat, krádeži identity uživatelů, nabourání do firemních systémů, finanční ztrátě apod.[17]

2.2 Způsoby ohrožení kybernetické bezpečnosti

V dnešní době se mnoho z nás pohybuje na internetu. Ovšem, že mnoho z nás ví, jaké jim může hrozit nebezpečí. S přibývajícími uživateli se ale tyto hrozby zvyšují a je tak méně osob, které umí skutečně odhalit, jaké nástrahy na ně mohou být nastraženy. Nesmíme však opomínat, že jednotlivci tvoří také jednotky základu různých společností a firem. Právě tito neopatrní, neproškolení nebo neznalí jednotlivci se často stávají zdrojem zkázy. Mnoho firem opomíjí školení na téma kybernetické bezpečnosti, která je však v dnešní době nezbytností. Je zapotřebí, aby se chránili nejen jedinci samotní, ale také celé kolektivy jako například zaměstnanci.

2.2.1 Hesla

V oblasti kybernetické bezpečnosti hrají významnou roli hesla, která používáme ať už na sociálních sítích, herních serverech nebo v internetovém bankovnictví. Hesla lze rozdělit na několik kategorií a probrat jednotlivé chyby v jejich tvorbě. Úplně základně můžeme hesla rozdělit na slabá a silná. Slabá hesla se vyznačují nízkým počtem znaků (v řádu jednotek), jsou složena pouze z písmen nebo pouze z číslic, přičemž na sebe jednotlivé znaky navazují a mají logickou strukturu. To znamená, že znaky nejsou volené náhodně, ale například písmena dávají dohromady slovo, čísla tvoří řadu a podobně. Takováto hesla jsou v případě pokusu o napadení účtu nejsnáze prolomitelná a uživatel je v případě použití tohoto typu hesel nejvíce ohrožen. Slabá hesla s sebou nenesou pouze rizika, že jedinec přijde o účet na dané platformě. Slabé heslo u jednoho účtu může vést k prolomení hesel u dalších účtů, které jsou spolu propojené například přes e-mail. Příklady slabých hesel: 12345, Viktor, heslo, qwert. Druhou kategorií jsou středně silná hesla, jejichž délka se pohybuje v rozmezí 8-12 znaků. Tato hesla již využívají kombinaci velkých a malých písmen a číslic. Ovšem stále mohou mít velkou řadu chyb. Opět se může jednat o logickou návaznost jednotlivých znaků,

[17] ČERMÁK, Miroslav. CIA: Důvěrnost-Integrita-Dostupnost. Online. *Bezpečnost*. 2008. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/duvernost-integrita-dostupnost/. [cit. 2023-11-26].

použití kombinace jména a čísla, názvu ulice a popisného čísla, zaměnění některý písmen za čísla (například 3 místo E) a další podobné. Poslední kategorií jsou silná hesla, složena ideálně z více než 15 znaků, které nemají logickou souvislost, používají náhodné kombinace velkých a malých písmen, číslic a speciálních znaků.

2.2.1.1 Dvoufázové ověření

Pojistkou proti napadení nebo odcizení uživatelského účtu může být dvoufaktorové ověření. Je založené na dvou po sobě jdoucích krocích, přičemž prvním krokem je zadání správného uživatelského jména a hesla na dané platformě. Po splnění tohoto kroku přichází na řadu druhá část, která se může lišit ve způsobu provedení, ale princip zůstává stejný. Uživatel je vyzván, aby potvrdil svoje přihlášení. Tato fáze může probíhat tak, že uživateli přijde na jeho osobní telefonní číslo kód, který zadá do aplikace a tím své přihlášení ověří. Někdy může služba požadovat po uživateli přihlášení do emailu, kde potvrdí své přihlášení. Těchto způsobů je několik, zjednodušeně jde o to, aby uživatel prokázal, že zná tuto kombinaci přihlašovacích náležitostí a má k nim přístup.[18]

2.2.1.2 Nejčastější chyby při tvorbě a užívání hesel

Největším problémem při tvorbě hesla je používání osobních informací jako jsou jména a data narození jednotlivých členů rodiny, adresa bydliště, název oblíbené kapely nebo sportovního týmu. Problémem těchto hesel je zejména to, že jsou veřejně dohledatelná na sociálních sítích. V současnosti existují programy (crackery) na prolamování hesel, které cíleně prohledávají sociální sítě a snaží se z dostupných informací vytěžit možné podoby hesla uživatele. Tento program poté dosazuje možné kombinace takto vytěžených informací v kombinaci s emailem a snaží se do účtu dostat. Ochranou před tímto typem útoku není ani dodání číslice za dané heslo, jelikož útočníci o těchto věcech vědí a programy na prolamování hesel jsou nastavené na zkoušení kombinací veřejně dostupných informací a číslic.

[18] ESET. *Vícefázové ověření*. Online. Praha, 2024. Dostupné z: https://www.eset.com/cz/vicefazove-overeni-a-zabezpeceni-firemnich-hesel/. [cit. 2024-03-05].

Dalším problémem může být špatná aktualizace hesla. Toto se děje zejména ve společnostech, kde firemní politika vyžaduje jednou za určité časové období změnu hesla a zároveň není firmou určeno kolik znaků se v hesle musí minimálně změnit. Pokud firma vyžaduje změnu alespoň jednoho symbolu, často je tímto symbolem číslice na konci hesla. Když pak dojde k napadení firemních serverů, a k úniku byť jen starých hesel, útočníci mohou zkoušet pouze měnit poslední číslice na konci hesla a tím se dostat i k aktuálnímu heslu.[19]

2.2.4 Sociální sítě

Každá osoba má dle Listiny základních práv a svobod právo na ochranu osobních údajů. Ochrana se týká především života, zdraví, lidské důstojnosti, ale také chránění svého soukromí, jména a projevů osobnosti. Za osobní údaj může být považována jakákoliv informace, a to bez ohledu na její přesnost nebo objektivitu. Především je hlavní, že údaj je možné přiřadit k určité osobě. Může se tedy jednat o jméno, příjmení, rodné číslo, kontaktní údaje, biometrický údaj nebo dokonce IP adresu. Sociální sítě jsou založeny na principu sdílení těchto informací o svých uživatelích. Osoba, která si založí na síti svůj osobní profil s informacemi o jméně, příjmení nebo přezdívce, e-mailu, datu narození, adrese, zaměstnání, dosaženém vzdělání nebo telefonním čísle je vystaven hrozbě jejich zneužití. Před ní je má do jisté míry chránit poskytovatel sociální sítě, který se založením profilu stává správcem osobních údajů uživatele. Tím mu vzniká řada povinností, například informační, ke které patří obeznámit uživatele o rozsahu a účelu zpracování osobních údajů včetně kdo a jakým způsobem bude mít k těmto údajům přístup. Aby mohl poskytovatel sociální služby zpracovávat údaje, potřebuje souhlas uživatele. Nejčastěji se uděluje již při zakládání profilu. Háček je ovšem v tom, že poskytovatelé v rámci smluvních podmínek, se kterými uživatel musí opět souhlasit, aby mohl službu sociálních sítí využívat, omezují svou odpovědnost za škodu. Projevuje se to například tím, že nezaručují trvalý a nerušený přístup ke službám sociálních sítí a bez předchozího upozornění mohou uživateli omezit přístup nebo smazat jeho profil. Dále si také vyhrazují

[19] MANAGEMENT NEWS. *5 častých chyb při tvorbě a využívání hesel*. Online. 2021. Dostupné z: https://www.managementnews.cz/manazer/trendy-id-2698721/5-castych-chyb-pri-tvorbe-a-vyuzivani-hesel-id-4091480. [cit. 2024-02-05].

právo na využití poskytnutých osobních údajů pro účely cílené reklamy. Nutné je ovšem zmínit, že po zveřejnění obrazového nebo zvukového záznamu na profilu zůstává uživatel jejím vlastníkem. Uživatelé si však ve většině případů nejsou vědomi, že poskytovateli udělí nevýhradní, převoditelnou a přenosnou licenci na používání fotografie, a to po celém světě.[20] Četné užívání sociálních sítí je v dnešní době podstatnou součástí života světové populace. Některé společnosti mohou vyžadovat po svých zaměstnancích stažení a užívání některých sociálních sítí pro komunikaci mezi jednotlivými odděleními, účtárnou či jako prostředek pro sdílení interních novinek. Soukromě pak na sociální sítě přidávají jednotlivci kromě svých osobních údajů a dalších informací fotografie, videa či jiné záznamy, které chtějí mít na platformě umístěné pro snazší přístup z ostatních svých zařízení nebo se s nimi pochlubit. Důležité je poznamenat, že všechny tyto příspěvky jsou nesmazatelné. Nejedná se jen o hlavní stránku, ale také komunikační chaty. Veškerá komunikace, která proběhne přes danou službu sociální sítě, je ošetřena jen slabě. Poskytovatel nemůže odpovídat za to, jaké heslo si osoba nastaví nebo jaké informace o sobě dá vědět. To vše dělá daný jedinec sám a může se tak stát cílem útoku. Veškeré zveřejněné informace jsou dalším vodítkem a klíčem k úspěchu útočníků, kteří mohou podniknout podvodné jednání na tuto osobu. Při phishingu, spear phishingu nebo vishingu, které zmíním na následujících stránkách, lze využít informace získané na těchto platformách k manipulaci osoby. Při dnešních vymoženostech, jako jsou některé AI programy, lze upravit hlasový či obrazový záznam, kde je možné pozměnit jednotlivé části tak, aby vypadala pro oběť věrohodně, a na podvod se nachytala. Důsledkem toho je potenciální ztráta osobních údajů či financí.

2.2.5 Cookies

Cookies, v překladu sušenky, jsou malé datové soubory ukládané v prohlížeči navštíveného webu. Jejich funkce spočívá v odlišení jednotlivých uživatelů a personalizaci webových stránek. To znamená, že při opakované návštěvě stránky je již jedinec identifikován, neboť jsou o něm již uložené informace. Příslušný server si tak díky souborům cookies pamatuje nastavení

[20] KINCL, Petr. *Sociální sítě a osobní údaje: Jak se bránit zneužití?* Online. 2016, 11.12.2016. Dostupné z: https://www.pravniprostor.cz/clanky/obcanske-pravo/socialni-site-a-osobni-udaje. [cit. 2024-03-03].

jazyka, který při minulé návštěvě vybrán nebo jaké má předvyplnit přihlašovací jméno do formuláře. Stejně tak v prostředí e-shopu dokáží zobrazit naposledy prohlížené produkty nebo obsah nákupního košíku při další návštěvě. Princip cookies je také využíván pro různé statistiky, které si ukládají identifikátor návštěvníka, čas a další informace. Údaje se pak načítají a doplňují při otevření dříve navštívených nebo nových webových stránkách. Díky tomuto sběru informací jsou pak přiřazovány jednotlivé nabídky produktů a služeb ke konkrétním návštěvníkům. Kromě toho jsou také cookies využívány k uložení potvrzení přihlášení uživatele. Jedná se například o přihlášení na sociální sítě, e-shopy a podobně. Tyto autentizační cookies slouží především pro jednotlivé servery, aby věděli, že přihlášení a ověření uživatele proběhlo a nemusel tak vyžadovat nové zadání uživatelského jména a hesla. Do souboru cookies si může server uložit informace co uživatel na webu vyhledává, jaké produkty nakupuje a na základě těchto informací zobrazovat cílenou reklamu.[21] Tyto informace jsou však lehce zneužitelné. Bezmyšlenkovitým přijímáním podmínek služeb webových stránek a aplikací se vzdáváme svého soukromí. Mohou být totiž sledovány naše online aktivity, což jsou informace, které mohou být prodány společnostem třetích stran bez našeho vědomí nebo souhlasu. Kromě toho mohou být cookies zneužity ke kybernetickému útoku, především z pohledu přihlašovacích údajů. Pokud se tedy bude jednat o uživatele, který využívá podobná, ne-li stejná hesla pro většinu svých účtů, může dojít nejen ke ztrátě těchto účtů, ale také k přístupu do soukromých zpráv, se kterými mohou útočníci dále nakládat. Právě z toho důvodu by návštěvníci webových stránek měli cookies buďto odmítnout nebo zvolit v nastavení jen nezbytné.[22]

2.3 Incidenty v oblasti kybernetické bezpečnosti

V dnešním digitálním věku se stále stáváme svědky nejrůznějších incidentů, které mohou ohrozit naše osobní informace, ekonomickou situaci nebo v nejhorším případě i národní bezpečnost. V online prostředí tak čelíme

[21] ŠTRÁFELDA, Jan. *HTTP cookies – kompletní průvodce*. Online. 2024. Dostupné z: https://www.strafelda.cz/cookies. [cit. 2024-03-05].

[22] JANOUŠ, Vilém. *Lidé bezmyšlenkovitě přijímají cookies. Nechtěně se vzdávají soukromí*. Online. 2022, 20. 6. 2022. Dostupné z: https://www.denik.cz/pocitace-a-mobily/web-cookies-soukromi.html. [cit. 2024-03-03].

potenciálním hrozbám, které mají nemalý rozsah. V následujících odstavcích zmíním některé z hlavních kybernetických incidentů, které ovlivňují oblast kybernetické bezpečnosti.

2.3.1 Malware

Malware neboli zkráceně „malicious software“ je škodlivý software, který má za úkol zajistit tajný přístup do počítače nebo mobilního zařízení. Nejčastěji se šíří přes internet a e-mail. Hackeři ho používají k získávání osobních údajů nebo hesel, krádežím peněz, k blokování přístupu do zařízení či jiných nekalých záměrů. Do zařízení, se dostává několika způsoby. Například prostřednictvím napadených webových stránek, panelů nástrojů, různých programů, bezplatných služeb, zkušebních verzí her, hudebních souborů, či jakýchkoli stažených dat. Malware lze odhalit několika následujícími způsoby. Známkou může být pomalý počítač, opakované zobrazování vyskakovacích oken, rozesílání spamů nebo časté pády systému. Pokud se tak stane, je zapotřebí provést jednoduchou kontrolu, která spočívá v použití nástroje na vyhledávání malwaru, který je součástí všech antimalwarových nástrojů. K odstranění škodlivého softwaru lze použít nástroje na odstraňování malwaru, který je součástí každého kvalitního antimalwarového programu. Tento škodlivý software má další různé typy jako spyware, adware, phishing, viry, trojské koně, červy, rootkity, ransomware a změny nastavení prohlížeče. Některým z nich se v práci budu věnovat podrobněji a některé z důvodu zaměření své práce nebudou využity, tudíž ani popsány.[23]

2.3.2 Ransomware

Jak již autorka zmínila, ransomware je typ malwaru. Šifruje data ve smyslu uzamknutí celého počítače nebo souborů tak, že je nelze otevřít. Za odemčení neboli získání klíče k dešifrování požadují výkupné. Počítač se tak stane pastí, ve které uvíznou přístupy ke svým nejdůležitějším finančním dokumentům či práci nebo fotografiím a videím. Účelem ransomwaru je vydělat peníze útočníkům tím, že donutí uživatele zaplatit za obnovení přístupu. Pokud oběť odmítne zaplatit, o svá data přijde. Obvykle však cílem nebývá trvale poškodit či smazat soubory

[23] Malware [online]. Česká republika: AVAST Software, 2023. Dostupné z: https://www.avast.com/cs-cz/c-malware. [cit. 2023-09-06].

nebo dokonce ukrást identitu, ale přesvědčit uživatele, aby zaplatil za dešifrovací klíč. Obětí se může stát kdokoli.

Ransomwarové útoky jsou velice svízelné, neboť mohou napadnout nejen počítače, ale také mobilní zařízení Android či Apple. Druhů ransomwaru je nespočet, ovšem všechny mají jedno společné a tím je získání finančního obnosu. Nejběžnějším druhem ransomwaru je tzv. Krypto-malware, neboli kryptografický ransomware. Funguje tak, že se k počítači uživatel může přihlásit, avšak jednotlivé soubory jsou zašifrované. Dalším druhem je Locker, který zcela uzamkne počítač a nelze se tak již k němu ani přihlásit. Poté je zde Doxware, jehož funkcí je přenášení citlivých souborů do počítače hackera. V okamžiku dokončení transferu souborů se útočník dožaduje výkupného s pohrůžkou, že pokud uživatel neposkytne finanční obnos, budou tyto citlivé soubory zveřejněny. Může se jednat o fotografie, videa nebo cokoliv jiného, co by mohlo daného člověka zkompromitovat. Následující druh je Scareware. Tento falešný software oznamuje, že se v počítači nalezl problém, a za jeho opravu požaduje peněžní obnos. Obrazovka se pak neustále zaplňuje vyskakovacími okny či výstrahami nebo je počítač zcela uzamčen. Největší hrozbu představuje ale jakýkoliv ransomware tím, že na zařízení může zaútočit bez přičinění osoby. Tím se také liší od některých virů, které požadují, aby si uživatel stáhl napadený soubor nebo aby klikl na škodlivý odkaz. Naopak ransomware dokáže napadnout počítač „sám od sebe“.

Ochrana před všemi typy ransomwaru se nejlépe zajistí dodržením následujících pěti kroků. Zaprvé aktualizovat operační systém a aplikace. Zadruhé aktualizovat počítačový software, především webové prohlížeče. Zatřetí je zapotřebí zálohovat soubory. Začtvrté pravidelně používat aktualizovaný antivirus. Zapáté být obezřetní vůči manipulativním útokům např. obdržení e-mailu, SMS nebo zprávy na sociálních sítích s podezřelou přílohou.

Zbavení se ransomwaru. Existuje několik možností podle rozsáhlosti šifrování. Pokud byly v počítači napadeny soubory, ale stále se můžeme přihlásit, restartujeme počítač do nouzového režimu a smažeme pomocí antivirového programu. Jestliže jsme se však ocitli v situaci, kdy se počítač zcela uzamkl, je zapotřebí buď přeinstalovat operační systém, nebo z externího disku provést

kontrolu počítače, případně pomocí nástroje na obnovení systému obnovit Windows do původního stavu před útokem ransomwaru.

Ransomware však může poškodit nejen jednotlivce, ale také státní organizace, nemocnice, univerzity nebo různé společnosti. Důkazem toho je druh nazývající se WannaCry, který se v průběhu května 2017 rozšířil po celém světě[24] a postihl více než 230 000 počítačů se systémem Windows. Zneužíval známou chybu zvanou EternalBlue. Umožňovala hackerům spustit ransomware na dálku přes požadavek na sdílení souborů a tiskáren Windows. Microsoft sice opravu této chyby vydal, jenže řada jednotlivců a firem si tuto aktualizaci včas nenainstalovala, a tak se staly jeho obětí. Nejvíce útoků bylo napácháno v Rusku, v Číně, na Ukrajině, na Tchaj-wanu, v Indii a Brazílii.[25]

2.3.3. Phishing

Další způsob k získání citlivých informací, hesel a bankovních údajů je phishing. Tuto hrozbu autorka rozvádí do větších detailů v souvislosti se zaměřením této práce. Jedná se o kybernetický útok, který může probíhat několika způsoby. Metody se liší, ovšem vytyčený cíl je stejný, vylákat důvěrnosti o dotyčné oběti. Tento název je překroucený z anglického výrazu slova pro rybolov. Názvosloví nás má přivést na myšlenku, že hacker je rybář, který se snaží svou oběť chytit na nahozenou udici, neboli v našem případě nastraženou hrozbu, kterou připravil. Fishing se tedy změnil za phishing, tudíž písmeno f za ph. Důvodem je původ názvu „phreaks“, který používala hackerská skupina z USA, která v devadesátých letech ilegálně experimentovala s telekomunikačními systémy.

2.3.3.1. E-mailový phishing

E-mailový phishing by se dal popsat jako maskovaná nástraha. Toto maskování spočívá ve vydávání se za známé organizace, úřady, banky nebo jiné instituce. Vzhledem k tomu, že e-mail je v dnešní době velmi významný komunikační kanál, jak v pracovní, tak soukromé sféře, je možné rozeslat tisíce

[24] EMPEY, CHARLOTTE. Vše, co potřebujete vědět o ransomwaru a jak se před ním ochránit. Avast [online]. Česká republika: Avast Blog, 2018. Dostupné z: https://blog.avast.com/cs/co-je-ransomware. [cit. 2023-09-06].
[25] WannaCry [online]. Česká republika: AVAST Software, 2023. Dostupné z: https://www.avast.com/cs-cz/c-wannacry. [cit. 2023-09-06].

takovýchto nástrah. V e-mailech se často vyměňují údaje důvěrné, příkladem mohou být výpisy z bank, údaje o platbách, zprávy o kreditních nebo debetních kartách a další. Tyto údaje jsou pro hackery zlatý důl, neboť se dostanou k informacím potřebným pro další možné páchání nebo je jinak zneužít. Hlavním cílem těchto útoků je získat osobní údaje tím, že příjemce oklamou svým dokonale upraveným e-mailem od známé instituce. Příjemce e-mailu je naveden, aby kliknul na napadený odkaz nebo si do svého zařízení stáhl přílohu obsahující malware. Podvodný odkaz pak může navést uživatele na webovou stránku, která je opět upravená k oklamání dané osoby se záměrem získání přihlašovacích údajů internetového bankovnictví, e-mailů či údaje platebních karet.[26] Tím, že se tak stane, se hacker může dostat k citlivým informacím příjemce, které mohou vést ke ztrátě identity nebo k finanční újmě. Pokud si tyto situace představíme v rámci pracovního procesu, kdy zaměstnanec dostane e-mail od známé instituce, se kterou může firma spolupracovat a tyto všechny okolnosti mu nejsou známy, může tak svého zaměstnavatele připravit o nemalou finanční částku. Kromě toho se také phishingový útočník může dostat nejen k e-mailům na ostatní zaměstnance, ale také k citlivým informacím o produktech či připravovaných projektech. Následně může dojít k vydírání ohledně prozrazení těchto skutečností a požadování platby za zachování mlčenlivosti. E-mailový phishing se světově nejvíce rozšířil v době koronaviru. Důkazem toho jsou níže zmíněné přehledy nárůstu phishingu ve statistických přehledech. Podniky nebyly na tuto hrozbu dostatečně připraveny, a tak přicházely o své výdělky. Obranou proti těmto útokům bylo zavedení legislativy, jejímž účelem bylo stíhat ty, kteří budou shledáni vinnými z tohoto podvodného jednání. Kromě těchto zákonů bylo zapotřebí připravit organizace a firmy na tyto útoky a vzdělat zaměstnance o typech trestných činů krádeže identity. Opatření k řízení rizik spojených s krádeží citlivých informací se vztahují i na poskytovatele internetových služeb. Bylo vyvinuto několik způsobů filtrování a blokací podezřelých e-mailů týkající se krádeže identity. Čas i rozvoj je však neúprosný a uživatelé e-mailů se stále musí chránit, ať už se jedná o sektor pracovní či osobní. Je zapotřebí se mít v tomto odvětví neustále na pozoru

[26] RATHEE, Dhruv; MANN, Suman. Detection of E-mail phishing attacks–using machine learning and deep learning. *International Journal of Computer Applications*. 2022, roč. 183, č. 47, Dostupné z: https://eprints.cs.univie.ac.at/248/1/GanstererPoelz.pdf. [cit. 2024-01-22], s. 1-3.

a nezanedbat informace a doporučení z institucí věnujících se problematice kybernetické bezpečnosti.

Tím, že se phishingoví útočníci nesnaží využívat technologické slabiny v operačním systému zařízení, ale používají sociální inženýrství, je tento systém lehčí, a bohužel velmi efektivní. Žádný operační systém není před phishingem zcela bezpečný, bez ohledu na jeho výkonnou ochranu. Faktem je, že se hackeři často uchýlí k phishingu z důvodu, že nevidí žádné technologické slabiny. Pro snazší pochopení je následně rozdělena existence cyklu phishingu do jednotlivých etap. Toto rozlišení bude demonstrováno na jednom z nejjednodušších postupů, jakým se může tato hrozba připravit.

Prvním úkolem útočníka je vytvoření falešné webové stránky, která je velmi podobná oficiální. Vzhledem k tomu, že stránka nemůže být založena na zcela identických údajích, užívají zločinci různé techniky. Jedná se o obdobné abecední znaky, pravopisné chyby a další postupy pro vytvoření legitimní webové stránky adresy URL. Z důvodu odborné terminologie je třeba vysvětlení významu URL a její tvorby. URL (Uniform Resource Locator) neboli webová adresa je jedinečný identifikátor používaný k vyhledání zdroje na internetu. Adresy URL se skládají z několika částí. První je název protokolu, který je zapotřebí pro přístup ke zdroji, včetně názvu zdroje. Určuje, jaký protokol se má použít jako prvotní přístupové médium. Nejčastější formát pro webové zdroje jsou HTTP (Hypertext Transfer Protocol) a HTTPS (HTTP Secure). HTTPS je novější verze, která zajišťuje komunikaci mezi webovým serverem a prohlížečem. Na rozdíl od původního HTTP přenášená data šifruje a snižuje tak riziko zneužití osobních údajů, záměny obsahu či odposlech online komunikace. Druhá část identifikuje IP adresu nebo název domény, eventuálně subdomény, kde se nachází zdroj. Stručně řečeno, jde o sdělení webovému prohlížeči, jak a kde má načíst zdroj. Koncový uživatel zadá adresu URL přímo do adresního řádku prohlížeče, nebo kliknutím na hypertextový odkaz na webové stránce, v e-mailu, seznamu záložek nebo jiné aplikaci.[27]

[27] SCARPATI, Jessica, BURKE, John (ed.). *URL (Uniform Resource Locator)*. Online. 2020. Dostupné z: https://www.techtarget.com/searchnetworking/definition/URL. [cit. 2024-01-22].

Po dokončení webové stránky je druhou etapou vytvoření e-mailové schránky, která je názvem velice podobná dané organizaci. Opět jsou zde využity techniky uvedené výše, včetně překlepů a znaků, které na první pohled nemusí být patrné (změna písmena i za l a podobně). Následně zformuluje strukturu obsahu e-mailu, který je vesměs stejný pro všechny příjemce, kteří mají být poškozeni. V předmětu i obsahu je uvedena vysoká urgence, nutnost provést požadovanou činnost okamžitě. Odesilatel tím chce docílit, aby byl adresát pod tlakem, nezamyslel se nad tím, zda je možnost jiného řešení a ihned žádanou věc učinil.

K rozpoznání phishingového e-mailu lze využít několik způsobů. Počátkem může být kontrola jména a e-mailové adresy odesilatele. Doména odesilatele by měla být shodná s názvem společnosti. Je důležité si dávat pozor na překlepy či změněná písmenka (m za rn). Dále se můžeme zaměřit na obsah zprávy a gramatiku, kdy jednotlivé fráze jsou neobvyklé nebo slovní spojení nedává smysl. Odesilatel mohl k překladu vět využít překladač, a tak lze zjistit určité nedostatky i v gramatice. Kromě toho by měl adresát dbát zvýšené pozornosti při časovém nátlaku, nenechat se vyprovokovat k neuvážené reakci a zamyslet se nad následky svého jednání. Další veliký „vykřičník“ tvoří odkazy a přílohy. Ať už jsou v e-mailu či na webových stránkách, kdy jsou uživatelé často nuceni přílohy otevřít či stáhnout, je zapotřebí si uvědomit i možná rizika s tím spojená (ztráta osobních údajů, instalace škodlivého softwaru). Pouhým kliknutím lze naše zařízení infikovat. Jedním z řešení je se přihlašovat ke stránkám přímo v prohlížeči, nebo aplikaci. Pro možné ověření legitimity odkazu je možné u počítačů najet myší na odkaz, kdy se nám zobrazí URL adresa stránky, na kterou máme být přesměrováni. Pokud jsou i v ní gramatické chyby, překlepy či jiné nedostatky, s největší pravděpodobností se jedná o phishing.[28]

2.3.3.2 Spear phishing

Kybernetické útoky typu spear phishing zastupují další významnou hrozbu v oblasti kybernetické bezpečnosti. Tento poddruh phishingu může být vážnější, neboť je cílenější, než phishingové e-maily, ačkoliv vypadá velice podobně.

[28] ČESKÁ BANKOVNÍ ASOCIACE. *Podvodné e-maily — phishing*. Online. 2022. Dostupné z: https://www.kybertest.cz/nejcastejsi-typy-podvodu/phishing-podvodne-e-maily. [cit. 2024-02-06].

Zaměřuje se na konkrétní osoby nebo organizace s cílem ukrást citlivé informace jako přihlašovací údaje nebo infikovat cílové zařízení malwarem. Útočníci zkoumají své cíle pečlivěji, tím se zvyšuje i jejich účinnost. Útok je ve většině případů proveden tak, aby vypadal, že pochází od důvěryhodného odesilatele.[29] Z toho důvodu nejsou pro uživatele už tak lehce odhadnutelné a tím pádem i nebezpečnější. Hodnocení koncového uživatele ohledně myšlenky, zda se jedná o spear phishing lze ovlivnit využitím osobnostních rysů. Naléhavost odpovědi na konkrétní e-mail nebo autorita obsažená ve zprávě může vést k ignorování rizik spojených s tímto jednáním.[30] V tomto případě mohou být vztahy nadřízenosti a podřízenosti silnějším faktorem v rámci rizikových rozhodnutí. Spear phishingový e-mail využívá, podobně jako phishingový e-mail, techniky sociálního inženýrství, aby přiměl adresáta ke kliknutí na škodlivou přílohu či odkaz. Může se jednat o nespočet případů. Příkladem může být zaplacení faktury, která je zaslána účetní ve firmě z podvodného e-mailu zaměstnance firmy, který ji žádá o realizaci platby do určité hodiny.

