Sociální inženýrství jako klíčový faktor kybernetické bezpečnosti organizace

Bc. Romana Nováková

Diplomová práce
2022

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav informatiky a umělé inteligence

Akademický rok: 2021/2022

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Romana Nováková**
Osobní číslo:	**A20616**
Studijní program:	**N0613A140022 Informační technologie**
Specializace:	**Kybernetická bezpečnost**
Forma studia:	**Kombinovaná**
Téma práce:	**Sociální inženýrství jako klíčový rizikový faktor kybernetické bezpečnosti organizace**
Téma práce anglicky:	**Social Engineering as a Key Risk Factor for an Organization's Cyber Security**

Zásady pro vypracování

1. Vypracujte literární rešerši na dané téma.
2. Popište současné metody sociálního inženýrství a možnosti obrany proti těmto útokům.
3. Uveďte konkrétní hrozby zaměřující se na různé skupiny populace a uveďte současnou osvětu o kybernetických hrozbách, včetně analýzy legislativního rámce v ČR.
4. Proveďte šetření kybernetické gramotnosti populace v ČR včetně jeho vyhodnocení.
5. Navrhněte možnosti zlepšení vzdělávání pro podporu snížení hrozeb vyplývajících ze sociálního inženýrství.
6. Vyhodnoťte výstupy své práce s ohledem na její přínos a cílové skupiny.

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

Seznam doporučené literatury:

1. EDMÜLLER, Andreas a Thomas WILHELM. *Velká kniha manipulativních technik*. Praha: Grada, 2011. ISBN 978-80-247-3778-2.
2. HADNAGY, Christopher. *Social Engineering: The Science of Human Hacking*. Second edition. John Wiley, 2018. ISBN 9781119433385.
3. JAMES, Lance. *Phishing bez záhad*. Praha: Grada, 2007. ISBN 8024717662.
4. JIRKOVSKÝ, Václav. Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada Publishing, 2007. ISBN 978-80- 247-1561-2.
5. KOLOUCH, Jan. *Cybercrime*. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8.
6. Long, J. 2008. No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Burlington: Syngress.
7. MITNICK, Kevin, SIMON, William. *Umění klamu*. 1. vyd. Gliwice: Helion, 2003. 345 s. ISBN 83-7361-210-6.

Vedoucí diplomové práce: **prof. Mgr. Roman Jašek, Ph.D., DBA**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **3. prosince 2021**
Termín odevzdání diplomové práce: **23. května 2022**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

prof. Mgr. Roman Jašek, Ph.D., DBA v.r.
ředitel ústavu

Ve Zlíně dne 24. ledna 2022

Romana Nováková:

Sociální inženýrství jako klíčový faktor kybernetické bezpečnosti organizace:

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne

Bc. Romana Nováková v.r.
podpis studenta

ABSTRAKT

Diplomová práce se zabývá problematikou sociálního inženýrství a jeho dopadů na veřejnost v konceptuálním pojetí kybernetické bezpečnosti. V práci jsou popsány kybernetické hrozby, metody sociálního inženýrství, které útočníci využívají k vytěžování osob, za účelem získání cenných informací. Je zde provedena analýza informovanosti o kybernetických hrozbách ze strany Národního bezpečnostního úřadu, bankovních institucí či firemního prostředí. Současně je v práci provedeno dotazníkové šetření, které slouží jako nástroj pro ověření informační a kybernetické gramotnosti.

Klíčová slova:

Sociální inženýrství, kybernetická bezpečnost, kybernetické hrozby, politika hesel, phishing

ABSTRACT

This diploma thesis deals with the issue of social engineering and its impacts on the public in the concept of cyber security. This thesis describes cyber threats, methods of social engineering that attackers use to exploit people in order to obtain valuable information. There is an analysis of awareness of cyber threats from the National Cyber and Information Security Agency, banking institutions and the corporate environment. Thera is also a questionnaire survey included, which serves as a tool for verifying information and cyber literacy.

Keywords:

Social Engineering, Cyber Security, Cyber Threats, Password Policy, Phishing

Ráda bych poděkovala:

Panu prof. Mgr. Romanu Jaškovi Ph.D., DBA za odborné vedení mé diplomové práce, za jeho vstřícný přístup, trpělivost a jeho cenné rady. Mgr. Miroslavě Lodeové za podporu a korekturu práce a své rodině za trpělivost a podporu v době studia.

Motto:

Nic na světě není nebezpečnější, než upřímná neznalost a svědomitá hloupost.

Martin Luther King

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Diplomová práce se zabývá aspekty sociálního inženýrství a jeho dopady na veřejnost v konceptuálním pojetí kybernetické bezpečnosti a kybernetických hrozeb. Jsou v ní definovány základní pojmy, jako jsou kyberprostor a internet, kybernetické hrozby typu malware, pojmy z odvětví sociálního inženýrství, jako je phishing, pharming, whaling, OSINT apod. Je zde popsán průběh a metody sociálního inženýrství, bezpečné chování v digitálním prostředí, pravidla zálohování, či pravidla pro tvorbu bezpečných hesel. V práci jsou shrnuty hrozby v online prostředí s přihlédnutím na jednotlivé věkové skupiny, jako je kyberšikana, netholismus, dezinformace apod. Dále je v práci představeno bankovní prostředí, vysvětleno co je bankovní identita a porovnání aplikací mobilního bankovnictví vybraných bankovních institucí. Dále jsou v práci uvedeny právní aspekty s ohledem na kybernetickou bezpečnost. V práci je provedeno dotazníkové šetření na téma sociální inženýrství a kybernetická bezpečnost, které má za úkol zjistit, jakým způsob se respondenti pohybují v digitálním prostředí. Součástí je vyhodnocení dotazníkové části s ohledem na věkové skupiny, nejvyšší dosažené vzdělání a obor pracovního zaměření. V práci jsou analyzovány možnosti informovanosti veřejnosti ze strany Národního bezpečnostního úřadu pro kybernetickou a informační bezpečnost, Ministerstva vnitra České republiky, Policie České republiky, bankovních institucí a dalších subjektů.

I. TEORETICKÁ ČÁST

1 KYBERPROSTOR A INTERNET

Termín kyberprostor poprvé použil americký prozaik William Gibson na počátku osmdesátých let ve své povídce Burning Chrome. Později ve svém románu Neuromancer popsal kyberprostor jako konsensuální halucinaci, která je každý den zakoušená miliardami oprávněných operátorů všech národů, dětí, které se učí základy matematiky, grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému, nedomyslitelnou komplexnost, linii světla seřazené v neprostoru mysli, shluky a souhvězdí dat, jako světla města ustupující. Tato definice je v prostředí kybernetiky ovšem příliš prozaická a dále neuchopitelná. Dle oxfordského slovníku slovo pochází z anglického Cyberspace a jedná se o virtuální počítačový svět, který tvoří světovou globální počítačovou síť, jejímž základem je online komunikace. Je tedy zřejmé, že pro kyberprostor a internet máme podobnou definici. Internet je globální systém, který spojuje uživatele různých zařízení do jedné soustavy vzájemně propojených počítačů, které mezi sebou sdílejí, komunikují a přistupují k informacím v rámci celé sítě tzv. kyberprostoru. Vše začalo v období studené války, kdy americká armáda vznesla návrh na vytvoření vědeckého projektu na rychlou a bezpečnou komunikaci mezi jednotlivými vládními složkami. První síť měla název ARPANET a byla dokončena na konci roku 1969. Základní komunikační protokol telnet byl vyvinut později v roce 1972. O další dva roky později se začal využívat protokol TCP a za další čtyři roky došlo ke specifikaci modelu TCP/IP. V 80. letech minulého století se začaly vyvíjet další sítě, jako například MILNET, USEnet nebo BITnet. V roce 1992 došlo k oficiálně prvnímu napojení československé instituce do internetu. Jednalo se o České vysoké učení technické v Praze. Pokusy s internetem ale v bývalém Československu probíhaly již od konce roku 1991. K internetu se připojovalo výhradně prostřednictvím telefonní přípojky a internet byl spíše pro užší skupiny odborníků. V dnešní době něco absolutně nemyslitelného, když připojení k internetu má, kromě počítačů a mobilních telefonů, i další zařízení, jako jsou webové kamery, ledničky, televize, pračky apod. Čím více zařízení je do internetu zapojeno, tím větší je riziko potenciálního nebezpečí útoku. [12], [13], [14]

Kyberprostor, tak jak ho zná většina uživatelů, je jen zlomek toho, co internetová síť nabízí. Pokud vyhledáváme informace na Google či na Seznamu, můžeme prohlížet jen určité množství internetu. Na internetu existují také místa a obsah k němuž se běžným způsobem dostat nelze. K přístupu je totiž potřeba speciální software. Jedná se o Darkweb a o Deepweb. Především Darkweb bývá často spojován s nekalou, kriminální činností. Je to proto, že v tomto prostředí se může člověk pohybovat naprosto anonymně. Pomocí služby World

Wide Web – WWW je možné vytvářet a prohlížet obsah internetu. Rozlišujeme tři základní složky internetu.

1. Surface web
2. Deepweb
3. Darkweb

1.1 Surface web – povrchový web

Jedná se o část WWW, která je indexována roboty, díky čemuž je možné vyhledávat různé informace, či prezentace, které jsou na internetu dostupné. Náš pohyb je při prohledávání surface webu monitorován, a firmy typu Google o tomto pohybu sbírá informace. Mají pak tedy k dispozici informace o tom, co bylo vyhledáváno, jakým způsobem se uživatel pohybuje na různých stránkách, na co klikl, kdy odešel ze stránky apod. Tato informace se poté vyhodnocují a je nám nabízena personalizovaná reklama.

1.2 Deepweb – hluboký web

Tato část WWW není indexována, a to buď z důvodu, že to majitel stránek neumožňuje, nebo je s indexací problém. Do Deepwebu je možné se dostat například tak, že budeme mít přímý odkaz. I zde je možné o uživateli sbírat informace. Zhruba 90 % veškerého internetu je tvořen právě Deepwebem. Nejedná se o nelegální prostor, pouze není umožněna jeho indexace. Představit si jej můžeme jako přihlášení do emailové schránky, internetového bankovnictví, či do dalších prostor, která jsou chráněna. Dostat se na něj lze pomocí běžného prohlížeče.

1.3 Darkweb – temný web

Jedná se o část internetu, která není stejně jako Deepweb indexována, ale na rozdíl od Deepwebu je nutné použití speciálního prohlížeče, aby bylo možné se k obsahu Darkwebu dostat. V tomto prostředí se může uživatel pohybovat naprosto anonymně, to znamená, že pokud zde uživatel něco zveřejní, či s někým komunikuje, tato aktivita by neměla být vysledovatelná. Je to tedy místo bez absolutní kontroly nebo cenzury. A co je nekontrolovatelné, je samozřejmě velmi lákavé k páchání nelegální činnosti. Darkweb obecně nelegálním či nebezpečným místem není, záleží opět na uživateli, kde a za jakým účelem se pohybuje. Na Darkwebu jsou diskusní fóra uzavřených komunit, či další neškodný obsah. Na druhou stranu jsou zde různé markety s nelegálním zbožím, jako jsou drogy, dětská

pornografie, falešné doklady, odcizené kreditní karty a zbraně. Lze zde také získat škodlivý malware, zcizené citlivé či přihlašovací údaje, databáze s odcizenými zákaznickými daty, či hacker na objednávku. Pokud se uživatel rozhodne Darkweb navštívit, je nutná jistá dávka obezřetnosti. K přístupu do Darkwebu je potřeba mít nainstalovaný speciální prohlížeč TOR – The Onion Router, který umí zobrazovat adresy s koncovkou onion, VPN připojení, aby nebyla IP adresa uživatele vysledovatelná a v neposlední řadě konkrétní stránku, která se na Darkwebu nachází. Jelikož na Darkwebu nejsou stránky indexované, není možné jen tak prohledávat jako je tomu například v případě Google vyhledávače, touto funkcí TOR nedisponuje. Adresa pak může mít následující tvar: mlmdk88.onion. I přes fakt, že na Darkwebu je možné nalézt opravdu velké množství ilegálních věcí, jsou i další stránky, které zákony neporušují. Původním účelem bylo poskytovat anonymní přístup k informacím a obcházet cenzuru. Z tohoto důvodu jsou na Darkwebu i informace, které mají legální podtext, ovšem v některých zemích jsou zcela zakázány. Jedná se třeba o fotografie, videa, různé druhy umění. Dále slouží například investigativním novinářům či disidentům jako nástroj pro bezpečnou komunikaci. Při procházení tímto prostorem je potřeba být velmi opatrný. Jelikož se Darkweb neřídí žádnými pravidly, neexistuje žádná záruka, že to, co si zde uživatel stáhne nebo zakoupí, bude bezpečné. Zboží také nemusí obdržet, může být v jeho zemi zakázané, nelegální, nebo si jednoduše může stáhnout malware.

Obrázek 1. Darkweb – drogové tržiště Empire [16]

Pokud již uživatel má tu touhu Darkweb navštívit, je dobré dodržovat některé zásady:

- Vyhýbat se jakékoliv nelegální činnosti, protože zabezpečení nikdy nemusí být stoprocentní.
- Chovat se neviditelně a zbytečně se nezapojovat do žádných diskusí.
- Neotvírat a nestahovat neznámý obsah, který může obsahovat malware.
- Nic nenakupovat, protože vždy je možno st, že zboží je z nelegální činnosti.
- Nepřevádět částky na cizí účty, neboť by žádné zboží dorazit nemuselo.
- A nikdy nikomu nesdělovat své údaje, jako jsou telefon, email, adresa, či hesla a uživatelské přístupy. [15], [16], [17]

2 KYBERNETICKÉ HROZBY

Kybernetické útoky v oblasti Evropské Unie vykazovaly v letech 2020 a 2021 nárůst. Z čehož vyplývá, že jsou hrozby v oblasti kybernetiky na vzestupu. Tyto útoky se radikálně změnily oproti útokům z minulosti. V dnešní době se již nejedná o rozsáhlé útoky, ale útočníci spíše přecházejí k útokům, které jsou komplexní a sofistikované. Používají se pokročilejší metody. Jsou kvalitně a podrobně plánované, přesně cílené, ale hlavně trvalé. Je tedy zcela logické, že se v poslední době objevují čím dál častěji zprávy o cílených útocích. Útoky se především zaměřují na získání cenných osobních informací, či informací, které mají charakter duševního vlastnictví. Takto cílený útok se poté skládá z několika škodlivých částí, které vcelku spolupracují tak, aby bezpečnostní systém dané organizace obešly. Po průniku do systému napadené organizace začne probíhat průzkum zdrojů a informací. Následným krokem může být fáze, kdy útočník vyčkává na vhodný okamžik, kdy zaútočit, případně čas, kdy se na útok připravuje. V této fázi většinou dochází i k tomu, že útočník začne infikovat další koncové body. V závěrečné fázi poté dochází k odesílání dat mimo napadenou organizaci, případný prodej takto odcizených citlivých dat. Nástroje útočníků se příliš nemění, vyvíjí se hlavně metodika útoků, které jsou čím dál tím sofistikovanější, a cílí především na lidský faktor. Odborníci na kybernetickou bezpečnost odhalili v poslední době velký nárůst technik pokročilého vyhýbání, které mají za cíl zabránit odhalení daného útoku a bez povšimnutí deaktivovat bezpečnostní funkce zařízeních v síti. Díky čemuž útočník získá nepozorovaně neomezený přístup do napadené společnosti. Společnosti v dnešní době neutrácejí peníze za bezpečnost, pokud nemusí, jelikož firmy kybernetickou bezpečnost nepovažují za svou priorit. A to i přesto, že dle průzkumu společnosti Fortinet vyplynulo, že se útočníci raději zaměřují na bezpečnostní díry z roku 2007 než na nejnovější chyby. Útočníci totiž vycházejí z předpokladu, proč vyvíjet nový malware, když ten starý je u některých firem stále dostačující k průniku do sítě. [1], [2]

Typy kybernetických hrozeb:

1. Škodlivý kód (Malware),
2. Útoky na webové bázi (Web Based attacks),
3. Síť infikovaných počítačů (Botnets),
4. Odepření služby (Denial of Service),
5. Interní hrozby (Insider threat),
6. Phishing,

7. Nevyžádaná pošta (Spam),
8. Bezpečnostní díry (Exploit kits),
9. Krádež identity (Identity Theft),
10. Únik informací (Information Leakage),
11. Zašifrování dat (Ransomware),
12. Kybernetická špionáž (Cyber Espionage),
13. Dezinformace. [2]