Rekomandace ochrany před spear phishingem pro uživatele jsou zpracovány různými způsoby řadou organizací či institucemi. V mezích své práce využiji doporučení od Národního centra kybernetické bezpečnosti, ze kterého lze udělat jednodušší výňatek. Především jde o:

- kontrolu e-mailové adresy v případě neobvyklých požadavků
- otvírat přílohy a odkazy v e-mailech rozvážně
- omezit sdílení informací o zaměstnání na sociálních sítích
- v případě nejistoty kontaktovat IT oddělení[31]

[29] LENAERTS-BERGMANS, Bart. *What is Spear-phishing? Definition with examples*. Online. 2023, 6.11.2023. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/phishing/spear-phishing/. [cit. 2024-01-24].
[30] HALEVI, Tzipora; MEMON, Nasir; NOV, Oded. Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. *Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks,* 2.1. 2015. Dostupné z: https://www.researchgate.net/profile/Tzipora-Halevi/publication/317904745_Spear-Phishing_in_the_Wild_A_Real-World_Study_of_Personality_Phishing_Self-Efficacy_and_Vulnerability_to_Spear-Phishing_Attacks/links/5da079eea6fdcc8fc3474953/Spear-Phishing-in-the-Wild-A-Real-World-Study-of-Personality-Phishing-Self-Efficacy-and-Vulnerability-to-Spear-Phishing-Attacks.pdf. [cit. 2024-01-24], s. 3.
[31] NÁRODNÍ CENTRUM KYBERNETICKÉ BEZPEČNOSTI. *Spear-phishing a jak se před ním chránit*. Online. 2020. Dostupné z: https://www.govcert.cz/cs/informacni-servis/doporuceni/2748-spear-phishing-a-jak-se-pred-nim-chranit/. [cit. 2024-02-06].

2.3.3.3 Vishing

Phishingový útok probíhající přes hlasový hovor se nazývá vishing. Názvosloví se vyvinulo z anglických názvů „voice“ (hlas) a phishing. Tento typ phishingu je odlišný od výše popsaných tím, že se odehrává mimo prostředí e-mailu či škodlivých webových stránek. Probíhá prostřednictvím hovoru, kdy se útočník snaží vylákat z oběti, které volá, osobní údaje a ty poté následně využít. Cíl je tedy stejný jako u předchozích kategorií – získat co nejvíce informací nebo osobních dat. V současné době plné elektronických vymožeností, tabletů, chytrých telefonů a hotspotů jsou útoky na mobilních zařízeních rozšířenější, a tím i manipulace s osobami jednodušší. Osoba páchající vishing se může domáhat informace související s přihlašováním do bankovnictví, převodu finanční částky, vyzrazení identifikačních čísel platební karty, nebo ověření totožnosti, která může v konečné fázi dojít až ke krádeži identity. Rozpoznávání podvodného jednání v rámci vishingu může být složitější v případě, že volající je velmi dobrý a přesvědčivý řečník, takže v osobě vyvolá pocit důvěry, a tak jsou veškeré potřebné informace pro další páchání sděleny. Naopak slabší vyjadřovací schopnosti vedou k zamyšlení volaného, zda se opravdu jedná o stav, ve kterém musí požadovanou věc učinit okamžitě, jak je na něho naléháno.

V minulosti se podvodné telefonáty objevovaly od osob, které se vydávaly za technickou podporu společnosti Microsoft nebo za zaměstnance bankovní instituce. V případě podvodníků vydávajících se za technickou podporu Microsoftu se pomocí lámané angličtiny dožadovali instalace programů, díky kterým získali vzdálený přístup k počítači. Tyto programy umožnily na dálku ovládat zařízení a tím také dosáhnout škodlivého cíle (získání informací ze zařízení, o dalších zaměstnancích apod.) Po splnění pokynů podvodníků bylo zařízení cenným prostředkem pro získání citlivých údajů a dat (přihlašovací údaje) nebo došlo k zašifrování ransomwarem. [32] Co se týče podvodníků jako „zaměstnanců bankovních institucí“, ti se snaží vylákat kromě údajů citlivých či přihlašování do internetového bankovnictví, také čísla účtu nebo PIN a CVV/CVC kódu na

[32] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Upozornění na podvodné telefonáty od falešné technické podpory Microsoft*. Online. 2021. Dostupné z: https://nukib.gov.cz/cs/infoservis/aktuality/1699-upozorneni-na-podvodne-telefonaty-od-falesne-technicke-podpory-microsoft/. [cit. 2024-02-05].

platebních kartách, jak již bylo zmíněno výše. Po zjištění se útočníci snaží zrealizovat převod finančních částek na své účty. Pro podvržení telefonního čísla je zneužíváno služeb VOIP (Voice Over Internet Protector). Jedná se o volání přes internet odkudkoliv, prostřednictvím počítače nebo tabletu, kdy volaný obdrží hovor, který vypadá jako z legitimní klientské linky. Je tak skoro nemožné identifikovat reálné číslo volajícího. V případě, že si daná osoba není jistá, zda se jedná o danou bankovní instituci, je nejlepší reakcí hovor zavěsit a zavolat na číslo klientské linky pro ověření. [33]

2.3.3.4 Smishing

Poslední formou phishingu, který probíhá přes podvodné SMS zprávy se nazývá smishing. Existují dva postupy, jakými lze tento podvod provést. První zahrnuje přijetí textové zprávy pocházející údajně z důvěryhodného a známého zdroje, jakým mohou být například bankéři nebo správci systému. Druhý je obdržení textové zprávy o odcizení identity nebo zmrazení čísla účtu s odkazem na webovou stránku nebo telefonní číslo pro ověření informací. Osoby páchající smishing po obdržení informací tak mohou podniknout několik následujících kroků. Počínaje výběrem peněz z účtu či otevření nové kreditní karty na osobní údaje oběti až po stažení přílohy s malwarem, která následně zajistí, aby neoprávněné osoby měly přístup ke všem kontaktům, aplikacím nebo doručeným zprávám a mohly tak mít kontrolu nad svou obětí.[34] Tyto postupy však nemusí být jediné, s pozvolným vývojem se do praktik zapojily také SMS s lákadlem vyzvednutí výhry nebo poskytnutí jiných výhod například od operátorů či jiných známých firem. Přijaté zprávy vypadají jako legitimní, a proto je úspěšnost podvodného jednání závislá na kvalitě provedení i načasování. Příkladem může být období před Vánoci, kdy lidé ztrácejí přehled o doručovaných zásilkách a smishingoví podvodníci tak mohou být úspěšnější. Odhalení není jednoduché, a to i vzhledem k možnému provázání se spoofingem, kdy lze napodobit v podstatě jakéhokoliv

[33] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Upozornění na vishing zneužívající identitu bankovních institucí*. Online. 2021. Dostupné z: https://nukib.gov.cz/cs/infoservis/hrozby/1705-upozorneni-na-vishing-zneuzivajici-identitu-bankovnich-instituci/. [cit. 2024-02-05].

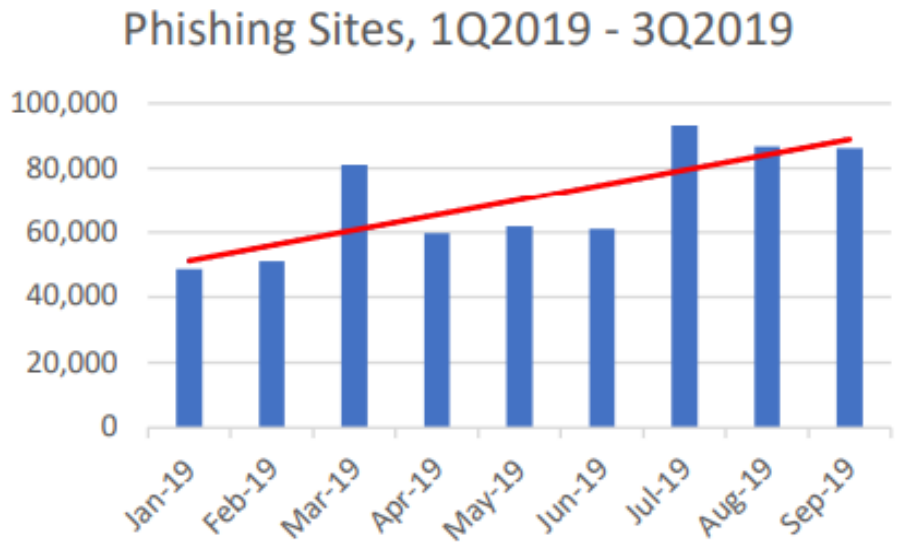
[34] YEBOAH-BOATENG, Ezer Osei a AMANOR, Priscilla Mateko. Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices. Online. *Journal of Emerging Trends in Computing and Information Sciences*. 2014, roč. 5, č. 4. ISSN 2079-8407. Dostupné z: https://e-tarjome.com/storage/btn_uploaded/2020-09-12/1599891065_11216-etarjome%20English.pdf. [cit. 2024-02-06], s. 297-307.

odesilatele zprávy. Některé zprávy se tak mohou automaticky přiřadit k předchozímu komunikačnímu kanálu s oprávněným subjektem. V těchto případech je dobré se bránit tím způsobem, jaký byl uveden i výše, kontaktovat klientské centrum banky, finančního úřadu či jiné instituce a ověřit si danou informaci.[35]

2.4 Phishing a Covid-19

Dle statistických údajů z Anti-Phishing Working Group (APWG), mezinárodní koalice odpůrců kybernetické kriminality zabývající se phishingem je zřejmé, že největší nárůst phishingu byl v době pandemie Covid-19. Níže jsou uvedeny grafické přehledy s daty a komentáři z roků 2019-2021, které jsou důkazem tohoto tvrzení. U shrnutí z roku 2020 jsou využity grafické znázornění od výše zmíněné koalice, které autorka upravila do českého jazyka pro snazší přehlednost zásahu phishingu v rámci průmyslových odvětví.

Graf č. 2: Statistický přehled phishingových stránek od prvního do třetího čtvrtletí roku 2019



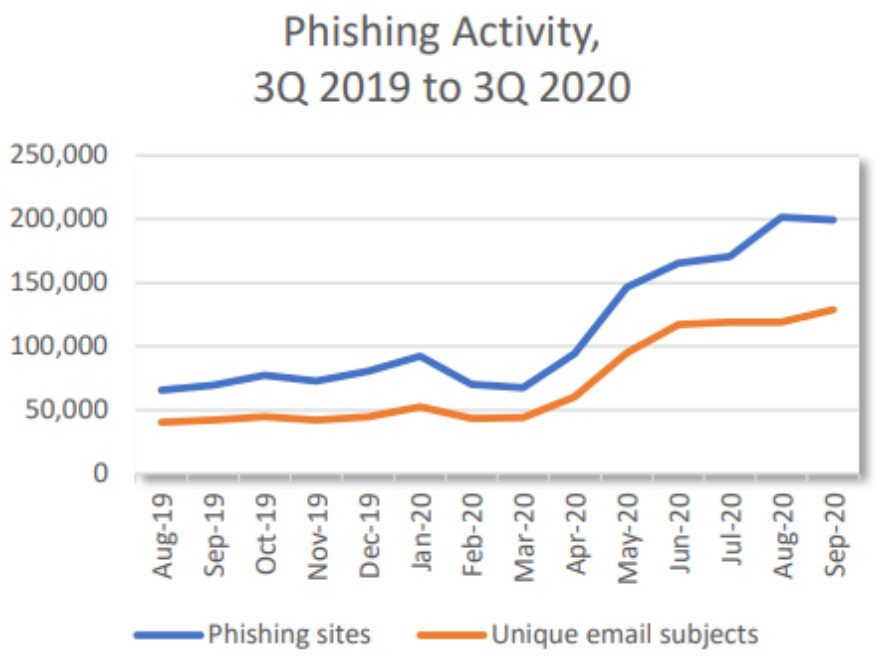
Zdroj: Zpráva APWG o trendech phishingových aktivit za třetí čtvrtletí roku 2019

Z přehledu je možné vidět nárůst phishingových stránek od prvního čtvrtletí až do třetího čtvrtletí roku 2019, kde konečný počet činil 266 387. Nárůst mezi druhým a třetím čtvrtletím byl o 46 %, kdy jich bylo zaznamenáno 182 465, a téměř dvakrát více než ve čtvrtém čtvrtletí 2018 (138 328). Greg Aaron, vedoucí

[35] ČESKÁ BANKOVNÍ ASOCIACE. *Podvodné SMS (tzv. smishing)*. Online. 2022. Dostupné z: https://www.kybertest.cz/nejcastejsi-typy-podvodu/smsishing-podvodne-sms-zpravy. [cit. 2024-02-06].

výzkumný pracovník APWG a prezident společnosti Illumintel Inc. uvedl, že se jedná o nejhorší období phishingu, které APWG zaznamenala za poslední tři roky, od čtvrtého čtvrtletí roku 2016 (277 693 útoků).

Graf č. 3: Statistický přehled phishingových aktivit



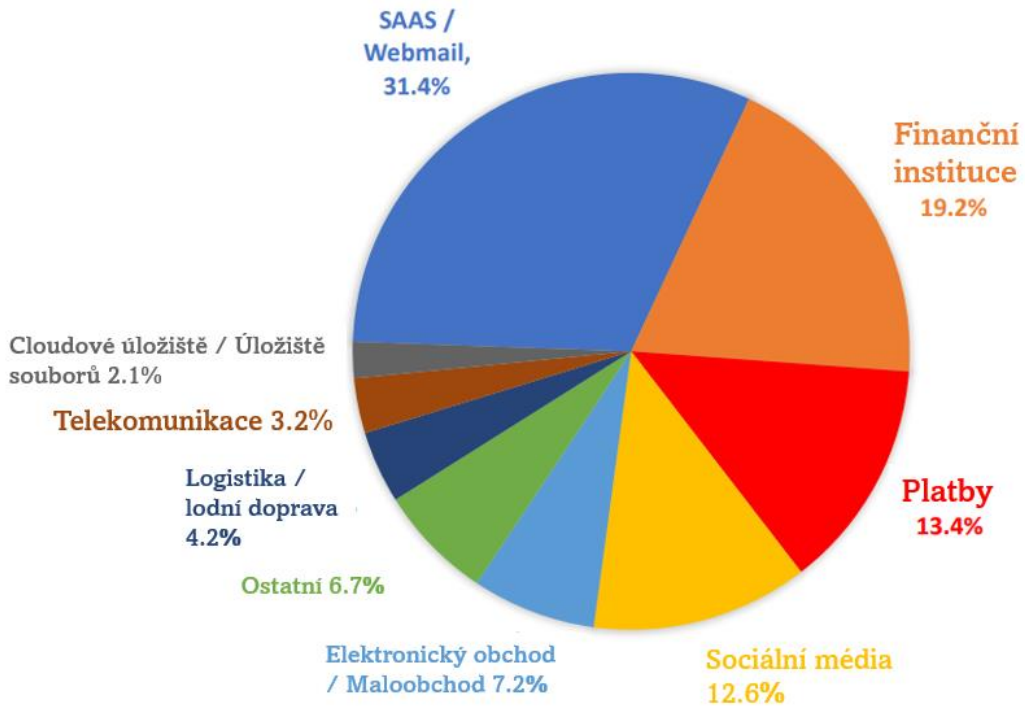
Zdroj: Zpráva APWG o trendech phishingových aktivit za třetí čtvrtletí roku 2020

Modrá barva představuje phishingové stránky, jejichž měřítko vychází z nahlášeného phishingu po celém světě. Určilo se dle adres URL phishingových stránek nalezených v podvodných e-mailech nahlášených do úložiště APWG. Zde je zapotřebí zmínit, že jediná phishingová stránka může být inzerována tisíci přizpůsobenými adresami URL, které vedou na stejný cíl útoku. APWG měří nahlášené phishingové stránky na základě, který přihlíží k způsobu, jakým hackeři vytvářejí phishingové adresy URL. Počet zjištěných phishingových webových stránek jen z června do srpna vzrostl z 171,040 na 201,591 útoků. APWG ve své zprávě dále uvádí, že údaje o rok zpět byly nižší, takže počet phishingových útoků od března roku 2020 stoupl.

Oranžová barva demonstruje subjekty phishingových e-mailů. Zahrnuty jsou zde různé předměty e-mailu a nástrahami v jejich obsahu. Phishingové kampaně mohou užívat stejný předmět, ale inzerovat různé škodlivé stránky.

Jedná se tedy o měřítko rozmanitosti phishingových útoků a hrubého ukazatele množství prováděného phishingu.

Graf č. 4: Nejvíce sledovaná průmyslová odvětví

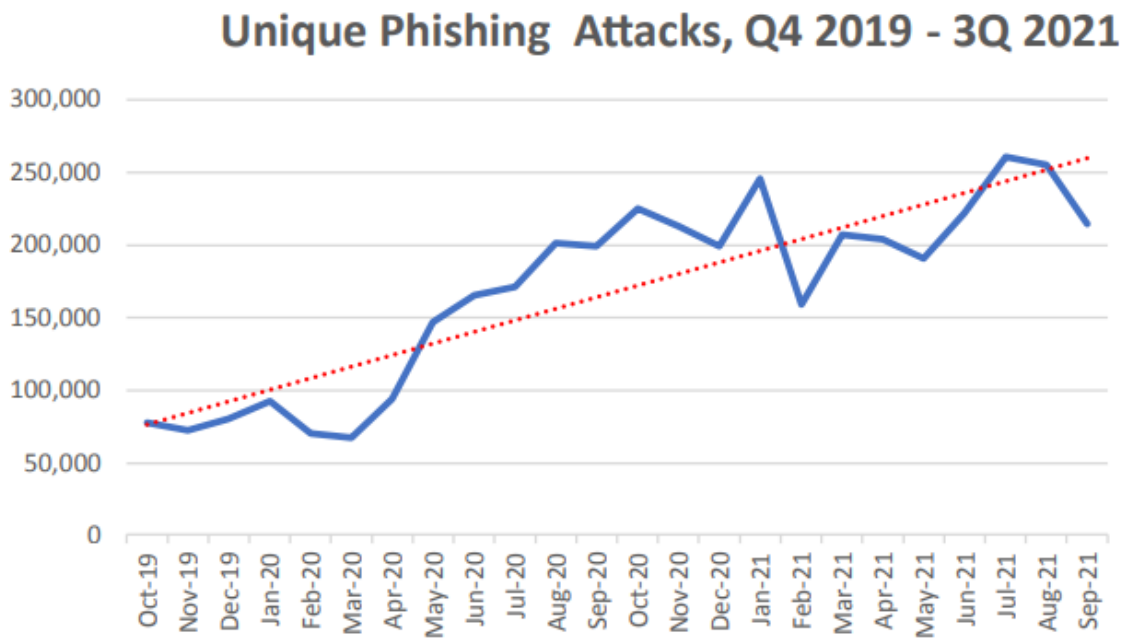


Zdroj: Zpráva APWG o trendech phishingových aktivit za třetí čtvrtletí roku 2020

Toto znázornění poukazuje na to, že phishingové útoky nejsou vedeny pouze na určité osoby, ale prostřednictvím nich také na instituce a jiná průmyslová odvětví, kterým mohou způsobit značné škody. Z grafu lze vyčíst, že nejčastějším cílem phishingu jsou weby SaaS a webmaily. SaaS (Software jako služba) umožňuje uživatelům připojit se přes internet ke cloudovým aplikacím. Obvyklými příklady jsou e-mail, kalendáře nebo kancelářské nástroje (jako je Microsoft Office 365).[36] Procento všech útoků zde dosahuje výše 31,4. Dle dodatečných informací ze zprávy Anti-Phishing Working Group vztahující se k tomuto přehledu, byla tato kategorie opětovně nejčastějším cílem, jak v roce 2020, tak i 2019.[37]

[36] AZURE. *Co je SaaS?* Online. 2024. Dostupné z: https://azure.microsoft.com/cs-cz/resources/cloud-computing-dictionary/what-is-saas. [cit. 2024-01-22].
[37] APWG. *Phishing Activity Trends Report: 3 rd Quarter 2020*. Online. 2020. Dostupné z: https://docs.apwg.org/reports/apwg_trends_report_q3_2020.pdf?_gl=1*bjfq1j*_ga*MTkzMzI0OTQ4NC4xNzA4OTYzMzc4*_ga_55RF0RHXSR*MTcwODk2ODgwMi4yLjAuMTcwODk2ODgwMi4wLjAuMA. [cit. 2024-03-08], s. 2-5.

Graf č. 5: Phishingové útoky v období 4. čtvrtletí 2019 až 3. čtvrtletí 2021



Zdroj: Zpráva APWG o trendech phishingových aktivit za třetí čtvrtletí 2021

Grafické znázornění uvedené výše slouží spíše jako přehled, nebude tedy v práci více rozebírán z důvodu jeho rozsahu. Níže je představena sumarizace z celkové zprávy, která na něj bude navazovat. V rozmezí od října 2019 do září 2021 dosáhl phishing měsíčního rekordu v červenci roku 2021, kdy APWG zaznamenala 260 642 phishingových útoků. Tento počet byl nejvyšší v historii reportování. Útoky se od začátku roku 2020 vyšplhali na dvojnásobek. Co se týče průmyslových odvětví, opět bylo nejvíce ohroženy weby SaaS a webmaily 7(29,1 %). Druhé místo zaujmuly opět finanční instituce se 17,8 % a třetí elektronický obchod a malobchod (13,1 %).[38]

3. Legislativa kybernetické bezpečnosti

Již od počátku nežádoucích aktivit byly snahy o právní regulaci a postih trestné činnosti páchané prostřednictvím informačních a komunikačních technologií. Kybernetická trestná činnost se výrazně liší od jiných druhů kriminality, a to především díky možnosti jejího dynamického vývoje a okamžitých změn, které mohou nastat v závislosti na úspěchu nebo neúspěchu konkrétního typu útoku.

[38] APWG. *Phishing Activity Trends Report: 3 rd Quarter 2021*. Online. 2021. Dostupné z: https://docs.apwg.org/reports/apwg_trends_report_q3_2021.pdf?_gl=1*1l87p3k*_ga*MTkzMzI0OTQ4NC4xNzA4OTYzMzc4*_ga_55RF0RHXSR*MTcwODk2ODgwMi4yLjAuMTcwODk2ODgwMi4wLjAuMA. [cit. 2024-03-08], s. 2-4.

Tato dynamika může přinášet určité problémy v oblasti legislativy. V mezích trestního práva platí zásada, že nelze aplikovat analogii k tíži pachatele. Tudíž nelze automaticky přenášet pravidla nebo tresty navržené pro jednu formu trestného činu na jinou, pokud nejsou výrazně podobné. I přesto lze kybernetické útoky často zařadit pod zákonné ustanovení určité skutkové podstaty, jejíž podstata byla původně směřována na jiné formy páchání. Typickým příkladem může být útok spojený s porušováním autorských práv. Nicméně již existuje řada nových útoků, u nichž tato možnost nepřichází v úvahu. Legislativní pracovníci se proto snaží reagovat na nové druhy trestné činnosti a zaplnit tak slepá místa ve vnitrostátní právní úpravě. Před samotnou analýzou platné legislativy v oblasti kybernetické kriminality, je důležité zdůraznit, že úsilí o implementaci efektivnějších právních nástrojů, které by byly schopny zajistit včasnou a adekvátní reakci se vyskytuje nejen v rámci Evropské unie, které je Česká republika součástí. Vzniká tak postupné odstranění rozporů a nedostatků v právních normách členských států EU a dalších zemí, které se rozhodly aktivně angažovat v boji proti kybernetické trestné činnosti.[39] V rámci této kapitoly je nejprve uvedena legislativa, která se zabývá celkovou problematikou kybernetické bezpečnosti, následně na ni navazují ty předpisy, které se vztahují na jednotlivé druhy kyberkriminality.

3.1 Zákon o kybernetické bezpečnosti

V České republice se problematikou phishingu a dalších kybernetických hrozeb zabývá několik zákonů a legislativních opatření. Pro účel této práce je zaměření upřeno na klíčové, které s nimi nejvíce souvisejí. Prvním z nich je zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Tento zákon vstoupil v platnost 29. srpna 2014 s účinností od 1. ledna 2015. Byl zpracován na základě Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii a zároveň navázal na Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci

[39] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z. s. p. o., 2016. ISBN 978-80-88168-18-8, s. 331.

kybernetické bezpečnosti informačních a komunikačních technologií. Zákon upravuje několik agend, jedná se o úpravu práv a povinností osob, působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti a zajišťování bezpečnosti sítí elektronických komunikací i informačních systémů. Zákon se naopak nevztahuje na oblast nakládání s utajovanými informacemi u informačních nebo komunikačních systémů. Tím se zabývají jiné příslušné zákony či vyhlášky, kterými jsou zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor a zákon č. 106/1999 Sb., o svobodném přístupu k informacím. Kromě vymezení základních pojmů jako je například kybernetický prostor či bezpečnost informací (zajištění důvěrnosti, integrity a dostupnosti informací a dat) se zabývá také bezpečnostním opatřením (§4), kybernetickou bezpečnostní událostí a kybernetickým bezpečnostním incidentem, společně s povinnými subjekty (§7), hlášením kybernetického bezpečnostního incidentu (§8), evidencí, opatřeními, a také stavem kybernetického nebezpečí (§21). V jeho znění je též upraven Národní úřad pro kybernetickou a informační bezpečnost, a také Národní a vládní CERT, kterým se budu věnovat v následující kapitole této práce.

Orgány a osobami, kterým se zákonem o kybernetické bezpečnosti ukládají povinnosti v této oblasti, jsou:

a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací,

b) orgán nebo osoba zajišťující významnou síť,

c) správce a provozovatel informačního systému kritické informační infrastruktury,

d) správce a provozovatel komunikačního systému kritické informační infrastruktury,

e) správce a provozovatel významného informačního systému,

f) správce a provozovatel informačního systému základní služby,

g) provozovatel základní služby,

h) poskytovatel digitální služby.

Pro zajištění kybernetické bezpečnosti je důležité mít bezpečnostní opatření, které utváří souhrn úkolů plněný povinnými subjekty, jehož cílem je zajistit bezpečnost informací v informačních systémech a dostupnost a spolehlivost služeb a sítí elektronických komunikací v kybernetickém prostoru. Tato opatření jsou nezbytná pro zajištění prevence před kybernetickou bezpečnostní událostí či incidentem. Kybernetická bezpečnostní událost může způsobit narušení jak bezpečnosti informací v informačních systémech, tak bezpečnosti služeb nebo integrity sítí elektronických komunikací. Incident poté představuje stejné hrozby jako v události, avšak odlišností je, že jeho vznik byl právě v důsledku kybernetické bezpečnostní události. Povinné subjekty uvedené pod písmeny b) až f) proto musí detekovat kybernetické bezpečnostní události a mají povinnost bezodkladně hlásit kybernetické bezpečnostní incidenty po jejich detekci v jejich významné síti, informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury, informačním systému základní služby nebo významném informačním systému. Informační povinnost nebo ochrana osobních údajů tím není dotčena. Pokud by incident měl významný dopad na kontinuitu poskytování základní služby, oznámí to provozovatel Národnímu úřadu pro kybernetickou a informační bezpečnost. NÚKIB vede evidenci kybernetických bezpečnostních incidentů, která obsahuje hlášení, identifikační údaje systému (ve kterém se incident vyskytl), údaje o zdroji incidentu, postup při řešení a výsledek. NÚKIB kromě evidence také vydává opatření, kterými je varování, reaktivní opatření a ochranné opatření. Varování zveřejňuje na svých internetových stránkách a oznamuje je povinným orgánům a osobám. Reaktivní a ochranné opatření vydává úřad rozhodnutím, ve kterém uloží provedení reaktivního opatření k řešení kybernetického bezpečnostního incidentu anebo k zabezpečení informačních systémů nebo sítí a služeb elektronických komunikací před incidentem. Zákon o kybernetické bezpečnosti upravuje také stav kybernetického nebezpečí, ve svém znění jej popisuje jako „*stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost služeb elektronických komunikací anebo bezpečnost a integrita sítí elektronických komunikací*“. Mohl by tak být

porušen nebo ohrožen zájem České republiky ve smyslu zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. O vyhlášení rozhoduje ředitel Národního úřadu pro kybernetickou a informační bezpečnost. V případě, že by se tak stalo, jej vyhlásí vyvěšením na úřední desce NÚKIB, současně také informuje veřejnost prostřednictvím celoplošného rozhlasového a televizního vysílání.

3.2 Vyhláška o kybernetické bezpečnosti

K výše zmíněnému zákonu o kybernetické bezpečnosti se nepochybně váže tato vyhláška, která vstoupila v platnost i účinnost stejného dne, 28. května 2018. Jedná se o vyhlášku č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat. Zpracována byla na základě Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Její úprava je klíčová pro informační a komunikační systémy kritické informační infrastruktury, významný informační systém i informační systém základní služby, ale zároveň pro informační systém či síť elektronických komunikací užívané poskytovatelem digitálních služeb. Ustanovení této vyhlášky se týká bezpečnostní dokumentace z hlediska obsahu a struktury, bezpečnostního opatření společně s jeho rozsahem a obsahem, vzor oznámení kontaktních údajů a jejich formu a způsob likvidace dat včetně provozních údajů, informací a jejich kopií. Kromě toho jsou zde popsány kybernetické bezpečnostní incidenty z pohledu typů, kategorií a hodnocení významnosti, také způsob a náležitosti hlášení i oznámení o provedení reaktivního opatření a dosaženého výsledku. Pro sjednocení kompletního znění vyhlášky o kybernetické bezpečnosti následuje stručná analýza celkového obsahu. Jedná se o pokyny pro zajištění bezpečnosti informací při vytváření, výběru, hodnocení, řízení a ukončení dodavatelských vztahů v oblasti informačních a komunikačních technologií. Dále podílení se na procesu řízení rizik a vyhodnocování vhodných a účinných bezpečnostních opatření. Vyhláška tak upravuje organizační a technické bezpečnostní opatření, která cílí na zkvalitnění ochrany informačních systémů a dat.