Fakt, že firmy nepovažují kybernetickou bezpečnost jako prioritu, může mít do budoucna velký vliv. Aby bylo možné se do budoucna kybernetickým hrozbám plnohodnotně bránit, měly by společnosti začít používat stejné druhy technologií a strategií k obraně svých sítí. Z toho vyplývá, že je nutné zvolit novou strategii a zainvestovat do technologií, které využívají nové možnosti obrany s veškerou silou proti potenciálnímu útočníkovi. Největší nadějí je pro nás příchod a vývoj umělé inteligence – AI. Cílem je vyvinout takový systém, který bude adaptivním, imunitním systémem, obdobným jako je v lidském těle, kde systém reaguje autonomně v boji proti infekci a zároveň zasílá informace do mozku pro další zpracování. V dnešní době se umělá inteligence používá primárně k analýze velkého množství dat. Vývojáři, zabývající se vývojem umělé inteligence, se snaží vyvinout umělou inteligenci do formy samostatného agenta, který sám bude způsobilý k vyřešení určitého problému v napadeném systému. Takový agent by měl spoléhat na vzájemně propojené neurony, které budou shromažďovat místní a dále je centrálně analyzovat. Pokud poté nastane problém, a systém bude infikován, agent automaticky zasáhne. Existuje mnoho zajímavých trendů, které budou hrát do budoucna velkou roli v kybernetické bezpečnosti. Mezi nejzajímavější můžeme zařadit kombinaci statistické analýzy základních vzorců útoků a strojového učení, která bude predikovat možnost útoku. Takový systém umělé inteligence bude poté schopen predikovat další krok potenciálního útočníka a předpovídat, kde se s největší možnou pravděpodobností uskuteční další útok. Jako další zajímavou technologií je možné uvést FortiDeceptor, která bude schopna vytvořit nepropustnou obranu sítě, aniž by musela být brána v potaz velikost a struktura sítě. Vše má ovšem i svou temnou stránku. Jelikož jde vývoj dopředu na straně obrany proti kybernetickým útokům, jde s tím ruku v ruce i vývoj nových technologiích na straně útočníků, kteří taktéž mohou umělou inteligenci použít pro páchání trestné činnosti a infikovat tak informační systémy. Díky rozvoji strojového učení, je tento nástroj pro útočníky nyní dostupnější. Software, který je potřeba se nabízí za malé částky a návody ke strojovému učení je možné jednoduše získat na internetu. Dnes již technologie

pomocí strojovému učení umějí rozeznávat obrazy, díky tomu je například již možné ovládat autonomní vozidlo spolehlivě navigovat na rušné silnici. Výborným příkladem je tomu kontrola pomocí technologie CAPTCHA. Pokud má uživatel vyřešit takovou, která je velmi zkreslená a pokroucená, je úspěšnost v případě lidského faktoru 33 %, oproti tomu systém špičkového optického rozpoznávání znaků, má úspěšnost 99,8 %. Útočníci dnes již hojně využívají sítě botnetů, což jsou napadené a zotročené zařízení běžných uživatelů, které jsou útočníkem vzdáleně ovládány z centrálního místa, ze kterého je může řídit a posílat příkazy k útokům. Útok pomocí botnet sítě pomáhá útočníkovi zamaskovat fakt, že se nějaký útok blíží a potenciální oběť tedy nemůže útok dopředu predikovat. Přichází-li z jedné IP adresy velké množství dat, existuje vysoká šance, že se jedná o předzvěst zločinné aktivity. Tuto aktivitu mohou společnosti vyhodnotit jako predikci útoku a útočník tak přichází o moment překvapení. Oproti tomu, použije-li útočník síť botnetů, musejí IT experti hledat mírnější náznaky toho, že se k útoku schyluje. Dalším znakem, že útočníci již umělou inteligenci využívají, je velký nárůst útoků pomocí emailů. Umělá inteligence jim umožňuje zautomatizovat přizpůsobení obsahu emailů na míru jednotlivcům. Jelikož je pomocí umělé inteligence možné provádět kategorizaci dat, je možné ji využít i k automatizaci procesu při vyhledávání nejlepší oběti, vyhledávání zranitelných míst v napadeným systému, skrývání se a tím i déle setrvat uvnitř podnikových sítí. Umělou inteligenci mohou také využívat na proces rozpoznávání, na jaké vzorce chování se zaměřují obranné systémy počítače. To lze využít tím způsobem, že se otestuje velké množství špatného a dobrého software prostřednictvím antivirového programu a poté se mohou zaměřit na vzorce, které antivirové programy odhalily. Prozatím nebyl nalezen žádný důkaz o tom, že útočníci již umělou inteligenci využívají. [10], [11]

2.1 Malware

Malware je zkratka, která pochází z anglického malicious software a znamená škodlivý software. Takovýto software má za úkol útočníkovi zajistit tajný přístup do počítače či jiného zařízení oběti. Mezi typický malware patří:

- Spyware,
- Adware,
- Počítačové viry,
- Počítačoví červi,
- Trojské koně,

- Ransomware,
- Rootkity,
- Apod.

Šíření malwaru probíhá nejčastěji pomocí internetu, emailu, zkušebních verzí her, hudebních souborů, bezplatných služeb či prostřednictvím stažených dat. Do koncových zařízení se malware dostane díky neopatrnosti a v některých případech absenci antivirového software. Jednou ze známek, že je počítač napaden škodlivým kódem, je jeho přehřívání a zpomalení systému. Napadený software poté může rozesílat spam, zobrazovat vyskakovací okna nebo způsobovat pády systému. [9]

2.1.1 Spyware

Spyware a adware jsou určitou třídou softwaru, který se instaluje do počítače bez vědomí uživatele za účelem nahlášení jeho chování směrem k útočníkovi. Útočník se v tomto případě může vydávat za inzerenta, marketingového specialistu nebo internetového uživatele. Kromě zjevných problémů s ochranou soukromí, ve většině případů tento software není škodlivý. Existují však určité formy spywaru, které využívají technologii keyloggeru k zaznamenání informací o tom, co za klávesu uživatel stlačil s následným odesláním dat do centrální databáze. V takovém případě mohou být shromažďována hesla a finanční informace a tento spyware by měl být považován za vysokou hrozbu pro uživatele nebo organizace. [18]

2.1.2 Adware

Jedná se o software, který slouží k zobrazování nevyžádané reklamy, která je pro uživatele obtěžující. Realizuje se několika možnými způsoby, které se mohou navzájem doplňovat. Jedná se především o tyto metody:

- Upravuje nastavení internetového prohlížeče.
- Nechává zobrazovat pop-up okna.
- Zaznamenává činnost uživatele na zařízení.
- Ukládá vzorec chování uživatele na internetových stránkách a data o jeho návštěvě.

Po stažení tohoto software může dojít k modifikaci prohlížeče, který umí měnit některé uživatelské nastavení. Mezi takovéto změny můžeme zmínit například změnu domovské adresy, změna nástroje pro vyhledávání, změna panelů nástrojů. V některých případech je zahlcení prohlížeče v takové míře, že není téměř možné v něm pracovat, a prohlížeč

je zpomalen až do míry únosnosti. K nainstalování tohoto malware dochází většinou nepozorností ze strany uživatele, který si adware stáhne jako bonus společně s primárním programem, který původně požadoval. Stažení primárního programu ve většině případů není z oficiálních zdrojů. Pokud již uživatel takovýto software stahuje, je nutné dbát na velkou obezřetnost a dobře si přečíst, které další doplňky se chtějí společně se software do zařízení instalovat a jestli je uživatel opravdu požaduje. Další velmi obtěžující variantou adwaru je zobrazování vyskakovacích oken s reklamou. V některých případech se může stát, že vyskakovací okna absolutně zahltí počítač, na kterém je znemožněna jakákoliv práce. Občas může dojít i k situacím, kdy je pomocí vyskakovacích oken nabízen další škodlivý software. Adware nejčastěji monitoruje, jaké má uživatel nákupní návyky a co vyhledává. Tyto informace je poté možné využít k osobnějším reklamním nabídkám. [19]

2.1.3 Počítačové viry

Je škodlivý program nebo část programového kódu, který je schopen se spustit bez vědomí uživatele. Počítačový vir má za cíl získat kontrolu nad zařízením uživatele, či nad celým systémem a následně způsobit škodu potenciální oběti útočníka. K šíření počítačový vir využívá jiné soubory, jako svého hostitele. Do těchto souborů je zkopírováno tělo viru samotného, které poté využívá ostatní soubory ke svému šíření, aby mohl infikovat další zařízení a systémy. K šíření se využívají hlavně soubory typu EXE, SYS, COM, DOC, XLS, PDF, EML apod. Počítačový vir vykazuje obdobné známky chování jako vir, který útočí na lidský organismus a je schopen své vlastní replikace do ostatních buněk. První vir byl pravděpodobně do světa vypuštěn v roce 1986. Tento virus pocházel z Pákistánu a nesl název Brain. Virus se šířil prostřednictvím disketových jednotek a jeho účelem byla propagace firmy svých stvořitelů, kterými byli bratři Farúkovi. Jelikož šlo pouze o propagaci, virus nesl kompletní identifikační údaje o svých tvůrcích. [20], [21]

Počítačové viry můžeme rozdělit do několika skupin z hlediska toho, jaké objekty napadají.

Boot viry

Tento typ počítačového viru napadají systémovou oblast disky. Do systému se zavádí při restartu počítače, který má povoleno zavádět do systému z mechaniky či USB portů. Spuštění samotného viru je poté díky jednotce, která obsahuje médium s bootovacím virem. Vir je spuštěn a napadá systémové oblasti pevného disku. Při dalším spuštění počítače se boot vir inicializuje z pevného disku počítače uživatele a napadá vyměnitelné zařízení, které uživatel použije.

Souborové viry

Souborové viry napadají pouze soubory, které obsahují prováděný kód. Fungují tím způsobem, že v napadeném programu přepíší část kódu svým kódem, či vlastní kód k programu připojí a tím se změní velikost souboru, ale zároveň i jeho chování.

Multiparitní viry

Jsou kombinací bootovacích a souborových virů, takže napadají jak systémovou oblast disku, tak i spustitelné soubory.

Makroviry

Nadají dokumenty, které jsou vytvořeny v určitých aplikacích. Tyto viry využívají toho, že soubory kromě dat, obsahují i makra, které viry využívají ke svému šíření. Napadány jsou tedy aplikace skupiny MS Office, převážně díky jazyku VBA – Visual Basic for Applications, které jsou velmi rozšířené a jejich bezpečnost je minimální.

Viry také můžeme rozdělit dle jejich určitých vlastností.

Stealth viry

Jedná se o rodinu počítačových virů, které se chrání před detekcí pomocí antiviropvého programu za použití schovávačích a úhybných manévrů. Tento typ viru se pokouší převzít kontrolu nad některými funkcemi operačního systému a při pokusu o čtení infikovaných objektů, stealth virus vrací hodnoty, které systém očekává a odpovídají původnímu stavu před napadením.

Polymorfní viry

Tyto počítačové viry se pokouší znesnadnit svou vlastní detekci tím způsobem, že mění svůj vlastní kód. V napadeném souboru poté není možné najít sekvence, které by odpovídaly stejnému kódu.

Rezidentní viry

Rezidentní viry zůstávají po jejich spuštění stále přítomni v paměti systému. [22]

2.1.4 Trojské koně

Výrazem trojský kůň neboli Trojan je označován takový škodlivý kód, který je ukryt v počítačovém programu a vypadá užitečně. Může se jednat o menší hru, spořič obrazovky či program na vyčištění paměti nebo na odstranění malwaru samotného. Šíří se tak,

aby vzbuzoval co možná největší legitimitu a oběť tak uvěřila, že se jedná o software, který by si měla nainstalovat. Trojský kůň může být doručen prostřednictvím emailu, který na první pohled vykazuje známky, že je odeslán přímo od společnosti určitého antivirového programu. Samotný název pochází z řecké mytologie, z bajky o dobytí Troje, kdy byl použit dřevěný kůň, ve kterém se ukrývali vojáci, kteří zaútočili v noci na spící Trojany. Bylo zde zneužito důvěry, neboť si trojané mysleli, že jde o dar. Stejný smysl má i počítačový trojan, jehož posláním je získání moci nad systémem, kam byl v legitimní podobě propašován, manipulace a mazání dat, ovládání běžících systémů, vzdálená zpráva systému, vytvoření zadních vrátek – backdoor či získávání hesel. [20], [21]

Trojský kůň není schopen své vlastní replikace a infekce ostatních soubor. Jedinou formou dezinfekce tohoto souboru je jeho smazání, neboť není připojen k žádnému vlastnímu hostiteli. Trojské koně mají nejčastěji tuto podobu.

Password stealing – PWS

Tyto trojské koně většinou sledují jednotlivé stisky kláves, které ukládá a následně odesílá na emailové adresy útočníkovi, který tímto způsobem může získat výjimečné a velmi citlivé informace, jako jsou uživatelská jména a hesla, čísla bankovních karet, či přístupy do bankovnictví oběti a další citlivý materiál. Tato infiltrace je ve své podstatě vlastně spyware, kde trojský kůň zafungoval jako prostředek doručení tohoto keyloggeru do systému potenciální oběti.

Destruktivní

Tímto způsobem je trojský kůň běžně chápán. Jinak řečeno, jde o běžnou formu výkladu, která nás napadne při názvu trojský kůň. Po spuštění destruktivní trojan totiž likviduje soubory na disku nebo rovnou provede kompletní zformátování pevného disku. Do této skupiny se běžně řadí i BAT trojské koně, což jsou škodlivé, dávkové soubory s příponou BAT.

Backdoor

V tomto případě se jedná o specifickou skupinu trojských koní, podobné aplikacím typu klient – server. Tyto backdoory vystupují vesměs anonymně, aby nebyly prozrazeny a uživatel pozorován. Vytvářejí totiž útočníkovi možnost neautorizovaného vstupu do systému oběti, kde může nepozorovaně vyhledávat informace, o které má zájem. Backdoor, neboli zadní vrátka, jsou ve své podstatě vzdálená správa počítače a vesměs se nejedná o nebezpečnou aplikaci. Nebezpečí, které v sobě ukrývá je její použití. Pokud bude na druhé straně útočník,

který bude chtít škodit, případně odcizit citlivá data, jedná se samozřejmě o nebezpečí vytvořené vzdáleným útočníkem. Princip funkčnosti zadních vrátek je přitom taková, že klientská část vysílá požadavky útočníka serverové části, která tyto požadavky plní, nebo odesílá zpět klientovi požadované informace. Klientskou část aplikace tedy vlastní samotný útočník a serverová část by měla být umístěna v počítači oběti. Komunikace poté probíhá prostřednictvím komunikačního protokolu TCP/IP.

Dropper

Jedná se o škodlivý program, většinou spustitelný soubor – EXE, který po jeho spuštění v počítači oběti ze svých vnitřností vyvrhne další škodlivou havěť do zařízení.

Trojan Downloader

Jeho úkol je obdobný jako v případě Dropperu. Rozdíl je v tom, že Downloader si havěť nenese s sebou, ale pokouší se o jejich stažení z internetu, z adres, která má v kódu napevno definované. V praxi to poté může znamenat, že stažení jednoho programu, provede vlnu stažení dalších škodlivých programů, které budou stahovat další a další. Může dojít k tomu, že počítač oběti bude zcela nepoužitelný.

Troja Proxy

Proxy trojské koně mají za úkol infikovaný počítač zneužít pro například rozesílku nevyžádané pošty – spamu. Díky použití proxy serveru je téměř nemožné vypátrat skutečného útočníka. [19]

2.1.5 Počítačové červy

Počítačový červ je typ počítačového kódu, který umí automaticky rozesílat kopie sama sebe na jiné počítače. Po infikování systému, začne kontrolovat prostředky, které jsou zodpovědné za síťovou komunikaci, kterou dále využívá ke svému šíření. Je to typ zákeřného malware, který se snaží nakazit co možná největší počet počítačů. Pokud je počítač infikován počítačovým červem, dokáže výrazně zpomalit počítač, případně způsobit další škody. Počítačoví červi se v mnoha případech přenášejí pomocí infikovaných příloh emailu, úložišť pro sdílení souborů, případně jako odkaz na nebezpečné internetové stránky. Počítačový červ, je většinou snadno odhalitelný, neboť využívá velké množství systémových prostředků, případně vytěžuje linku internetového připojení. V důsledku toho jsou většinou servery a počítače zpomalené a nereagují na běžné příkazy. Mimo své replikace vykonává obvykle počítačový červ v počítači i sekundární činnost, která je červem nesena jako náklad,

čemuž se anglicky říká „payload“. Většinou se jedná o odstranění souborů v počítači uživatele, zašifrování uložených dat v zařízení a následné vydírání, vytvoření zadních vrátek do systému, která mohou být později využita jako přímá cesta do systému a k infikování dalších počítačů v síti, prohledávání počítače za účelem získání určitého typu citlivých dat, či ke znemožnění užívání zařízení. Tento malware stejně jako jakýkoliv jiný malware, byl vyvinut hlavně z důvodu obohacení jeho autora a pro finanční poškození obětí. [23]

Historicky první počítačové červy vyvinuli John F. Schoch a John A. Hupp ve středisku Xerox PARC, kde monitorovali vytížení procesů počítačů, které byly připojené k síti. Velmi prospěšnými červy byli ti, kteří patřili do rodiny Nachi. Tito červi odstraňovali ostatní malware, stahovali bezpečnostní aktualizace z internetových stránek Microsoft Update a instalovali tyto updaty na infikované počítače. Počítačoví červi tedy opravovali ty samé chyby, které sami využívají ke své replikaci. Zvyšovali úroveň zabezpečení počítačů, ale způsobovali zpomalení sítě, neboť po každé instalaci aktualizací restartovali systém. Původním záměrem počítačových červů tedy nebylo škodit a napadat uživatelská data, ale zlepšovat práci s počítačem. Úkolem je napadat osobní počítače a servery, které jsou připojeny do sítě. Červi umí replikovat sami sebe a na dálku aktivovat svou repliku. Obdobně jako u počítačových virů či ransomware, tak i počítačových červů existuje více druhů. Typy jednotlivých počítačových červů rozlišujeme dle toho, jakým způsobem se šíří z jednoho zařízení na další. [24]

Emailoví červi

Jak již název napovídá, tento typ červa se šíří prostřednictvím elektronické pošty od jednoho uživatele k dalšímu. Ve chvíli, kdy infikují počítač, začnou odesílat další emaily na emailové adresy, které získají z emailového adresáře oběti napadaného počítače, nebo tak, že prohledávají obsah uložených souborů či extrahovaných řetězců, které mají znaky emailové adresy. Jiným případem jsou infikované počítače, které jsou přizpůsobeny k tomu, aby byly infikovaným určitým druhem červa, který na příkaz svého autora odesílá SPAM, případně uskutečňuje na jiné počítače útoky typu DDoS. Sítě, které jsou složeny z takto infikovaných počítačů se nazývají botnet. Infikované emaily, které jsou rozesílány červem, obvykle již v obsahu obsahují vlastní škodlivý kód jako přílohu. V jiných případech je v obsahu uveden odkaz na internetové stránky, který dokáže infikovat zařízení příjemce. Výhodou těchto červů je přístup k emailové schránce a možnost její využití, v této kombinaci se jedná o velké riziko, neboť oběť napadení obdrží email od věrohodného odesílatele, kterého i sama má nejspíše uloženého ve svém adresáři. [24]

Internetoví červi

Tento typ červa využívá všech dostupných síťových prostředků počítače, aby mohl skenovat ostatní počítače umístěné v síti. Útok provede ve chvíli, kdy v síti nalezne zranitelný počítač, pokud ovšem umí této zranitelnosti využít. Pokud se mu povede zranitelnosti využít, replikuje se pomocí zranitelnosti na tento počítač a provede instalaci škodlivého kódu. Velkou výhodou internetových červů je, že pokud dokážou uskutečnit tento typ útoku a získat tak přístup do jiného zařízení, je možno zařízení infikovat bez jakéhokoliv vědomí nebo přičinění uživatele daného zařízení. [24]

Červi ve sdílených souborech

Červi, kteří využívají sdíleného prostoru, replikují svůj škodlivý kód jako spustitelný soubor do sdílených umístění, např. do sdílené složky lokálního počítače, případně na vzdálený počítač, kde je tento spustitelný soubor volně k dispozici ke stažení. V případě, že dojde ke stažení a spuštění tohoto souboru, dojde k infikování počítače. Soubor je většinou pojmenován tak, aby nevzbuzoval podezření, že se jedná o škodlivý soubor. Výhodou tohoto typu červů je, že jsou sdílené prostory hojně využívány ve firmách ke sdílení obsahu mezi uživateli a jako jeden z druhů úložiště. [24]

IM a IRC červi

Jedná se o druh počítačových červů, které ke svému šíření využívají sociální sítě, které jsou určené ke komunikaci v reálném čase. IM červi většinou rozesílají odkazy na internetové stránky, které jsou schopné počítač oběti infikovat. IRC červi svůj škodlivý kód zasílají sítí jako spustitelný soubor. IRC červi jsou tudíž méně nebezpeční, jelikož k infikování je zapotřebí uživatelská součinnost. Musí tedy spustitelný soubor stáhnout, uložit a spustit. Výhoda je v tomto případě obdobná jako u emailových červů, kdy je obsah obětem odesílán z důvěryhodných emailových adres. [24]

2.1.6 Ransomware

Ransomware je vyděračský, škodlivý software, jehož účelem je blokování počítače či šifrování dat, která jsou na něm uložena. Ransomware pochází z anglického slova ransom, což znamená výkupné. Po napadení a dokončení šifrování, útočník většinou požaduje výkupné za odšifrování, respektive dodání dešifrovacího klíče, který je použit k obnově dat. Oběť nemá bohužel nikdy záruku, že dešifrovací klíč bude funkční a dojde k obnovení zašifrovaných dat. Platba za dešifrování je většinou požadována v kryptoměně, například

v bitcoinech. Nejprve byl ransomware velice populární v Rusku, postupně se ovšem rozšířil do celého světa. Šíření ransomware je zajištěno většinou formou trojského koně, popřípadě červa, který je importován do systému společně se staženým souborem nebo prostřednictvím chyby v zabezpečení. Program poté zatěžuje systém šifrováním souborů. Méně odhalitelný je takový typ ransomware, který používá kombinaci náhodné symetrické šifry a veřejného klíče, jehož párový privátní klíč zná pouze útočník. Některé typy ransomware počítač uzamknou pomocí MBR (Master Boot Record), Windows shell či změnou diskového oddílu a poté uživateli dovolí pouze zaplatit poplatek za odemčení. Důvodem, proč je ransomware vytvářen a útočníci jej šíří do kybernetického světa, je finanční zisk z provedených útoků. V roce 1989 byl objeven první známý ransomware AIDS trojan, jehož autorem je Joseph Popp. Tento software prohlašoval, že nějakého software v počítači vypršela licence. Došlo k zašifrování souborů na disku a požadoval po napadeném platbu ve výši 189 dolarů, která měla být zaplacena firmě PC Cyborg Corporation, která měla zajistit odemknutí systému. Aby se Popp vyhnul soudu, byl prohlášen za duševně chorého a přislíbil, že přispěje na podporu výzkumu onemocnění AIDS. V srpnu roku 2010 bylo v Rusku zatčeno deset osob, které byly napojeny na ransomware červa WinLock. Tento ransomware zobrazoval uživateli pornografické obrázky a vyzýval jej k zaslání prémiové SMS zprávy, která měla cenu zhruba deset dolarů. Další ransomware, který se začal šířit v roce 2012 se jmenoval Reventon. Tento ransomware zobrazil na obrazovce varování, že byl počítač použit pro nelegální činnost, například stahování dětské pornografie či stahování software bez licence. Byl rozšířen převážně v západní Evropě a v USA. Ruský občan, který byl údajně na tento ransomware napojen, byl zatčen v Dubaji v roce 2013. Později bylo zatčeno dalších deset osob. V září 2013 byl poprvé zaznamenán ransomware CryptoWall či CryptoLocker, který byl rozšířen nejprve v anglicky mluvících zemích, později se rozšířil do celého světa. Za dešifrování dat útočníci nejprve požadovali výkupné v částce 300 dolarů či eur. V České republice to byla částka 10 000 korun. Pokud poškozený nezaplatil, částka se zdvojnásobila. Do mobilních zařízení se od dubna 2015 do března 2016 rozšířil ransomware Fusob. Útočníci požadovali výkupné od 100 do 200 dolarů. Zhruba 40 procent uživatelů bylo napadeno v Německu, dále byl rozšířen do Velké Británie a později do USA. Zřejmě nejznámějším ransomware i pro laickou veřejnost je WannaCry či WannaCryptor 2.0. Tento ransomware v květnu roku 2017 napadl 300 000 počítačů v zhruba 150 zemích. V Česku bylo napadeno zhruba 600 počítačů. Jednalo se o největší útok, který napadl jednotlivé uživatele, univerzity, železnice, nemocnice a další firmy. Výkupné bylo požadováno v bitcoinech ve výši od 300

do 600 dolarů. Díky tomuto útoku vzrostla hodnota akcií společností, které se věnují kybernetické bezpečnosti. Další ransomware, který je rozšířený od roku 2017, nalezli analytici ze společností Kaspersky, kteří jej nazvali exPetr, nyní znám pod jménem Petya. Ransomware zasáhl řadu společností a institucí po celém světě, včetně České republiky. Nejvíce byla zasažena Ukrajina a Rusko, útoky byly ovšem hlášeny i z USA a západní Evropy. Dle statistik firmy Eset byla Česká republika devátým nejvíce napadeným státem. Výkupné bylo ve výši 300 dolarů. [27], [28]

Stejně jako u ostatních typů malware i ransomware má své vlastní dělení dle funkcí, které vykonává.

Kryto malware – šifrovací ransomware

Tento typ ransomware zasahuje uložená data v počítačích, serverech, mobilních telefonech, tabletech a v dalších zařízeních, které jsou zašifrované šifrou. Klíč, umožňující dešifrování, zná pouze útočník. Aby napadený získal dešifrovací klíč, je nutné zaplatit výkupné. Šifrovací ransomware je možné rozdělit na další typy. Některé zašifrují pouze určitý typ dokumentů, nejčastěji jpg, txt, doc, docx, pdf apod. Jiné typy ransomware zašifrují celý obsah zařízení či diskový oddíl. Další typy ransomware dokázaly zašifrovat také připojené externí zařízení – externí disky či síťové disky. Pokud je použit tento typ ransomware, přijdou uživatele i o zálohovaná data. V některých případech útočníci dešifrovali několik souborů, aby získali důvěru, že dešifrovací klíč je zcela funkční. [29], [30]

Locker – blokovací ransomware

Blokovací ransomware je nazván dle způsobu znemožnění přístupu zařízení. Tento typ ransomware zablokuje zařízení jako celek a žádá o zaplacení výkupného. Nejznámější ransomware tohoto typu je Policejní virus, který na napadeném počítači zobrazí výzvu Policie ČR, v němž uživatele informuje, že se dopustili trestné činnosti, a proto je počítač zablokován. K odblokování a počítače a vyřešení trestného činu je nutné zaplatit částku 2000 Kč prostřednictvím PaySafeCard. Jsou zaznamenány i případy, kdy se napadení dostavili na policejní stanici. [29], [30]

Doxware

Tento typ ransomware přenáší citlivé soubory z napadaného zařízení do zařízení útočníka. Útočník poté napadanému vyhrožuje zveřejněním jeho dat, pokud nezaplatí výkupné. Příkladem tohoto typu je Ransoc. [30]

Scareware

Jedná se o falešný software, který oznamuje, že v zařízení napadaného nalezl potíže a za odstranění těchto potíží požaduje zaplatit. Nejčastěji uzamyká počítač, zobrazuje velké množství vyskakovacích oken či výstrahy. [30]

Ransomware využívá více možností šíření na potenciální oběti. Jde především o následující případy šíření:

Bezpečnostní chyba software

Některé typy ransomware se šíří podobně jako počítačový červ, který využívá zranitelnost software. Tato zranitelnost je zneužita, a poté je ransomware lavinově distribuován na další počítače v síti. Takto se šířil například ransomware WannaCry2, který zneužíval zranitelnost protokolu SMB v Microsoft Windows (Server Message Block – síťový protokol zajišťující sdílený přístup k objektům v síti a interakci mezi uzly). [30]

Šíření prostřednictvím emailové přílohy

Jde o nejčastější metodu šíření ransomware, kdy je škodlivý kód uložen přímo v příloze emailu nebo je dostupný na odkazu, jehož URL adresa je uvedena v těle emailu. V tomto případě útočník využívá sociálního inženýrství proto, aby přinutil napadaného na infikovanou přílohu kliknout a otevřít ji, případně stáhnout infikovaný kód z odkazované internetové stránky. Nejznámějším ransomware, který se tímto způsobem šířil je Locky. [30]

Sociální inženýrství

Tato metoda šíření ransomware spočívá v tom, že internetová stránka, která je napadena vyžaduje interakci od uživatele. Po provedení požadované akce, většinou se jedná o neškodnou aktualizaci systému, se infikovaný kód stáhne do zařízení. Velmi časté na takto napadené stránce je bezpečnostní upozornění, které varuje, že je na stránce zastaralý plugin nebo je nutné stáhnout doplněk, který tento ransomware obsahuje. Jedním z příkladů je možné uvést ransomware BadRabbit, který se vydával za aktualizaci Adobe Flash Player. [30]

2.1.7 Rootkity

Definice rootkitu se částečně vyvinula, ale dnes se běžně vztahuje na kategorii softwaru, který skrývá sebe a další software před správci systému, aby mohl provést nějaký úkol, ke kterému byl stvořen. Dobrý rootkit poskytuje určitou formu schopnosti přežití v systému po jeho restartu a dokáže skrýt procesy, soubory, položky registru, síťová připojení,

a co je nejdůležitější, skryje se sám. Rootkit pomáhá útočníkovi skrýt jeho nekalou činnost v systému, kterou tam prováděl. Můžeme tedy říct, že jde o zametání stop. Typickým příkladem provádění modifikace cest je podchyceni, přesměrování u některých důležitých API funkcí operačního systému. Rootkit je v tomto případě na cestě mezi aplikací uživatele a DLL knihovnou, která danou API funkci obsahuje. Oproti tomu druhá metoda, která se zabývá modifikací systémových struktur, obvykle upravuje nesnadno dokumentovatelné systémové struktury. Takováto úprava může vést k tomu, že rootkit dokáže zcela zakrýt jakýkoliv vybraný proces před jiným software. [18], [19]

2.1.8 Pokročilé, perzistentní hrozby – APT

Advanced Persistent Threat – APT je pojem, který je využíván k popisu sofistikovaných, hackerských technik, které jsou zaměřeny na konkrétní cíl. Tímto cílem mohou být velké, velmi úspěšné společnosti, různé organizace, ambasády, vojenský či finanční sektor či dokonce se může jednat o napadení vládních zařízení samostatných států. Pokud existuje nějaká věc, která profesionálům v oblasti kybernetické bezpečnosti nedá spát, je to právě pokročilá perzistentní hrozba. Tato metoda využívá řadu sofistikovaných a velmi pokročilých technických metod, které jsou navrženy tak, aby útočníci získali cenné, důvěrné a velmi citlivé informace o napadeném subjektu. Pokročilá perzistentní hrozba využívá tajné, nepřetržité a hackerské techniky k získání přístupu do systému a setrvání uvnitř systému co možná nejdelší dobu. Čím déle není APT odhaleno tím více informací proudí ven k útočníkovi a tím větší je potencionální destrukce subjektu. Díky vysoké technické úrovni znalostí, které jsou potřeba k vykonání takového útoku, jsou obvykle tyto útoky zaměřeny na vysoce postavené cíle s účelem odcizovat informace po velmi dlouhou dobu. Není tedy divu, že se nejedná o jednoho útočníka, ale o skupinu několika útočníků, kteří mají i ve většině případů napojení na vládní organizace pro účely provádění kybernetické špionáže. Cílem APT skupin je získání vysoce důvěrných a citlivých dat a jejich zneužití. Časté jsou krádeže identit, účtů, získávání přístupu do kritické infrastruktury a tam poklidně setrvávat co nejdelší dobu a odčerpávat cenné informace, případně škodit. K takovému útoku je potřeba velmi kvalifikované technické znalosti, jelikož se většinou jedná o soubor technických metod, nikoliv o jednu metodu nabourání do systému. V poslední době se útočníci obracejí i k menším „cenným“ společnostem, které tvoří třeba dodavatelský řetězec jejich primárního cíle. Takovou společnost používají jako prostředníka pro doručení škodlivého malware do koncové společnosti. Tyto společnosti jsou využívány pro jejich nižší bezpečnost. Jsou tedy méně chráněné a lépe útočníkům dostupné a poslouží účelu přepravce. Účelem APT

útoku je získat trvalý přístup do systému. Většinou tohoto útočníci dosáhnou v pěti fázích. V první fázi je důležité získat přístup do systému. Jejich cílem tedy je najít takovou zranitelnost, díky níž se do systému dostanou. Musí tedy zdolat síťové a zabezpečovací prvky. K doručování infikovaných souborů se nejčastěji používají metody phishingu, spear-phishingu, technik sociálního inženýrství či známých zranitelností. Ve druhé fázi dochází k vytvoření opory, kdy útočníci implementují malware, který umožňuje vytvoření zadních vrátek a tunelů používaných k nepozorovanému pohybu v systémech. Malware většinou používá techniky přepisování kódu, aby mohl za sebou zamést stopy. Ve třetí fázi se útočníci snaží o prohloubení přístupu v systému. Ve chvíli, kdy je útočník uvnitř systému, používají se techniky jako je prolomení hesla pro možnost přístupu k privilegovaným účtům, jako jsou správcovské účty a tím mohli získávat vyšší práva. Ve čtvrté fáze se útočník pohybuje velmi opatrně, zkoumá oběť a získává postupně moc nad celým systémem. V páté fázi probíhá sběr informací a plnění příkazů. Po dokončení buď v systému nadále setrvávají nebo se stáhnou, ale zadní vrátka zůstávají pro budoucí účely. V mnoha případech je nejslabším článkem člověk, přes kterého je umožněn přístup do sítě společnosti. Může se jednat o oběť některé metody sociotechnik či může mít skupina napojení na někoho uvnitř, což se většinou nestává. Hlavním nebezpečím APT útoku je, že i když je útok odhalen či ukončen, bezprostřední hrozba může stále trvat, vzhledem k možným zadním vrátkům v systému a možnosti návratu útočníka. Obranou je systém bezpečnostních politik, pravidelné školení zaměstnanců, a propracovaný systém bezpečnostních řešení. [37]