3.3 Směrnice NIS 2

Začátkem roku 2023 vstoupila v platnost nová směrnice Evropského parlamentu a Rady (EU) 2022/2555 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii. NIS představuje zkrácený tvar pro Network a Information Security. Tato směrnice navazuje původní směrnici Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii („NIS“). Její úprava však nebyla dostačující, a proto Evropská unie přijala v roce 2022 její revidovanou verzi. Implementace NIS 2 do právního řádu České republiky se má uskutečnit 18. října roku 2024 a má jím být nahrazen stávající zákon o kybernetické bezpečnosti. Směrnice si klade za cíl posílit kybernetickou odolnost poskytovatelů základních služeb, zlepšit připravenost Evropské unie na kybernetické útoky a také zvýšit účinnost kybernetické odolnosti díky přísnějším bezpečnostním požadavkům a sankcím za jejich porušení.[40] Nová směrnice s sebou přinesla mnoho změn a požadavků. Významně rozšířila okruh subjektů, na které se budou vztahovat požadavky zajištění kybernetické bezpečnosti. Směrnice NIS 2 rozděluje povinné subjekty do dvou kategorií s ohledem na jejich velikost a předmět činnosti. Dělí se na „základní“ a „důležité“, přičemž záleží na kritické důležitosti daného odvětví nebo služby, a úroveň závislosti jiných na tomto odvětví. Jsou zde ale i určité výjimky, kde se na některé subjekty bude vztahovat regulace i bez ohledu na velikost. Příkladem jsou poskytovatelé služeb elektronických komunikací nebo subjekty, na které se vztahuje Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů. Nově tedy NIS 2 přidává kritérium velikosti subjektu. Díky tomu budou novému zákonu podléhat všechny velké a střední podniky ve vybraných odvětvích a malé podniky a mikropodniky spadající pod čl. 2 odst. 2 návrhu směrnice NIS 2. Jedná se zejména o subjekty plnící podstatnou úlohu pro společnost, hospodářství, veřejné sítě elektronických komunikací, orgány veřejné správy apod. Počet povinných subjektů se tedy vyšplhá na více než 6000. Úlohou směrnice je přimět subjekty k zavádění

[40] LIPTÁKOVÁ, Karolína. *Nová směrnice EU o kybernetické bezpečnosti „NIS2“*. Online. Právní prostor. 2023. Dostupné z: https://www.pravniprostor.cz/clanky/mezinarodni-a-evropske-pravo/nova-smernice-eu-o-kyberneticke-bezpecnosti-nis2. [cit. 2024-02-15].

preventivních opatření pro posílení kybernetické bezpečnosti. Zejména, aby přijaly technická a organizační opatření k řízení bezpečnostních rizik, jimž čelí informační systémy a sítě, které tyto subjekty užívají pro poskytování služeb. Tím, že NIS 2 jednotlivé povinnosti konkretizuje, má dojít k tomu, aby vedení organizací bylo povinno schvalovat a zavádět bezpečnostní opatření, které zahrnuje mimo jiné i nutnost pravidelných školení vrcholného managementu i řadových zaměstnanců. Kromě toho se také změní doposud zavedená terminologie, příkladem může být incident. Ten má být vykládán v novém zákoně jako „*jakákoli událost ohrožující dostupnost, autenticitu, integritu nebo důvěrnost uložených, přenášených nebo zpracovávaných údajů nebo služeb nabízených nebo přístupných prostřednictvím sítí a informačních systémů*“.[41] K přípravě nového zákona o kybernetické bezpečnosti byl pověřen Národní úřad pro kybernetickou a informační bezpečnost. Kroky, které NÚKIB učinil, byly, alespoň dle názoru autorky, nadčasové. Po sepsání znění směrnice verzi zveřejnil na oficiálních webových stránkách a vyzval občany České republiky k tomu, aby podaly příslušné návrhy a podněty pro změnu jejího znění. Tento krok byl velmi užitečný, neboť se do úpravy mohly zapojit i pracovníci vysokých škol, právníci, odborníci na kybernetickou bezpečnost atd. Úřad tak otevřel možnost pro vyjádření těch, jichž se nový zákon bude přímo týkat.

Celková úprava nového zákona bude zcela odlišná od stávající, avšak některá základní specifika z dosavadního zákona o kybernetické bezpečnosti budou uchována, jedná se o varování, reaktivní opatření a stav kybernetického nebezpečí. Naopak některé agendy z roztroušených zákonů a vyhlášek řešící tuto problematiku se díky této nové legislativě spojí. Bude tak možnost z jednoho předpisu nahlížet i na mechanismus prověřování rizikovosti dodavatelů a proces prověřování rizikovosti dodavatelů. K novému zákonu jsou navrhované i dva prováděcí právní předpisy, vyhlášky, které by byly významné především pro určení

[41] *Směrnice NIS 2 a Nový zákon o kybernetické bezpečnosti*. Online. Cyber Security Compliance Audit kybernetické bezpečnosti. 2024. Dostupné z: https://www.cybersecuritycompliance.cz/smernice-nis-2-a-normy-iso-iec/. [cit. 2024-02-16].

povinných osob. Jednalo by se o vyhlášku o regulovaných službách a vyhláška o nepominutelných funkcích stanoveného rozsahu.[42]

3.4 Trestní zákoník

Jak již bylo uvedeno v úvodu této kapitoly, většina dosavadních platných právních předpisů nebyla sepsána přímo pro jednotlivé druhy kybernetických útoků. Avšak jednotlivá znění se dají „napasovat“ na určité podvodné jednání, kterého se pachatelé dopustí. Zákon č. 40/2009 Sb., trestní zákoník uvádí ve zvláštní části několik úprav, které jsou v dnešní době prozatímně využívány pro sankcionování kybernetického podvodného jednání. Prvotní zmínku představují příklady některých majetkově trestných činů, které jsou v páté hlavě zvláštní části tohoto zákoníku. Neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací upravuje §230. Úprava tohoto paragrafu by se tak mohla interpretovat na kybernetické hrozby typu malware a ransomware. Následující § 231 uvádí trestný čin opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat. Toto znění by mohlo ztvárnit rámec východiska pro trestání hrozeb jako je malware, ransomware, e-mailový phishing, vishing a smishing. Pro snazší přehlednost těchto paragrafů autorka vytvořila přehledné tabulky, ve kterých uvádí, o jaké trestné činy se dle zákona jedná, pachatelovo jednání pro naplnění skutkové podstaty trestného činu a výčet sankcí. Včetně této tabulky vytvořila další, ve které bodově uvádí okolnosti spáchání trestného činu, které jsou brány jako přitěžující, tím pádem jsou i sankce za takové spáchání vyšší. Zkratka PS v tabulkách představuje počítačový systém.

[42] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *10. Další specifika úpravy v České republice*. Online. 2023. Dostupné z: https://osveta.nukib.cz/mod/page/view.php?id=2625. [cit. 2024-02-16].

Tabulka č. 2 : Majetkové trestné činy dle §230 Trestního zákona související s phishingem

Majetkové trestné činy	Pachatelovo jednání	Konkretizované jednání pachatele	Sankce
§ 230 Neoprávněný přístup k počítačovému systému (PS) a neoprávněný zásah do počítačového systému nebo nosiče informací	Kdo překoná bezpečnostní opatření	- neoprávněně získá přístup k PS nebo k jeho části	a) odnětí svobody až na 2 léta b) zákaz činnosti c) propadnutím věci
	Kdo zasáhne do počítačového systému nebo nosiče informací	Data uložená v PS nebo na nosiči informací - užije neoprávněně - neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými, - padělá nebo pozmění tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná nebo - neoprávněně vloží nebo přenese data do PS nebo na nosič informací - učiní jiný zásah do programového nebo technického vybavení PS nebo jiného technického zařízení pro zpracování dat	a) odnětí svobody až na 3 léta b) zákaz činnosti c) propadnutím věci

Zdroj: autorka

Tabulka č. 3 : Přitěžující okolnosti sankcionování dle §230 Trestního zákona souvisejících s phishingem

Přitěžující okolnosti sankcionování §230
Spáchá-li čin v úmyslu - způsobit jinému škodu, jinou újmu - získat sobě nebo jinému neoprávněný prospěch - neoprávněně omezit funkčnost PS nebo jiného technického zařízení pro zpracování dat <u>Sankce:</u> a) odnětí svobody na 6 měsíců až 4 léta b) zákaz činnosti c) propadnutím věci **Spáchá-li čin jako člen organizované skupiny** - způsobí-li činem značnou škodu - spáchá-li čin proti PS, jehož narušení by mělo závažný dopad na fungování státu, zdraví osob, bezpečnost, hospodářství nebo zajištění základních životních potřeb obyvatel - získá-li činem pro sebe nebo pro jiného značný prospěch - způsobí-li činem vážnou poruchu v činnosti právnické nebo fyzické osoby, která je podnikatelem <u>Sankce:</u> a) odnětí svobody na 1 rok až 5 let b) peněžitý trest **Spáchá-li čin a tím** - způsobí-li škodu velkého rozsahu (nejméně 10 milionů Kč) - získá-li činem pro sebe nebo pro jiného prospěch velkého rozsahu (nejméně 10 milionů Kč) <u>Sankce:</u> a) odnětí svobody na 3-8 let

Zdroj: autorka

Tabulka č. 4 : Majetkové trestné činy dle §231 Trestního zákona související s phishingem

Majetkové trestné činy	Pachatelovo jednání	Konkretizované jednání pachatele	Sankce
§ 231 Opatření a přechovávání přístupového zařízení a hesla k PS a jiných takových dat	Kdo vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává	- zařízení nebo jeho součást - postup - nástroj - jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do: ➢ sítě elektronických komunikací ➢ PS nebo k jeho části k neoprávněnému zásahu do: ➢ PS nebo nosiče informací - počítačové heslo - přístupový kód - data - postup - jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k: ➢ PS ➢ části PS v úmyslu, aby jej bylo užito ke: ➢ spáchání TČ porušení tajemství dopravovaných zpráv ➢ neoprávněného přístupu k PS a neoprávněného zásahu do PS nebo nosiče informací	a) odnětí svobody až na 2 léta b) zákaz činnosti c) propadnutím věci

Zdroj: autorka

Tabulka č. 5 : Přitěžující okolnosti sankcionování dle §231 Trestního zákona souvisejících s phishingem

Přitěžující okolnosti sankcionování §231
Spáchá-li čin - jako člen organizované skupiny, nebo - získá-li takovým činem pro sebe nebo pro jiného značný prospěch Sankce: a) odnětím svobody až na 3 léta b) zákaz činnosti c) propadnutí věci **Získá-li činem pro sebe nebo pro jiného prospěch velkého rozsahu** Sankce: a) odnětí svobody na 6 měsíců až 5 let

Zdroj: autorka

Následující paragraf není sice přímo spojený s bezpečností IT, ale může být v některých případech také užit pro různé typy kybernetických hrozeb. Trestní zákoník upravuje v §270 Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi. Tato úprava popisuje pachatele trestného činu jako toho, „kdo neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání, tiskové publikaci nebo databázi“. Tento zákon zmiňuje zásah do chráněných práv k databázi. V jeho následujících odstavcích jsou uvedeny i další, pro účely práce podstatné dovětky, a to, vykazuje-li čin znaky obchodní činnosti nebo jiného podnikání, získá-li takovým činem pro sebe nebo pro jiného značný prospěch nebo prospěch velkého rozsahu, způsobí-li tím jinému značnou škodu nebo škodu velkého rozsahu, nebo dopustí-li se takového činu ve značném nebo velkém rozsahu. Zásah do chráněných práv by mohl být proveden malwarem i ransomwarem. Díky škodlivému softwaru, který spustí uživatel ať už na soukromém nebo pracovním zařízení je velkou hrozbou. Může se jednat o neoprávněné nabourání do databáze zaměstnance významných institucí, subjektu kritických infrastruktur a podobně. Phishingem či spear phishingem může dojít k získání přístupových údajů k interní databázi významných státních složek, jejíž obsahem mohou být důvěrné obrazové či zvukové záznamy.

4. Komponenty bezpečnostního systému zabývající se problematikou kybernetické bezpečnosti

Následující podkapitoly se věnují institucím a orgánům, jejichž činnost směruje k ochraně kybernetické bezpečnosti. První části se zaměřuje na ústřední správní orgán v této oblasti, který bude rozebrán podrobněji společně s týmy a sekcí, která k němu přísluší.

4.1. Národní úřad pro kybernetickou a informační bezpečnost

NÚKIB je od 1. srpna 2017 ústředním správním orgánem pro kybernetickou bezpečnost. Zaměřuje se na ochranu utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Kromě tohoto výsadního postavení je správním úřadem pro veřejně regulované služby navigačního systému Galileo, který je globálním navigačním družicovým systémem Evropské unie, jehož funkce poskytuje rádiové signály pro určování polohy a času.[43] Úřad vznikl na základě zákona č. 205/2017 Sb., zákon kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Hlavní sídlo NÚKIB se nachází v Brně v ulici Mučednická, další úřad se nachází v Praze na Žižkově. Současným ředitelem je Ing. Lukáš Kintr, který byl do funkce jmenován na základě usnesení vlády České republiky 1. července 2022.[44] Úlohou Národního úřadu pro kybernetickou a informační bezpečnost je příprava národních bezpečnostních standardů v oblasti kyber bezpečnosti a stanovení bezpečnostních standardů pro kritickou informační infrastrukturu. Stanovuje také ochranu utajovaných informací v oblasti informačních a komunikačních systémů a zároveň připravuje a koordinuje kybernetická cvičení jak v České republice, tak v zahraničí. Úřad plní také funkci legislativní, kdy připravuje zákony a podzákonné normy v oblasti kybernetické bezpečnosti. Podporuje také vzdělávání v oblasti kyber bezpečnosti a zajišťuje vlastní výzkum a vývoj v tomto odvětví, se zaměřením na šifrování. NÚKIB hájí

[43] *Počáteční služby systému Galileo: Co je potřeba vědět*. Online. 2017. Dostupné z: https://www.mdcr.cz/Dokumenty/Kosmicke-aktivity/Pocatecni-sluzby-systemu-Galileo-Co-je-potreba-ve. [cit. 2024-02-24].

[44] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Novým ředitelem NÚKIB je Lukáš Kintr*. Online. 2022. Dostupné z: https://nukib.gov.cz/cs/infoservis/aktuality/1851-novym-reditelem-nukib-je-lukas-kintr/. [cit. 2024-02-24].

zájmy České republiky v oblasti kybernetické bezpečnosti na mezinárodní úrovni a společně s tím také vytyčuje národní strategie kybernetické bezpečnosti.[45] NÚKIB spolupracuje nejen s CERT (Computer Emergency Response Team), ale také s CSIRT (Computer Security Incident Response Team). CERT je označení týmu zabývající se bezpečnostními incidenty, reakcí na ně, jejich řešení a koordinací tohoto řešení. Co se týče CSIRT jedná se o národní tým České republiky pod názvem CSIRT.CZ. Jeho pole působnosti se vztahuje na celou Českou republiku, všechny sítě provozované na území ČR. Tento národní tým může působit i jako „poslední záchrana“ v případech, kdy napadená síť nedokáže kontaktovat správce sítě, která je zdrojem útoku, nebo kdy správa dané sítě na hlášení nereaguje.[46]

4.1.1 Vládní a Národní CERT

Pod NÚKIB spadá Vládní CERT, který je vládním bezpečnostním týmem řešící ochranu kritické informační infrastruktury a významných informačních systémů podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Jeho úloha spočívá ve schopnosti účelně a efektivně čelit bezpečnostním výzvám, pokud jsou kritické systémy připojeny k internetu. To zahrnuje také nutnost reakce na incidenty, koordinovanou činnost při jejich řešení a také účelné působení při předcházení incidentů. Kromě plnění těchto funkcí působí jako prvotní zdroj bezpečnostních informací a pomoci pro orgány státu, organizace, ale také občany. Rovněž se také věnuje zvyšování vzdělanosti v oblasti bezpečnosti na internetu.[47] Za zmínku stojí také Národní CERT. V současnosti je provozován sdružením CZ.NIC dle uzavřené veřejnoprávní smlouvy s Národním úřadem pro kybernetickou a informační bezpečnost.[48] Dle Zákona o kybernetické bezpečnosti zajišťuje sdílení informací na národní a mezinárodní úrovni v oblasti kybernetické bezpečnosti. Plní roli týmu CSIRT podle čl. 9 směrnice Evropského parlamentu

[45] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *O úřadu*. Online. 2020. Dostupné z: https://nukib.gov.cz/cs/o-nukib/o-uradu/. [cit. 2024-02-24].
[46] CSIRT.CZ. *FAQ*. Online. 2019. Dostupné z: https://csirt.cz/cs/hlaseni-incidentu/faq/#cojecert. [cit. 2024-02-24].
[47] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Vládní CERT*. Online. 2020. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vladni-cert/. [cit. 2024-02-24].
[48] CSIRT.CZ. *Národní CSIRT České republiky*. Online. 2019. Dostupné z: https://www.csirt.cz/cs/. [cit. 2024-02-24].

a Rady (EU) 2016/1148 a spolupracuje s ostatními týmy CSIRT jiných členských států Evropské unie. Kromě toho také přijímá hlášení o kybernetických bezpečnostních incidentech od orgánů a povinných osob. Pokud to jeho kapacity umožňují, tato hlášení zpracovává a poskytuje orgánům nebo osobám dotčeným kybernetickým bezpečnostním incidentem metodickou podporu, pomoc a součinnost.

4.1.2 Národní centrum kybernetické bezpečnosti

Výkonnou sekcí Národního úřadu pro kybernetickou a informační bezpečnost je Národní centrum kybernetické bezpečnosti (NCKB). Tato sekce zajišťuje prevenci před kybernetickými hrozbami proti prvkům kritické informační infrastruktury, informačním systémům významným i základní služby a vybraným informačním systémům veřejné správy. Zaopatřuje řešení a koordinaci řešení kybernetických bezpečnostních incidentů u orgánů veřejné správy, subjektů kritické infrastruktury a provozovatelů základní služby. Vyhodnocuje rizika, přijímá příslušná nápravná a preventivní opatření na úseku kybernetické bezpečnosti. Dále kromě zabezpečení činnosti Vládního CERT spolupracuje s národními a mezinárodními organizacemi, které se podílejí na zajišťování bezpečnosti kybernetického prostoru. Pořádá a účastní se kybernetických cvičení na národní i mezinárodní úrovni, poskytuje osvětu a vzdělání v oblasti kybernetické bezpečnosti a provádí výzkum a vývoj v tomto odvětví. Zastupuje Českou republiku v orgánech mezinárodních organizací, v rozsahu své působnosti uplatňuje bezpečnostní politiku Národního úřadu pro kybernetickou a informační bezpečnost při plnění mezinárodních závazků.[49]

4.2 Národní centrála proti terorismu, extremismu a kybernetické kriminalitě

Tato poměrně nová centrála útvaru služby kriminální policie a vyšetřování vznikla 1. ledna 2023. Útvar s celostátní působností se sídlem ve Zbraslavi byl vybudován vyčleněním sekcí terorismu, extremismu a kybernetické kriminality z Národní centrály proti organizovaného zločinu služby kriminální policie a vyšetřování. Policie jako zdůvodnění pro vytvoření mimo jiné uvedla, že

[49] NÁRODNÍ CENTRUM KYBERNETICKÉ BEZPEČNOSTI. *Co je NCKB*. Online. 2020. Dostupné z: https://www.govcert.cz/cs/. [cit. 2024-02-26].

odhalování a objasňování trestné činnosti v kyberprostoru patří mezi nejdůležitější úkoly Policie ČR, neboť se jedná o problematiku s vysokou specifičností, kde se kladou vysoké nároky na odbornost analytiků, operativců, vyšetřovatelů i managementu všech řídících úrovní. Jeho zvláštním posláním je zvýšení schopnosti čelit útokům na kritickou informační infrastrukturu. Ředitel útvaru je v současnosti plk. JUDr. Břetislav Brejcha, dále jsou v útvaru dva náměstci ředitele. První náměstek řeší problematiku terorismu a extremismu, druhý kybernetickou kriminalitu. Vedení útvaru společně s téměř 170 policisty a občanskými zaměstnanci mají zajistit kontinuitu prověřovaných a vyšetřovaných trestních případů a také podporovat a spolupracovat se všemi součástmi Policie České republiky v případové i koordinačně metodické oblasti. Rozvoj a posílení spolupráce má probíhat s tuzemskými i zahraničními partnery v oblasti boje proti terorismu, extremismu i kybernetické kriminalitě.

4.3 The European Cybercrime Centre

Evropské centrum pro počítačovou kriminalitu, jinak také známo pod zkratkou EC3, byl zřízen Europolem v roce 2013. Od svého založení si klade za cíl posílit reakci vymáhání práva na počítačovou kriminalitu v Evropské unii za účelem ochrany občanů, podniků a vlád před online zločinem. Zaměřuje se na tři typy kybernetické kriminality, jimiž jsou kybernetická kriminalita, platební podvod a sexuální zneužívání dětí, a to na úrovni operací. Zaměření se vztahuje také na na boj proti kriminalitě na Dark webu[50] a alternativních platformách. Centrum nabízí operativní, analytickou, strategickou a forenzní podporu vyšetřování členských států pro každý z výše uvedených typů kybernetické kriminality. Zároveň slouží jako centrála pro kriminální informace a zpravodajství, podporuje operace a vyšetřování prováděné členskými státy EU a poskytuje vysoce specializovanou technickou a digitální forenzní podporu pro vyšetřování a operace. Poskytuje nonstop provozní a technickou podporu LEA pro okamžitou reakci na naléhavé kybernetické incidenty a/nebo kybernetické krize. Kromě toho také zajišťuje komplexní kontaktní funkci propojující orgány činné v trestním řízení, jež se zabývají kyberkriminalitou, se soukromým sektorem, akademickou sférou

[50] Dark web je řada webových stránek, které jsou široké veřejnosti skryté, neboť nejsou dostupné prostřednictvím běžných vyhledávačů a mohou tak být užity k usnadnění zapojení do trestné činnosti jako výměně odcizených dat, obchodu s lidskými orgány nebo nelegální koupi zbraně.

a dalšími partnery, kteří nejsou donucovacími orgány a zároveň přispívá k přípravě a realizaci preventivních a osvětových kampaní a činností v oblastech kybernetické kriminality. Struktura EC3 by se dala shrnout do třech základních skupin. Prvním z nich jsou odborné a manažerské týmy, které primárně provádí preventivní a osvětové školení, strategické a taktické analýzy a také výhledová a technologická hodnocení. Druhým jsou týmy pro dokumentaci a digitální forenzní analýzy, kteří se zaměřují na poskytování forenzní podpory v místě potřeby, udržují dešifrovací platformu připravenou pro podporu vyšetřování, a provádějí výzkum a vývoj. Poslední jsou operační týmy. Ty především poskytují podporu při vyšetřování kybernetické trestné činnosti v několika oblastech. Páchání organizovanou skupinou, která má velké zisky z trestné činnosti (podvody na internetu); činnost, která způsobuje vážnou újmu obětem (sexuální zneužívání dětí online); nebo kybernetická trestná činnost včetně kybernetických útoků s dopadem na kritickou infrastrukturu a informační systémy v EU a také trestná činnost na Dark webu a alternativních platformách. Vyjma toho také identifikuje vznikající hrozby a vzorce a sdílí je s příslušnými zúčastněnými stranami.

4.4 Anti-Phishing Working Group

Pracovní skupina pro boj proti phishingu vznikla na základě sjednocení celosvětové reakce na kybernetickou kriminalitu prostřednictvím výměny dat, výzkumu a informovanosti veřejnosti. Již od svého založení roku 2003 má postavení mezinárodní koalice, která se skládá z odborníků. Zaměření jeho členů je rozlišné, jedná se o forenzní vyšetřovatele, orgány činné v trestním řízení, technologické společnosti, firmy poskytující finanční služby, univerzitní výzkumníky, nevládní organizace a mnohostranné smluvní organizace, které fungují jako neziskové. Ředitelé, manažeři a výzkumní pracovníci pracovní skupiny poskytují jako uznávaní odborníci poradenství Organizaci spojených národů v rámci Úřadu pro drogy a kriminalitu. Také vládám (např. parlamentní sdružení Commonwealthu) i mnohostranným orgánům a organizacím jako Evropská komise, podskupina G8 pro kriminalitu v oblasti špičkových technologií, Evropské centrum pro počítačovou kriminalitu EC3, Organizace pro bezpečnost a spolupráci v Evropě, Mezinárodní telekomunikační unie a další. APWG se specializuje na eliminaci krádeží identity a podvodů, které jsou důsledkem

rostoucího problému phishingu a podvržených e-mailů. V rámci své specializace nabízí členství finančním institucím, online prodejcům, poskytovatelům internetových služeb, komunitě orgánů činných v trestním řízení, vládním agenturám, mnohostranným smluvním organizacím a nevládním organizacím. V současnosti je zapojeno více než 2300 podniků po celém světě. Pracovní skupina sídlí ve Spojených státech amerických, nicméně má evropskou pobočku v Barceloně, která byla založena v roce 2013 jako nezisková výzkumná nadace, je registrovaná ve Španělsku a řízená nezávislou správní radou. Anti-Phishing Working Group spustila kampaň STOP. THINK. CONNECT. (STOP. MYSLI.PŘIPOJ SE.) na zvýšení povědomí o kybernetické bezpečnosti. Kurátoři kampaně z 26 zemí se oficiálně zapojili a dislokovali STOP. THINK. CONNECT. prostřednictvím ministerstev a nevládních organizací s celostátní působností. Kromě toho pracovní skupina pořádá konference zaměřené na budování komunit pro profesionály v oblasti řízení počítačové kriminality, vládní a donucovací orgány a průkopnické výzkumníky v oblasti počítačové kriminality z celého světa. Dává tak možnost pro vznik veřejných vzdělávacích nástrojů pro prevenci kybernetické kriminality, datové standardy a vývoj politiky pro výměnu dat o kybernetické kriminalitě společně s programy na podporu výzkumu v této oblasti.

5. Případová studie

Případová studie se zaměřuje na hackerskou skupinu XDSpy a její phishingové útoky. Otázky, na nichž chce autorka v rámci případové studie zjistit odpověď, jsou tři. Jakým způsobem provádí skupina XDSpy phishingové útoky? Které subjekty jsou cílem phishingových útoků? Jaké dopady měly phishingové útoky páchané touto skupinou? Cílem případové studie je analyzovat jednání skupiny provádějící phishingový útok, které autorka následně podrobněji rozebírá, aby utvořila podrobný, ucelený přehled na celkový postup těchto útoků a jejich dopady.

5.1 Charakteristika phishingových útočníků XDSpy

XDSpy je skupina APT neboli Advanced Persistent Threat. Jde se o seskupení kybernetických útočníků, kteří se zaměřují na pokročilé přetrvávající hrozby. Pod zkratkou APT se většinou míní kyberzločinci z řad státních organizací či organizací pracujících na základě státní objednávky.[51] Jak už název XDSpy napovídá, jedná se o špionážní skupinu, která je dodnes z velké části nedetekována. Její aktivita započala v roce 2011, avšak nezaujala pozornost veřejnosti, vyjma doporučení od běloruského CERT v únoru 2020. V tomto časovém mezidobí kompromitovala mnoho vládních agentur i soukromých společností, včetně ministerstev zahraničních věcí a armád ve východní Evropě a na Balkáně. Několik případů je následně uvedeno podrobněji.