2.1.9 Zajímavý malware

ILOVEYOU

Tento červ byl vytvořen v jazyce VBScipt a tím bylo omezeno šíření na počítače s operačním systémem Windows. Šířil se prostřednictvím emailu, jako jeho příloha a k jeho spuštění byla potřeba součinnost uživatele, který musel přílohu otevřít. Po spuštění se automaticky dále rozeslal na všechny emailové adresy v adresáři, které byly uložené v aplikaci Microsoft Outlook. Díky tomuto mechanismu bylo zajištěno rychlé šíření dál mezi uživatele, neboť byl email odeslán od důvěryhodného odesílatele. Pomocí uživatelského účtu oběti mazal systémové soubory, upravoval registry Windows a přepisoval určité typy souborů. Spustitelný soubor, který běžel na pozadí, v počítači vyhledával uložená hesla či čísla a hesla kreditních karet, která poté odesílal zpět útočníkovi. Předmětem emailu byl uveden text „ILOVEYOU“ a ke zprávě byl připojen soubor LOVE-LETTER-FOR-YOU.TXT.vbs a případně další

spustitelné soubory. Počítačový červ si uměl vytvořit vstupy v systémových registrech, aby si zajistil opakované spuštění při startu operačního systému. Jako další činnost, který tento červ prováděl bylo odstraňování určitého typu souboru, které měly příponu: jpeg, vbs, vbe, js, jse, css, wsh, doc atd. Infekce byla vypuštěna 4. května roku 2000 a první případy byly evidovány na Filipínách, odkud se infekce rozšířila do Hongkongu, dále do Evropy a na konec dorazila do USA. Napadeno bylo celkově 10 procent ze všech připojených počítačů do sítě. Jelikož bylo odesláno velké množství emailových zpráv, zkolabovaly některé emailové servery, vládní instituce, jako třeba Pentagon, CIA či britský parlament. Jedná se o druhý nejnebezpečnější malware všech dob. O prvenství přišel díky nástupu ransomware WannaCry. [25]

Obrázek 2. Nejpodlejší virus ILOVEYOU [20]

Stuxnet

Tento červ je určený k sabotáži průmyslových procesů, které jsou řízeny řídícími systémy Siemens SIMATIC WinCC a PCS 7. Červ využíval známých i v té době neznámých zranitelností k šíření sama sebe, aby byl dostatečně silný a vyhnul se nejmodernějším bezpečnostním technologiím, které by jej mohly odhalit. Stuxnet byl objeven v roce 2010. Byl naprogramován tak, aby útočil na systémy SCADA, speciální systémy, které řídí elektrárny, distribuční sítě, dopravní infrastrukturu a další klíčové prvky. Stuxnet dokáže tyto systémy napadnout, přeprogramovat jejich řídící jednotky a zamést za sebou stopy. Využíval zranitelnosti nultého dne v OS Microsoft Windows. Další chybou, kterou červ používal ke svému šíření, je chyba MS Windows při čtení souborů s příponou *.lnk. Ve chvíli, kdy chtěl uživatel

otevřít svůj přenosný USB disk, na kterém se nacházel tento poškozený soubor, došlo ke spuštění škodlivého kódu, který byl uložen ve stejném adresáři a poté započala instalace počítačového červa do systému. Stuxnet je neobvyklý svou malou velikostí půl megabajtu a také tím, že byl naprogramován v různých programovacích jazycích, včetně C a C++. Po proniknutí do systému červ zkontroloval, zda je v systému nainstalován řídící software Siemens, ze kterého jsou sledovány specifické automaty S7-300, které mají připojené moduly CP-342-5, které řídí frekvenční měniče. Pokud ano, červ upravil software PLC tak, aby docházelo k opakované změně výstupní frekvence měničů. Pro zamaskování své činnosti, podstrčil do Step7 své knihovny DLL, aby uživatel infikovaného zařízené neměl tušení, že je infikován. Dle dostupných zdrojů měl Stuxnet napadnout cíle v Íránu. Konkrétně se mělo jednat o jadernou elektrárnu Búšehr a o továrnu na obohacování uranu v Natanzu. Tyto spekulace vycházejí z faktu, že 60 procent napadených zařízení bylo právě ze zmíněné země. Experti uvádějí, že výrobcem červa je zřejmě znepřátelený Izrael a že se jedná o počítačového červa armádního původu. [26]

WannaCry

Jedná se o nejznámější ransomware všech dob, který dokázal během jednoho dne infikovat více než 300 000 počítačů se systémem Windows ve více než 150 zemích. Velké množství těchto počítačů je v majetku vládních agentur a nemocnic. První verze WannaCry se objevila začátkem roku 2017. Ransomware se šířil prostřednictvím spustitelné emailové přílohy, kdy ještě nezpůsobil tak ničivé škody. Druhá verze WannaCry byla za to velice ničivá. Útočníci spustili útok dne 12. května 2017. Jeho síla byla tak ničivá, že během několika málo hodin napadl více než 300 000 zařízení, kdy polovina byla detekována v Rusku. Tento ransomware se občas objeví i v dnešní době.

WannaCry2 se taktéž jako WannaCry v první vlně šířila pomocí emailu. K šíření se taktéž využívala zranitelnost v protokolu SMB verze 1. Konkrétně se jedná o zranitelnost MS17-010 EternalBlue. Tato zranitelnost postihuje operační systémy Windows, které nejsou aktualizovány a záplatovány. Konkrétně se jedná o Windows 2000, Windows XP, Windows Vista, Windows 7, 8 i 10. Dále serverové operační systémy Windows Server 2008 i 2008 R2, Windows Server 2012, 2016, a další. Zranitelnost umožňuje vzdálené spuštění infikovaného kódu, a to bez nutnosti uživatelské interakce. Ransomware využívá velmi silné šifrování AES-128, které je zkombinováno s RSA-2048. V důsledku této kombinace je nemožné soubory dešifrovat bez znalosti dešifrovacího klíče. Analytici zjistili, že se WannaCry2 chová jako červ, který používá dva způsoby útoku – EternalBlue a DoublePulsat.

Útoky jsou spojovány se severokorejskou skupinou Lazarus. Šíření sítí není na první pohled možný detekovat, jelikož k napadení není třeba žádná aktivita ze strany uživatele. Jakmile dojde k napadení počítače, spustí se WannaCrypt, který začne šifrovat uživatelské soubory. Po dokončení se zobrazí informace o napadení a údaje, které nabádají k zaplacení částky 300 či 600 dolarů, které jsou splatné v bitcoinech do tří či do šesti dnů od napadení. Pokud napadený nezaplatil, dešifrovací klíč byl zničen. [31], [32], [33]

SaveTheQueen

Nový ransomware, který používá příponu SaveTheQueen, byl nalezen v prosinci uživatelem Twitteru @malwrhunterteam. K šíření a sledování infekce použil útočník sdílení SYSVOL na řadiči domény vytvořením naplánované úlohy a vytvořením souborů protokolu pro každé infikované zařízení. Možnost zápisu do sdílené složky SYSVOL znamená, že útočník již dříve dosáhl práv správce domény. Autor ransomware se snažil zkomplikovat analýzu, včetně kódování base64 binárního komprimovaného souboru pomocí gzip, který byl použit k vložení shell kódu do winlogon.exe. Ukázalo se, že shell kód je úplná aplikace chráněná pomocí nástroje s názvem ConfuserEx a převedena na shell kód pomocí jiného nástroje s názvem Donut. Původní nechráněný binární soubor je jednoduchý spustitelný soubor .NET, který provádí akce typu:

- hledá soubory k šifrování,
- ukončení jakéhokoliv procesu,
- výčet všech disků, včetně sdílených,
- přidá do souboru před šifrováním příponu SaveTheQueenING,
- po dokončení šifrování změní příponu na SaveTheQueen
- do adresáře přidá výkupné.

Data na internetu jsou bohužel nepřesná. S tímto ransomware jsem se setkala osobně v jedné korporátní firmě. Útok proběhl systematicky tak, aby si uživatelé nebyli schopni ničeho všimnout a zabránit šíření. Útok začal v 15:00 a během několika málo minut byla zašifrována veškerá data na všech zařízeních, která byla připojena v síti, což bylo zhruba 90 procent všech zařízení. Napadená byla Česká republika, Brazílie, Mexiko, Francie, Bulharsko, Rumunsko a Polsko. V plánovači úloh, v systému Windows byla nastavena automatická aktualizace systému Windows. V okamžiku spuštění se spustilo samotné šifrování dat. Pokud se podařilo zařízení odpojit od sítě, šifrování bylo zastaveno a dál se data v zařízení nešifrovala. Po dokončení se zobrazil soubor s požadovaným výkupným. V Brazílii se podařilo

během třech dnů dešifrovat klíč a zachránit zašifrovaná data. Tento klíč nefungoval ve všech zemích. Jiný zdroj uvádí, že injektor, byl jednoduchý .NET soubor, který nebyl vůbec chráněn. Zdrojový kód odhalil, že jeho účelem bylo vložení shell kódu do procesu winlogon.exe. Ransomware nenapadal zálohovací systém, a proto byla možná obnova dat. [34], [35]

Cerber

Tento ransomware je ukázkou vývoje této technologie. Ransomware Cerber je nabízen jako služba Ransomware-as-a-Service – RaaS. To znamená, že kdokoliv si může koupit útok, a to za provizi 40 procent ze získané finanční částky. Ransomware cílil na cloudové uživatele Office 365 pomocí rozsáhlé a velice propracované phishingové kampaně. Díky této kampani ovlivnil a zasáhl miliony uživatelů napříč celým světem. Jedná se o země jako Arménie, Ázerbájdžán, Bělorusko, Gruzie, Kyrgyzstán, Moldavsko, Rusko, Ukrajina apod. Útočník rozešle phishingovou emailovou kampaň mířící na potenciální cíle. Oběť obdrží email, který obsahuje infikovaný dokument Microsoft Office. Po spuštění ransomware, běží šifrovací fáze na pozadí, aniž by vzbudil podezření. Když je šifrování dokončeno, uživatel je informován o napadení a o částce výkupného v zašifrovaných složkách, a i na pozadí tapety. V období svého vrcholu představoval Cerber 26 procent všech infekcí pomocí ransomware. Cerber používá velmi silné šifrování RSA a do dnešní doby nejsou k dispozici žádné dekodéry, které by dokázaly získat dešifrovací klíč. [36]

Lazarus MATA

V červnu roku 2021 bylo zaznamenáno, že skupina Lazarus útočí na obranný průmysl pomocí malwarového frameworku MATA. Tento Framework umožňuje napadat operační systémy Windows, MacOS a Linux. Framework byl dříve skupinou používán na útoky za účelem krádeže zákaznických databází či pro šíření ransomware. V roce 2021 bylo vyzkoumáno, že se Framework MATA využívá za účel kybernetické špionáže. Byla vytvořena verze trojanu, o které útočníci věděli, že ji oběť využívá. Díky tomu došlo ke kompromitaci webových serverů a nahrání skriptů pro filtrování a vzdálené ovládání škodlivých kódů. Framework MATA útočníci používají, kromě útoků na obranný průmysl i pro napadání IT a e-commerce firem v Německu, Polsku, Koreji, Turecku, Japonsku a Indii. MATA obsahuje několik komponent, jako je zavaděč či pluginy, které infikují již zmíněné operační systémy. Framework se používá k načítání zásuvných modulů do běžících příkazů operačního systému k infikování a manipulaci se soubory a procesy vkládáním DLL knihoven. Útočník najde databázi s citlivými údaji zákazníků a spustí databázové skripty, kterými zákaznická

data získá. MATA je v balíčku se sadou hackerských nástrojů dostupný ke stažení na legitimním webovém serveru. Tímto způsobem byl zřejmě tento malware distribuován. Součástí balíčku byl linuxový nástroj pro výpis složek, skripty pro používání serveru Atlassian Confluence Server (CVE-2019-3396), nástroj socat, a samozřejmě samotný framework MATA. [38], [39]

Lazarus AppleJeus

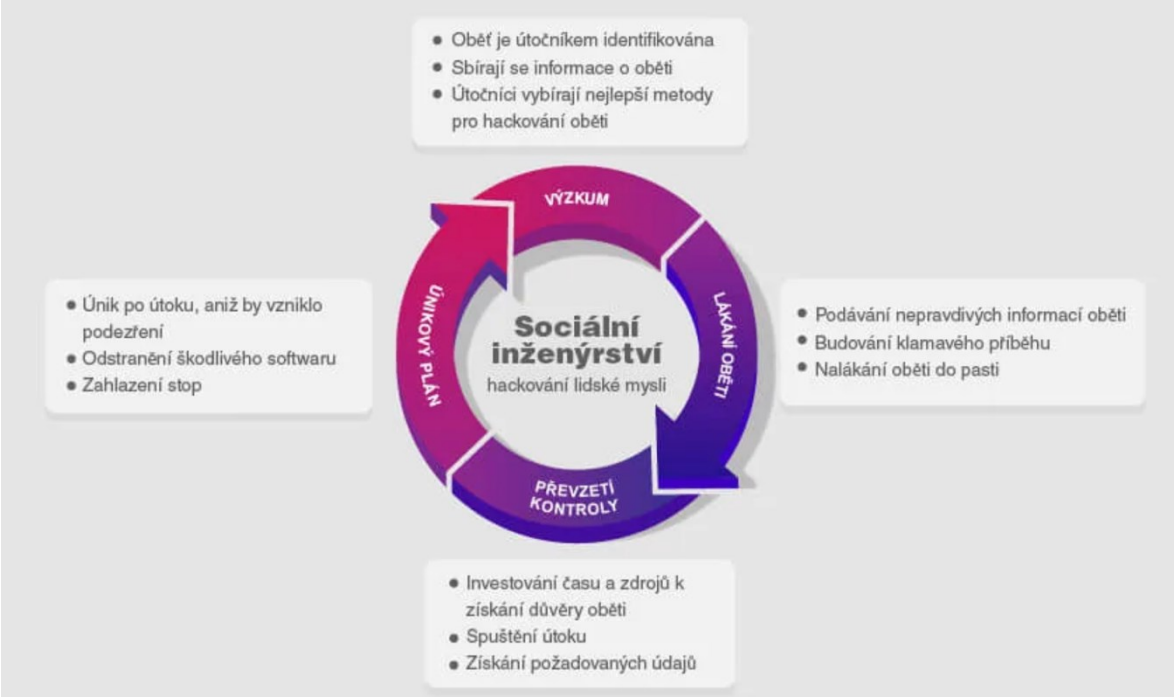
AppleJeus je severokorejský malware, který útočí na kryptoměny. Tento malware se soutředí na jednotlivce a společnosti, včetně kryptoměnových směnáren a na společnosti, které se zabývají poskytováním finančních služeb. Zjednodušeně řečeno malware napadá peněženky s kryptoměnami. Zaměření APT bylo po celém světě ve více jak třiceti zemích. Aktéři útoků považují upravené aplikace pro obchodování s kryptoměnami za prostředek k obcházení mezinárodních sankcí, které byly uvaleny na Severní Koreu. Aplikace umožňuje získat přístup do společností, které provádějí transakce s kryptoměnami a kryptoměny z těchto účtů odcizují. Malware identifikovala vláda USA, která označila APT za napojený na Severokorejskou vládu. AppleJeus je tedy platforma, která je určená pro obchodování s kryptoměnami. Vznik platformy se datuje do roku 2018. Platforma se na první pohled zdá jako legitimní. Díky tomu klame jednotlivce, kteří si aplikaci stáhli do svých zařízení. K distribuci jsou využívány phishingové metody, sociální sítě či pokročilé techniky sociálního inženýrství tak, aby nalákaly uživatele ke stažení tohoto zákeřného malware. Skupina používala několik verzí malware AppleJeus od roku 2018 pro napadení firem podnikajících v sektorech energetiky, financí, vlády, průmyslu, technologií a telekomunikacích. Zasažený byl celý svět od Argentiny přes Austrálii, Maďarsko, Indii, Japonsko, Nizozemí, Rusko, Velkou Británii, Slovinsko až po USA. Škodlivý program, známý jako Celas Trade Pro, byl upravenou verzí neškodné aplikace QT Bitcoin Trader. Tento incident vedl k tomu, že oběť byla infikována nástrojem pro vzdálenou správu FALLCHILL, který je plně funkčním RAT s více příkazy, které je možné vydávat ze vzdáleného serveru. K dalšímu šíření docházelo pomocí phishingovému mailu od společnosti Celas LLC, který doporučoval AppleJeus jako aplikaci pro obchodování s kryptoměnami. Email samozřejmě obsahoval bonus ve formě trojského koně. Další verze malwaru se již moc nelišily, akorát byly použity jiné webové servery pro možnost stažení nebezpečného malware. Jedním z nich byla i peněženka Kupay, která obsahovala bonus ve formě malware AppleJeus. Po instalaci Kupay Wallet, byl zaveden upgrade, díky němuž došlo ke shromáždění informací o oběti a následně k jejich odeslání útočníkovi. Finanční dopad byl vyčíslen na stovky milionů amerických dolarů. [40]

3 SOCIÁLNÍ INŽENÝRSTVÍ

Sociální inženýrství je způsob psychologicky vedené manipulace, díky níž se útočník snaží z lidí vylákat osobní informace, které mají být poté zneužity v útočníkův prospěch. Jako sociální inženýrství označujeme veškeré metody, které mají za úkol přesvědčit své oběti o důvěryhodnosti pro účely úspěšného vykonání důkladně vedeného kybernetického, kriminálního útoku. Útočník se snaží ze svých obětí vylákat takové informace, jako jsou například hesla, bankovní údaje či případně získat plný přístup k počítači oběti za účelem instalace škodlivých programů. Důvod, proč je tato metoda využívaná je jednoduchý. Je totiž jednodušší vylákat podvodem uživatelské heslo, než složitým způsobem obcházet zabezpečení počítače či firemní sítě. Je známým faktem, že nejslabším článkem každého bezpečnostního řešení je člověk. Sociotechniky především vsázejí na určité lidské vlastnosti či vzorce chování. Jedná se především o strach, zvědavost, lidskou závist či chamtivost. Útočník se vždy snaží upoutat pozornost oběti na tolik, aby potenciální oběť donutil provést předem promyšlenou akci, která má za cíl získat určité informace či získat práva do počítačového systému. Mezi nejrozšířenější techniky sociálního inženýrství patří: [41]

- Phishing
- Pharming
- Baiting
- Pretexting
- Scareware
- Blagging
- Vishing
- Whaling

Je tedy na místě být na pozoru v případě jakékoliv nevyžádané rady nebo žádosti o pomoc. V tomto případě je na místě vše posuzovat se zvýšenou opatrností. A to obzvlášť v případě, že protistrana požaduje kliknutí na odkaz, je totiž velmi pravděpodobné, že se jedná o pokus o podvod pomocí technik sociálního inženýrství. Pozornost je také nutné věnovat výzvám, kdy protistrana žádá o zaslání hesel či finančních údajů. Žádné instituce nikdy nevyžadují po svých klientech o zaslání těchto údajů emailem či po telefonu. Důležité je také před otevřením podezřelého emailu ověřit důvěryhodnost odesílatele. Schopný útočník využívá pro efektivní útok základní vlastnosti lidské povahy, kterými jsou: [3], [4]



Obrázek 3. Životní cyklus útoku prostřednictví sociálního inženýrství [3]

Autorita

Lidé mají tendenci se podřídit osobě s vyšší mocí, jedná se především o vyšší funkci, vedoucí pozici ve firmě, ve škole apod. Pokud se tedy útočník vydává za asistenta manažera, jeho slova mají vůči běžnému zaměstnanci vyšší váhu.

Sympatie

Pokud k někomu oběť chová sympatie, ráda jeho požadavkům vyhoví. Sympatie si lze získat různými způsoby. Jedná se třeba o stejné názory na určitý řešený problém, nebo podobným zájmům apod.

Vzájemnost

Pokud se bude oběť cítit být útočníkovi nějak zavázána, je vysoce pravděpodobné, že bude se sociotechnikem spolupracovat. Jedná se o situace, kdy útočník pro svou oběť něco udělá, např. něco nainstaluje, sežene film nebo opraví určitý, počítačový problém a na oplátku oběť vybídne, aby si nainstaloval nějaký program, který v sobě nese určitý bonus v podobě malware, spyware, trojského koně, keylogger nebo program pro vzdálený přístup k ploše uživatele.

Důslednost

Lidé mají obecně tendenci se podřídit, pokud předtím veřejně vyhlásili svou podporu a angažovanost k určitému tématu či věci. Je to především veřejná sázka či slib.

Společenský souhlas

Sociotechnik v tomto případě oběti oznámí, že potřebuje vyplnit nějaký dotazník, který již předtím všichni ostatní vyplnili. Oběť nabude dojmu, že když dotazník vyplnili ostatní, proč by jej nevyplnila oběť samotná? Poté již záleží na sociotechnikovi, na jaké otázky bude vyžadovat po oběti odpovědi. Může se jednat o otázky osobního charakteru, či o citlivé údaje, např. o bankovním účtu či o kartě.

Zvláštní příležitost, akční nabídka

V tomto případě se jedná o vliv reklamy či akční nabídky, která je limitována počtem nebo časem. Toto samozřejmě v potenciální oběti vyvolá pocit neodmítnutelnosti tak lákavé nabídky. Útočník může různými způsoby manipulovat s potenciální obětí tak, že např. nabídne jistý dárek či jinak lákavou nabídku. Může se jednat o registraci zdarma, či registraci s nějakým dárkem. Pomocí registrace uživatele na uměle vytvořené podvržené stránce, útočník získá od obětí osobní údaje, jako jsou jméno a příjmení, uživatelské jméno, heslo a emailový účet. Vzhledem k faktu, že někteří uživatelé používají univerzální heslo či emailovou adresu, získá útočník zajímavou databázi s uživatelskými jmény a hesly, které se může pokusit použít na běžně dostupných stránkách či sociálních médiích. [3], [4]

V oblasti informatiky se pojem sociální inženýrství začal používat v osmdesátých letech 20. století, kdy se o zpopularizování postaral Kevin Mitnick. Tento ve své době nejslavnější hacker na světě se proslavil tím, že dokázal velmi účinně využívat metody sociálního inženýrství. Díky tomuto svému umu se dostal několikrát do potíží se zákonem. Byl dokonce považován za nejnebezpečnějšího osobu a vyhlášen americkou FBI za nejhledanějšího zločince v historii. Zasloužil si to díky svým neoprávněným průnikům do počítačových sítí velkých organizací, za což mu hrozil trest odnětí svobody ve výši několika set let. Za jeho hackerskou kariéru přišel již ve dvanácti letech na způsob, jak využívat městskou hromadnou dopravu zdarma. Dalším jeho počinem bylo seznámení se s technikami phreakingu na střední škole. Phreaking má za cíl využívání telefonních linek a služeb bez platby provozovateli. Na vysoké škole při studiu informatiky našel ve školní počítačové síti bezpečnostní díru v operačním systému, pomocí níž získal moc nad všemi počítači. Za tento počin mu hrozilo vyloučení ze školy, ze kterého se mohl vykoupit prostřednictvím školního projektu, ve kterém dostal za úkol zabezpečení opravit. Na svém kontě má průniky do systému firem

DEC, Nokia, Motorola, Fujitsu Siemens či Sun Microsystems. Za tyto skutky byl odsouzen a po propuštění v roce 2000 dostal zákaz používání počítačových a mobilních technologií. Úspěch Kevina Mitnicka se vyznačoval tím, že bravurně ovládal techniky sociálního inženýrství, které kombinoval s technickými znalostmi. V dnešní době je Kevin Mitnick profesionálním konzultantem na poli kybernetické bezpečnosti. [42]

3.1 Phishing

Dle výkladového slovníku kybernetické bezpečnosti, které vydalo národní centrum kybernetické bezpečnosti, je phishing, v překladu rybaření, podvodná metoda, která usiluje o odcizení digitální identity oběti, jeho hesel, přihlašovacích údajů, bankovních účtů, čísel platebních karet apod., jejichž účelem je zneužití těchto prostředků. Údaje jsou z oběti přitom vylákány pomocí podvodné zprávy, která je většinou šířena elektronickou poštou. Zprávy jsou maskovány tak, aby v co největším měřítku napodobili důvěryhodného odesílatele, s kterým může mít oběť nějaký vztah. Nejčastějším typem je například žádost z banky, která po svém klientovi žádá vyplnění čísla bankovního účtu a hesla. Vše se může jevit jako legitimní, neboť útočník může použít i dialogové okno, typické pro konkrétní bankovní instituci. [6]

Nejběžnější formou výkladu je, že phishing je forma útoku, která využívá technik sociálního inženýrství. Metoda tohoto útoku spočívá v tom, že se útočník vydává za důvěryhodnou autoritu, která má za cíl získat od oběti citlivá data. Útočník se v tomto případě zaměřuje převážně na elektronickou komunikaci, kdy útočník své oběti zašle email, který na první pohled vypadá jako legitimní. Může se jednat o email z banky, státní organizace, pojišťovny či od jiného pro oběť důvěryhodného subjektu. Při bližším zkoumání takového emailu ovšem vyplynou některé nedostatky. Jedná se především o adresu odesílatele, která je odlišná od skutečné adresy. Dalším vodítkem k tomu, jak rozpoznat, že se jedná o phishing může být i špatná až lámaná čeština. Email dále může obsahovat části nepřeložených cizích slov apod. Cílem těchto útoků je jednoznačné vylákání citlivých dat od důvěřivého uživatele. Tyto data se dále mohou stát předmětem prodeje na černém trhu či může dojít i k vydírání oběti. Jak tedy takovýto útok funguje? Phishing patří mezi velmi oblíbenou sociotechniku, a proto se jí snaží útočníci stále vylepšovat. Nejčastěji útočníci vyvíjejí snahu o získání přístupu do internetového bankovnictví či k informacím o kreditní kartě oběti. Phishingový email vypadá na první pohled velmi věrohodně a působí určitou formou nátlaku na oběť, aby informace neprodleně poskytla. Takový email nejčastěji obsahuje formulář na zadání

údajů o kreditní kartě včetně CVV kódu, případně je v emailu uveden odkaz na webové stránky, které mají podobnou úlohu. Získat od oběti citlivá data, která by mohl útočník zneužít. V případě, že oběť tento krok provede a uvede své údaje a následně si do mobilního telefonu nainstaluje i podvodnou aplikaci, která dokáže obejít dvoufázové zabezpečení účtu, pak má útočník veškeré údaje o oběti a může mu zcizit finanční prostředky z jeho účtu. V dnešní době bylo již zabezpečení internetových a mobilních bankovnictví povýšeno na novou úroveň, kdy k ověření přístupu dochází přímo v samotné aplikaci, což uživateli přináší větší pohodlí a lepší bezpečnost. Díky četné diakritice v českém jazyce byl dříve phishing lehce odhalitelný. Text byl většinou psán velmi špatnou češtinou a doména neodpovídala webové adrese finanční organizace. V dnešní době ovšem došlo v této oblasti k velkému zlepšení a odhalení podvodného emailu je stále těžší a většinou jej odhalí jen velmi pozorný uživatel. Je tedy velmi důležité si pamatovat, že bankovní instituce nikdy po svých klientech nepožaduje žádné citlivé informace, které by měl uživatel bance posílat emailem. Jak tedy phishingový email poznat? Existuje několik varovných signálů i přesto, že email může obsahovat oficiální logo či další prvky finanční organizace. Jedná se především o:

1. Neformální oslovení
2. Výzva k zadání citlivých údajů
3. Špatná gramatika
4. Nevyžádaný email
5. Email obsahuje určitou formu nátlaku
6. Příliš výhodná nabídka
7. Odkaz na podezřelou doménu

U neformálního oslovení se přitom nemusí automaticky jednat o znak phishingu, ale většinou mají již ve finančním sektoru snahu o personifikaci oslovení daného klienta. Je to tedy jedno z pojítek, kdy by uživatel měl zpozornět a dávat větší pozor, zda se neobjeví další signály, jako jsou špatná čeština, požadavek na citlivé informace, které banky nikdy po svých klientech nevyžadují či velká naléhavost, která v uživateli může vyvolat paniku.

Obecnou obranou proti phishingu jsou následující zásady:

1. Neposkytovat své citlivé údaje emailovou či jinou formou digitální komunikace.
2. Nejprve je potřeba se zamyslet nad tím, proč klikat na odkaz či na tlačítko v emailu nebo na webové stránce. Nutné si ověřit, zda email či webová stránka nevykazuje známky phishingu.

3. Používat kvalitní antivirový program, který dokáže provést kvalitní zabezpečení počítače a dokáže odhalit i phishingové zprávy. [5], [42]

3.1.1 Příklady phishingových zpráv

Phishingovou zprávou to mnohdy jen začíná. Jedním z takových případů byl malware Nemucod, který byl velmi rozšířeným v České republice v roce 2016. Tento malware se šířil po internetu právě prostřednictvím emailových zpráv. Příloha v emailu byla označena jako nezaplacená faktura, nebo pozvánka k soudu. V tomto případě útočníci tlačili na oběť prostřednictvím zvědavosti a strachu. Pokud oběť email otevřela i s infikovanou přílohu, do počítače se instaloval Nemucod, který umožňoval útočníkovi na počítač oběti, zasílat další škodlivý malware. Nemucod byl ransomware, který zapříčinil zašifrování dat na počítači oběti a následný požadavek na zaplacení výkupného. [5]

3.2 Spear phishing

Jednou ze zákeřnějších forem phishingu je spearphishing. Jedná se o cílený phishingový útok, kdy si útočník dopředu získá veškeré možné dostupné informace o oběti, a vytvoří phishingovou zprávu přímo na míru svým potřebám, aby subjekt zaujmul. Takovýto phishingový email je velmi obtížné odhalit. Typickým znakem spear phishingového emailu je rozesílka mířena na konkrétní společnost či osobu, oproti phishingu, který se zaměřuje na rozesílku velkého množství emailů, a to i na špatné adresy. Spear phishing funguje tak, že útočník odešle email osobě na vysoké, manažerské pozici, případně na určité specifické pozici, přes kterou se útočník chce do systému společnosti dostat. Pokud je email namodelován na míru určité osobě, je poté těžko odhalitelný anti-phishingovým filtrem. To je zapříčiněno tím, že je email vyroben na míru pro určitou osobu a tím pádem, adresa odesílatele, ani adresa SMTP serveru nebude zaznamenána na žádném blacklistu. Technika spear phishingu spočívá i v takovém umění, že je email může být odeslán přímo z dané firmy, v tomto případě oběť ani nepojme sebemenší podezření, že se může jednat o nebezpečný phishingový email. Hlavními rysy spear phishingové kampaně jsou následující:

- Email má námi známého odesílatele, např. firemní doménu.
- Email disponuje skvělou češtinou.
- Obsahuje přílohu s atraktivním názvem, která nutí příjemce přílohu otevřít.
- Součástí přílohy je škodlivý kód, který neodhalí žádný antivirus a po jejím otevření, je kód automaticky spuštěn.

- Škodlivý kód neprovádí žádnou akci, ale shromažďuje data, která dále šifruje a odesílá je útočníkovi, který se vzdáleně připravuje na útok.

Spear phishing je velmi propracovaná metoda ze strany útočníka, který si vybírá svou oběť dle jeho vlastního zájmu. Útočník v první fázi shromažďuje data o potenciální oběti a snaží se jí co nejvíce poznat, aby v další fázi mohl vytvořit email na míru svých potřeb. Pečlivě připravený email, který v tomto případě pochází ze známého a tím pádem i pro oběť důvěryhodného zdroje, je obohacen o přílohu se škodlivým kódem, který se dále používá v rámci útoku APT. Nic netušící oběť email otevře a společně s ním i přiloženou přílohu, která spustí škodlivý kód. Tento škodlivý kód poté využije některou ze známých zranitelností, např. zero-day k tomu, aby byl úspěšně zaveden do paměti počítače a tím si škodlivý kód zajistil své spuštění i po restartu PC. Jak je již z uvedeného patrné, největší, podstatný rozdíl mezi phishingem a spear phishingem je právě již v přípravě emailu samotného. Tradiční phishing se zaměřuje na velké počty respondentů, kdežto spear phishing, jak již ze samotného názvu vyplývá se zaměřuje především na velké „ryby“. Spear v angličtině znamená harpuna, a ta se v rybaření používá na lov velkých ryb. Další rozdíly mezi phishingem a spear phishingem jsou:

- U phishingu se v emailu většinou nachází odkaz na URL adresu, u spear phishingu je to většinou již příloha se škodlivým kódem.
- U spear phishingu je odesílatel oběti známí, čímž se liší od běžného méně sofistikovaného phishingu.
- Phishing od své oběti vyžaduje vyplnění určitých údajů, toto ve spear phishingovém emailu oběť nenalezne.
- Phishingový email, na rozdíl od spear phishingového neobsahuje žádnou přílohu.
- Cílem phishingového emailu je získání přihlašovacích či osobních údajů, u spear phishingu je cílem získání citlivých informací, které jsou předmětem duševního vlastnictví.