5.2 Postupy při phishingových útocích

Jejich zaměření se vztahuje na kybernetické operace, které jsou cílené a sofistikované. Vše probíhá ve snaze proniknout do systémů vládních organizací či korporací a nepozorovaně v nich setrvat delší dobu pro účel dlouhodobé kybernetické špionáže a odcizení citlivých údajů. Díky svým poznatkům, vyspělým technikám a nástrojům dokáží využít tzv. zero day útoku, který využívá neznámé zranitelnosti systému, pro kterou zatím neexistuje obrana. Vývojáři většinu softwarových chyb odhalují a opravují pomocí aktualizací. V případě zero day ale útočníci chybu zneužijí předtím, než může být objevena. Útočník ve snaze

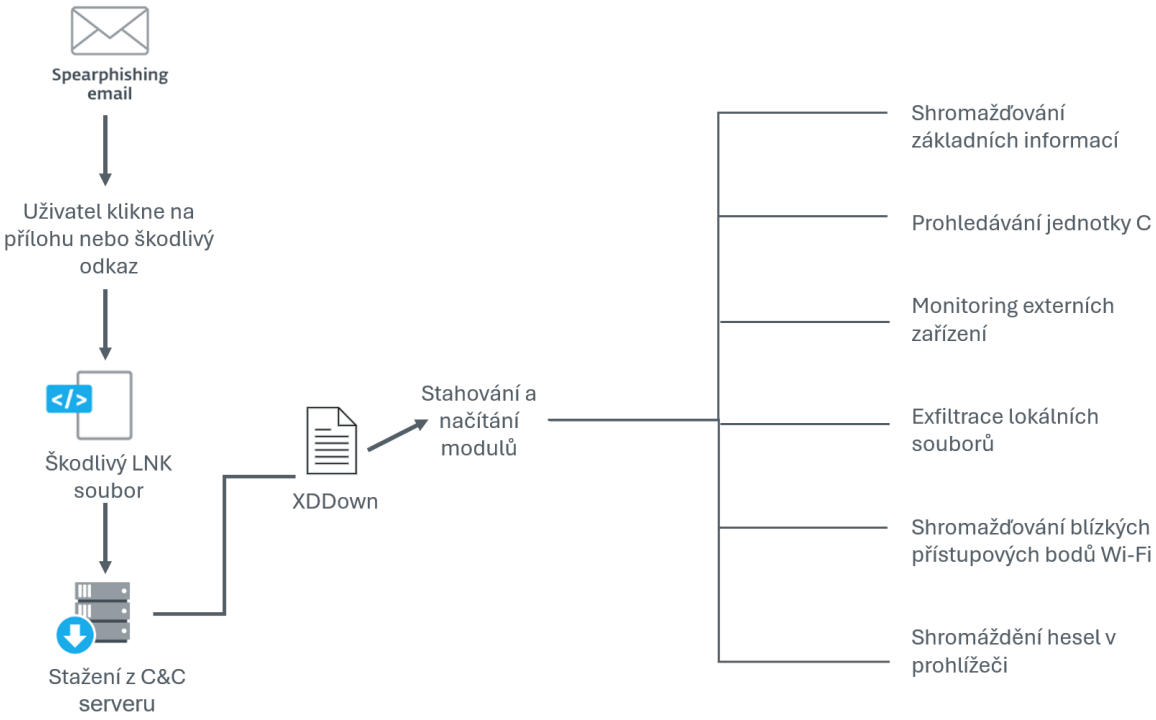
[51] ESET. *APT skupina*. Online. 2022. Dostupné z: https://www.eset.com/cz/aptskupina/. [cit. 2024-02-28].

proniknout do systému využívá tuto neobjevenou chybu k infikování systémů spywarem, ransomwarem, nebo jiným malwarem. Může dojít k odcizení dat nebo dokonce k převzetí kontroly nad cílovým zařízením.[52] Skupina XDSpy využívá pro své útoky především spearphishingové e-maily. Své cíle tak zkompromitují. V e-mailech se však dost často mění jeho obsah. Některé zahrnují přílohu, jiné odkaz na škodlivý soubor. V obou případech využívají obvykle archivy ZIP, nebo WinRAR, sloužící pro sloučení či archivaci několika souborů do jedné složky. Tyto archivy obsahují LNK soubor, který stahuje škodlivý skript[53]. Ten dále stahuje a instaluje nejvýznamnější malware této skupiny, známý jako XDDown.

Roku 2020 na konci června příslušníci XDSpy vylepšili tento postup. Začali zneužívat chybu zabezpečení v aplikaci Internet Explorer zvanou jako CVE-2020-0968. Tato chyba byla opravena vývojáři v dubnu 2020, ačkoliv, jak je možné vidět, ne zcela. Postup se tedy lišil tím, že namísto dodání archivu se souborem LNK doručoval server C&C soubor RTF[54], který po otevření stáhl soubor HTML využívající výše uvedenou chybu zabezpečení. V době zneužití nebyl k dispozici žádný důkaz o konceptu a velice málo informací o této specifické zranitelnosti. Ve stejném roce užila skupina nejméně dvakrát téma pandemie Covid-19. Poprvé tuto záminku užila ve ve spearphishingové kampani, která mířila proti běloruským institucím v únoru téhož roku. V září pak tento námět aplikovala proti cílům, které mluvili rusky. Opět šlo o stažení malwaru XDDown, tentokrát byl ale v archivu, který obsahoval škodlivý soubor Windows Script File (WSF).[55] Vzhledem k množství provedených útoků autorka níže představuje obrázek ukazující obecný postup XDSpy.

[52] ESET. *Zero day útok*. Online. 2020. Dostupné z: https://www.eset.com/cz/zero-day/. [cit. 2024-02-28].
[53] Skript je souvislou sérií příkazů s úkoly, např. stažení webové stránky do počítače
[54] RTF neboli Rich Text Format je soubor obsahující několik typů formátování textu, a podporuje objekty a obrázky uložené v textovém souboru
[55] FAOU, Matthieu. *XDSpy: Stealing government secrets since 2011*. Online. 2020, 02 Oct 2020. Dostupné z: https://www.welivesecurity.com/2020/10/02/xdspy-stealing-government-secrets-since-2011/. [cit. 2024-02-28].

Obr. č. 1: Ukázka postupu XDSpy při phishingovém útoku



Zdroj: autorka

5.3 Významné phishingové útoky

Na začátku října roku 2022 hackeři podnikli distribuci škodlivých e-mailů znovu. Tentokrát se jednalo o zprávy doručené zaměstnancům ruských organizací, osoby byly vyzvány ministerstvem obrany k odvodu pro záměr mobilizace. Bylo zde uvedeno, že důvodem pro zaslání e-mailu bylo odmítnutí převzetí odvolání a urgence, aby se adresát naléhavě dostavil na určené místo a čas. Podrobnější informace byly uvedeny ve formátu PDF, který nabádal ke stažení z odkazu. Obsah e-mailu byl velmi věrohodný, neboť zahrnoval odkazy na články trestního zákoníku Ruské federace společně s případnými pokutami a trestní odpovědností, která by osobu postihla, pokud nebude na výzvu reagovat. V odkazu byl opět pečlivě schovaný malware, který pronikl do koncového zařízení, a tak se útočníci mohli dostat k systémům a informacím dané organizace. Vzhledem k tomu, že ruský prezident Vladimír Putin oznámil v září tohoto roku mobilizaci ozbrojených sil Ruska, nebyla tato zpráva pro adresáty nijak zavádějící. Její koncept, zpracování i časové hledisko bylo vytvořené tzv. na míru. Tento útok

může působit jako ukázka dobře připravené hrozby, na kterou se mohou lidé nachytat.[56]

Poslední objevené útoky této skupiny se objevily 21. a 22. listopadu 2023. Útoky byly mířené na e-mailovou adresu zaměstnance ruských hutních podniků a ústavu zabývajícího se vývojem a výrobou řízených raketových zbraní. V obou případech hackeři posílali phishingové e-maily. V případě ústavu se vydávali se za výzkumný ústav specializující se na návrh jaderných zbraní. U ruských hutních podniků o sobě tvrdili, že jsou zaměstnanci logistické společnosti z Kaliningradu.[57] Navíc se přišlo také na podvodný e-mail zaslaný ruským metalurgům z běloruské adresy. Zda se celé uskupení, či jednotlivec ukrývají právě v Bělorusku, není dodnes známo. Jejich záměrem bylo získání přístupu k systémům metalurgického podniku i ústavu raketových zbraní. Ruské společnosti se však s těmito podvodnými e-maily nesetkaly poprvé. V červenci téhož roku se již skupina XDSpy snažila získat přístupy tím, že se vydávali za ruské ministerstvo pro mimořádné situace a v přílohách zasílali škodlivé přílohy PDF.

5.4 Odhalení aktivit XDSpy

Většinu doposud objevených informací o aktivitě této skupiny jsou výsledky práce ESET. Tato slovenská firma se zabývá kybernetickou bezpečností a monitoruje XDSpy od roku 2020. Sledování potvrdilo, že spearphishingové kampaně jsou zaměřené především na strategické organizace jako na vládní, vojenské a finanční instituce, ale také na výzkumné, energetické a těžařské společnosti ve východní Evropě. Dle ESET jsou nejvyhledávanější cíle skupiny státy Rusko a Bělorusko. Dotčené subjekty byly zjištěny ale i v Moldavsku, Srbsku a na Ukrajině.[58]

[56] KRASNOGOLOVY, Vladimir. *Hacker Group XDSpy Distributes Malware in Russia under the Guise of Subpoenas for the Army*. Online. 2022. Dostupné z: https://gridinsoft.com/blogs/hacker-group-xdspy/. [cit. 2024-03-01].
[57] F.A.C.C.T. *Кибершпионы из XDSpy атакуют российских металлургов и предприятия ВПК*. Online. 2023. Dostupné z: https://habr.com/ru/companies/f_a_c_c_t/news/775944/. [cit. 2024-03-01].
[58] ANTIVIROVÉ CENTRUM. *ESET odhalil skupinu hackerů XDSpy*. Online. 2020. Dostupné z: https://www.antivirovecentrum.cz/aktuality/eset-odhalil-skupinu-hackeru-xdspy.aspx. [cit. 2024-03-01].

5.5 Vyhodnocení případové studie

V následujících odstavcích autorka zodpoví otázky, které si stanovila na začátku této případové studie.

Jakým způsobem provádí skupina XDSpy phishingové útoky?

Útoky této skupiny jsou prováděné zejména spearphishingovými e-maily. Tento způsob útoku může být z pohledu provedení jednoduchý, avšak velmi účinný. Útočníci již musí pracovat s informacemi o daných osobách či organizacích, na které se daný útok zaměřuje. K tomu jim mohou dopomáhat aktuálně zveřejněné informace, nabídky nebo poptávky dostupné na internetu anebo současné mezinárodní dění. V přílohách či odkazech se objevuje soubor, který stáhne škodlivý skript společně s malwarem XDDown.

Které subjekty jsou cílem phishingových útoků?

Převážně se jedná o země, jejichž obyvatelé mluví ruským jazykem. Subjekty, na které byl spáchán phishingový útok jsou z organizací vládních nebo vojenských, také se jednalo o finanční instituce a těžařské i energetické společnosti především ve východní Evropě. Země, které si XDSpy označila jako své cíle bylo Rusko, Bělorusko, Srbsko, Moldavsko a Ukrajina. Vzhledem k tomu, že se ve většině případů jedná o země, které nejsou v rámci těchto hrozeb příliš sdílné, je velmi těžké dohledat informace týkající přesnějších detailů dalších možných subjektů.

Jaké dopady měly phishingové útoky páchané touto skupinou?

Kybernetické útoky byly prováděné za účelem dlouhodobě infiltrovat cílový systém a vytěžit strategické, utajované nebo neveřejné informace. Kompromitovali tak výše zmíněné subjekty ve státní i soukromé sféře. Vzhledem k tomu, že jsem již na začátku této studie zmínila, že skupina XDSpy pracuje na základě státní objednávky, je s velkou pravděpodobností i dotovaná tímto státem. Dodnes se ovšem nezjistilo, který stát tyto útoky financuje a tím i nelegálně získává data subjektů. Útočníci jsou sice dále sledováni, avšak technika jejich zabezpečení je téměř bezchybná. Právě z tohoto důvodu bylo v minulosti téměř nemožné zjistit ilegální jednání tohoto uskupení.

6. Výzkumné šetření

V praktické části práce je provedeno výzkumné šetření využívající metod kvantitativního a i kvalitativního výzkumu s cílem získat relevantní data pro formulování navazujících návrhů a doporučení.

6.1 Metodologie výzkumu

Níže autorka přiblíží metodologii zpracování výzkumného šetření. Jedná se o cíl výzkumu společně s výzkumnými předpoklady, technice sběru dat, vzorku respondentů a zpracování dat.

6.1.1 Cíl výzkumu a stanovení výzkumných předpokladů

Phishing či jiné hrozby v oblasti kybernetické bezpečnosti jsou ustavičně vyvíjející se problematikou. S neustálým technologickým pokrokem a novými způsoby útoku dochází k celkové modernizaci. Na to autorka navazuje i v rámci svého výzkumu, který by tomuto rozvoji odpovídal. Utvořila proto online dotazník, který zaslala přes sociální síť Instagram a e-maily. Prostřednictvím přiloženého odkazu se tak dostal do povědomí lidí, kteří se stali respondety pro výzkum. Kromě dotazníku také oslovila odborníka na kybernetickou bezpečnost, zaměstnance subjektu kritické infrastruktury T-Mobile, Mgr. Šimona Kubrta. Učinila tak z důvodu následné komparace názoru respondentů a specialisty na dané téma.

Cílem výzkumu je zjistit jaké povědomí mají respondenti o možných kybernetických hrozbách a současně vymezit, jaká stanoviska a opatření k problematice zaujímá specialista kybernetické bezpečnosti.

Odpovědi respondentů jsou koncipované jako jednotlivé pokládané otázky a následně je uveden celý řízený rozhovor s panem Kubrtem. V závěru práce autorka výsledky obou šetření komparuje, a odpovídá na následující výzkumné předpoklady:

P 1: Více než polovina respondentů vyplní v dotazníku postup při vytváření hesel, který by mohl být využit k phishingovému útoku, ačkoliv dle specialisty jsou dostupné informace, které varují před tímto jednáním.

P 2: Nastane shoda mezi odpovědí specialisty a nejvíce zastoupeného počtu respondentů v rámci nejohroženější věkové kategorie z pohledu kybernetické kriminality.

P 3: Více než polovina respondentů i specialista zná osobu, která se stala obětí podvodného jednání v oblasti kybernetické bezpečnosti.

P 4: Více než 30 % respondentů by při zjištění, že se stali obětí kybernetického útoku, jako první kontaktovali zkušeného IT technika, stejně, jako zaměstnanci subjektu kritické infrastruktury.

P 5: Více než polovina respondentů se doposud nesetkala s kybernetickou hrozbou vishing, stejně, jako specialista.

6.1.2 Technika sběru dat

Šetření je provedeno formou kvantitativní metody ve formě dotazníkového šetření, a na ni navázaná kvalitativní metoda, řízený rozhovor se specialistou v oblasti kybernetické bezpečnosti a vzdělávání. Zvolením obou metod autorka zajistila zaměření na větší množství respondentů, kteří nejsou odborníky na danou problematiku, a zároveň jejich připravenost porovnala s výsledky zaznamenaných zkušeností ze vzdělávání a praxe osoby, která je v dané oblasti velmi znalá. Tím, že se jedná o experta, zaměstnance korporátní společnosti, která je ale zároveň subjektem kritické infrastruktury, je poukázáno na to, že tato osoba postupuje dle interních ale také zákonných postupů a metod. Shrnul se tak pohled fyzické osoby, která pracuje v soukromém sektoru, ale výrazně zasahuje do státní sféry. Data z dotazníkového šetření i z řízeného rozhovoru jsou shrnuté k zpracování a vyhodnocení. Koncepce anonymního dotazníku je určena pro osoby starší 18 let, kteří se profesně nezabývali danou problematikou.

6.1.3 Vzorek respondentů

Cílovou skupinou výzkumu byla veřejnost, která není z pracovního či vzdělávacího pohledu oborníkem v oblasti kybernetické bezpečnosti. Na dotazník odpovědělo celkem 74 respondentů, které jsem dotazovala přes e-mail a sociální síť Instagram.

6.1.4 Zpracování dat

Získaná data z dotazníkového šetření byla zpracována pomocí Google documents, díky kterým autorka získala potřebné výstupní hodnoty. Následně je zpracovala v programu Microsoft Office Excel v podobě tabulek a některých grafů pro lepší přehlednost. Co se týče řízeného rozhovoru, níže jsou uvedené otázky kladené specialistovi společně s jeho odpověďmi. Na konci tohoto výzkumného šetření je uvedena komparace výstupu od respondentů jako laiků, a odborníka na kybernetickou bezpečnost.

6.2 Vyhodnocení dotazníkového šetření

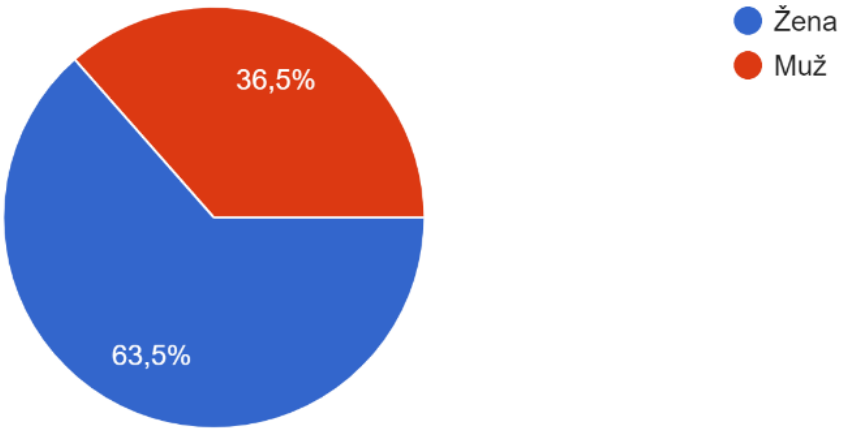
Otázka č. 1 Jaké je Vaše pohlaví?

Tabulka č. 6: Pohlaví respondentů

Pohlaví	Procenta	Počet
Žena	63,5%	47
Muž	36,5%	27
Celkem	100%	74

Zdroj: autorka

Graf č. 6: Procento zúčastněných žen a mužů



Zdroj: autorka

Z grafu i tabulky můžeme vyčíst, že se zúčastnilo 63,5 % žen, to znamená 46 žen a 36,5 % mužů, což je 27 osob mužského pohlaví. Výzkum měl tedy početnější zastoupení žen.

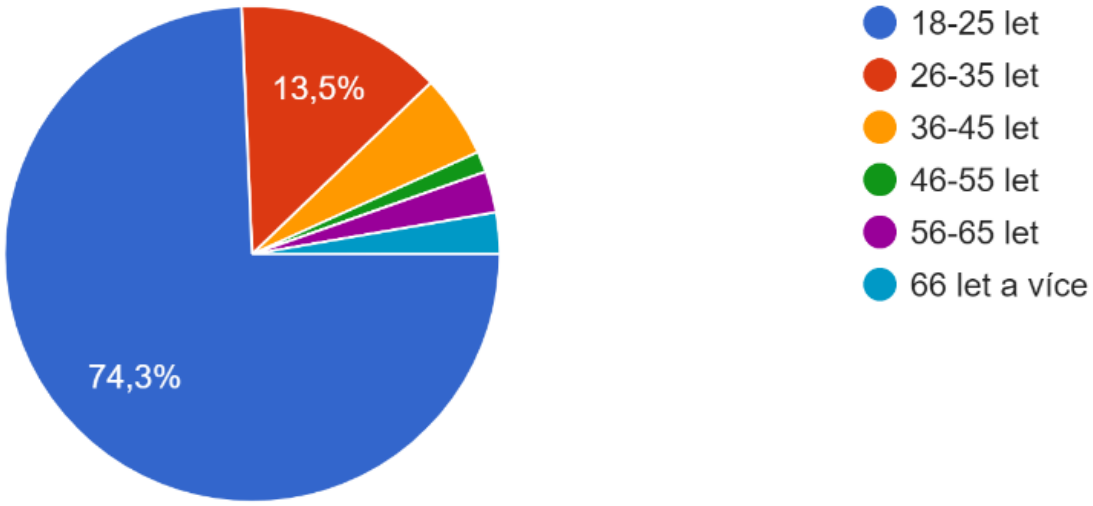
Otázka č. 2 Jaký je Váš věk?

Tabulka č. 7: Věk respondentů

Věk	Procenta	Počet
18-25	74,3%	55
26- 35	13,5%	10
36-45	5,4%	4
46-55	1,4%	1
56-65	2,7%	2
66 a více	2,7%	2
Celkem	100%	74

Zdroj: autor

Graf č. 7: Věk respondentů



Zdroj: autor

Dotazníkového šetření se v nejvyšším počtu zúčastnili respondenti ve věku 18-25 let (74,3 %), poté ve věku 26-35 let (13,5 %), třetí nejpočetnější skupinou byla věková kategorie od 36 do 45 let.

Věková hranici nad 18 let byla určena z důvodu zaměření na plnoleté jedince, kteří mají ze zákona vlastní odpovědnost, a mohli se setkat s hrozbou v oblasti kybernetické bezpečnosti.

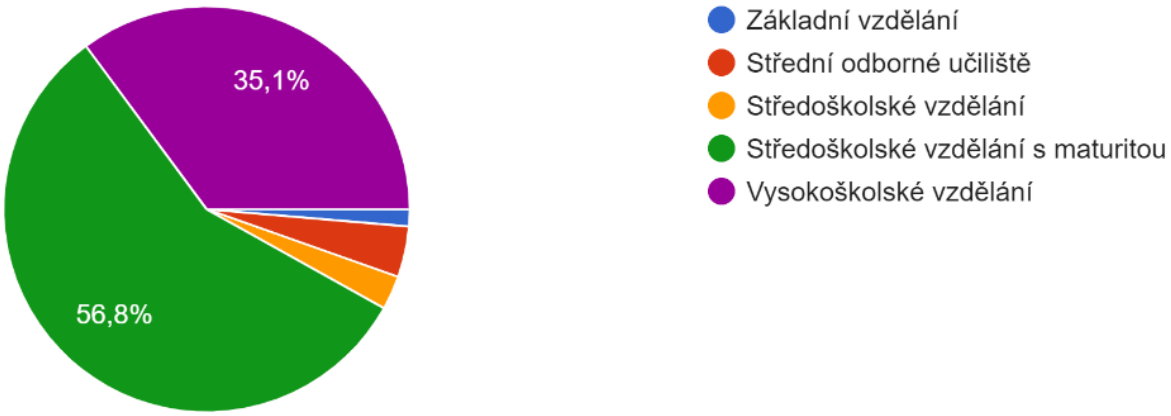
Otázka č. 3 Jaké je Vaše nejvyšší dosažené vzdělání?

Tabulka č. 8: Dosažené vzdělání respondentů

Vzdělání	Procenta	Počet
Základní vzdělání	1,4%	1
Střední odborné učiliště	4,1%	3
Středoškolské vzdělání	2,7%	2
Středoškolské vzdělání s maturitou	56,8%	42
Vysokoškolské vzdělání	35,1%	26
Celkem	100%	74

Zdroj: autorka

Graf č. 8: Dosažené vzdělání respondentů



Zdroj: autorka

Danou otázku autorka do dotazníku zařadila z důvodu zaznamenání kategorií osob dle dosaženého vzdělání. Toto rozřazení je pro šetření důležité, neboť na jeho základě lze uvážit, zda ovlivňuje povědomí respondentů o phishingu či jiných hrozbách v oblasti kybernetické bezpečnosti vzdělání či vlastní iniciativa.

Nejpočetnější skupinu tvoří respondenti se středoškolským vzděláním s maturitou (56,8 %). O necelých 22 % méně a na druhém, nejvíce zastoupeném místě jsou vysokoškolsky vzdělaní lidé, kteří činili 35,1 %. Zbylých 6 dotazovaných uvedlo, že mají dokončené buď základní vzdělání, střední odborné učiliště nebo střední školu bez maturity.

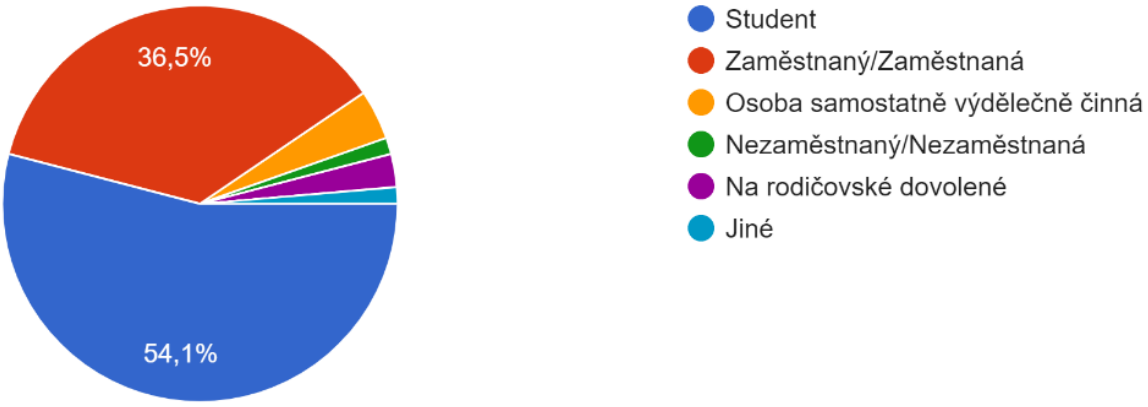
Otázka č. 4 Jaký je Váš aktuální status?

Tabulka č. 9: Status respondentů

Současnost	Procenta	Počet
Student	54,1%	40
Zaměstnaný/Zaměstnaná	36,5%	27
Osoba samostatně výdělečně činná	4,1%	3
Na rodičovské dovolené	2,7%	2
Nezaměstnaný/Nezaměstnaná	1,4%	1
Jiné	1,4%	1
Celkem	100%	74

Zdroj: autorka

Graf č. 9: Status respondentů



Zdroj: autorka

Důvodem pro určením současného stavu respondentů bylo, zda se dotazovaní pohybují ve školských zařízeních, v pracovním prostředí nebo aktuálně čerpají rodičovskou dovolenou či jsou nezaměstnaní. Otázka byla uvedena z důvodu domněnky, že aktuální status ovlivní následující odpovědi respondentů v dotazníku. Na odpovědi tak může mít vliv prostředí, ve kterém se nacházejí.

Souhrnně bylo dotazovaných 40 studentů (54,1 %), zaměstnaných 27 (36,5 %). Následující kategorie se pohybovaly v řádu jednotek. Výzkumného šetření se však zúčastnili i 3 osoby samostatně výdělečně činné (4,1 %).

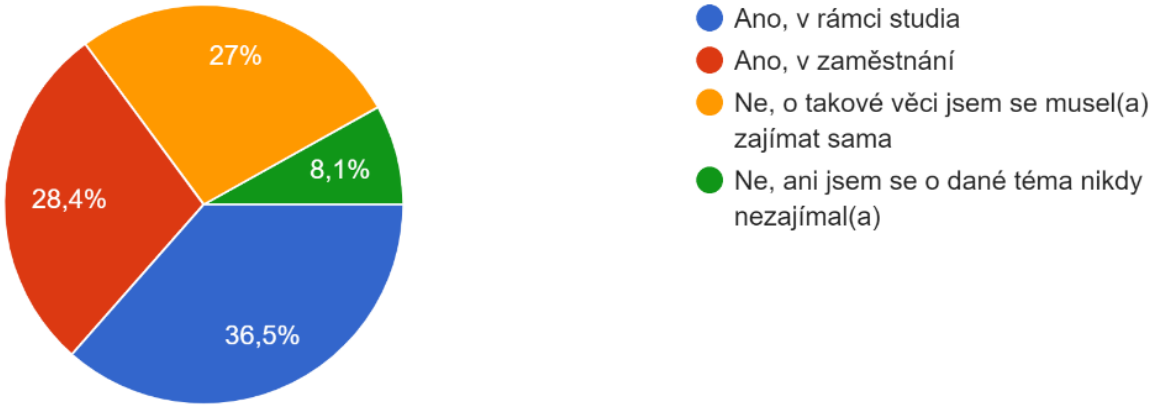
Otázka č. 5 Byla Vám poskytnuta možnost v rámci Vašeho studia či zaměstnání seznámit se s prevencí před kybernetickými hrozbami?

Tabulka č. 10: Přehled respondentů, kteří se seznámili s prevencí před kybernetickými hrozbami

Možnost seznámení s prevencí před kybernetickými hrozbami	Procento	Počet
Ano, v rámci studia	36,5%	27
Ano, v rámci zaměstnání	28,4%	21
Ne, o takové věci jsem se musel(a) zajímat sama	27%	20
Ne, ani jsem se o dané téma nikdy nezajímal(a)	8,1%	6
Celkem	100%	74

Zdroj: autorka

Graf č. 10: Procentuální ukazatel počtu respondentů, kteří se seznámili s prevencí před kybernetickými hrozbami



Zdroj: autorka

Z celkového počtu 74 respondentů má povědomí o prevenci před kybernetickými hrozbami 68 dotazovaných. V rámci studia se s ní setkalo 27 osob (36,5 %), v rámci zaměstnání 21 (28,4 %) a 20 tázaných (27 %) se s prevencí sice nesetkalo v pracovním nebo školním prostředí, avšak sami se o dané téma zajímali. V dotazníkovém šetření se však objevili i ti, kteří se s prevencí před kybernetickými hrozbami nikdy nesetkali a ani se o ni nezajímali.

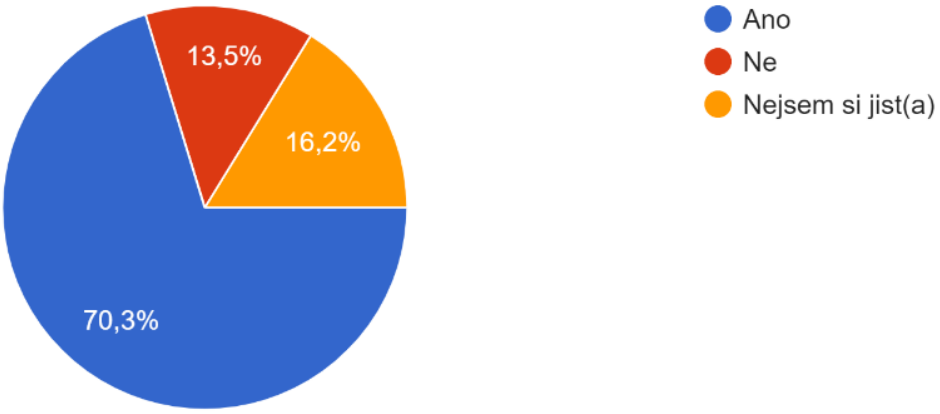
Otázka č. 6 Domníváte se, že jste se někdy setkal(a) s hrozbou v oblasti kybernetické bezpečnosti?