Obrana proti spear phishingu ve své podstatě neexistuje. Jelikož se jedná o velmi sofistifikovaný způsob, musela by oběť paranoidně před otevření každé přílohy, kontaktovat odesílatele, zdali email opravdu odeslal a příloha je tedy bezpečná. Pokud by k těmto krokům příjemce přistoupil, i tak nemá žádnou jistotu, že je příloha v pořádku. Bohužel v případě spear phishingu neuspějeme ani s radami typu neotvírat přílohy od odesílatelů, které příjemce nezná či neotvírat přílohy, které neočekáváme, či o které jsme nežádali. Jediná

možnost, na kterou se v tomto případě lze trochu spolehnout je host-based DLP nebo NBA řešení, které mohou činnost takového malwaru zastavit, či na něj oběť alespoň upozornit poté, co selhal antimalware na serveru, přes který emaily prochází. [7]

Produkty DLP mají za cíl zabránit úniku citlivých informací, ke kterému by mohlo dojít ze strany uživatele neúmyslně, či úmyslně. DLP se dělí na dvě řešení, host based DLP a network based DLP. První zmíněné DLP – host based, se instaluje na koncová zařízení uživatelů ve vnitřních sítí společností. Pomocí tohoto DLP je možné sledovat, jakým způsobem uživatel s citlivými informacemi zachází, kontrolovat pokusy o zkopírování dat na USB či jiné digitální médium. Je také možné kontrolovat tisk, přenos dat přes bluetooth nebo paralelní. Další možnosti, které toto DLP řešení nabízí je kontrola zkopírování dat přes schránku a jejich následného vložení do nového dokumentu, včetně zašifrování tohoto dokumentu. Druhé zmíněné řešení, network based DLP, je síťová služba, která je obvykle nainstalována na server v perimetru, který analyzuje všechen emailový a webový provoz, který dále kontroluje, zda ze společnosti neunikají citlivá data. Network based DLP oproti host based DLP se neinstaluje na koncová zařízení, ale není schopno zabezpečit kontrolu nad všemi cestami, kterými mohou data ze společnosti uniknout. I tohoto řešení je nutné se o něj správně starat, nastavovat pravidla a aktualizovat je podle potřeb společnosti. [8]

3.3 Whaling

Je metoda sociálního inženýrství, kterou kybernetičtí útočníci používají k tomu, aby se vydávali za vysoce postaveného zaměstnance v organizaci, kteří mají za cíl zcizit z firmy citlivé informace, získat přístup k počítačovým systémům, či odcizit peněžní prostředky. Pojmenování Whalling vychází z lovu velryb, které jsou velmi vzácné. Metoda je takto označována, jelikož se cílí na vysoce postavené cíle ve společnosti. Útok je podobný jako phishingový tím, že využívá emailu či spoofingu internetových stránek, aby přinutil svou oběť ke konkrétní akci, tedy aby útočník získal citlivé informace, přístupy k účtům či odcizení finančních prostředků. Phishingové podvody se ovšem zaměřují na předem blíže nespecifikované jedince. Útočník vlastně čeká, kdo se chytí a útoku podlehne, spear phishing se zaměřuje na konkrétní jedince a příprava na útok je velmi propracovaná. Útok prostřednictvím metody Whalling je zdvojnásoben tím, že se nezaměřuje pouze na klíčové osoby ve společnosti, ale je proveden způsobem, že podvodná sdělení, která útočník zasílá, vypadají tak, že pocházejí od vysoce postavené, vlivné osoby v organizaci. Může se jednat o finančního ředitele či generálního ředitele, což přidává další prvek sociálního inženýrství, kdy

se zaměstnanci zdráhají odmítnout žádost takto vysoce postaveného člena organizace. Hrozba těchto útoků je velmi reálnou v posledních letech. Jako příklad tohoto útoku, můžeme uvést whalling email, který byl doručen na mzdové oddělení společnosti Snapchat, ve kterém útočník, který se vydával za generálního ředitele, žádal o informace o mzdách svých zaměstnanců. Dalším zajímavým příkladem je útok na společnost Mattel, v níž nejvyšší finanční ředitel obdržel žádost o převod peněz od útočníka, který se vydával za nového generálního ředitele. Společnost útočníkovi zaslala téměř 3 miliony amerických dolarů. Můžeme tedy podotknout, že Whalling je nejvíce propracovaná metoda sociálního inženýrství, která využívá emailové komunikace. Má znaky Spear phishingu, kdy využívá osobnějšího přístupu k oběti, ale zároveň využívá prvku vyšší autority, kdy žádost pochází od vyšších či nejvyšších pracovníků organizace. Díky tomuto je tato metoda velice účinná a velmi dobře cílená. Emailová adresa je samozřejmě podvržena a vypadá jako by byla od legitimního odesílatele, tedy skutečného zaměstnance společnosti. Takový email může obsahovat firemní loga, ale i odkazy na podvodné webové stránky, které jsou navrženy tak, aby působily legitimním dojmem. Vzhledem k tomu, že úroveň důvěry a přístupu obětí v rámci organizace bývá vysoká, stojí to útočníkům za vyvinutí většího úsilí, aby jejich počínaní vypadalo věrohodně. Obrana proti těmto útokům začíná ve vzdělání klíčových jednotlivců v organizaci, kteří by měli být ve střehu, že se mohou stát obětí takového útoku. Je dobré, aby na těchto pozicích vždy panoval určitý stupeň paranoi, obzvlášť v případech, pokud jde o nevyžádaný kontakt, hlavně v případě, jedná-li se o poskytnutí důležitých, citlivých informací či o finanční transakce. Další možností obrany, je samotná kontrola legitimnosti emailu, jako je kontrola odesílatele emailu a jeho celá adresa, kterou je možné zkontrolovat v hlavičce emailu. Další obranou proti útoku tohoto typu, je proškolení vysoce postavených zaměstnanců na udržování si značné anonymity na sociálních sítích a nesdílet osobní obsah, který by mohl útočník využít ve svůj vlastní prospěch. Jedná se o podrobnosti jako jsou koníčky, svátky, narozeniny, dovolené, pracovní pozice, služební cesty, postup na vyšší pozici či osobní vztahy. Jednou z vynikajících metod obrany, je označení emailů ke kontrole, které přišly z prostředí mimo firemní síť, ze strany IT oddělení. Označení externích emailů usnadňuje odhalení falešných emailů, které vypadají legitimně, a to i pro ty méně zkušené uživatele. Pokud bude email označen jako příchozí email mimo organizaci, tak většina uživatelů zpozorní, neboť generální ředitel nebude zřejmě požadovat citlivá data či zaslání peněz po svém zaměstnanci neoficiální cestou, odesláním emailu z jiné než firemní adresy.

Také je vhodné si informace ověřit, a to buď telefonicky s tím, kdo informace či finance požaduje, nebo osobně. [46]

3.4 Pharming

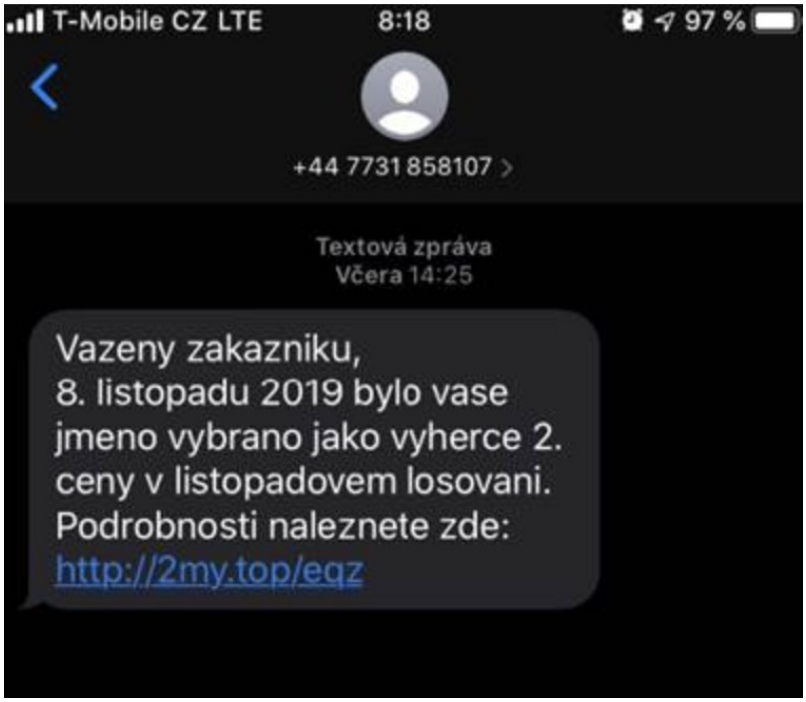
Pharming je online vedená metoda sociálního inženýrství, při které dochází ke zmanipulování provozu internetových stránek a odcizení důvěrných informací. Jedná se o počin, kdy útočník vyvine falešnou internetovou stránku, která je obdobná k nějaké instituci, jako je například banka. Po výrobě takové stránky se útočník snaží svou potencionální oběť na stránku přesměrovat a vylákat z ní přihlašovací údaje. Tento druh kybernetického útoku pracuje se záměnou legitimní stránky za podvodnou. Primárním účelem je zachytit přihlašovací údaje oběti, hesla, rodná čísla, čísla účtů apod. Útočníci, kteří se zabývají Pharmingem se hlavně zaměřují na podvržené internetové stránky finančních institucí, bank, online platebních platforem či e-shopů s elektronickým zbožím, přičemž jejichž konečným cílem je obvykle krádež identity. Tato metoda využívá podvržení DNS serverů, které se starají o překlad IP adres, pod kterými běžně internetové stránky fungují v kybernetickém světě, na pro běžného uživatele čitelnou formu. Uživatel tedy zadá do svého internetového prohlížeče www.seznam.cz, a dále DNS server se postará o správný překlad na IP adresu. A zde začíná útok typu Pharming. Útočník může využít více možností, jakým způsobem provést podvržení DNS. První možností je zaslání škodlivého kódu oběti emailem, který nainstaluje virus nebo trojan do zařízení uživatele. Tento škodlivý kód poté změní soubor hosts v počítači tak, aby směřoval uživatele na podvodnou internetovou stránku, než uživatel původně zamýšlel. V tomto případě nemá potenciální oběť možnost útok rozpoznat. I když zadá správnou cílovou adresu, je díky podvržení hosts souboru v počítači přesměrována na internetovou stránku útočníka. Další techniku, kterou může útočník využít je DNS poisoning. Což znamená, že útočník při této technice upraví DNS tabulku přímo na serveru, a tím způsobí, že více uživatelů neúmyslně navštíví podvodné stránky namísto těch legitimních, které původně zamýšleli navštívit. Na servery DNS je přitom těžší zaútočit, jelikož jsou umístěny v síti organizace a jsou tak více chráněny. Přitom pokud některý z poskytovatelů přijme informace ze DNS serveru, který má podvržené informace v tabulce, je zde velká pravděpodobnost uložení do mezipaměti na dalších DNS serverech a díky tomu rozšíření těchto podvržených informací na více směrovačů a zařízení, což poté značí i větší dosah útoku. Nebezpečí pharmingových útoků tkví v tom, že od uživatelů nepožaduje žádnou akci. Uživatel se může stát obětí i přesto, že je jeho systém čistý a neobsahuje žádný malware.

Nestačí zde ani opatření, jako je ruční zadání adresy webové stránky nebo používání důvěryhodné záložky, protože k nesprávnému směrování dojde poté, co zařízení odešle požadavek na připojení k webu. Obrana proti pharmingu:

- Prověřený poskytovatel internetových služeb, který dokáže odfiltrovat podvržené DNS či použití spolehlivého DNS serveru, který nabízí větší zabezpečení proti podvržení DNS.
- Kontrola, zda internetová stránka je na protokolu HTTPS, což značí, že je internetová stránka zabezpečena protokolem TLS proti odposlechu. Stejně tak je možné i zkontrolovat bezpečnostní certifikát webu.
- Účinnou obranou je neotvírání příloh od neznámých uživatelů, či neotvírání odkazů v podezřelých emailech.
- Kontrola adresy URL pohledem, zda se v nich nevyskytují překlepy či záměny podobných znaků.
- Vyhýbat se podezřele vypadajícím webovým stránkám.
- Kde je to možné, používat dvou faktorové ověřování, které znesnadňuje průnik do uživatelských účtů. Pokud útočníci získají přihlašovací údaje pomocí pharmingu, a účet bude mít dvou faktorové zabezpečení, znesnadní to proniknutí do např. emailu nebo internetového bankovnictví.
- Provést změnu výchozího nastavení svého routeru, včetně pravidelné aktualizace. [41], [46]

3.5 Další metody sociálního inženýrství

Smishing je ve své podstatě to samé jako phishing. Rozdílnost tkví pouze v tom, na které zařízení je zpráva zaslaná. V tomto případě se jedná o textové zprávy v podobě SMS, které jsou doručovány na mobilní telefon obětí. Zpráva cílí opět na strach, zvědavost a tlačí svou oběť, aby neprodleně klikla na uvedený odkaz a aby vyplnila své přihlašovací údaje. V některých případech dokonce nabádá k rozesílce zprávy dalším potenciálním obětem, které by taktéž mohli poskytnout své přihlašovací údaje. Pokud nebude oběť ve střehu a SMS zpráva bude vypadat jako důvěryhodná, oběť poté dobrovolně odevzdá své údaje útočníkovi, a ještě zprávu rozšíří dál. Obrana je v tomto případě jednoduchá. Neposkytovat veřejně své telefonní číslo, na příchozí zprávu nereagovat a rozhodně nevolat na číslo, ze kterého byla zpráva odeslána. Telefonní číslo útočníka je také možné si ověřit v internetovém prostředí.



Obrázek 4. Textová zpráva formy Smishing [44]

Vishning je forma phishingu, kdy útočník využívá podvodného zavolání na vytipovanou oběť a snaží se z ní vylákat citlivá data. Většinou se jedná o přihlašovací údaje k bankovním účtům, včetně ověřovacího PINu. Tato technika je v poslední době čím dál tím více rozšířená, jelikož uživatelé jsou většinou školeni na techniky phishingu, což je jen střípek sociotechnik, které útočník může využít. Pokud je útočník obratným řečníkem a dokáže vyvinout dostatečný nátlak, emoční empatii a psychologii, je možné tímto způsobem získat velmi důležité informace. Zaznamenány jsou i telefonáty ze zahraničních čísel, které jsou po prvním zazvonění ukončení a ve chvíli, kdy oběť zavolá zpět a hovor je započat, jsou účtovány velmi vysoké mezinárodní poplatky. [43], [44]

Blagging je metoda sociálního inženýrství, která se snaží zmanipulovat oběť velmi naléhavým, lživým příběhem, kdy útočník prosí o zaslání peněžní částky. Ve většině případů si útočník vytipuje například kolegu, který je na služební cestě a zašle žádost o finanční pomoc. Oběti přijde email z podvržené emailové adresy, a tak nemusí ani tušit, že se jedná o útok.

Baiting je metoda sociálního inženýrství, která využívá lidské zvědavosti. Jde o pohozené digitální médium, na kterém se nachází škodlivý software. Může se jednat o CD, DVD či flash disk. Pokud oběť takovéto médium nalezne a vloží jej do svého počítače, například,

aby zjistila, zda se nejedná o disk některého z kolegů, v okamžiku vložení do počítače se začne instalovat škodlivý software, který může, ale také nemusí zachytit antivirový program.

Quid pro Quo je metoda podobná technice Baitingu, s tím rozdílem, že využívá bezkontaktního přístupu. V tomto případě se jedná o poskytnutí něčeho, co může mít pro oběť hodnotu. Tedy útočník poskytne oběti své služby, například se může jednat o technickou pomoc, při které útočník navede oběť na své internetové stránky, které mohou obsahovat škodlivý kód či back door. Jako další příklad je možné uvést zpráva s vyděračským podtextem, kdy útočník tvrdí, že má v držení nahrávky nebo fotografie z webkamery oběti, které ovšem vymění za peníze i za přístupy do chráněných prostor společnosti. [43], [44]

Shoulder surfing je založen na systému odpozorování důležitých informací a dat přímo z displeje zařízení útočníkem, který se své oběti dívá přes rameno a čeká na vhodnou příležitost.

Tailgaiting využívá situací nepozornosti pracovníků především ve velkých organizací, ve kterých se pracovníci většinou navzájem neznají. Aby byl tento útok úspěšný, stačí aby byl útočník sebejistý a předstíral, že v organizaci pracuje a poté se obětí nechal dovnitř vpustit. Pokud se útočník dostane na pracoviště s omezeným přístupem, může způsobit velkou škodu či potíže. Může se jednat o odcizení dat z nezašifrovaných disků či instalaci odposlechů nebo škodlivého software do zařízení pracovníků.

Trashing je technika sociálního inženýrství, kdy se útočník snaží získat informace o společnosti mezi vyhozenými odpadky z kanceláří. Obrana proti této metodě je velmi prostá, nikdy nevyhazovat dokumenty s citlivými údaji do koše, ale řádně provést jejich skartaci.

Watering-hole je nejsofistikovanější forma sociálního inženýrství, kdy si útočník pečlivě sbírá data o předem vytipované osobě, kterou má v plánu napadnout. K tomuto používá více sociotechnik jako je Trashing, Vishing či Spear phishing spojený z dalšími technikami jako například pharming. U této techniky není tedy vyžadována osobní účast oběti. Prostřednictvím této metody je narušena bezpečnost stránek, které oběť často navštěvuje. Na stránky je útočníkem umístěn škodlivý kód, či odkaz ke stažení. Pokud oběť na tento lep útočníkovi sedne, je útočníkem provedena injektáž kódu do počítače. Takovýto útok je většinou vykonáván elitní skupinou hackerů či dokonce skupinou, která je sponzorována některý. Státem, a to z důvodu, že je většinou nutné identifikovat zranitelnosti nultého dne, což je útok, který

zneužívá zranitelnosti software, která ještě není známá, a tudíž pro ni neexistuje záplata. [41], [43], [44]

Pretexting je metoda, kdy se útočník využívá falešné identity a vydává za IT podporu, za vedoucího pracovník či za investora společnosti. V tomto případě je z pohledu postavení osoby využito velkého nátlaku na oběť, která může být snadno zmanipulovatelná k poskytnutí citlivých informací.

Scareware je technika, při které útočník doručí na zařízení oběti internetovou stránku, aplikaci či službu, která obsahuje falešnou informaci o napadení zařízení oběti. Ve zprávě je informace s instrukcemi, které má oběť učinit, tedy stáhnout si speciální software, který má škodlivý kód odstranit. Pokud oběť na tuto falešnou zprávu zareaguje, stáhne si do svého zařízení aplikace, která pro útočníka zajistí neomezený přístup k zařízení a díky tomu může útočník instalovat další software či podnikat útoky.

Honey trap je technika využívána v kybernetickém světě, kdy se útočník vydává za známou, autorativní osobnost. Může to být moderátor, investor, mediálně známá osobnost či zástupce významné organizace, který prostřednictvím emailu, sociálních sítí, seznamky žádá oběť o informace o technologie, o zaměstnancích nebo o nějaké situaci, ze které může během několika minut vylákat zajímavé, citlivé informace o systémech, lidech a o společnosti, které poté využije ve svůj prospěch.

Cleaners je metoda, při které útočník využívá přímého průniku do společnosti po pracovní době, kdy se vydává za údržbáře či uklízeče. Po infiltrování se do společnosti, má možnost do zařízení umístit zařízení typu key logger, screen grabber či USB flash disky, které mají za úkol zaznamenávat stisknuté klávesy, zaznamenávat obrazovku se zvukem či po zapnutí počítače automaticky instalovat škodlivý software. Tato metoda se často kombinuje s metodou Dumster diving, kdy útočník vybírá koše přímo v organizaci a snaží se zachytit vyhozené citlivé údaje, jako jsou uživatelská jména a hesla, telefonní kontakty na zaměstnance, informace o infrastruktuře, seznamy IP adres a další. [41], [43], [44]

3.6 OSINT

OSINT neboli Open Source Intelligence je shromažďování informací z otevřených zdrojů. Tyto metody se staly nedílnou součástí sociotechnik při vytěžování zkoumaných subjektů pro účely zpravodajských služeb, útočníků, zabývajících se sociálním inženýrstvím či společností v rámci konkurenčního boje. OSINT přitom využívá výhradně veřejně dostupné

zdroje, které jsou otevřeny všem bez výjimky. Ovšem sbírání při sbírání informací tímto způsobem musí podléhat velkému důrazu na ověřování relevantních informací. Jedná se o využívání pokročilých technik k prohledávání velkého množství dat, kde útočníci hledají určité informace, které mohou později využít k sofistikovanějšímu phishingovému útoku, který bude zacílen na určitou osobu v určité společnosti. OSINT je v mnoha ohledech obrazem operační bezpečnosti OPSEC, což je bezpečnostní proces, kterým organizace chrání svá veřejná data, která by mohla odhalit škodlivé informace, za předpokladu, že by byla správně analyzována. Tuto metodu provozují některá IT oddělení ve vlastních organizacích za účelem podpoření provozní bezpečnosti. Je tedy zcela logické, že se těmto metodám věnují i útočníci. Důležité je proto si vždy uvědomit, co se může stát ve chvíli, kdy běžný uživatel na internetu zveřejní nějakou informaci. Je nutné si vždy položit otázku, zdali nám tato informace veřejně může uškodit? Například sdílení své polohy veřejně, může ukázat obraz toho, co potenciální oběť dělá, kde se pohybuje, kdy je doma, kde pracuje, s kým se stýká, jaké má koníčky apod. Je logické, že OSINT je tedy i pro společnosti zásadní pro udržení přehledu šíření informací o jejich společnostech. Existují nástroje, které hledání těchto informací využívá. Primární funkcí těchto nástrojů je mapování, jaké informace uživatelé vlastní a mohly by tak přispět k potenciálnímu útoku. Zaznamenávají informace, které jsou veřejně dostupné, třeba seznam zaměstnanců, o majetku společnosti apod. Sekundární funkcí, které tyto nástroje vykonávají, je vyhledávání relevantních informací mimo organizaci. Jedná se především o příspěvky na sociálních sítích. Vzhledem k extrémnímu růstu a popularitě sociálních médií je hledání citlivých informací mimo společnost užitečné pro jakoukoli skupinu. Ať už se jedná o útočníka, jiné společnosti, které si ověřují informace o společnosti, zpravodajských službách apod. Jako terciální funkci, nabízejí některé OSINT nástroje možnost, shromažďovat a seskupovat všechny nalezené informaci a sortují je dle užitečnosti a použitelnosti. Mezi takovéto nástroje patří například Maltego, Mitaka, SpiderFoot a mnoho dalších.

Maltego se specializuje na odhalování vztahů mezi lidmi, společnostmi, doménami a veřejně přístupnými informacemi na internetu. Mezi jeho hodnotné funkce patří, že vezme velké množství zjištěných informací a vše rozsortuje do snadno čitelných tabulek a grafů. Ve chvíli, kdy Maltego shromáždí potřebné informace, vytvoří se spojení, která mohou odhalit skryté vazby mezi jmény, emailovými adresami, aliasy, společnostmi, internetovými stránkami, vlastníky různých dokumentů, a dalšími přidruženými informacemi.

Mitaka je k dispozici jako rozšíření pro Google Chrome a jako doplněk pro prohlížeč Firefox. Tento nástroj umožňuje vyhledávat v mnoha vyhledávačů IP adresy, domény, URL adresy, hashe, adresy bitcoinových peněženek a další.

SpiderFoot je bezplatný nástroj, který umí integrovat více zdrojů dat a shromažďuje a analyzuje IP adresy, rozsahy CIDR, domény a jejich subdomény, emailové adresy, telefonní čísla, uživatelská jména či skutečná jména osob. Aplikace je dodávána s více než 200 moduly, díky čemuž je vhodná pro průzkumné aktivity a pro zjišťování více informací o potenciálním cíli.

OSINT je tedy především využíván k:

- Zjišťování informací o konkurenčním subjektu a jeho vazby v rámci zkoumaného prostředí.
- Hledání záznamů o událostech, osobách, subjektech a vzájemných vztazích.
- Zjišťování digitálních stop definované entity.
- Přípravě podkladů k primárnímu výzkumu v terénu. [47]

4 BEZPEČNOST V INTERNETOVÉM PROSTŘEDÍ

V online prostředí číhá na uživatele mnoho nástrah, a proto aby bylo možné úspěšně čelit nástrahám v internetovém prostředí, je třeba dodržovat několik hlavních pravidel o zabezpečení zařízení, ze kterého do internetového prostředí přistupujeme.

4.1 Zásady zabezpečení zařízení

- Pravidelně aktualizovaný operační systém.
- Pravidelně aktualizovaný software na PC.
- Aktualizovaný spolehlivý antivirový program.
- Používání firewallu.
- Router s vlastním zabezpečením, a ne z továrního nastavení.
- Pravidelné provádění zálohování dat.

Tyto zásady je dobré dodržovat, jelikož útočníci často využívají známých chyb operačních systémů zařízení. Pokud tedy není systém řádně aktualizovaný, může tyto známé zranitelnosti obsahovat a útočník může proniknout do systému. [48]

4.1.1 Aktualizace operačního systému

Vydavatele operačních systémů, pravidelně vydávají opravy programového kódu operačního systému. Tyto záplaty slouží k minimalizaci zranitelnosti zařízení. Stejně tak, jako dochází k opravám kódu operačních systémů, stejně tak se snaží o zajištění co možná nejvyšší bezpečnosti vydavatele různých software, které má uživatel nainstalované ve svém zařízení.

4.1.2 Kvalitní antivirová ochrana

Další kapitolou je antivirový program, bez kterého není doporučeno se k internetu vůbec připojovat. Pokud uživatel dobrovolně nepoužívá antivirový program, dalo by se toto jeho počínání přirovnat ke kybernetické sebevraždě, kdy uživatel sám sebe záměrně vystavuje nebezpečí, s kterým je kyberprostor spojován. Takovýto uživatel vystavuje nebezpečí své zařízení, ale může se stát i prostředkem, kterého útočník využije a provede útok z jeho zařízení, čímž ohrožuje i ostatní uživatele kyberprostoru. Samozřejmě je nutné podotknout, že mezi legitimními a spolehlivými antivirovými programy je nepřeberné množství antivirových programů, které plní opačnou funkci a místo, aby systém chránili, tak naopak třeba sbírají data apod. [48]

4.1.3 Firewall

Pokud se chce uživatel na internetu cítit bezpečněji, je dobré zvážit použití programu Firewall, který má za úkol kontrolovat datový tok mezi zařízeními ve vnitřní síti a v síti vnější. Firewall má nepřeberné množství možností, jak ovlivnit bezpečnost vnitřní sítě. Umí kontrolovat datový tok, regulovat přenosy dat či při podezření na škodlivý datový tok, jej zastavit.

4.1.4 Zabezpečený router

V neposlední řadě je dobré myslet i na zabezpečení routeru, který uživatel využívá. Toto zařízení propojuje dvě různé počítačové sítě a směruje mezi nimi datový tok. Pokud je tedy uživatel routeru, který má slabé nebo dokonce žádné zabezpečení, vystavuje se tím velkému riziku průniku do své infrastruktury. Pokud by se do sítě útočník dostal, může se v ní pohybovat a napadat zařízení uvnitř sítě, které může postupně ovládnout a poté z této sítě naplánovat útok v rámci kyberprostoru na další subjekt. Zabezpečením sítě, ke které se uživatel přihlašuje ze svého prostředí to ovšem jen začíná. Důležité je také provést zabezpečení přístupu do samotného nastavení routeru. Z továrního nastavení je totiž uživatelské jméno a heslo admin. Toto je známá věc, a pokud nedojde ke změně nastavení v administrátorském rozhraní, útočník má přímou cestu k ovládnutí routeru. [48]

4.1.5 Pravidelné zálohování

Pro každého uživatele dobré provádět opakující se zálohování dat. Pokud uživatelé zálohují, chrání se před ztrátou a ochranou důležitých dat. Ztráta dat může v dnešní době představovat ztrátu třeba fotografií, dokumentů či další důležitá data. Při zálohování dat je ovšem potřeba myslet na několik pravidel. Ve firemním prostředí se doporučuje provádět zálohování pravidlem 3-2-1, což znamená, že se vytvoří tři kopie dat, z nichž dvě mohou být v síti na různých médiích a minimálně jedna záloha bude mimo firemní prostředí a off-line. Podobné zálohování se doporučuje i běžným uživatelům, důležité je mít svou zálohu mimo počítačovou síť. Záloha je možná provádět na média typu CD, DVD, na externí pevné disky, na síťové úložiště dat NAS, které je ovšem přímo v síti a pokud třeba dojde k napadení systému ransomware a tento disk bude připojen do sítě, budou i tato zálohovaná data zašifrovaná. Dalším možným řešením je cloudové úložiště. Což je datový prostor na serveru provozovatele cloudu, který je dostupný odkudkoliv a z kteréhokoliv zařízení. Mezi velké

výhody patří okamžitá synchronizace dat mezi všemi zařízeními uživatele. Nevýhodou je závislost na rychlosti připojení a fakt, že uživatel svá data svěřuje do péče třetí straně. [49]

4.2 Hesla, jejich tvorba a ověření bezpečnosti

Heslo slouží jako prostředek k ověření totožnosti, takzvané autentizaci uživatele, kterým se k danému systému, programu či webu přihlašuje. Uživatele považujeme za oprávněného ke vstupu do chráněného prostředí po jeho správné autentizaci, tedy pokud se prokáže znalostí správného hesla ve spojení s uživatelským jménem. To, jak je autentifikace uživatele bezpečná, záleží na síle jeho hesla a jakým způsobem má uživatel heslo zabezpečené a zároveň na zabezpečení ze strany systému, který dané heslo ověřuje. Uživatel tedy musí zvolit takové heslo, které je silné, tedy odolné vůči prolomení ze strany možného útočníka, který by chtěl heslo zcizit. Historie hesel sahá do dávné minulosti, kdy byli pomocí hesel rozeznáváni bojovníci vlastní a nepřátelští. Jednalo se většinou o předem domluvené slovo. Hesla taktéž používáme ve formě PINu. Jedná se o číselný kód, který se používá například ve spojení s platební kartou pro ověření oprávnění kartu používat. Nejčastější použití hesel je ovšem v oblasti informačních technologií, kdy za pomoci přihlašovacího jména (loginu) je uživatel odlišen od jiného uživatele. Při přihlašování poté uživatel zadává heslo, pomocí něhož je ověřena jeho totožnost a práva ke vstupu do systému. Uživatelské jméno je většinou známé a veřejné, tedy nikterak ho uživatel neskrývá, oproti heslu, které je tajné. Hesla se také využívají k zabránění přístupu dětí k různým kanálům či webovým stránkám. Pokud by hesla neexistovala, mohl by se kdokoliv přihlašovat na jakýkoliv účet a vydávat se za někoho jiného. Spravovat cizí e-mail, e-shop, zadávat platební příkazy na jakékoliv účty či administrovat intranet libovolné firmy. [48], [50]

4.2.1 Pravidla pro vytvoření silného hesla

Hesla jsou důležitým klíčem, kterým se ověřuje naše identita v online prostředí, proto je nutné se o heslo dobře starat, chránit ho a snažit se mít heslo co nejsilnější proti prolomení.

1. **Originalita hesla**

   Jedná se o takové heslo, které nelze s uživatelem jednoduše spojit a není jednoduše uhodnutelné. Nejedná se tedy o rodné číslo, domácího mazlíčka, jméno dětí či partnera, či oblíbený sportovní klub. Velice nevhodné je používat hesla v angličtině, jelikož se jedná o velmi celosvětově rozšířený jazyk. Naopak

je vhodné využívat jazyk, který se málo používá, může být i smyšlený. Také se doporučuje v původním slově přeházet písmena, jedná se o tzv. přesmyčku.

2. **Heslo nesouvisí se jmény osob**

   Nedoporučuje se, aby heslo mělo souvislost s blízkou osobou, ani se slavnou osobou bez ohledu na to, jestli jí máme rádi či nikoliv. Heslo, které je jednoduše vymyšlené, je i snadno prolomitelné. Nejčastěji používaná hesla v jakémkoliv jazyce jsou jména osob a domácích mazlíčků.

3. **Dlouhé heslo**

   Dlouhé heslo je vždy silnější než heslo kratší. Jako minimální délka hesla se obecně doporučuje 8 znaků, ovšem jako bezpečnější se považuje heslo, které má znaků minimálně 12. Heslo samozřejmě může mít znaků i více. Čím více znaků, tím větší zabezpečení účtu a šance, že heslo nebude možné prolomit.

4. **Používání rozšířených znakových sad**

   Síla hesel roste s použitím různých znaků z různých znakových sad. Čím větší je kombinace znakových sad, tím je heslo pestřejší a pro útočníka špatně prolomitelné. Pokud vezmeme v úvahu heslo dlouhé 7 znaků s použitím malých, velkých písmen, číslice a speciálního znaku je cca 65 biliónů možných kombinací. Oproti tomu, pokud použijeme pouze číslice, muselo by heslo obsahovat minimálně 14 znaků, aby bylo přibližně stejné síly. U takového hesla by existovalo 100 biliónů možných kombinací.

   a. Malá písmena a–z
   b. Velká písmena A–Z
   c. Číslice 0–9
   d. Diakritika (např. ě, í, á)
   e. Speciální znaky (např.:,. -!?)

5. **Generovaná hesla**

   Lidský mozek neumí pracovat s náhodou, a proto vymýšlí neustále se opakující vzorce. Proto jakékoliv heslo, které vymyslíme, nebude nikdy náhodné a je možné jej predikovat. Při tvorbě hesla je lepší využívat generátor hesel. V generátoru hesel si sami nastavíme délku hesla, jaké znakové sady chceme použít a třeba první znak. Aplikace nám pak sama vytvoří heslo, na které bychom jen tak nepřišli.

6. **Vyhnout se náhradám podobných znaků**

   Vkládáním čísel nebo jiných znaků do hesel, která jsou si podobná, nikdy není možné

zaručit dobré zabezpečení hesla, jelikož je to pro potenciálního útočníka předvídatelné. Použití číslic místo podobných písmen je zcela běžné. Například pro zvýšení bezpečnosti slova heslo, použijeme znaky #3510, kdy tyto znaky nahrazujeme vždy tak, aby byly podobné písmenu, které nahrazují. Tento způsob není již bezpečný, neboť útočníci s takovýmto chováním uživatelů počítají.

7. **Každé heslo použít jen jednou**

   Mnoho uživatelů používá jedno heslo k více přístupům. To je ale velmi špatně, neboť každé heslo by mělo umožňovat přístup právě k jednomu systému. Pokud jej použijeme u deseti různých systému, tak heslo oslabíme zhruba desetkrát oproti heslu, které je použito právě jednou. Používáním stejného hesla se vystavujeme riziku, že jedno z nich unikne a ohrozíme přístup i do dalších systémů.

8. **Používání správce hesel**

   Je celkem nemožné pamatovat si několik desítek hesel, když je každé úplně jiné. Proto se nabízí jednoduché řešení a tím je správce hesel. Jedná se o aplikaci, která si pamatuje přihlašovací jména a hesla k systémům za nás. Tím, že si hesla nemusíme pamatovat, se nám otevírají dveře k vytváření silných a bezpečných hesel. Hesla si může zapamatovat i náš webový prohlížeč, pokud klikneme na ikonu zapamatovat si heslo, nemusíme si již heslo pamatovat. Zde se ovšem vystavuje určitému riziku odcizení hesel. K našim heslům se poté může dostat kdokoliv, kdo má přístup k našemu počítači. Oproti tomu dobrý správce hesel má své vlastní zabezpečení, a pokud ho nikdo neodemkne, nedostane se ani k heslům, které v něm máme uložená.

9. **Dvoufázové ověření**

   Ještě lepší zabezpečení je možné dosáhnout s dvoufázovým ověřením. Po správném zadání hesla nám přijde SMS zpráva či e-mail s kódem, který je vyžadován systémem, kam se chystáme přihlásit. Teprve poté, co vložíme kód, se nám systém odemkne. Velkou výhodou je, že druhý faktor nikterak nesouvisí s heslem a tím je celkem nemožné se do účtu nabourat a zneužít jej. Toto funguje za předpokladu, že útočník nemá přístup do našeho telefonu či e-mailové schránky. Nevýhodou je, že každá aplikace či služba, dvoufázové ověření neposkytuje. Pohodlnější a bezpečnější alternativou je mobilní aplikace, která nám vygeneruje šestimístný ověřovací PIN kód s platností nejvýše 20 sekund.