Tabulka č. 11: Přehled odpovědí respondentů, zda se setkali s kybernetickou hrozbou

Setkání s kybernetickou hrozbou	Procento	Počet
Ano	70,3%	52
Ne	13,5%	12
Nejsem si jist(a)	16,2%	10
Celkem	100%	74

Zdroj: autorka

Graf č. 11: Procentuální ukazatel odpovědí respondentů, zda se setkali s hrozbou v oblasti kybernetické bezpečnosti



Zdroj: autorka

Z tabulkového i grafického znázornění je patrné, že s kybernetickými hrozbami se setkala více než polovina dotazovaných. Celkem 52 respondentů (70,3 %) uvedlo, že se osobně setkali s hrozbou v oblasti kybernetické bezpečnosti. Dalších 12 tázaných (13,5 %) uvedlo, že tuto zkušenost doposud neměli a zbylých 10 jedinců (16,2 %) si nebyli jisti, zda se jednalo o kybernetickou hrozbu či nikoli.

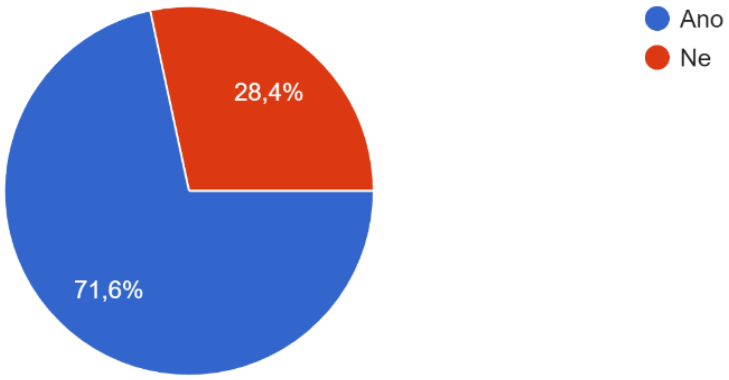
Otázka č. 7 Znáte někoho ve svém okolí, kdo byl obětí podvodného jednání v oblasti kybernetické bezpečnosti?

Tabulka č. 12: Přehled respondentů, kteří znají oběť podvodného jednání

Podvodné jednání v okolí respondentů	Procento	Počet
Ano	71,6%	53
Ne	28,4%	21
Celkem	100%	74

Zdroj: autorka

Graf č. 12: Procentuální ukazatel respondentů, kteří znají oběť podvodného jednání



Zdroj: autorka

Ze všech 74 oslovených se 53 (71,6 %) zná s obětí některého podvodného jednání v oblasti kybernetické bezpečnosti. Zbylých 21 dotazovaných (28,4 %) nemá ve svém okolí poškozenou osobu.

Otázka byla zvolena z důvodu navázání na předchozí dotaz, ve kterém se autorka ptala na možnou osobní zkušenost s některou z hrozeb. Respondenti se mohli s hrozbou setkat, avšak nemuseli se stát obětí. Dotaz je proto zaměřen na okolí respondentů, z důvodu dvou zjištění. Zaprvé, možné povědomí dotazovaného na dané téma a zadruhé, zda se v jeho okolí lidé setkávají s hrozbami v oblasti kybernetické bezpečnosti.

Otázky, které následovaly, byly založené na principu hodnocení respondentů od 1 do 5, kdy jednička představovala minimum a pětka maximum. Takto autorka koncipovala následující 4 otázky, které uvádí souhrnně.

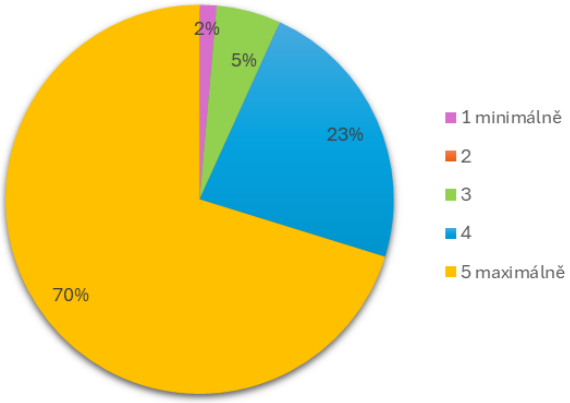
Otázka č. 8 Je podle Vás důležité se kybernetickou bezpečností zabývat?

Tabulka č. 13: Ohodnocení důležitosti kybernetické bezpečnosti respondenty

Důležitost zabývání se kybernetickou bezpečností	Procenta	Počet
1 minimálně	1,4%	1
2	0%	0
3	5,4%	4
4	23%	17
5 maximálně	70,3%	52
Celkem	100%	74

Zdroj: autorka

Graf č. 13: Procentuální ukazatel ohodnocení důležitosti kybernetické bezpečnosti respondenty



Zdroj: autorka

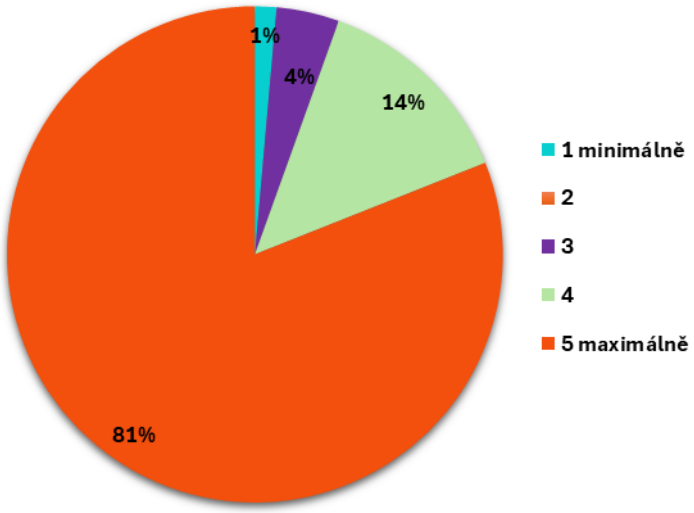
Otázka č. 9 Je podle Vás důležité proškolení dětí/mládeže v rámci prevence a hrozeb kybernetické bezpečnosti?

Tabulka č. 14: Ohodnocení důležitosti respondenty o proškolení dětí/mládeže v rámci prevence a hrozeb kybernetické bezpečnosti

Důležitost proškolení prevence a hrozeb kybernetické bezpečnosti u dětí/mládeže	Procenta	Počet
1 minimálně	1,4%	1
2	0%	0
3	4,1%	3
4	13,5%	10
5 maximálně	81,1%	60
Celkem	100%	74

Zdroj: autorka

Graf č. 14: Procentuální ukazatel ohodnocení důležitosti respondenty o proškolení dětí/mládeže v rámci prevence a hrozeb kybernetické bezpečnosti



Zdroj: autorka

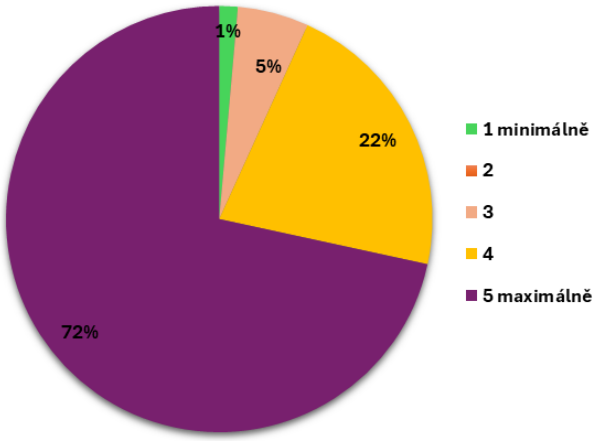
Otázka č. 10 Je podle Vás důležité proškolení dospělých v rámci prevence a hrozeb kybernetické bezpečnosti?

Tabulka č. 15: Ohodnocení důležitosti respondenty o proškolení dospělých v rámci prevence a hrozeb kybernetické bezpečnosti

Důležitost proškolení prevence a hrozeb kybernetické bezpečnosti u dospělých	Procenta	Počet
1 minimálně	1,4%	1
2	0%	0
3	5,4%	4
4	21,6%	16
5 maximálně	71,6%	53
Celkem	100%	74

Zdroj: autorka

Graf č. 15: Procentuální ukazatel ohodnocení důležitosti respondenty o proškolení dospělých v rámci prevence a hrozeb kybernetické bezpečnosti



Zdroj: autorka

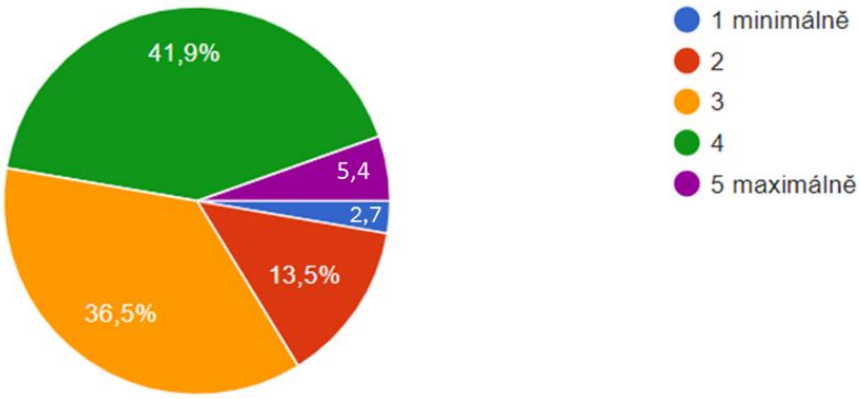
Otázka č. 11 Jak byste ohodnotil(a) svou připravenost na možný kybernetický útok

Tabulka č. 16: Ohodnocení vlastní připravenosti respondentů na kybernetické útoky

Ohodnocení vlastní připravenosti na kybernetické útoky	Procenta	Počet
1 minimálně	2,7%	2
2	13,5%	10
3	36,5%	27
4	41,9%	31
5 maximálně	5,4%	4
Celkem	100%	74

Zdroj: autorka

Graf č. 16: Procentuální ukazatel ohodnocení vlastní připravenosti respondentů na kybernetické útoky



Zdroj: autorka

Srovnáním všech výsledků těchto čtyř otázek je patrné, více než polovina respondentů hodnotí kybernetickou bezpečnost jako důležitý obor, kterým by se měli zabývat nejen dospělí, ale také děti a mládež ve školských zařízeních. První dotaz zaměřený na to, zda je důležité se kybernetickou bezpečností zabývat byl ohodnocen především od tří do pěti. Maximální důležitost, čili číslo pět v tomto případě zvolilo 52 dotázaných (70,3 %). Čtyřku označilo 17 osob (23 %) a 4 tázaní zvolili střední cestu, neboli číslo tři. Minimální důležitost označil z celého počtu 74 respondentů pouze 1 člověk. To znamená, že respondenti tuto problematiku považují převážně za podstatnou.

Navazuje další otázka se zaměřením na proškolení dětí/mládeže v této oblasti. Zde jsou výsledky jednoznačně na vyšší úrovni, než předtím. Proškolení prevence a hrozeb kybernetické bezpečnosti u dětí stanovilo na maximální úroveň 60 dotazovaných (81,1 %). Zde je důležité poznamenat vzrůstající hodnoty oproti předchozí otázce, kde nejvyšší důležitost označilo 52 tázaných, ovšem u dětí se tato hranice zvýšila na 60, čili o 8 lidí více. Opět se zde setkáváme s jedním respondentem, který neshledává proškolení dětí za podstatné.

Následně jsem pokračovala s otázkou stejného typu, ovšem lišící se zaměřením na jinou kategorii lidí, kterým byli dospělí jedinci. Důležitost proškolení dospělých v dané oblasti ohodnotilo 53 respondentů (71,6 %) číslem pět. Zde vidíme provázanost na první otázku z tohoto souhrnu, kde výsledky

ukazují stejné zastoupení, s výjimkou jednoho jednotlivce. Opět se zde ale setkáme s hodnocením minimální úrovně jedním dotazovaným.

Závěrečná otázka ze sekce tohoto bodového ohodnocení bylo posouzení vlastní připravenosti na kybernetické útoky. Zde již nejsou výsledky na vyšších bodových úrovních, ale spíše se pohybují na číslech od čtyřky do jedničky. Pouze 4 ze 74 respondentů (5,4 %) označili svou připravenost za maximální. Následuje 31 dotazovaných (41,9 %), kteří by svou akceschopnost hodnotili číslem čtyři. Následuje 27 tázaných (36,5 %), kteří si zvolili průměr, tudíž číslo tři. Druhou nejnižší připravenost zvolilo 10 osob (13,5 %) a nejnižší možnou úroveň zbylí 2 (2,7 %).

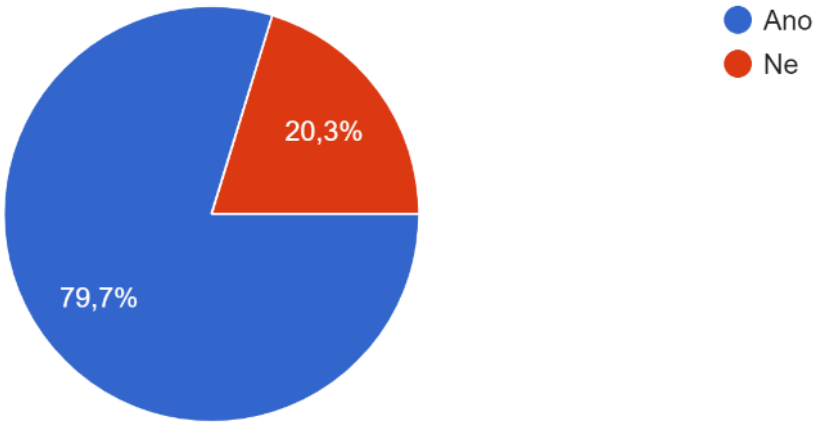
Otázka č. 12 Máte nainstalovaný antivirový program na svém počítači?

Tabulka č. 17: Přehled respondentů s instalovaným antivirovým programem

Instalovaný antivirový program	Procento	Počet
Ano	79,7%	59
Ne	20,3%	15
Celkem	100%	74

Zdroj: autorka

Graf č. 17: Procentuální ukazatel respondentů s instalovaným antivirovým programem



Zdroj: autorka

Daný dotaz byl do dotazníkového šetření zahrnut s cílem zjištění, zda se poměrná část respondentů může cítit zabezpečená z důvodu nainstalování antivirového programu. Vzhledem k předchozí otázce je možné usoudit, že vlastní připravenost mohli dotazovaní hodnotit lépe na základě této instalace, neboť si myslí, že jejich ochrana je dostatečná.

Z celkového počtu 74 tázaných má 59 (79,9 %) nainstalovaný antivirový program na svém zařízení. Zbylých 15 (20,3 %) tímto zabezpečením nedisponuje.

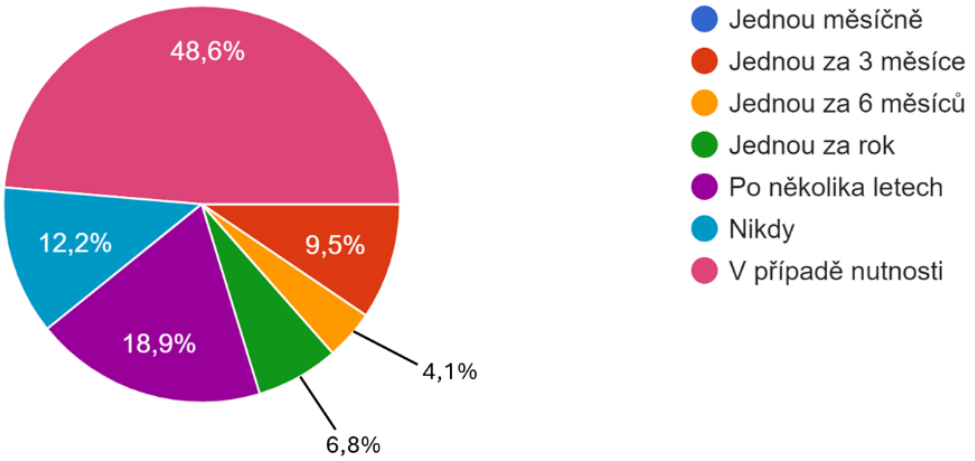
Otázka č. 13 Jak často aktualizujete svá hesla na zařízeních?

Tabulka č. 18: Přehled časového rozmezí mezi aktualizacemi hesel respondentů

Aktualizace hesel	Procenta	Počet
Jednou měsíčně	0%	0
Jednou za 3 měsíce	9,5%	7
Jednou za 6 měsíců	4,1%	3
Jednou za rok	6,8%	5
Po několika letech	18,9%	14
Nikdy	12,2%	9
V případě nutnosti	48,6%	36
Celkem	100%	74

Zdroj: autorka

Graf č. 18: Procentuální ukazatel časového rozmezí mezi aktualizacemi hesel respondentů



Zdroj: autorka

Aktualizace hesla je jednou z klíčových prevencí před kybernetickými hrozbami. Právě z toho důvodu se autorka v dotazníkovém šetření zaměřila i na tuto oblast v této a následující otázce.

Z dosažených výsledků vyplývá, že z celkového počtu 74 respondentů si hesla aktualizuje v určitém časovém úseku 65 osob, zbylých 9 (12,2 %) uvedlo, že si svá hesla neaktualizují nikdy. Jednou za tři měsíce provádí změnu svých hesel 7 dotazovaných (9,5 %), jednou za šest měsíců 3 (4,1 %) a jednou ročně 5 tázaných (6,8 %). Po několika letech si dosavadní hesla mění 14 dotazovaných

(18,9 %) a v případě nutnosti 36 osob (48,6 %). Poslední zmíněná možnost zahrnovala situaci, kdy byli respondenti jako uživatelé zařízení vyzváni k obměně svých hesel na jednotlivých účtech jako je např. Google.

Otázka č. 14 Jak postupujete při vytváření hesla na svých účtech či zařízeních?

Tato otázka byla koncipovaná tak, jak by ji mohl užít útočník v určité transformaci. Obětí potencionálního útoku by se tak mohli stát ti, kteří na tuto otázku reagovali. Cílem bylo rozpoznání respondentů, kteří se nechají ovlivnit procesem vyplňování dotazníku a tím prozradí svůj proces tvorby hesla. V případě, že by byly pro účely vyplnění dotazníku shromažďovány e-mailové adresy, byla by vidět i individuální odpověď respondenta. Čili, pokud by autorka byla hacker, mohla by tyto informace využít a zkoušet prolomit hesla. Což samozřejmě neučinila. Tázaní, kteří na tento dotaz odpověděli, odkryli, zda užívají slabá či silná hesla pro zabezpečení svého soukromí na internetu, počítačích, mobilu či tabletu.

V rámci tvorby otázek byl ponechán prostor na to, aby si respondenti mohli zvolit několik možností najednou v případě rozhodnutí vyplnit tuto část dotazníku. Účelem bylo dosáhnout toho, aby byla jejich možnost volby rozšířena a zároveň, aby nebylo na první pohled zřejmé, že se jedná o otázku, na kterou mají být chyceni.

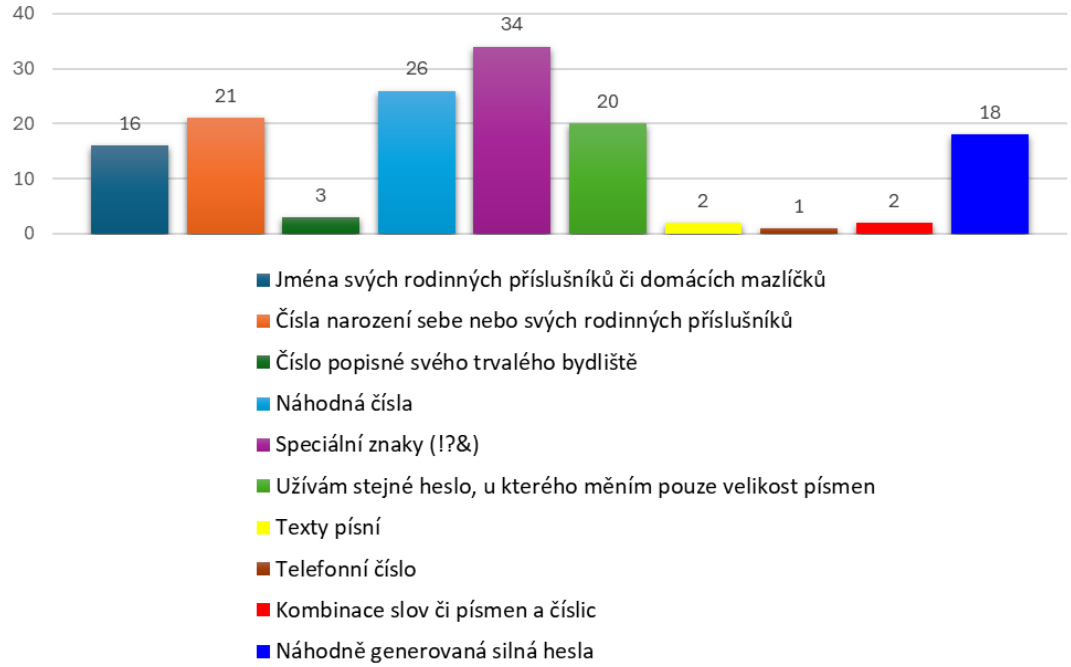
Tabulka č. 19: Postup respondentů při tvorbě hesla

Postup při vytváření hesel	Počet
Jména svých rodinných příslušníků či domácích mazlíčků	16
Čísla narození sebe nebo svých rodinných příslušníků	21
Číslo popisné svého trvalého bydliště	3
Náhodná čísla	26
Speciální znaky (!?&)	34
Užívám stejné heslo, u kterého měním pouze velikost písmen	20
Texty písní	2
Telefonní číslo	1
Kombinace slov či písmen a číslic	2
Náhodně generovaná silná hesla	18
Neuvedlo	2

Zdroj: autorka

Na tuto otázku z celkového počtu 74 respondentů neodpověděli pouze 2. Tudíž ostatní se nechali pohltit procesem vyplňování. Neuvědomili si, že údaje, které o sobě zveřejňují jsou citlivé, a neměli by je tudíž oznamovat ani autorce tohoto dotazníkového šetření.

Graf č. 19: Ukazatel výběru možností při tvorbě hesla respondenty



Zdroj: autorka

Každé heslo, které uživatel tvoří, by mělo být v nejlepším případě od něho odosobněno. Z toho důvodu není vhodné užívat jména svých příbuzných či mazlíčků nebo čísla narození. Všechny tyto informace jsou dohledatelné ať už na sociálních sítích či v různých portálech e-shopu. To stejné platí s číslem svého bydliště. Náhodná čísla a speciální znaky jsou výborným prostředkem zabezpečení, tudíž 27 respondentů, kteří tuto možnost zvolili jsou lépe zabezpečeni. Texty písní jsou dle názoru autorky dobře zapamatovatelnými hesly, pozor by si měli však dát dotazovaní na stránky cookies či různých platforem jako je např. Spotify, které sledují aktivitu uživatele a zaznamenávají nejoblíbenější songy. Může to velmi zúžit výběr možných variant. Co je naopak velkou hrozbou, je užívání telefonního čísla, který v mém dotazníku poznamenal pouze jeden respondent. Vzhledem k tomu, že jsou snadno dostupné, se jich může zmocnit útočník, který heslo prolomí téměř okamžitě. To samé platí u formulace stejného

hesla, u kterého uživatel pozmění pouze velikost písmen. Vzniká tu velká pravděpodobnost prolomení tohoto hesla, obzvlášť, pokud se o to v minulosti útočník již pokusil. Náhodně generovaná silná hesla jsou jedním z nejúčinnějších zabezpečení, které si může osoba zvolit. Avšak dle výsledků tuto možnost využívá pouze 18 respondentů ze 74.

Otázka č. 15 Jak uchováváte své heslo?

Uchování hesla je stejně tak důležité, jako jeho tvorba a aktualizace. Mnoho lidí si neuvědomuje, že jejich soukromí může být ohroženo také tím, že svá hesla sdílí s ostatními lidmi. Nemusí to být však vždy vědomě. Může se jednat o situaci, kdy si zaměstnanec firmy napíše heslo na lepící papírek a umístí ho k obrazovce počítače či notebooku. Poté může z daného místa na chvíli odejít a jeho kolega, který situace využije, se tak dostane díky přístupnému heslu do zařízení. Stejně tak se se může stát, že si někdo zapisuje svá hesla do poznámkových bloků v mobilních zařízeních, které mu může být odcizeno. Případný zloděj se tak nedostane nejen k mobilu, ale také k cenným informacím o poškozeném.

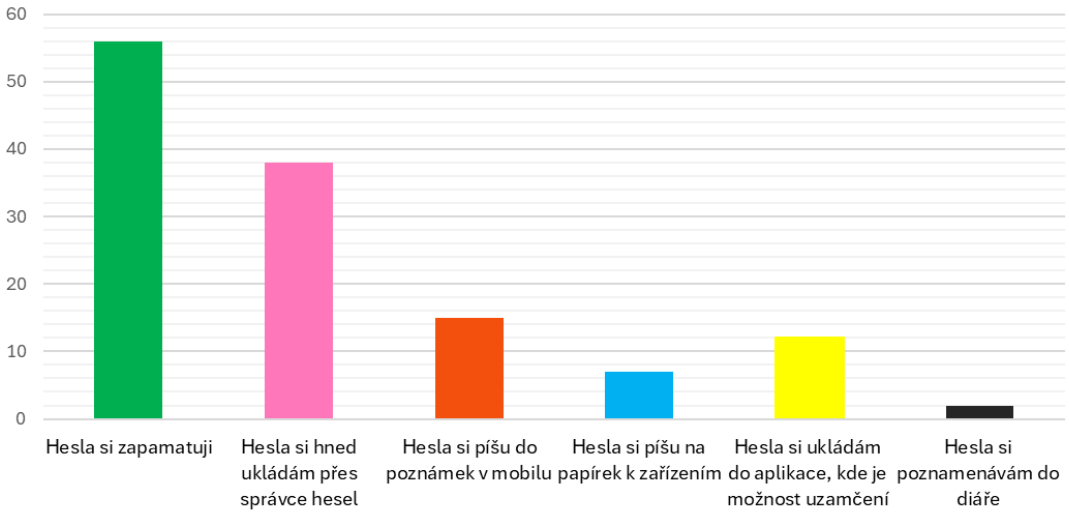
Tabulka č. 20: Uchování hesel preferované respondenty

Uchování hesel	Počet
Hesla si zapamatuji	56
Hesla si hned ukládám přes správce hesel	38
Hesla si píšu do poznámek v mobilu	15
Hesla si píšu na papírek k zařízením	7
Hesla si ukládám do aplikace, kde je možnost uzamčení	12
Hesla si poznamenávám do diáře	2

Zdroj: autorka

Možnosti výběru byly u této otázky otevřené. Tudíž se respondenti mohli rozhodnout pro více variant či napsat své vlastní. Výsledky ukazují, že dotazovaní si svá hesla více méně pamatují, případně si je ukládají přes správce hesel. Naopak jsou zde i výsledky, které jsou v oblasti zabezpečení znepokojivé. Jak je již zmíněno výše, není bezpečné uchování hesel v poznámkách zařízení či napsáním na papír či do diáře. Všechny tyto informace mohou být dohledány a zneužity.

Graf č. 20: Ukazatel preferovaného uchování hesel respondenty



Zdroj: autorka

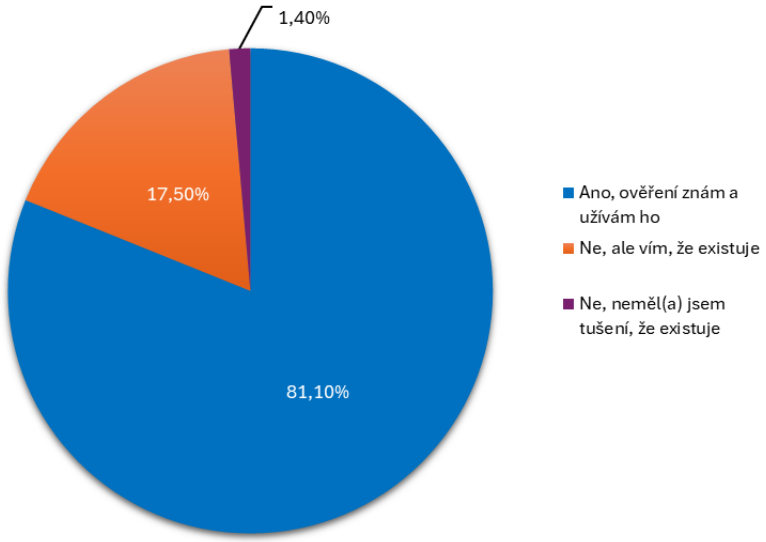
Otázka č. 16 Máte ponětí o tom, co znamená dvoufázové ověření a využíváte ho?

Tabulka č.21: Přehled respondentů se znalostí a využíváním dvoufázového ověření

Znalost a využívání dvoufázového ověření	Procento	Počet
Ano, ověření znám a užívám ho	81,1%	60
Ne, ale vím, že existuje	17,5%	13
Ne, neměl(a) jsem tušení, že existuje	1,4%	1
Celkem	100%	74

Zdroj: autorka

Graf č.21: Přehled respondentů se znalostí a využíváním dvoufázového ověření



Zdroj: autorka

Cílem této otázky byla snaha zjistit, zda mají respondenti ponětí o tom, co je dvoufázové ověření, zda ho využívají a do jaké míry jsou jakožto uživatelé internetu obeznámeni s možností chránit své účty dvoufázovým ověřením a kolik z nich tuto možnost reálně využívá. Využívání dvoufázového ověření u účtu zvyšuje jeho ochranu před napadením a odcizením účtu, zároveň také upozorňuje majitele účtu o pokusech se do účtu přihlásit a v neposlední řadě také usnadňuje možný návrat účtu původnímu majiteli.

Většina respondentů, konkrétně 60 (81,1 %) zná funkci dvoufázového ověřování a také ji využívá. Dalších 13 (17,5 %) respondentů o této funkci ví, ale zároveň ji aktivně nevyužívají. Pouze 1 respondent o této funkci vůbec nevěděl (1,4 %).

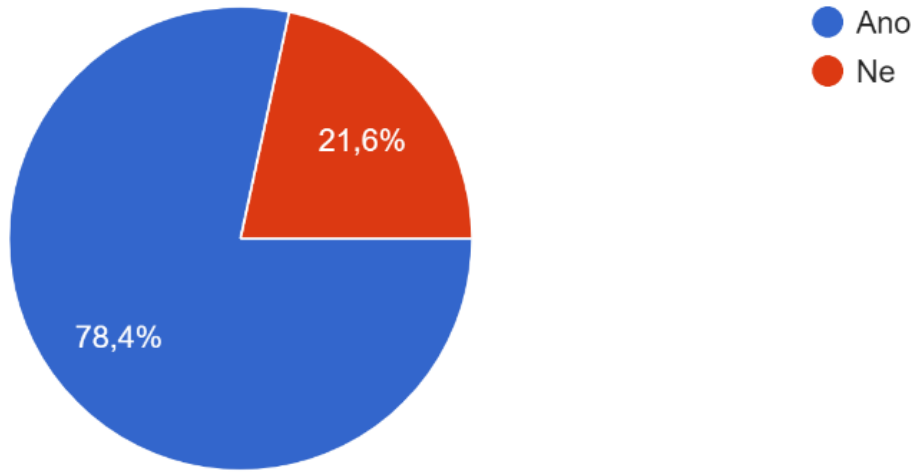
Otázka č. 17 Zálohujete si pravidelně svá data a soubory (fotografie, dokumenty, e-maily, účetnictví)?

Tabulka č. 22: Přehled respondentů zálohující si svá data a soubory

Zálohování dat a souborů	Procento	Počet
Ano	78,4%	58
Ne	21,6%	16
Celkem	100%	74

Zdroj: autorka

Graf č. 22: Procentuální ukazatel zálohování dat a souborů respondenty



Zdroj: autorka

Smyslem tohoto dotazu bylo zaměřit se na možnost kybernetického útoku v podobě ransomware. Zálohování dat a souborů je jedním z prvků ochrany proti této hrozbě.

Více než polovina respondentů si pravidelně zálohuje svá data a soubory, jedná se o 58 osob (78,4 %). Zbylých 16 dotazovaných (21,6 %) tuto činnost neprovádí pravidelně či vůbec.

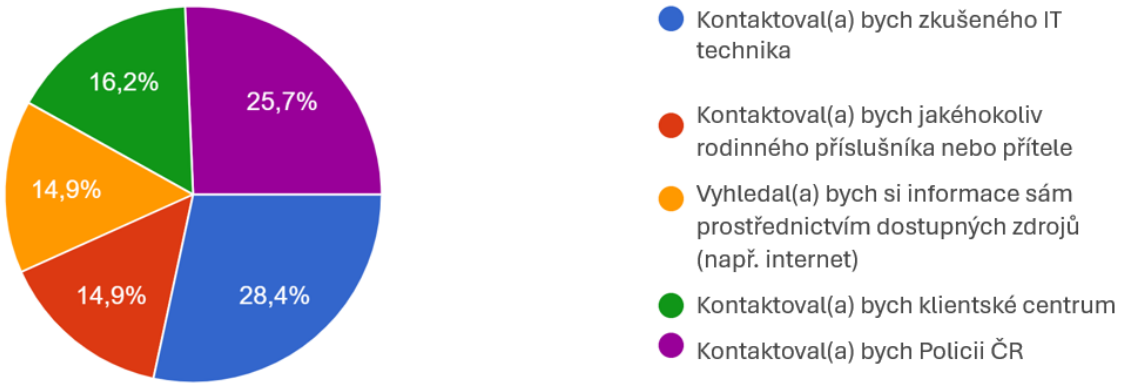
Otázka č. 18 V případě, že byste se stal(a) obětí kybernetického útoku, koho byste kontaktoval(a) jako prvního?

Tabulka č.23: Přehled respondentů a jejich osobní přístupu k řešení kybernetického útoku

V případě, že byste se stal(a) obětí kybernetického útoku, koho byste kontaktoval(a) jako prvního?	Procento	Počet
Kontaktoval(a) bych zkušeného IT technika	28,4%	21
Kontaktoval(a) bych jakéhokoliv rodinného příslušníka nebo přítele	14,9%	11
Vyhledal(a) bych si informace sám prostřednictvím dostupných zdrojů (např. internet)	14,9%	11
Kontaktoval(a) bych klientské centrum	16,2%	12
Kontaktoval(a) bych Policii ČR	25,7%	19
Celkem	100%	74

Zdroj: autorka

Graf č.23: Přehled respondentů a jejich osobní přístupu k řešení kybernetického útoku



Zdroj: autorka

Tato otázku byla do dotazníku zařazena z důvodu zjištění preferovaného řešení respondentů. Každý kybernetický útok se liší v závislosti na závažnosti útoku a prostředí, ve kterém nastane. V soukromém prostředí by v podstatě všechna navrhovaná řešení mohla v jistém smyslu fungovat, případně by bylo možné využít kombinaci více z nich. Ve firemním prostředí je velice důležité

neprodleně informovat IT technika a nadřízeného, kteří problém začnou řešit. Například odpojí napadenou část systému a začnou shromažďovat důkazy pro budoucí šetření. Ať už se jedná o sektor soukromý nebo firemní, je ze všeho nejdůležitější problém řešit okamžitě, neoddalovat ho, nenechat se vydírat útočníkem a podobně.

Dle názoru autorky se respondenti v této otázce rozhodovali dle jejich současného věku. Většina z nich 21 (28,4 %) odpověděla, že by kontaktovala IT specialistu. Druhou nejčastěji volenou variantou, kterou zvolilo 19 dotazovaných (25,7 %) bylo kontaktování Policie ČR. Jako třetí nejpreferovanější možnost kontaktování klientského centra vybralo 12 respondentů (16,2 %). Na posledním místě skočily shodně 11 (14,9 %) možnosti kontaktování rodinného příslušníka nebo kamaráda a vyhledání informací z volně dostupných zdrojů.

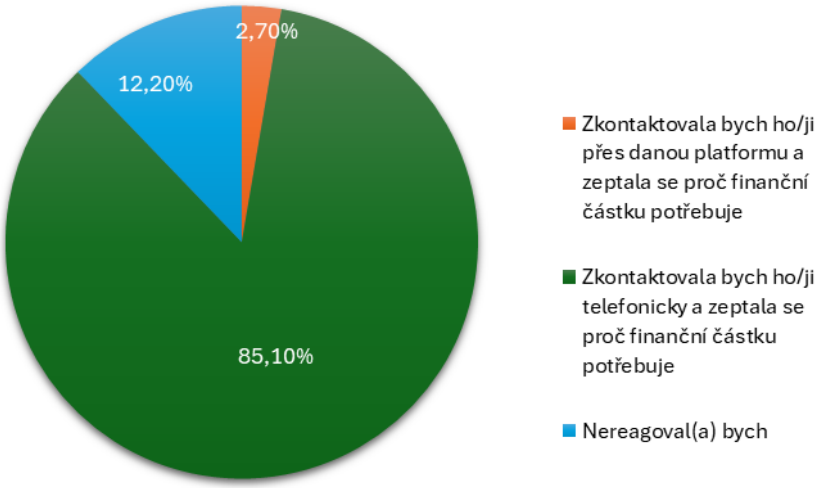
Otázka č. 19 Pokud by Vám známý, kamarád nebo rodinný příslušník napsal na sociálních sítích či v SMS, že potřebuje ihned poslat finanční částku, jaká by byla Vaše reakce?

Tabulka č. 24: Reakce respondentů na možné podvodné jednání s cílem získání financí

Reakce na možné podvodné jednání s cílem získání finanční částky	Procento	Počet
Okamžitě bych peníze poslal(a)	0%	0
Zkontaktovala bych ho/ji přes danou platformu a zeptala se proč finanční částku potřebuje	2,7%	2
Zkontaktovala bych ho/ji telefonicky a zeptala se proč finanční částku potřebuje	85,1%	63
Nereagoval(a) bych	12,2%	9
Celkem	100%	74

Zdroj: autorka

Graf č. 24: Procentuální ukazatel reakcí respondentů na podvodné jednání s cílem získání finančních prostředků



Zdroj: autorka

Napojení útočníků na sociální sítě či SMS je možné především díky spoofingu. Díky němu lze napodobit odesilatele zprávy a může se tak odeslaná zpráva navázat na předchozí komunikační kanál. Pokud by se tedy respondenti setkali s tímto podvodným jednáním, nejlepší variantou je zkontaktování dané osoby telefonicky, což by dle dosažených výsledků učinilo 63 dotazovaných (85,1 %). Na zprávu by vůbec nezareagovalo 9 tázaných (12,2 %) a zbylí 2 (2,7 %) by osobu zkontaktovali přes danou platformu. Tito dva respondenti by se v této situaci mohli eventuálně stát obětí kybernetického útoku, pokud by z následujících zpráv s danou osobou nerozpoznali podvodné jednání.

Následující otázky budou směřovány na kybernetickou hrozbu vishing, která je v dnešní době prováděná podvodníky vydávajícími se za zaměstnance bankovních institucí s cílem získání osobních dat od volaného. Je důležité zmínit, že bankéři či jiní pracovníci bank nekontaktují své zákazníky telefonicky pro ověření totožnosti či jiné potřebné údaje. Pokud by nastal jakýkoliv problém, který by vyžadoval okamžité řešení, bude daná osoba zkontaktována prostřednictvím telefonního hovoru a e-mailu, ve kterém mu budou shrnuty všechny informace společně s žádostí o dostavení se na nejbližší pobočku, kde se potřebné nedostatky vyřeší.

Další otázky budou opět shrnuty, z důvodu propojení na sebe navazujících dotazů, jejichž výsledky jsou hromadně sumarizovány.

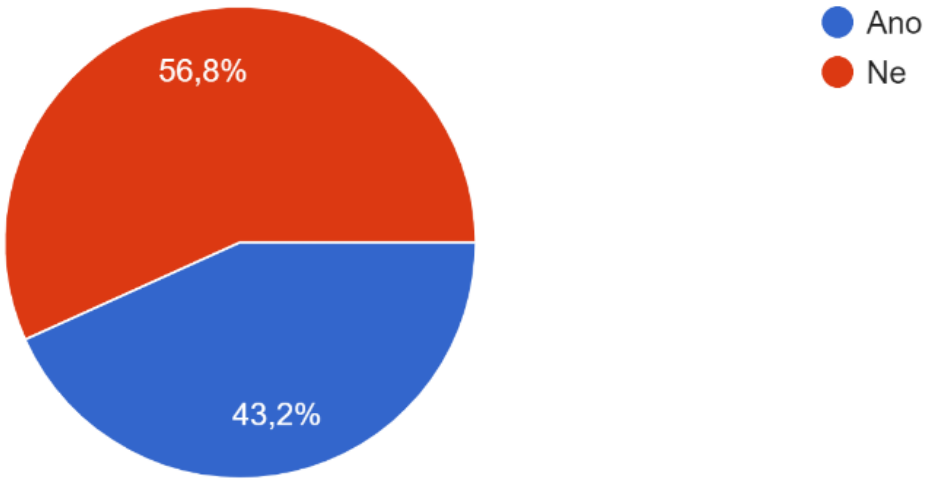
Otázka č. 20 Volal Vám někdy zaměstnanec banky a chtěl po Vás ověření totožnosti?

Tabulka č. 25: Přehled respondentů, kteří se mohli setkat s vishingem

Náhlý hovor bankéře s prosbou o ověření totožnosti	Procento	Počet
Ano	43,2%	32
Ne	56,8%	42
Celkem	100%	74

Zdroj: autorka

Graf č. 25: Procentuální ukazatel respondentů, kteří se mohli setkat s vishingem



Zdroj: autorka

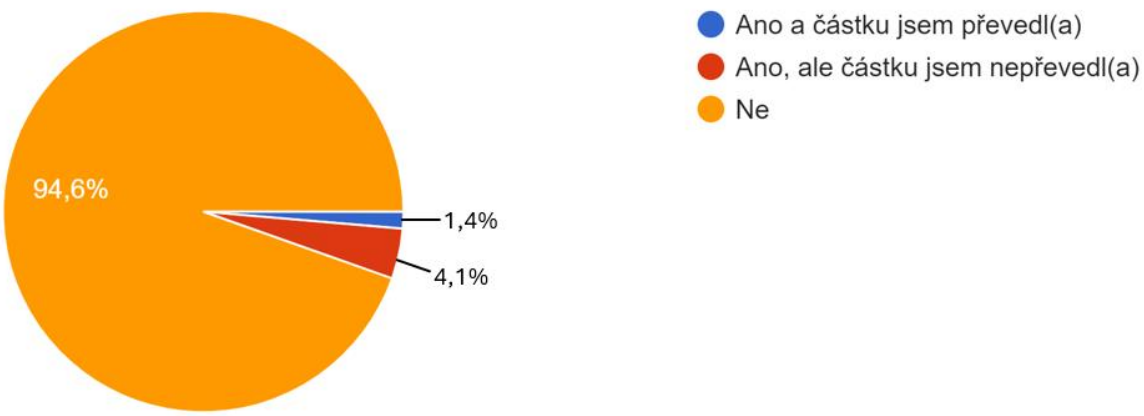
Otázka č. 21 Volal Vám někdy zaměstnanec banky s urgentní nutností převodu Vaší finanční částky na bezpečný účet?

Tabulka č. 26: Přehled odpovědí respondentů zaměřující se na vishing

Náhlý hovor bankéře s urgencí převodu finanční částky	Procento	Počet
Ano a částku jsem převedl(a)	1,4%	1
Ano, ale částku jsem nepřevedl(a)	4,1%	3
Ne	94,6%	70
Celkem	100%	74

Zdroj: autorka

Graf č. 26: Procentuální ukazatel počtu respondentů, kteří se mohli setkat s vishingem



Zdroj: autorka

Pokud se respondenti setkali s hovorem od bankovní instituce, která od nich požaduje bez jakékoliv předchozí komunikace informace jako ověření totožnosti, jedná se s největší pravděpodobností o podvodné jednání. Tuto zkušenost mělo dle výsledků šetření 32 dotazovaných (43,2 %). Zbývajících 42 osob (56,8 %) se s touto situací nesetkala.

Následoval dotaz na okolnosti, které by jednoznačně hrozbě vishing nasvědčovaly, tudíž hovorem s předmětem naléhání o převod financí na bezpečný účet. Z výsledků je patrné, že se s tímto podvodným jednáním setkali 4 respondenti, z nichž 3 (4,1 %) částku nepřevedli, ovšem jeden (1,4 %) ano. Je otázkou, zda tento respondent mohl případné následky zvrátit. Zbylých 70 dotázaných se s touto hrozbou doposud nesetkalo.

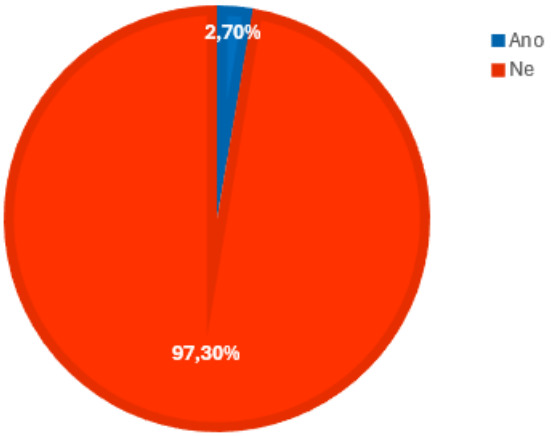
Otázka č. 22 Pokud byste dostal(a) e-mail s oznámením, že jste vyhrál(a) v soutěži, do které jste se ani nepřihlásil(a), a jediné, co po Vás v e-mailu chtěli je rozkliknutí přiložené adresy nebo stažení dotazníku k vyplnění Vašich údajů a adresy, učinil(a) byste tak?

Tabulka č. 27: Přehled odpovědí respondentů, zda by vyplnili osobní údaje v e-mailu

Podvodný e-mail	Procento	Počet
Ano	2,70%	2
Ne	97,30%	72
Celkem	100%	74

Zdroj: autorka

Graf č. 27: Procentuální ukazatel respondentů, kteří by vyplnili osobní údaje v e-mailu



Zdroj: autorka

Tato otázka je zaměřena na hlavní téma práce. Koncept tohoto e-mailového phishingu je jednou z možností, jak zlákat jedince k rozkliknutí či stažení dotazníku, který je v obou případech škodlivý. Nejenom, že tím respondent může přímo poskytnou útočníkovi své údaje, ale také je velká pravděpodobnost stažení malware či ransomware do koncového zařízení.

Z celkového počtu 74 respondentů by na tento phishingový útok zareagovaly pouze dva jedinci (2,70 %). Valná většina dotazovaných by v tomto případě odhalila podvodné jednání a na výhru by nezareagovala.

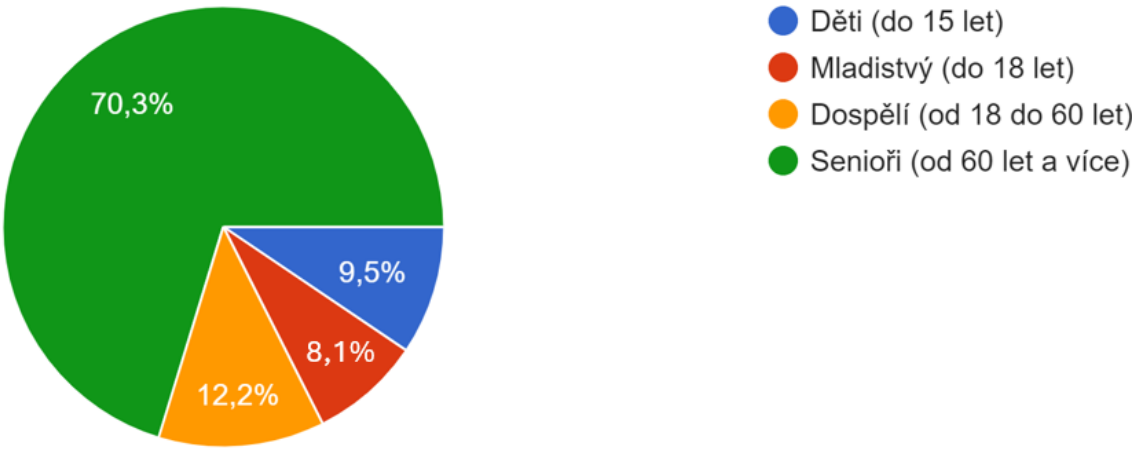
Otázka č. 23 Jaká je podle Vás neohroženější věková kategorie z pohledu kybernetické kriminality?

Tabulka č. 28: Přehled hodnocení nejohroženějších kategorií dle respondentů

Nejohroženější věková kategorie	Procenta	Počet
Děti (do 15 let)	9,5%	7
Mladistvý (do 18 let)	8,1%	6
Dospělí (od 18 do 60 let)	12,2%	9
Senioři (od 60 let a více)	70,3%	52
Celkem	100%	74

Zdroj: autorka

Graf č. 28: Procentuální hodnocení respondentů o nejohroženější věkové kategorii



Zdroj: autorka

Nejohroženější věková kategorie byla do dotazníkového šetření zahrnuta z důvodu komparace odpovědí respondentů a specialisty v oboru kybernetické bezpečnosti. Autorka považovala tento dotaz za důležitý z důvodu předpokladu zaměření na vzdělávání prevence a hrozeb v dané oblasti.

Více než polovina respondentů, konkrétně 52 (70,3 %) uvedla, že za nejvíce ohroženou kategorii z pohledu kybernetické kriminality považuje seniory. Druhý nejvyšší počet dotazovaných, a to 9 (12,2 %) označilo dospělé. Děti do věku patnácti let označilo 7 tázaných (9,5 %). Nejmenší počet v poměru zastoupení respondentů měla kategorie mladiství do osmnácti let, kterou vybralo 6 osob (8,1 %).

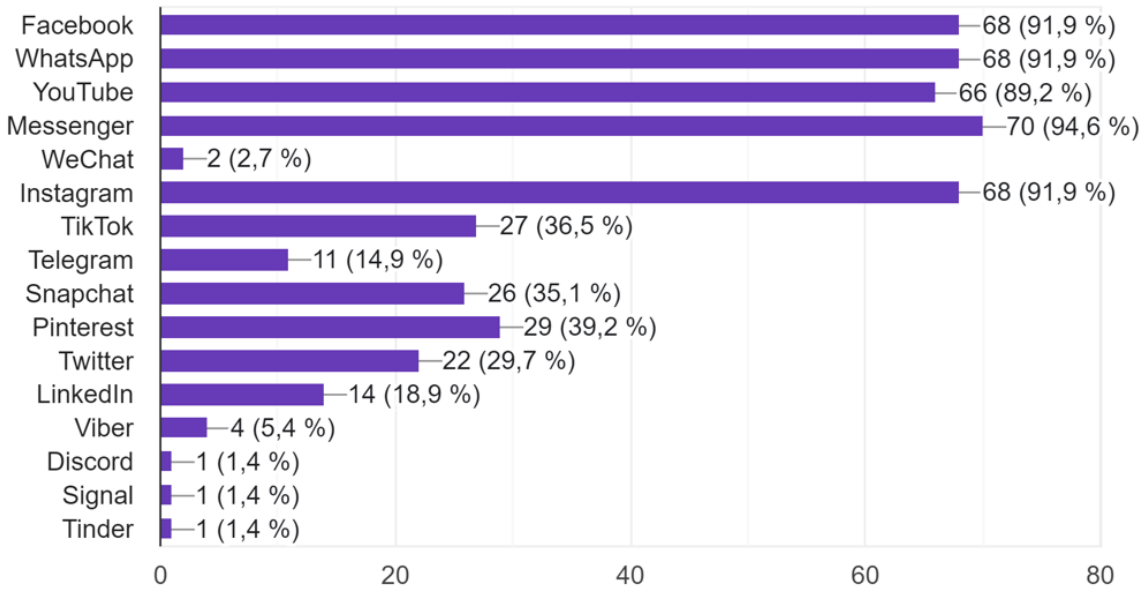
Otázka č. 24 Jaké sociální sítě a internetové platformy užíváte?

Tabulka č. 29: Sociální sítě a internetové platformy užívané respondenty

Užívané sociální sítě a internetové platformy	Počet
Facebook	68
WhatsApp	68
YouTube	66
Messenger	70
WeChat	2
Instagram	68
TikTok	27
Telegram	11
Snapchat	26
Pinterest	29
Twitter	22
LinkedIn	14
Viber	4
Discord	1
Signal	1
Tinder	1

Zdroj: autorka

Graf č. 29: Procentuální ukazatel užívání sociálních sítí a internetových platforem respondenty



Zdroj: autorka

Tato otázka měla opět možnosti zvolení více odpovědí. Záměrem bylo zjistit, zda se je mezi respondenty některý, který sociální sítě či internetové

platformy vůbec nevyužívá. Na tuto otázku však odpověděli všichni respondenti, tudíž je patrné, že digitální doba a bezpečnost na internetu se dotýká každého z nich.

Autorku nejvíce zajímal počet osob, kteří označí, že užívají aplikaci TikTok. TikTok byl totiž označen NÚKIBEM v roce 2023 za bezpečnostní hrozbu v oblasti kybernetické bezpečnosti. Přesněji řečeno, označil tuto hrozbu především pro uživatele, kteří mají zařízení přistupující k informačním a komunikačním systémům kritické informační infrastruktury, informačním systémům základní služby a významným informačním systémům. Varování se tedy týkalo především povinných osob dle zákona o kybernetické bezpečnosti. Ovšem, co je důležité, a mělo by být důležité i pro respondenty, jsou bezpečnostní hrozby, které tato platforma má. Množství shromažďovaných dat o uživatelích a způsob, jakým jsou sbírány a následně s nimi nakládáno představují hrozbu, která by měla být důvodem pro odinstalování. Neméně dobrým ukazatelem je také to, že tato služba podléhá právnímu a politickému prostředí Čínské lidové republiky[59], která nerespektuje lidská práva. To se může potvrdit také při nahlédnutí do podmínek, se kterými musí uživatelé TikTok souhlasit při vytváření účtu, kde se mimo jiné uvádí, že budou sledovány jejich klepy na zařízeních. To znamená, že jakékoliv kliknutí, ať už na mobilním nebo jiném zařízení bude sledováno a zaznamenáno. Pokud si uvědomíme, že se na všech platformách musíme přihlašovat jménem či e-mailem a zadáváme zde svá hesla, všechny tyto naše údaje jsou poskytnuty této druhé straně. TikTok dle dotazníkového šetření užívá 27 respondentů (36,5 %). Jejich osobní údaje jsou tak již zaznamenané, tudíž nechráněné a nezabezpečené.

Následující otázky jsou uváděny opět souhrnně, neboť souvisí s touto problematikou zmíněnou výše. Zaměření bude na Národní úřad pro kybernetickou a informační bezpečnost, také na podmínky při zakládání účtu aplikací či

[59] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Aplikace TikTok představuje bezpečnostní hrozbu*. Online. 2023. Dostupné z: https://nukib.gov.cz/cs/infoservis/hrozby/1941-aplikace-tiktok-predstavuje-bezpecnostni-hrozbu/. [cit. 2024-03-05].

webových stránek a zvlášť se poté autorka věnuje informacím sdílenými prostřednictvím sociálních sítí.

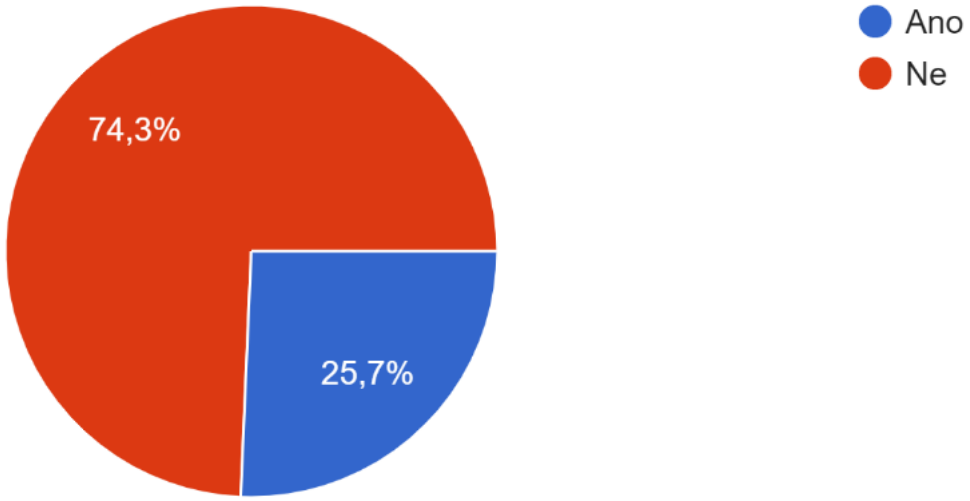
Otázka č. 25 Setkal(a) jste se někdy s doporučením od Národního úřadu pro kybernetickou a informační bezpečnost a máte ponětí o jeho činnosti?

Tabulka č. 30: Respondenti, kteří mají povědomí o činnosti NÚKIB

NÚKIB a jeho činnost	Procento	Počet
Ano	25,7%	19
Ne	74,3%	55
Celkem	100%	74

Zdroj: autorka

Graf č. 30: Procentuální ukazatel respondentů, kteří mají povědomí o činnosti NÚKIB



Zdroj: autorka

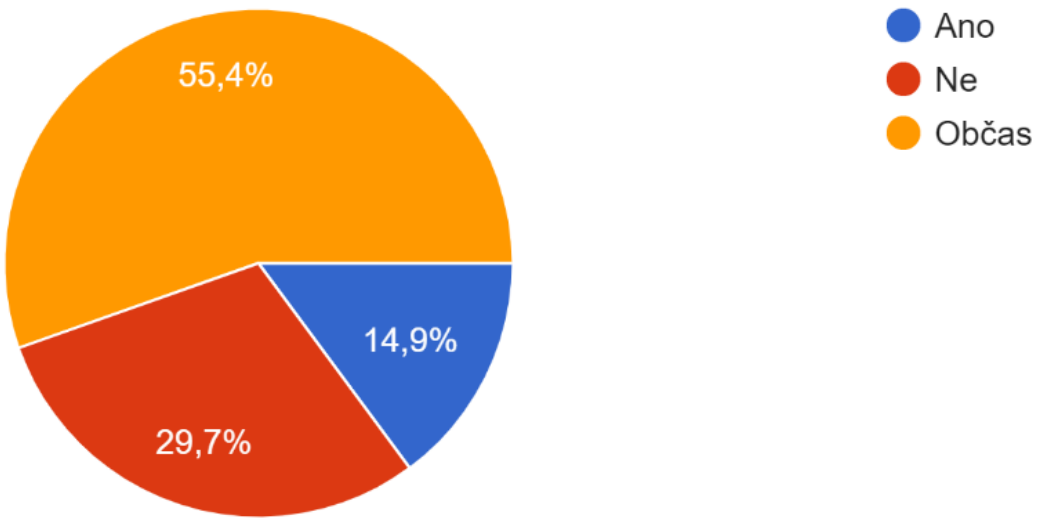
Otázka č. 26 Čtete si podmínky, než s nimi souhlasíte při založení účtu na některých webových stránkách či v aplikacích?

Tabulka č. 31: Přehled odpovědí respondentů ohledně čtení podmínek při založení účtů na webových stránkách a aplikacích

Čtení podmínek při založení účtu	Procento	Počet
Ano	14,9%	11
Ne	29,7%	22
Občas	55,4%	41
Celkem	100%	74

Zdroj: autorka

Graf č. 31: Procentuální ukazatel respondentů ohledně čtení podmínek při založení účtu na webových stránkách a aplikacích



Zdroj: autorka

Výsledky z dotazníkového šetření mohou nasvědčovat tomu, že respondenti, kteří v předchozí otázce označili, že užívají aplikaci TikTok se nemuseli setkat s varováním či jinými doporučeními od Národního úřadu pro kybernetickou a informační bezpečnost. Je zde určitá pravděpodobnost, že o této hrozbě nevědí, případně jsou s touto hrozbou obeznámeni, ale aplikaci chtějí dále užívat. S doporučením od NÚKIB se z celkového počtu 74 respondentů setkalo pouze 19 z nich (25,7 %). To znamená, že méně, než polovina respondentů má povědomí o tomto úřadu. Ostatních 55 dotazovaných (74,3 %) nemá ponětí o Národním úřadu pro kybernetickou a informační bezpečnost, ani o jeho činnosti.

Další otázka, která opět navazuje na předchozí problematiku, byla koncipována pro potvrzení, zda si respondenti čtou podmínky při založení účtu na webových stránkách či aplikací. Pouze 11 dotazovaných (14,9 %) si přečte podmínky před tím, než s nimi souhlasí. Dalších 41 (55,4 %) se s nimi seznámí občas. Zbylých 22 tázaných (29,7 %) se podmínkami nezabývá.

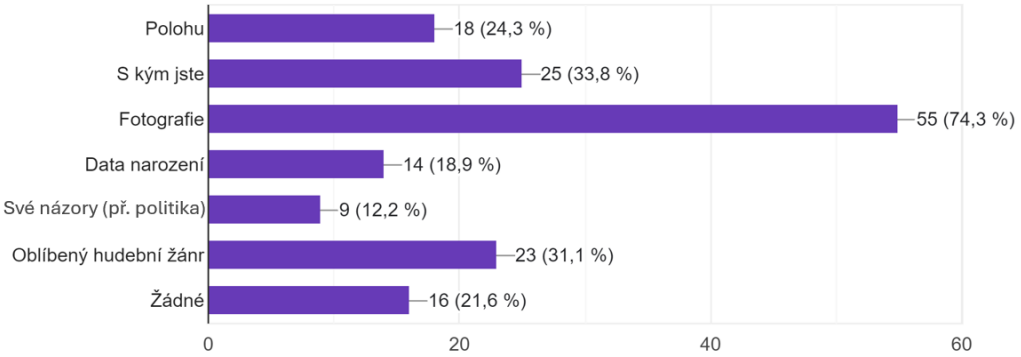
Otázka č. 27 Jaké informace o sobě dáváte vědět veřejně na sociálních sítích?

Tabulka č. 32: Přehled veřejně sdílených informací respondentů na sociálních sítích

Informace veřejně sdílené na sociálních sítích	Počet
Polohu	18
S kým jste	25
Fotografie	55
Data narození	14
Své názory (na politiku, aktuální dění ve světě apod.)	9
Oblíbený hudební žánr	23
Žádné	16

Zdroj: autorka

Graf č. 32: Procentuální ukazatel veřejně sdílených informací respondentů na sociálních sítí



Zdroj: autorka

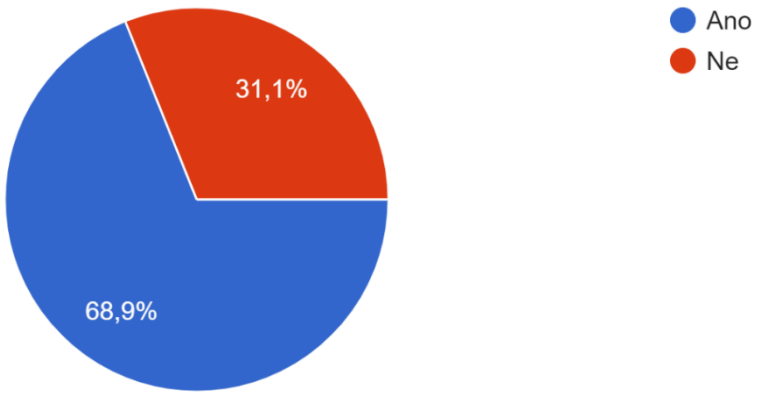
Otázka č. 28 Myslíte si, že Vás někdo může dle veřejně dostupných údajů na sociálních sítích kyberneticky ohrozit?

Tabulka č. 33: Přehled odpovědí respondentů ohledně kybernetického ohrožení z důvodu zveřejněných údajů na sociálních sítích

Kybernetické ohrožení díky údajům na sociálních sítích	Procento	Počet
Ano	68,9%	51
Ne	31,3%	23
Celkem	100%	74

Zdroj: autorka

Graf č. 33: Procentuální ukazatel odpovědí respondentů ohledně kybernetického ohrožení z důvodu zveřejněných údajů na sociálních sítích



Zdroj: autorka

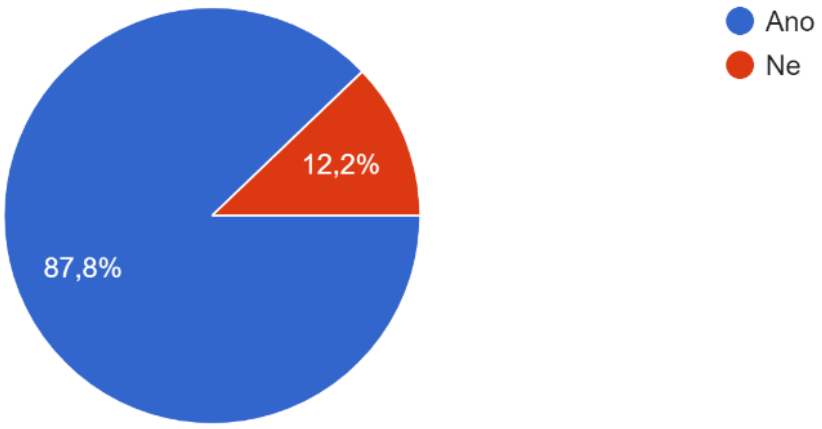
Otázka č. 29 Myslíte si, že v dnešní době jsou dostupné prostředky k tomu, aby s Vámi někdo manipuloval prostřednictvím Vašich sdílených fotek a videí?

Tabulka č. 34: Přehled odpovědí respondentů ohledně manipulace z důvodu sdílení obrazových a zvukových záznamů

Manipulace prostřednictvím sdílených obrazových a zvukových záznamů	Procento	Počet
Ano	87,8%	65
Ne	12,2%	9
Celkem	100%	74

Zdroj: autorka

Graf č. 34: Procentuální ukazatel odpovědí respondentů ohledně manipulace z důvodu sdílení obrazových a zvukových záznamů



Zdroj: autorka

Sdílení informací o sobě či jiných na sociálních sítích může představovat hrozbu představující jejich zneužití. Všechna data, která uživatel zveřejní na sociálních sítích či jiných platformách mohou hrát klíčovou roli pro potencionálního útočníka. Tyto informace lze užít jako prostředek pro phishingové útoky, které zahrnují získání přístupových údajů a v konečném případě mohou vést nejen ke ztrátě identity, ale také ke ztrátě finančních prostředků, nelegálně zajištěných úvěrů na údaje poškozeného a dalších nepříjemností. Kromě toho mohou být zveřejněné obrazové či zvukové záznamy upraveny tak, aby působily věrohodně pro rodinné příslušníky. Ti poté mohou být zmanipulováni podvodníkem k zaslání finanční částky či jiných údajů jenom proto, že se na daný podvod nachytají, neboť netuší, že osoba, která s nimi komunikuje není ten, za koho se vydává. V dnešním světě programů, jako je AI, lze již dokonale napodobit hlas pro zaslání hlasové zprávy či z fotografií udělat video, kdy oběť žádá o finanční částku. Všechny tyto prostředky jsou již dnes dostupné a útočníci tohoto technologického pokroku využívají.

Sdílení informací o poloze užívá 18 respondentů (24,3 %), dalších 25 (33,8 %) zveřejňuje i osoby, se kterými se nacházejí. Fotografie sdílí 55 dotazovaných (74,3 %), což je více než polovina z celkového počtu. Data narození sdílí 14 tázaných (18,9 %). Názory na politiku, aktuální dění ve světě a podobné náměty 9 osob (12,2 %). Oblíbený hudební žánr uveřejňuje 23 respondentů (31,1 %).

Údaje, které veřejně zpřístupní uživatel na sociálních sítích mohou být opět zdrojem pro možný kybernetický útok. S tímto názorem souhlasí 51 dotazovaných (68,9 %). Naopak nesouhlas projevilo 23 tázaných (31,3 %).

Co se týče poslední otázky z těchto souhrnných odpovědí, s myšlenkou manipulace osoby prostřednictvím sdílených obrazových a zvukových záznamů souhlasí 65 respondentů (87,8 %). Zbylých 9 (12,2 %) nevnímá zveřejňování fotografií a videí za potencionální hrozbu.

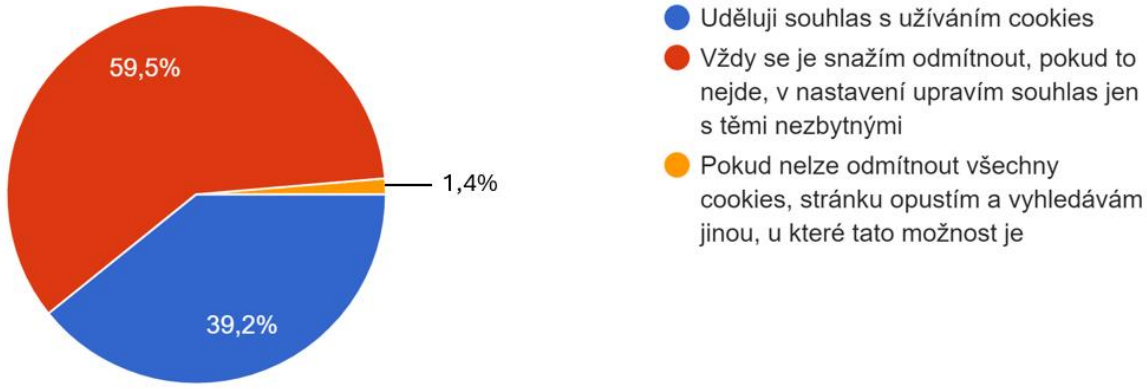
Otázka č. 30 Jak reagujete na soubory cookies?

Tabulka č. 35: Reakce respondentů na soubory cookies

Reakce na soubory cookies	Procento	Počet
Uděluji souhlas s užíváním cookies	39,2%	29
Vždy se je snažím odmítnout, pokud to nejde, v nastavení upravím souhlas jen s těmi nezbytnými	59,5%	44
Pokud nelze odmítnout všechny cookies, stránku opustím a vyhledávám jinou, u které tato možnost je	1,4%	1
Celkem	100%	74

Zdroj: autorka

Graf č. 35: Procentuální ukazatel reakcí na soubory cookies



Zdroj: autorka

Soubory cookies jsou popsány v teoretické části této práce. Je tedy také jedním z možných důvodů pro kybernetický útok z důvodu zaznamenávání informací o uživateli.

Souhlas s užíváním cookies, tedy se všemi jeho podbody, které zahrnují sběr informací pro reklamní a marketingové účely apod. uděluje dle výsledků 29 respondentů (39,2 %). Více než polovina dotazovaných, konkrétně 44 (59,5 %) však volí pouze nezbytné soubory cookies. Mezi tázanými se však našel i jedinec (1,4 %), který si své soukromí velice střeží, a označil možnost, která zahrnuje, že pokud nelze cookies zcela odmítnout, danou stránku opustí.

6.3 Vyhodnocení řízeného rozhovoru s expertem

Poslední šetření, které autorka učinila pro praktickou část práce je řízený rozhovor se specialistou na kybernetickou bezpečnost. Rozhovor jsem provedla v hlavním sídle společnosti T-Mobile v Praze na Roztylech 29. února 2024.

Mgr. Šimon Kubrt pracuje ve společnosti T-Mobile Czech Republic a.s. od června 2021 na pozici Senior specialista informační bezpečnosti. Tato pozice zahrnuje znalosti od Business Continuity Managementu, krizového řízení až po vzdělávání v oblasti kybernetické bezpečnosti a naplňování požadavků zákona o kybernetické bezpečnosti.

T-Mobile je subjekt kritické infrastruktury za oblast poskytování služeb v telekomunikačním prostředí. Tím pádem svou činností zasahuje i do státní správy. Kromě toho je jednou z největších telekomunikačních společností v České republice, která spadá pod Deutsche Telekom, což je největší telekomunikační společnost na světě.

1. **Proškoluje Vaše firma své zaměstnance na kybernetické hrozby? A pokud ano, jak často?**

Zaměstnance proškolujeme. Pro naši firmu se jedná o povinnost ze zákona. Proškolujeme formou E-Learningu, což je jednou ročně nebo při nástupu či změně pracovní pozice. Takže musí každý zaměstnanec projít E-Learningovým školením, kde se dozví aktuality o nových kybernetických hrozbách, se kterými se může potkávat ve vztahu k T-Mobile. Jedná se například o to, jak rozpoznat phishing, podvodné e-maily, a samozřejmě aby poznal proces, jak na ně reagovat. Toto je důležité během školení zmiňovat. Samozřejmě jsou i situace, které nelze do školení obsáhnout, což jsou nové hrozby. O nich informujeme prostřednictvím interní sociální sítě, kde jsou nejaktuálnější informace dostupné všem zaměstnancům. Ti se mohou k novinkám vyjádřit, doptat se, jedná se o „live poradnu“.

2. **Zapojuje se T-Mobile do programů na prevenci před kybernetickými hrozbami?**

Určitě, nejen, že máme interně nastavený systém vzdělávání, ale implementujeme je i do externího prostředí. Spolupracujeme s několika organizacemi v oblasti kybernetické bezpečnosti, jako s Českou bankovní asociací, nebo máme vlastní programy, které jsou jak pro seniory, tak pro děti. Snažíme se vzdělávat o tom, co na ně v digitálním prostoru číhá a jak se proti tomu bránit. Není to vztaženo pouze k phishingu, ale i k složitějším úrovním, aby mohli například rozpoznat ransomware, aby uměli s těmito hrozbami pracovat a aby se nebáli komunikace.

Proč se zaměřujete zrovna na děti a na seniory?

Považujeme to za slabší skupinu, obzvláště seniory. Z mého osobního pohledu se nedá ani moc divit, že s technologiemi neumí tak dobře pracovat. Nevidí, jak se mohou šířit dezinformace vlivem sociálních sítí apod. U dětí se jedná dnes o generaci, která v prostředí počítačů a telefonů vyrůstá. Z mých zkušeností v rámci proškolování jsem zjistil, že oproti seniorům jsou na tom velmi dobře. Nesmíme však dopustit zanedbání ani v této oblasti.

3. **Poskytuje T-Mobile nějaký program či aplikaci pro zaměstnance nebo zákazníky, která může upozornit na podvodné jednání?**

Poskytujeme program Klik pro klid. Jedná se o webovou stránku, kde uživatel najde desatero, které je nejzákladnější vzdělávací portál pro lidi mimo T-Mobile. Samozřejmě je dostupný i našim zaměstnancům. Nově, je od minulého měsíce v mobilní aplikaci Můj T-Mobile sekce bezpečnost. V ní si naši zákazníci mohou projít bezpečnostním kvízem, podívat se na hlubší desatero co a jak dělat. Není to pouze tedy o poukázání na hrozby jako je právě phishing, ale i jak ji poznat a co dělat, když se člověk nachytá.

Je zde tedy zahrnuta nějaká prevence a zároveň co mají dělat, pokud by daná hrozba přišla?

Ano, přesně tak.

4. **S jakými nejzávažnějšími kybernetickými incidenty se T-Mobile setkal? Jak jste případně reagovali a jaká opatření učinili?**

V dnešní době se incidentů děje mnoho. V naší společnosti máme spoustu filtrů a detekčních systémů, které dokážou rozpoznat hrozbu dříve, než se dostane k zaměstnancům. Každý den se setkáváme s mnoha pokusy o útoky, které odstraňujeme. Samozřejmě se může stát, že občas dojde k průniku. Bohužel jsme se před necelými dvěma lety staly obětí ransomwarového útoku, nicméně to nepostihlo naše zákazníky, to bylo nejdůležitější. Nedošlo k únikům dat a zákazníci měli dostupné své služby. Jednalo se spíše o interní ochromení firmy jako takové. Reagovali jsme poměrně rychle, situace nastala v neděli dopoledne, došlo k aktivaci krizového řízení a všech detekčních systémů, které máme. Co se týče opatření, dovolil bych si říct, že je máme až dodnes. Rozběhlo se mnoho projektů na zlepšení bezpečnosti. Samozřejmě to souvisí i s penězi, snažili jsme se zajistit budget na to, abychom mohli naši bezpečnost ještě vylepšit.

5. **Má T-Mobile určený interní postup pro zvládání kybernetických incidentů?**

Interní postup máme postavený na úrovni krizového řízení, je implementovatelný na většinu krizových situací. Samozřejmě jedna část je věnovaná právě kybernetickým incidentům. Je specifická v našem interním postupu, základem je však oznámení zaměstnance o jakémkoliv incidentu našemu IT oddělení, které se tímto zabývá. Tento postup neustále testujeme a snažíme se jí vylepšovat.

6. **Jak se Vás dotkla NIS 2?**

NIS2 se nás vlastně nedotkla. NIS 2 se především dotkla České republiky, u nás jde především o nový zákon o kybernetické bezpečnosti. Osobně si dovolím říct, že se nás dotkne pouze v určitých částech. Dnes se spíše řídíme vyhláškou o kybernetické bezpečnosti, která je v mnoha opatřeních velice podobná nové, připravované legislativě. Pro T-Mobile to bude znamenat, že nebudou ovlivněny pouze naše základní služby jako mobilní hlas a mobilní data, ale budou pod ní spadat i další služby jako je poskytování data center, případně cloud computing, který je teď, dle mého názoru, dosti známý. Opatření tedy budeme muset implementovat i na ostatní služby, nebo spíše ověřit si, že je tam máme. Zatím

provádíme přípravu a zjišťujeme, že opatření jsou zaváděna plošně, bez ohledu na to, jestli tam požadavek zákonu je či není. Spíše to tedy naši firmu dopadá v takových specifických oblastech jako je řízení dodavatelů nebo zajišťování služeb pouze z území České republiky.

7. **Měl v minulosti T-Mobile navázanou spolupráci s NÚKIBEM? Případně jak byste ohodnotil spolupráci s Národním úřadem pro kybernetickou a informační bezpečnost?**

Spolupráce s NÚKIB samozřejmě probíhá. Obzvlášť v posledních dvou letech velice intenzivně. Národní úřad pro kybernetickou a informační bezpečnost hovoří zcela otevřeně o všech svých záměrech a změnách, což je asi jeden z mála státních úřadů, který toto dělá. Pokud se bavíme o ostatních bezpečnostních sborech, vidím to i u Generálního ředitelství HZS, ale u NÚKIB to hodnotíme velice pozitivně. Jsme rádi, že nám otevřeně sdělují proč, co a jak zamýšlejí a především nám dávají možnost se k těmto věcem vyjádřit. Co stojí za zmínku je také to, že NÚKIB pořádá cvičení pro subjekty kritické infrastruktury, kterých jsme se účastnili.

8. **Jaké jsou dle Vás největší chyby, které běžný uživatel dělá, aniž by si uvědomil kybernetická rizika s tím spojená?**

Většinou jsou to ty nejbanálnější záležitosti, které existují. Například odejdete od počítače a nezamknete si ho. V pracovním prostředí, kde je open space, nebo jste v prosklené zasedačce, kde na vás každý vidí, si může někdo sednout a dělat na vašem zařízení co chce. To je za mě to největší riziko, které se mohou zaměstnanci nebo kdokoli dopustit. Můžete pracovat v kavárně, nechat si otevřený počítač, a scénář bude stejný. To stejné neplatí pouze pro počítač, ale i pro telefon nebo jakékoliv zařízení připojené k internetu a do digitálního světa. Zamknutí je dle mého názoru to nejzákladnější.

9. **Jakou nejzásadnější chybu vidíte v rámci phishingu?**

V souvislosti s phishingem je důležité kontrolovat odesilatele. Phishingy jsou velmi sofistikované, ale toto je základ, na který bychom si měli dávat pozor. Prevence se vždy odvíjí od toho nejzákladnějšího. V rámci vishingu či spoofingu to platí stejně. Banka nikdy neoslovuje své zákazníky, aby jim dali číslo karty nebo PIN.

Vždy by daná osoba měla zavolat bance zpět, pokud si nejsme jisti. I kdyby to banka opravdu byla, je lepší vždy zavolat nazpět.

10. **Jak se T-Mobile staví k únikům dat a jaký je postih za porušení interních pravidel pro kybernetickou bezpečnost?**

Únik dat můžeme brát buď jako úmyslný nebo neúmyslný čin. Úmyslný, čili jako trestná činnost může být zapříčiněn nespokojeným zaměstnancem, který bude z firmy odcházet, nebo právě pokud je kybernetický útok, který zapříčiní to, že data uniknou. S únikem dat jsme se doposud nesetkali, implementujeme spoustu opatření pro jeho podchycení. Co se týče interních zaměstnanců z pohledu kriminální trestné činnosti, můžeme si představit nespokojeného zaměstnance, který bude z firmy odcházet. Je naštvaný a svá data si chce vzít. Jenomže tyto data nejsou jeho. Cokoliv udělá pod hlavičkou právnické osoby, data z tohoto jednání patří společnosti. Na to je potřeba také nastavit opatření. V T-Mobile máme systém prevence krádeže informací, kde zjišťujeme objem dat, které se kopírují na flash disky nebo jiné datové nosiče. Pokud zjistíme, že by zaměstnanec chtěl data vzít, bude to pak předmětem interního vyšetřování.

11. **Setkal jste se někdy sám v rámci své práce s kybernetickým útokem, ať už osobně či Vaši kolegové?**

Osobně ne. Hodně útoků je mířeno na kolegy. Kolegyně se v nedávné době setkala s vishingem. Jednalo se o hovor od bankovní společnosti, kterou ani neměla. Volající se představil jako Petr Novák, ovšem jeho přízvuk byl jednoznačně ruský či ukrajinský. Byly tam všechny znaky vishingu, kolegyně samozřejmě na výzvy nereagovala. Útoky se opravdu dějí, nevyhýbají se ani nám, jsou všude. Mimo pracovní prostředí jsem se setkal s útokem u svého známého, kterého vodili za nos až do té doby, než skončil u bitcoinového automatu. Ten již takové štěstí neměl.

12. **Co by mohly fyzické/podnikající fyzické či právnické osoby udělat jinak, aby se nestaly obětí phishingu?**

Vzdělávat se, nic jiného nepomůže. Důležité je se zajímat o trendy. Není to o dlouhém čtení, jedná se o pár jednoduchých pravidel, které je schopný si

vyhledat každý. Platformy jak bankovní, tak telekomunikační poskytují nápovědy pro rozpoznání podvodného jednání, například bezpečností desatera, o kterých jsem již mluvil. Vždy platí jednoduché pravidlo, když jsi nejsem jistý, zeptám se. Každý je odpovědný sám za sebe a měl by si tyto věci hlídat, a mít chuť se v tomto odvětví vzdělávat. Každému se může stát, že se nachytá, protože útočníci jsou opravdu vychytralí. Útoky provádějí většinou ráno nebo v časech, kdy jde lidi nejvíce zblbnout. Vše dělají sofistikovaně, proto je zapotřebí být dokonale připraven, což není těžké. Můj osobní názor je ten, že pokud osoba čte o nových hrozbách a věnuje se jim, je možno škodlivému následku předejít. I kdyby šlo o jednoduché novinové články.

13. **Je problematika kybernetické bezpečnosti dostatečně implementovaná do výchovy a vzdělávání žáků na základních a středních školách?**

Když jsem měl přednášku pro děti ze základní školy obecně, velice mě překvapily, co všechno znají. Osobně si ale myslím, že se vše dozvěděly samy, než že by na to měly předmět. Slyšel jsem, že se na některých školách kybernetická bezpečnost již zmiňuje, ale spíše věřím, že se tomu děti věnují samy.

Takže věříte tomu, že si děti nebo žáci povědomí vytvářejí sami?

Ano, ale potvrzené to nemám. Jedná se spíše o mé tušení.

14. **Má dospělá populace dostatečné znalosti o této oblasti, a především o tom, jak se chránit, aby se nestali obětí takových podvodů?**

Zde je odpověď spíše negativnější. Přeci jen se jedná o generaci, která nevyrůstala s počítačem nebo chytrým telefonem, na což se samozřejmě musíme zaměřovat, především na starší ročníky. Věřím, že lidem, kterým je kolem čtyřiceti, padesáti let, si rizika uvědomují. Setkávám se spíše s tím, že se zeptají, než by se sami vzdělávali. Nestydí se ale zeptat, což je skvělé. U seniorů je však potřeba větší zaměření. Útočníci si jsou vědomi, že senioři jsou jejich nejúspěšnější skupina. Takže proto se i my v T-Mobile snažíme na ně zaměřovat.

7. Vyhodnocení výzkumného šetření

Pro konečné shrnutí praktické části práce je nutno se vrátit k výzkumným předpokladům, které byly určeny na začátku výzkumu. Vyhodnocení se vztahuje k oběma částem výzkumu, kvalitativní i kvantitativní.

P 1: Více než polovina respondentů vyplní v dotazníku postup při vytváření hesel, který by mohl být využit k phishingovému útoku, ačkoliv dle specialisty jsou dostupné informace, které varují před tímto jednáním.

Tento výzkumný předpoklad se dá považovat za hlavní, neboť byl cíleně umístěn uprostřed dotazníkového šetření jako otázka č. 14. Pro respondenty mohla působit zcela neškodně, ovšem její vyplnění představuje jedno z možných rizik. Dotazovaní, kteří vyplnili tuto otázku odkryli své osobní informace, aniž by si to uvědomovali. Pokud by se nejednalo o účely dotazníkového šetření, ale o běžnou situaci, mohlo by být jejich heslo prolomeno. Situování otázky a možnost výběru několika druhů řešení společně s možností dopsání svých vlastních informací měla tázané vybízet ke sdílnosti, především pak vyplnění. V procesu zodpovídání na všechny otázky se 72 respondentů (97,3 %) ani nepozastavilo nad tím, zda tyto informace nejsou příliš zasahující do jejich soukromí. Na tuto otázku, tudíž správně, neodpověděli pouze 2 dotazovaní (2,7 %). Odmítli sdělit tyto citlivé informace a lze tedy předpokládat, že mají povědomí o hrozbě, jakým může být právě phishing. Vědí, že tyto informace se nesmí za žádných okolností sdělovat.

Dle specialisty v oboru kybernetické bezpečnosti je důležité především vzdělávání v tomto odvětví. V rozhovoru, konkrétně v otázce č. 12, zmiňuje že platformy bankovních nebo telekomunikačních institucí poskytují nápovědy pro rozpoznání podvodného jednání jakým mohou být například bezpečnostní desatera. Zároveň zde uvádí, že každý jedinec je odpovědný sám za sebe a je nutné si tyto věci zabezpečit.

Na základě získaných výsledků je výzkumný předpoklad verifikován.

P 2: Nastane shoda mezi odpovědí specialisty a nejvíce zastoupeného počtu respondentů v rámci nejohroženější věkové kategorie z pohledu kybernetické kriminality.

K potvrzení či vyvrácení tohoto výzkumného předpokladu nalezneme odpověď v grafech a tabulkách č. 28. Nejvyšší počet respondentů uvádí kategorii seniorů, kterou v dotazníkovém šetření označilo 52 dotazovaných (70,3 %).

Specialista uvedl, že v rámci vzdělávání v oboru kybernetické bezpečnosti je jejich zaměření na kategorie dětí a seniorů. Po doplňující otázce, proč se upínají právě na tyto skupiny odborník odpověděl, že jsou považovány za slabší, obzvláště senioři, neboť neumí s danými technologiemi pracovat tak dobře. Dále uvedl, že děti jsou dle jeho osobních zkušeností znalostně na vyšší úrovni, než starší jedinci.

Díky odpovědi zaměstnance subjektu kritické infrastruktury zahrnuté v druhé otázce řízeného rozhovoru a výsledkům z dotazníku je výzkumný předpoklad verifikován.

P 3: Více než polovina respondentů i specialista zná osobu, která se stala obětí podvodného jednání v oblasti kybernetické bezpečnosti.

Dle výsledků z dotazníkového šetření u otázky č. 7 je zřejmé, že 53 respondentů (71,6 %) znají osobu, která se stala obětí podvodného jednání v oblasti kybernetické bezpečnosti.

Odborník v rozhovoru u otázky č. 11 uvedl, že u jeho kolegyně byl pokus o kybernetický útok vishing. Jednalo se o podvodný hovor z bankovní společnosti, který naplňoval všechny znaky tohoto podvodného jednání. Obětí se však nestala. Kromě toho se ale také zmínil o známém, který působí mimo pracovní prostředí subjektu kritické infrastruktury. Ten se obětí vishingu bohužel stal, neboť, jak uvádí sám odborník už skončil u bitcoinového automatu. Zde je možnost poukázat na odborné znalosti v oblasti kybernetické bezpečnosti. Kolegyně, která má vědomosti o daných hrozbách se úspěšně útoku vyhnula. U výše zmíněné osoby však došlo k dosažení cíle útočníků.

Na základě získaných výsledků je tento výzkumný předpoklad verifikován.

P 4: Více než 30 % respondentů by při zjištění, že se stali obětí kybernetického útoku, jako první kontaktovali zkušeného IT technika, stejně, jako zaměstnanci subjektu kritické infrastruktury.

Dle výsledků dotazníkového šetření z grafů a tabulek č. 23 by zkušeného IT technika kontaktovalo 21 respondentů (28,4 %). Jednalo se o výsledky preferovaného řešení dotazovaných, tudíž je nutné zohlednit možnosti, kterými disponují. Pokud bude autorka vycházet ze statusu v tabulce č. 9 je zřejmé, že 54,1 % tázaných byli studenti, 36,5 % zaměstnaní a 4,1 % osoby samostatně výdělečně činné. Tato otázka tedy směřovala také k tomu, v jakém prostředí se respondenti nejvíce pohybují a zda mají potřebné kontakty na zkušeného IT technika. Ať už v pracovním prostředí nebo mimo něj.

Specialista subjektu kritické infrastruktury uvádí v páté otázce rozhovoru informaci o interním postupu, kde kromě její specifičnosti také zmiňuje, že základem je oznámení jakéhokoliv incidentu oddělení IT, které se danou problematikou zabývá.

Na základě těchto výsledků je výzkumný předpoklad falzifikován.

P 5: Více než polovina respondentů se setkala s kybernetickou hrozbou vishing, stejně, jako specialista.

Odpovědi respondentů pro výsledné potvrzení či vyvrácení tohoto posledního výzkumného předpokladu nalezneme v otázkách č. 20 až 21. Dotazy byly stylizované jako situace, se kterými se respondenti mohli v minulosti setkat a naplňovaly by znaky kybernetické hrozby vishingu.

První z nich autorka koncipuje záměrně tak, aby bylo zřejmé, že zaměstnanec banky volá dotazovaným, nikoli naopak, a dožaduje se ověření totožnosti. Jak již bylo zmíněno v teoretické části práce nebo řízeném rozhovoru, banka nikdy neoslovuje zákazníky, aby jim poskytli zničehonic totožnost či číslo karty nebo dokonce PIN. Daná osoba by v takovém případě měla hovor ukončit a zavolat na klientskou linku, aby se ujistila, že se nejedná o podvodné jednání.

S náhlým hovorem od bankéře s výše zmíněnou prosbou se setkalo 32 tázaných (43, 2 %). Zbylých 42 (56, 8 %) se v této situaci neocitli.

Následující otázka se opět týkala hovoru se zaměstnancem bankovní instituce, tentokrát s urgencí převodu finanční částky na bezpečný účet. Pouze 4 (5,5 %) ze 74 dotazovaných se s takovým jednáním setkalo, avšak jeden z nich peněžní sumu skutečně převedl.

Odborník v oblasti kybernetické bezpečnosti ve své odpovědi na otázku č. 11 odpověděl, že se doposud s kybernetickým útokem nesetkal. Tudíž ani s hrozbou, kterou vishing představuje.

Na základě získaných výsledků je výzkumný předpoklad falzifikován.

8. Návrhy opatření

Než se autorka přiblíží k návrhům opatření jako takovým, je nutno zmínit několik poznatků. Hrozby, jaké známe dnes, v podobě útoků na koncová zařízení nejsou to jediné, čeho bychom se měli obávat. Dnes již mnoho lidí využívá elektromobily, jehož technika je opět naváděna přes software. Dle názoru autorky je jen otázkou času, než se začnou kybernetické útoky vztahovat i na tuto kategorii. Může dojít k újmě na zdraví či životech lidí. Vývojáři v automobilovém průmyslu by na tuto skutečnost měli myslet a zajistit bezpečnost před možným napadením.

Nyní blíže k návrhům opatření. V rámci zpracovávání práce se autorka ve svém okolí dotazovala na problematiku kybernetické bezpečnosti, phishingu a jiných útoků, které mohou zasáhnout kohokoliv. Většina pracujících odpověděla, že v zaměstnání mají povinnost být jedenkrát ročně na schůzce věnující se tomuto tématu. Studenti středních a vysokých škol uvedli, že se tomuto tématu věnují ve školských zařízeních jen formou kroužků či přednášek jednou za několik let. Sama autorka musí potvrdit, že na Policejní akademii se právo kybernetické bezpečnosti vyučuje jen jako nepovinný, povinně volitelný předmět. Tato prevence není považována za dostačující. Inovace naší společnosti je nezastavitelná stejně jako nové hrozby, které s ní přicházejí. Proto by autorka jako první návrh opatření zmínila, aby se této problematice věnovalo více času a prostoru. Pokud se tak stane, zaznamenáme zlepšení reakce lidí na kybernetické útoky, budou vědět s jakými riziky se mohou setkat, jak v těchto případech postupovat, a případní útočníci nebudou mít vysokou úspěšnost, jako tomu bylo v minulosti.

Kybernetická bezpečnost je jedním z bezpečnostních aspektů, které hrají a do budoucna budou hrát velice významnou roli. Neměli bychom tedy připouštět nedostatečné pojetí ze strany legislativy. Trestní zákoník je sice velice obsáhlý, avšak části, které by se mohli užít na sankcionování útočníků není dle názoru autorky dostatečný. Autorka doufá, že se v rámci sepsání nového zákona o kybernetické bezpečnosti zahrne i přímé pojmenování jednotlivých hrozeb jakými jsou phishing, malware, ransomware a podobných, a to společně s trestním sazebníkem. Tresty by neměly dosahovat řádu několika let nebo zákazu činnosti či propadnutí věci. Jejich koncept by měl být na vysoké úrovni.

Myšlenka, že nebohý senior poskytne své životní úspory pro to, aby pomohl někomu v nouzi nebo se sám do ní nedostal, a při dopadení útočníka bude jeho sankce pouze v těchto rovinách, je nedostatečná.

Dalším návrhem opatření je zavedení pravidelných školení na základních a středních školách i domovech pro seniory. V dnešní době existuje mnoho soukromých společností, které tuto problematiku řeší, poskytují možnosti proškolení, a především informují o prevenci. Tím se tato problematika dostane do povědomí nejohroženějších kategorií, které v rámci kybernetické bezpečnosti jsou. Jak je již zmíněno výše, nelze zapomínat také na pracovníky, ať už státní či soukromé sféry.

Zároveň by se v rámci školních předmětů měla vyučovat bezpečnost. Dle názoru autorky se jedná o klíčovou, někdy ale velmi opomíjenou vědu, která se vyučuje především na vysokých školách. Přitom obklopuje celý náš svět. V rámci výuky by se tedy mohla zahrnout problematika kybernetické bezpečnosti, která by byla pro žáky nejen prevencí, ale mohla by v nich vzbudit i zájem o dané téma, kterému by se mohli do budoucna věnovat. Mohla by tak vzniknout generace, která bude mít vynikající poznatky o bezpečnosti, kybernetické bezpečnosti a IT. Do budoucna by to mohlo být velmi potřebné, neboť digitalizace se bude neustále prohlubovat.

Dalším návrhem opatření je poskytnutí antivirových programů dotovaných státem společně s non stop linkou řešící potenciální útoky, na které by se osoby mohly ihned obracet. Jednalo by se o prostředek k ochraně občanů, kteří si nemohou toto zabezpečení dovolit nebo nemají ve svém okolí zkušené IT techniky, které by případnou hrozbu mohli vyřešit. Vzhledem k tomu, že Česká republika má hájit zájmy svých občanů a chránit jejich životy, zdraví, ale také majetek, je tato implementace z mého pohledu na místě. Pro tento účel by se mohla vytvořit státní IT služba, která by program nejen utvořila, ale také se stala jeho zabezpečovatelem a zároveň provozovatelem bezpečnostní linky pro hrozby útoků. Tudíž by byla zajištěná ochrana občanů státem v kybernetické oblasti a zároveň by se vytvořila nová pracovní místa. Autorka si je vědoma toho, že každý je v rámci kybernetických hrozeb odpovědný sám za sebe, ovšem v našem společenství jsou i ti, kteří si toto zabezpečení nemohou dovolit.

Nemusí se vždy jednat jen o sociálně slabší skupiny, ale také o studenty nebo seniory, kteří nemají potřebné kontakty či prostředky. Autorka se tedy opírá o výsledky v praktické části této práce. Při myšlence, že se v současnosti i ve školách připravují prezentace nebo slohové práce psané na počítači, je zapotřebí mít i dostatečnou ochranu pro tato zařízení. Toto řešení by bylo pokrokové a mohli bychom tak předejít nemalým újmám, které by v budoucnu mohly hrozit.

Posledním návrhem opatření je implementace umělé inteligence do většiny bezpečnostních systémů. AI může v tomto ohledu pomoci s detekcí útoků. Tím, že se neustále učí, by již na jednotlivé hrozby byla připravena a její chybovost by byla minimální. Zároveň by posloužila pro rychlejší zpracování a analýzu dat. Tento nástroj by tak mohl být využit nejen k sofistikovanějším útokům, ale také k ochraně. Je samozřejmé, že užití těchto programů by bylo do jisté míry riskantní, ovšem při správném podchycení všech počínajících rizik by tento systém mohl fungovat a vedl by k větší efektivitě.

Závěr

Oblast kybernetické bezpečnosti bude i v budoucnu jedním z nejdůležitějších aspektů bezpečnostního prostředí České republiky. Správné fungování informačních a komunikačních systémů je klíčové pro všechny státy na světě, neboť podporují rozvoj společnosti založený na vyspělé technologii. Pokud budou včas a řádně podchyceny počínající hrozby ohrožující tyto významné části, bude možné zajistit vyšší stabilitu celkového systému.

V úvodní části je první kapitola věnována vymezení základních pojmů, které jsou klíčové v návaznosti na téma práce. Definují se tedy pojmy bezpečnost, bezpečnost IT, kybernetická bezpečnost, kybernetický prostor, data a informace. Druhá kapitola je se více zaměřena na kybernetickou bezpečnost z pohledu rozsahu, způsobu ohrožení a incidentů. Z hlediska rozsahu je uveden kromě statistických ukazatelů užívaní internetu také pojem digitalizace a triády CIA a DAD, které má kybernetická bezpečnost chránit pro zachování dat a informací. U způsobu ohrožení se práce zaměřuje na zabezpečení formou hesel, kde je uvedeno, co jsou slabá a silná hesla, dvoufázové ověření jako možné řešení zabezpečení, užívání sociálních sítí společně s jeho zranitelností a soubory cookies, které mohou do jisté míry uživatele sledovat. Do incidentů jsou zařazeny nejznámější kybernetické hrozby, které představují malware, ransomware a phishing, kterému se autorka v následujících podkapitolách věnovala podrobněji. Určila jeho podkategorie společně se škodlivými následky, ale také prevencí a řešením. Na konci této části uvádí také jeho nejvýznamnější nárůst v době pandemie Covid-19. Třetí kapitola pojednává o legislativě užívané v rámci kybernetické bezpečnosti. Jedná se o zákon o kybernetické bezpečnosti společně s vyhláškou, která na něj navazuje, také novou směrnici Evropského parlamentu a Rady známou jako NIS 2, která bude v říjnu roku 2024 implementovaná do právního řádu České republiky jako nový zákon o kybernetické bezpečnosti. Čtvrtá kapitola zahrnuje komponenty bezpečnostního systému České republiky zabývající se problematikou kybernetické bezpečnosti. V práci je popsán Národní úřad pro kybernetickou a informační bezpečnost, který je ústředním správním orgánem v této oblasti. Navazuje na něj Vládní a Národní CERT, jehož postavení a činnost je dána především zákonem o kybernetické bezpečnosti. Poslední český

komponent v této kategorii je Národní centrum kybernetické bezpečnosti, které je výkonnou sekcí NÚKIB. Kromě výše zmíněných komponentů jsou součástí také dva zahraniční. Prvním je Evropské centrum pro počítačovou kriminalitu, kde je Česká republika jako členský stát Evropské unie členem. Druhým je Anti-Phishing Working Group neboli pracovní skupina pro boj proti phishingu. Poslední kapitola teoretické části se zabývá případovou studií na téma XDSpy. Tuto skupinu si autorka pro případovou studii zvolila, neboť užívá spear phishing jako prostředek pro nelegální získání informací o státech a institucích především ve východní Evropě.

Praktická část se zabývá výzkumným šetřením, které bylo provedeno formou dotazníkového šetření (kvantitativní část) a řízeného rozhovoru s odborníkem v oblasti kybernetické bezpečnosti (kvalitativní část), který je zaměstnancem subjektu kritické infrastruktury.

Cílem výzkumu je zjistit jaké povědomí mají respondenti o možných kybernetických hrozbách a současně vymezit, jaká stanoviska a opatření k problematice zaujímá specialista kybernetické bezpečnosti. V rámci dotazníkového šetření byla koncipována otázka, která by se za jiných okolností mohla přiblížit potenciálnímu phishingovému útoku. Účelem bylo zjištění, zda v procesu vyplňování dotazů dokážou respondenti rozpoznat možný zásah do jejich soukromí. Na tomto základě jsem stanovila svůj hlavní výzkumný předpoklad, kromě něj další čtyři, které jsem dle výsledků verifikovala či falzifikovala.

Cílem diplomové práce bylo analyzovat hrozby v oblasti kybernetické bezpečnosti se zaměřením na phishing, a na základě zjištění povědomí uživatelů internetu o těchto hrozbách a jejich chování na internetu koncipovat návrhy a doporučení k optimalizaci tohoto chování tak, aby byli lépe chránění před hrozbou phishingového útoku. Cíle práce tedy bylo dosaženo. Závěry a doporučení koncipované autorkou jsou zároveň v práci ověřeny a podpořeny vyhodnocením řízeného polostrukturovaného rozhovoru se specialistou na oblast kybernetické bezpečnosti.

Seznam zkratek

AI – (Artificial intelligece) umělá inteligence

APWG – (Anti-Phishing Working Group) mezinárodní koalice odpůrců kybernetické kriminality

ICT – informační a komunikační technologie

IS – informační systémy

IT – informační technologie

Kyberprostor – kybernetický prostor

NÚKIB - Národní úřad pro kybernetickou a informační bezpečnost

PS – počítačový systém

SaaS - Software jako služba

TČ - trestný čin

URL - webová adresa sloužící k přesné identifikaci umístění informací na internetu

Seznam použité literatury

Odborné monografie

1) JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6
2) KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z. s. p. o., 2016. ISBN 978-80-88168-18-8
3) KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7
4) SEDLÁK, Petr a KONEČNÝ, Martin a kol. *Kybernetická (ne)bezpečnost*. Brno: CERM akademické nakladatelství, 2021. ISBN 978-80-7623-068-2
5) SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Aleš Čeněk, 2022. ISBN 978-80-7380-849-5
6) ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5

Právní předpisy

7) Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor
8) Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat
9) Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů
10) Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti
11) Zákon č. 106/1999 Sb., o svobodném přístupu k informacím
12) Zákon č. 40/2009 Sb., Trestní zákoník

Elektronické zdroje

13) ANTIVIROVÉ CENTRUM. *ESET odhalil skupinu hackerů XDSpy*. Online. 2020. Dostupné z: https://www.antivirovecentrum.cz/aktuality/eset-odhalil-skupinu-hackeru-xdspy.aspx. [cit. 2024-03-01].
14) APWG. *Phishing Activity Trends Report: 3rd Quarter 2019*. Online. 2019. Dostupné z: https://docs.apwg.org/reports/apwg_trends_report_q3_2019.pdf?_gl=1*dm63ko*_ga*MTkzMzI0OTQ4NC4xNzA4OTYzMzc4*_ga_55RF0RHXSR*MTcwODk2MzM3Ny4xLjEuMTcwODk2MzgwMi4wLjAuMA. [cit. 2024-03-08].
15) APWG. *Phishing Activity Trends Report: 3 rd Quarter 2020*. Online. 2020. Dostupné z: https://docs.apwg.org/reports/apwg_trends_report_q3_2020.pdf?_gl=1*bjfq1j*_ga*MTkzMzI0OTQ4NC4xNzA4OTYzMzc4*_ga_55RF0RHXSR*MTcwODk2ODgwMi4yLjAuMTcwODk2ODgwMi4wLjAuMA. [cit. 2024-03-08].
16) APWG. *Phishing Activity Trends Report: 3 rd Quarter 2021*. Online. 2021. Dostupné z: https://docs.apwg.org/reports/apwg_trends_report_q3_2021.pdf?_gl=1*1l87p3k*_ga*MTkzMzI0OTQ4NC4xNzA4OTYzMzc4*_ga_55RF0RHXSR*MTcwODk2ODgwMi4yLjAuMTcwODk2ODgwMi4wLjAuMA. [cit. 2024-03-08].
17) APTIEN.COM. *Co je CIA triáda informační bezpečnosti*. Online. 2023. Dostupné z: https://aptien.com/cs/kb/articles/what-is-cia-triad. [cit. 2023-11-26].
18) AVAST SOFTWARE. *Malware*. Online. 2023. Dostupné z: https://www.avast.com/cs-cz/c-malware. [cit. 2023-09-06].
19) AVAST SOFTWARE. *WannaCry*. Online. 2023. Dostupné z: https://www.avast.com/cs-cz/c-wannacry. [cit. 2023-09-06].
20) AZURE. *Co je SaaS?* Online. 2024. Dostupné z: https://azure.microsoft.com/cs-cz/resources/cloud-computing-dictionary/what-is-saas. [cit. 2024-01-22].
21) CSIRT.CZ. *FAQ*. Online. 2019. Dostupné z: https://csirt.cz/cs/hlaseni-incidentu/faq/#cojecert. [cit. 2024-02-24].
22) CSIRT.CZ. *Národní CSIRT České republiky*. Online. 2019. Dostupné z: https://www.csirt.cz/cs/. [cit. 2024-02-24].

23) CYBER SECURITY COMPLIANCE AUDIT KYBERNETICKÉ BEZPEČNOSTI. *Směrnice NIS 2 a Nový zákon o kybernetické bezpečnosti*. Online.. 2024. Dostupné z: https://www.cybersecuritycompliance.cz/smernice-nis-2-a-normy-iso-iec/. [cit. 2024-02-16].
24) CZ.NIC, Z. S. P. O. *Úvod do problematiky dat*. Online. 2023. Dostupné z: https://www.jaknainternet.cz/page/2596/uvod-do-problematiky-dat/. [cit. 2023-11-26].
25) ČERMÁK, Miroslav. CIA: Důvěrnost-Integrita-Dostupnost. Online. *Bezpečnost*. 2008. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/duvernost-integrita-dostupnost/. [cit. 2023-11-26].
26) ČESKÁ BANKOVNÍ ASOCIACE. *Podvodné e-maily — phishing*. Online. 2022. Dostupné z: https://www.kybertest.cz/nejcastejsi-typy-podvodu/phishing-podvodne-e-maily. [cit. 2024-02-06].
27) ČESKÁ BANKOVNÍ ASOCIACE. *Podvodné SMS (tzv. smishing)*. Online. 2022. Dostupné z: https://www.kybertest.cz/nejcastejsi-typy-podvodu/smsishing-podvodne-sms-zpravy. [cit. 2024-02-06].
28) EMPEY, CHARLOTTE. Vše, co potřebujete vědět o ransomwaru a jak se před ním ochránit. Avast [online]. Česká republika: Avast Blog, 2018. Dostupné z: https://blog.avast.com/cs/co-je-ransomware. [cit. 2023-09-06].
29) ESET. *APT skupina*. Online. 2022. Dostupné z: https://www.eset.com/cz/aptskupina/. [cit. 2024-02-28].
30) ESET. *Vícefázové ověření*. Online. Praha, 2024. Dostupné z: https://www.eset.com/cz/vicefazove-overeni-a-zabezpeceni-firemnich-hesel/. [cit. 2024-03-05].
31) EUR-LEX. *Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES*. Online. 2024. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32022L2557&qid=1708034779985. [cit. 2024-03-05].
32) ESET. *Zero day útok*. Online. 2020. Dostupné z: https://www.eset.com/cz/zero-day/. [cit. 2024-02-28].

33) F.A.C.C.T. *Кибершпионы из XDSpy атакуют российских металлургов и предприятия ВПК*. Online. 2023. Dostupné z: https://habr.com/ru/companies/f_a_c_c_t/news/775944/. [cit. 2024-03-01].
34) FAOU, Matthieu. *XDSpy: Stealing government secrets since 2011*. Online. 2020, 02 Oct 2020. Dostupné z: https://www.welivesecurity.com/2020/10/02/xdspy-stealing-government-secrets-since-2011/. [cit. 2024-02-28].
35) HALEVI, Tzipora; MEMON, Nasir; NOV, Oded. Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. *Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks,* 2.1. 2015. Dostupné z: https://www.researchgate.net/profile/Tzipora-Halevi/publication/317904745_Spear-Phishing_in_the_Wild_A_Real-World_Study_of_Personality_Phishing_Self-Efficacy_and_Vulnerability_to_Spear-Phishing_Attacks/links/5da079eea6fdcc8fc3474953/Spear-Phishing-in-the-Wild-A-Real-World-Study-of-Personality-Phishing-Self-Efficacy-and-Vulnerability-to-Spear-Phishing-Attacks.pdf. [cit. 2024-01-24].
36) INVESTOPEDIA. *What Is the Dark Web and Should You Access It?* Online. 2023. Dostupné z: https://www.investopedia.com/terms/d/dark-web.asp. [cit. 2024-03-05].
37) IT SLOVNÍK.CZ. *Co je Skript?* Online. 2024. Dostupné z: https://it-slovnik.cz/pojem/skript. [cit. 2024-03-05].
38) IROZHLAS. *Prozrazená hesla jsou problém, Česko získalo zadarmo přístup k jejich databázi*. Online. Praha, 2021, 2024. Dostupné z: https://www.irozhlas.cz/zpravy-domov/bezpecnost-hesla-hibp-nukib_2109061432_cib. [cit. 2024-03-05].
39) IVRANA. *Co je směrnice NIS 2 a koho se týká*. Online. 2022. Dostupné z: https://nis2.tech/smernice-nis-2/. [cit. 2024-03-05].
40) JANOUŠ, Vilém. *Lidé bezmyšlenkovitě přijímají cookies. Nechtěně se vzdávají soukromí*. Online. 2022, 20. 6. 2022. Dostupné z: https://www.denik.cz/pocitace-a-mobily/web-cookies-soukromi.html. [cit. 2024-03-03].

41) KANIČÁROVÁ, Klára. *(Staro)nová skupina XDSpy špehuje inštitúcie vo východnej Európe*. Online. 2020. Dostupné z: https://cybersec.sk/spravy/zo-sveta/staronova-skupina-xdspy-spehuje-institucie-vo-vychodnej-europe/. [cit. 2024-03-05].
42) KINCL, Petr. *Sociální sítě a osobní údaje: Jak se bránit zneužití?* Online. 2016, 11.12.2016. Dostupné z: https://www.pravniprostor.cz/clanky/obcanske-pravo/socialni-site-a-osobni-udaje. [cit. 2024-03-03].
43) KRASNOGOLOVY, Vladimir. *Hacker Group XDSpy Distributes Malware in Russia under the Guise of Subpoenas for the Army*. Online. 2022. Dostupné z: https://gridinsoft.com/blogs/hacker-group-xdspy/. [cit. 2024-03-01].
44) LENAERTS-BERGMANS, Bart. *What is Spear-phishing? Definition with examples*. Online. 2023, 6.11.2023. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/phishing/spear-phishing/. [cit. 2024-01-24].
45) LIPTÁKOVÁ, Karolína. *Nová směrnice EU o kybernetické bezpečnosti „NIS2“*. Online. Právní prostor. 2023. Dostupné z: https://www.pravniprostor.cz/clanky/mezinarodni-a-evropske-pravo/nova-smernice-eu-o-kyberneticke-bezpecnosti-nis2. [cit. 2024-02-15].
46) MAGENTA EXPERIENCE CENTER. *Bezpečnostní desatero*. Online. Praha, 2024. Dostupné z: https://www.t-mobile.cz/microsites/klik-pro-klid/index.html#bezpecnostni-desatero-7. [cit. 2024-03-05].
47) MANA, Martin. ŽENY, MUŽI A DIGITALIZACE. Online. *Český statistický úřad*. 2023, č. CSU-007576/2023-63, article 062053-23, s. 1-41. ISSN 978-80-250-3417-0. Dostupné z: Odbor statistik rozvoje bezpečnosti, https://www.czso.cz/documents/10180/215504666/06205323.pdf/0cf505ab-bbdd-4005-bf25-98d5691b5576?version=1.1. [cit. 2023-11-26].
48) MANAGEMENT NEWS. *5 častých chyb při tvorbě a využívání hesel*. Online. 2021. Dostupné z: https://www.managementnews.cz/manazer/trendy-id-2698721/5-castych-chyb-pri-tvorbe-a-vyuzivani-hesel-id-4091480. [cit. 2024-02-05].
49) MINISTERSTVO DOPRAVY. *Počáteční služby systému Galileo: Co je potřeba vědět*. Online. 2017. Dostupné z: https://www.mdcr.cz/Dokumenty/Kosmicke-

aktivity/Pocatecni-sluzby-systemu-Galileo-Co-je-potreba-ve. [cit. 2024-02-24].

50) NÁRODNÍ CENTRUM KYBERNETICKÉ BEZPEČNOSTI. *Co je NCKB*. Online. 2020. Dostupné z: https://www.govcert.cz/cs/. [cit. 2024-02-26].
51) NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Další specifika úpravy v České republice*. Online. 2023. Dostupné z: https://osveta.nukib.cz/mod/page/view.php?id=2625. [cit. 2024-02-16].
52) NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Novým ředitelem NÚKIB je Lukáš Kintr*. Online. 2022. Dostupné z: https://nukib.gov.cz/cs/infoservis/aktuality/1851-novym-reditelem-nukib-je-lukas-kintr/. [cit. 2024-02-24].
53) NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *O úřadu*. Online. 2020. Dostupné z: https://nukib.gov.cz/cs/o-nukib/o-uradu/. [cit. 2024-02-24].
54) NÁRODNÍ CENTRUM KYBERNETICKÉ BEZPEČNOSTI. *Spear-phishing a jak se před ním chránit*. Online. 2020. Dostupné z: https://www.govcert.cz/cs/informacni-servis/doporuceni/2748-spear-phishing-a-jak-se-pred-nim-chranit/. [cit. 2024-02-06].
55) NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Upozornění na podvodné telefonáty od falešné technické podpory Microsoft*. Online. 2021. Dostupné z: https://nukib.gov.cz/cs/infoservis/aktuality/1699-upozorneni-na-podvodne-telefonaty-od-falesne-technicke-podpory-microsoft/. [cit. 2024-02-05].
56) NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Upozornění na vishing zneužívající identitu bankovních institucí*. Online. 2021. Dostupné z: https://nukib.gov.cz/cs/infoservis/hrozby/1705-upozorneni-na-vishing-zneuzivajici-identitu-bankovnich-instituci/. [cit. 2024-02-05].
57) NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Vládní CERT*. Online. 2020. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vladni-cert/. [cit. 2024-02-24].

58) NIS2: *Rozsah, účel a jaké změny očekávat*. Online. 2023. Dostupné z: https://www.safetica.com/cs/blog/nis2-rozsah-ucel-a-jake-zmeny-ocekavat. [cit. 2024-03-05].
59) POLICIE ČESKÉ REPUBLIKY. *Kontakty*. Online. 2024. Dostupné z: https://www.policie.cz/clanek/nctekk-kontakty.aspx. [cit. 2024-03-05].
60) POLICIE ČESKÉ REPUBLIKY. Organizační struktura NCTEKK. Online. 2024 Dostupné z: https://www.policie.cz/clanek/nctekk-organizacni-struktura.aspx. .[cit. 2024-03-05].
61) RATHEE, Dhruv; MANN, Suman. Detection of E-mail phishing attacks–using machine learning and deep learning. *International Journal of Computer Applications*. 2022, roč. 183, č. 47, Dostupné z: https://eprints.cs.univie.ac.at/248/1/GanstererPoelz.pdf. [cit. 2024-01-22].
62) SAFETICA. *NIS 2: Rozsah, účel a jaké změny očekávat*. Online. 2023. Dostupné z: https://www.safetica.com/cs/blog/nis2-rozsah-ucel-a-jake-zmeny-ocekavat. [cit. 2024-02-15].
63) SCARPATI, Jessica, BURKE, John (ed.). *URL (Uniform Resource Locator)*. Online. 2020. Dostupné z: https://www.techtarget.com/searchnetworking/definition/URL. [cit. 2024-01-22].
64) ŠTRÁFELDA, Jan. *HTTP cookies – kompletní průvodce*. Online. 2024. Dostupné z: https://www.strafelda.cz/cookies. [cit. 2024-03-05].
65) Terminologický slovník - krizové řízení a plánování obrany státu [online]. Ministerstvo vnitra České republiky: Odbor bezpečnostní politiky a prevence kriminality, 2016. Dostupné z: https://www.mvcr.cz/clanek/terminologicky-slovnik-krizove-rizeni-a-planovani-obrany-statu.aspx. [cit. 2021-11-05].
66) YEBOAH-BOATENG, Ezer Osei a AMANOR, Priscilla Mateko. Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices. Online. *Journal of Emerging Trends in Computing and Information Sciences*. 2014, roč. 5, č. 4. ISSN 2079-8407. Dostupné z: https://e-tarjome.com/storage/btn_uploaded/2020-09-12/1599891065_11216-etarjome%20English.pdf. [cit. 2024-02-06].