10. Nepodceňovat bezpečnostní otázky

Bezpečnostní otázky, které pomáhají chránit naše hesla, jsou velice zrádné. Pokud klikneme na „zapomněl jsem heslo“, zobrazí se nám bezpečnostní otázky, které ovšem ve většině případů přímo souvisí s naší osobou a může se tedy jednat o veřejná data. I tuto cestu útočníci zkouší. Na bezpečnostní otázky proto nesmí být snadné nalézt odpověď z veřejně dostupných zdrojů, jako jsou třeba sociální sítě. Mezi bezpečnostní otázky patří například: „Jaký je Váš oblíbený seriál“, mnoho odpovědí tedy může mít The Big Bang Theory či The Simpsons, což je velice prozíravé a pro útočníka jednoduché na vyzkoušení. Také se nedoporučuje mít nastavenou bezpečnostní otázku: „Jméno matky za svobodna, jméno oblíbené kapely, sportovního týmu, rodného města, první zaměstnání či jméno mazlíčka.“ Pokud už tyto bezpečnostní otázky použijeme, je nejlepší neuvádět pravdivou odpověď. Bezpečnostní otázky jsou již na ústupu a spíše se používá k obnově hesla jiná e-mailová adresa či telefonní číslo, což je daleko bezpečnější varianta. [48], [52]

4.2.2 Testování vybraného hesla

V následujícím příkladu uvedeme ukázku síly smyšleného hesla. Jako heslo bylo smyšleně zvolené slovo MICKA, jedná se tedy o smyšlené jméno, domácího mazlíčka. Už na první pohled je zřejmé, že heslo o pěti znacích, s dvěma stejnými písmeny nebude nikterak silné. Pomocí měřiče síly na https://hodza.net/password-meter/, provedeme pokus, jak by bylo možné heslo vylepšit, tak, aby bylo dostatečně silné a zároveň, aby bylo v rámci možností uživatele zapamatovatelné. Předem je tedy zřejmé, že bude potřeba použít rozšířené sady znaků, tedy číselné a speciální znaky. Bylo vytvořeno heslo, které kloubí jméno imaginárního mazlíčka a rok narození imaginární kočky, plus speciální znak. Heslo je v tomto případě snadno zapamatovatelné, a i za předpokladu, že nesplňuje pravidlo o jméně mazlíčka, je bezpečné. Skóring 100 % s výsledným heslem **MiCkA2010***. [51], [52]

Tabulka 1. Zvyšování bodového skóre u hesla Micka [51]

Heslo	Jaká změna byla v hesle provedena	Skóre
Micka	první písmeno velké	19 %
MiCkA	střídání malých a velkých písmen	25 %
MiCkA2010	přidání čísel	82 %
MiCkA2010*	přidání speciálního znaku	100 %

Obrázek 5. Vývoj bodového skóringu u hesla Micka [51]

4.3 Bezpečně na internetu

Kromě hrozeb ze strany útočníků, kteří se chtějí obohatit, na internetu číhá další nebezpečí, proto je nutné se v tomto prostředí chovat co možná nejvíce obezřetně a bezpečně. Každý pohyb v online prostředí zanechává stopu. Cokoliv, co nám unikne na internet se stává navždy veřejné. I přesto, že někteří lidé jsou ochotni vzdát se v určité míře svého soukromí,

je tato ztráta brána v dnešní digitální době jen jako malá daň za komfort, popularitu na sociálních sítích či jisté společenské výhody. Pokud se na internet dokument, fotografie či jiný soubor dostane, je vysoce pravděpodobné, že dojde k jeho šíření. Jeho zničení či zamezení dalšímu šíření, je zcela nereálné. Jako jeden z příkladů je možné uvést neúspěšné pokusy o zničení serveru WikiLeaks. Mnoho uživatelů si neuvědomuje fakt, že každý pohyb na internetu, který není podpořen jistou ochranou a zabezpečením, může být zpětně vysledován. Svou digitální stopu, která může být zpětně vysledována či monitorována, zanechává za sebou každý uživatel už i při obyčejném pohybu v síti. Tedy při běžném procházení internetu a vyhledávání informací. Tyto data využívají internetové společnosti pro své vlastní potřeby, třeba pro personifikaci reklamy. Je tedy dobré podotknout, že datová stopa každého z nás, je snadno zneužitelná v případě neopatrného chování. [53]

4.3.1 Anonymita na sítě

Pokud budeme hovořit o bezpečnosti a anonymitě, mnohým uživatelům se jako první vybaví možnost používání anonymního prohlížení prostřednictvím internetového prohlížeče. Tady je potřeba si uvědomit, že tato funkce nemá s anonymitou v síti vůbec nic společného. Funkcionalita pouze zabraňuje možnosti zobrazení historie prohlížeče na daném zařízení před ostatními uživateli. Stane se tedy to, že po ukončení prohlížení a uzavření okna prohlížeče se vymaže historie, cookies a údaje, které byly zadané do formulářů. Toto ovšem k ochraně anonymity na internetu není dostačující, navíc v počítači zůstanou stažené soubory. Aktivita, kterou uživatel provádí je i nadále viditelná pro správce sítě, navštívené webové stránky, tedy jejich servery a také pro kohokoliv kdo mohl infiltrovat síť a odposlouchávat jí. Pokud chce tedy uživatel zůstat opravdu na internetu anonymní, je doporučováno používat anonymní internetové prohlížeče. Tyto prohlížeče dokáží odstranit stopy po procházení společně s dalšími identifikačními znaky, které dokáží spojit pohyb uživatele v síti s konkrétním zařízením či uživatelem. Další možností je používání proxy serveru, které komunikaci zprostředkují. Výhodou je, že navštívené stránky nevidí IP adresu uživatele. Nevýhodou je, že neumožňují šifrování. Zde se poté naskytuje lepší možnosti a to, používání služby VPN, která umí komunikaci zašifrovat. Pro nejlepší anonymitu je dobré, použít kombinaci zmíněných řešení. Je také nutné si uvědomit, kde se uživatel připojuje, používali veřejné Wi-Fi sítě, vystavuje se velkému riziku možnosti odposlechů komunikace z jeho zařízení. Je proto dobré vždy zvážit rizika připojení se na cizí neznámou síť. [53]

4.4 Hrozby v online prostředí dle věkových skupin

Nebezpečí na internetu číhá na uživatele na každém rohu. Hrozby se ovšem v některých případech liší dle věkových skupin. Kde všude se uživatelé mohou setkat s podvodným či jinak zákeřným jednáním? Je to prakticky v celé šíři internetového spektra. Jedná se především o hrozby spojené s útoky hackerů prostřednictvím podvržených stránek, zasíláním phishingových zpráv, dále se s nebezpečným chováním můžeme setkat na sociálních sítích jako jsou Facebook, Instagram, Tik Tok apod. S jakým druhem se tedy můžeme setkat?

- Kyberšikana
- Netholismus
- Dezinformace
- Podvodníci
- Kyberstalking

4.4.1 Kyberšikana

Jedná se o druh šikany, která využívá informační a komunikační zařízení k ubližování jiné osoby. Za projev tohoto chování lze považovat ztrapňování, vydírání, ohrožování, zastrašování či obtěžování. Oběť kyberšikany je stejná jako u klasické šikany s tím rozdílem, že zde útočník využívá výhod kybernetického světa. Jedná se hlavně o anonymitu. Útočník je ve většině případů vzhledem ke své oběti anonymní, vystupuje pod falešným jménem, může mít více falešných profilů na sociálních sítí a může jednorázově používat různé emailové adresy. Díky anonymitě je posílena útočníkova odvaha k páchání agresivní formy útoku na svou oběť. Anonymita je jen fiktivní, odhalení takového útočníka není v dnešní době problém, pokud se útočník neschovává za anonymní technologické prostředky. V online světě se za útočníka může maskovat kdokoliv. Neplatí zde pravidla klasické šikany, nezáleží na pohlaví, věku, fyzické statnosti útočníka ani na sociálním postavení útočníka. U klasické šikany lze předpokládat, že se odehrává většinou na půdě školy a že silnější šikanuje slabšího. Toto lze ale v oblasti kyberšikany vyloučit. Ta může přijít kdykoliv, například prostřednictvím falešného profilu na Facebooku nebo SMS či emailovou zprávou. Intenzitu takového útoku zvyšuje možnost sdílení nebo následného přeposílání těchto příspěvků. Velký aspekt zde hraje publikum. Dopady kyberšikany nejsou fyzické, bývají naopak často psychické. Oběť se po takovémto útoku často uzavírá do sebe a přestává komunikovat se svým okolím. Tento projev může vyvolat strach z útočníka a jeho útoků, z pocitu studu nebo

strach, že rodiče či učitel nepochopí problém. Útočník sází na mlčenlivost oběti. Nejčastějšími projevy kyberšikany jsou:

- Zasílání zastrašujících či urážejících zpráv.
- Ukládání videí, fotografií, audio záznamů a následně jejich zveřejnění, či vyhrožování zveřejněním.
- Vytvoření stránky, která má charakter urážky, ponížení či pomlouvání.
- Vyprovokování a urážlivé napadání ostatních uživatelů v online diskusích.
- Vyzrazování cizích tajemství.
- Vydírání, pronásledování či obtěžování.

Jednotlivé útoky pak mohou vypadat následovně.

1. Happy Slapping – je předem promyšlený a naplánovaný fyzický útok na vybranou oběť. Tento akt je natáčen a celý záznam je poté zveřejněn na sociálních sítí, kde je dále šířen.
2. Sexting – je zasílání textových zpráv, které mají sexuální podtext nebo obsahují fotografie či videa se sexuálním podtextem. V tomto případě mohou být děti a mladiství útočníkem nuceni k zasílání takového obsahu. Poté jsou útočníkem vydírání, že obsah zveřejní. Toto jednání velký dopad na psychiku oběti, která má samozřejmě z útočníka strach. V tomto případě je tento čin kvalifikován jako trestný čin. Sexting se ovšem váže i k dospělé populaci, kdy se může jednat o zasílání obsahu v rámci milostného vztahu, který může být zneužit zejména po skončení vztahu k poškození druhého partnera. Může zde dojít ke zveřejnění či k vyhrožování zveřejněním obsahu se sexuálním podtextem. Pokud je takovýto materiál na internetu zveřejněn, je prakticky nemožné zajistit, že byl tento obsah smazán a neexistuje žádná další jeho kopie.
3. Kybergrooming – jedná se o psychickou manipulaci, která je prováděna prostřednictvím moderních, komunikačních technologií. Cílem je získat si důvěru oběti a vylákat ji na osobní schůzku se záměrem ji sexuálně zneužít. Tato metoda je útočníkem používána v prostředí sociálních sítích, jako je Facebook či Badoo a prostřednictvím zde zasílaných zpráv. Obětí v tomto případě může být prakticky kdokoliv. Ve většině případech se ovšem jedná o mladistvé dívky ve věku 11–17 let, které často tyto technologie používají a trpícími pocitem osamělosti. Tato věková skupina je ohrožená ve větší míře i díky neznalosti rizik, které online prostředí skrývá a bohužel jejich otevřenost k manipulaci ze strany útočníka. Útočník se často vydává za někoho

jiného, než ve skutečnosti je a postupně se snaží získat si důvěru své oběti. K tomuto využívá i formu podplácení formou dárků či penězi. Postupně získává a shromažďuje materiály k vydírání a pěstuje ve své oběti emocionální závislost, díky níž se snaží oběť vylákat na osobní schůzku za účelem sexuálního obtěžování či zneužívání.

Kyberšikana si tedy věk své oběti nevybírá, může být útočníkem praktikována na kohokoliv. Psychické dopady kyberšikany jsou poté obrovské a velmi těžké na jejich odstranění. [48], [54]

4.4.2 Netholismus

Jedná se o závislost na online prostředí, mezi něž patří závislost na sociálních sítích, hrách, online službách, televizi apod. Známky toho, že uživatel trpí netholismem, je silná touha například po zapnutí počítače, aniž by měl uživatel jasný cíl, co zde chce dělat, kontrola sociálních sítí, neschopnost vymezit začátek či konec aktivity na internetu, která vede k postupnému zanedbávání dalších aktivit. Závislost může být na virtuální sexualitě, závislost na počítači či telefonu, závislost na virtuálních vztazích či na hraní her apod. Typickými příznaky, že uživatel trpí netholismem jsou:

- Psychické projevy – frustrace či pocit prázdnoty, když uživatel nepoužívá své zařízení. Neklid až nervozita.
- Psychosociální projevy – ztráta dřívějších přátel, narušení vztahů s rodinou apod.
- Ztráta kontroly nad časem – brzké vstávání či ponocování pro potřebu být online.
- Pracovní potíže – uživatel vykoná méně práce, zanedbává své školní povinnosti, či zhoršující se prospěch.

Netholismus se v dnešním digitálním světě týká většiny populace. Nejvíce s touto závislostí bojují děti, senioři a osamělí jedinci produktivního věku. [48], [54]

4.4.3 Dezinformace

Dezinformace jsou známé jako lidstvo samo. Falešné zprávy patří mezi běžné informace v online prostředí. Bohužel někteří uživatelé těmto zprávám věří a berou je za legitimní informace, ovšem již bez ověření jejich pravosti. S dezinformacemi se na internetu uživatelé mohli setkat během pandemie koronaviru, kdy bylo na internetu nepřeberné množství lživých informací. Dalším fenoménem, který neunikl dezinformacím byla výstavba 5G sítí, dezinformace se šíří i ohledně lidí, kterým se v České republice zabývají bulvární plátky. Jaké jsou nejčastější typy nebezpečných a falešných zpráv? [55]

1. Fake news – jsou poplašné zprávy, které se šíří prostřednictvím uživatelům na internetu a sociálních sítí. Jedná se především o smyšlenou zprávu, kterou autor vytvoří a snaží se jí šířit online prostředím za účelem ovlivnění chování a myšlení ostatních uživatelů většinou ve svůj prospěch. Tyto zprávy často obsahují i zlomky pravdy, právě proto, aby podtrhly falešnou pravdivost celého obsahu. Fake news mohou být vytvořeny i za účelem zisku či návštěvnosti určitých stránek, kde je takovýchto zpráv velké množství. [56]
2. Hoax – je falešná zpráva, novinářská kachna, mystifikace, výmysl, kanadský žertík, poplašná zpráva či výmysl. Jedná se o poplašnou zprávu, která varuje pře smyšleným, neexistujícím nebezpečím, např. před počítačovým virem nebo chce pobavit, prosí o pomoc apod. Velmi často je zde zdůrazněno, aby uživatelé tuto opravdu skutečnou zprávu sdíleli mezi sebou a rychle ji rozšiřovali, neboť ji někdo může smazat a pravda upadne v zapomnění. Účelem těchto zpráv je vyvolat strach a paniku, poškodit nějakou instituci, firmu či značku, vystřelit si z důvěřivých uživatelů, šířit falešnou radu, zmanipulovat názory uživatelů či ohromit a přilákat pozornost. [57]

Jakým způsobem je možné dezinformaci rozpoznat? Existuje několik pravidel.

- Stačí používat rozum – pokud zpráva je bláznivá, je pravděpodobné, že to nebude pravda.
- Šokující titulek – pro utvoření celistvého obrazu, si nestačí přečíst jen titulek, je důležité si přečíst celý článek.
- Internetem může šířit informace kdokoliv za jakýmkoliv účelem, který uživatel nikdy nezná. Je proto důležité si zkusit zprávu ověřit z důvěryhodného zdroje.
- Názor vymyšleného odborníka – u některých zaručených prostředků je vždy uveden názor nějakého odborníka. V tomto případě stačí, si toto jména na internetu najít a zkontrolovat, zda se nejedná o fiktivní osobu.
- Pokud je ve zprávě příliš mnoho interpunkce a velkými písmeny výzva ke sdílení příspěvku, je velice pravděpodobné, že se bude jednat o dezinformaci. [56]

V tomto případě je dle zdrojů a průzkumu vysledováno, že nejohroženější věkovou skupinu k podlehnutí a uvěření dezinformaci, jsou lidé v seniorském věku. Tito uživatelé oplývají velkou mírou důvěřivosti a lze s nimi jednoduše manipulovat. Podle průzkumů až 40 % seniorů na internetu si pravdivost informací neověřují a dále je šíří, jako zaručeně pravdivou

informaci. Tyto dezinformace představují pro seniory riziko, protože utvářejí falešný obraz společnosti, které v mnoha případech útočí na základní principy demokracie. [58]

4.4.4 Podvodníci

Mezi další možnou hrozbu je nutné uvést podvodníky, kteří se snaží ze svých potencionálních obětí vylákat finanční prostředky. Toto se děje například pomocí nigerijských emailů, které svým obsahem uživatele lákají na velké bohatství z dědictví či uložením svých úspor. S těmito praktikami se můžeme potkat i na sociálních sítí, kdy někdo žádá finanční pomoc, vzhledem ke své tísni apod. Další hrozbou jsou nákupy od neznámých zdrojů na internetu, kdy si uživatel objedná zboží, zaplatí za něj, ale to již nikdy nedorazí. Může se také jednat o falešné charitativní akce, které vybírají finanční prostředky na postižené děti nebo na útulky zvířat. Tito podvodníci cílí na širokou veřejnost, takže je v ohrožení takřka kdokoliv, kdo přes internet nakupuje. V tomto případě je důležité si ověřit totožnost prodávajícího či organizace a zjistit si informace. [58]

4.4.5 Kyberstalking

Kyberstalking je forma nebezpečného pronásledování prostřednictvím informačních technologií v online prostředí, které se projevuje jako dlouhodobé, stupňované a opakované kontaktování oběti. Útočník chce ve své oběti vyvolat pocit strachu o své zdraví, život a soukromí. Mezi formy, které jsou u kyberstalkingu využívány můžeme zařadit:

- Obtěžující telefonáty a zasílání textových zpráv.
- Zasílání zpráv prostřednictvím messengerů a emailů.
- Krádež identity a vystupování pod jménem oběti.
- Komentování příspěvků či jejich vkládání na sociální sítě oběti.
- Kontaktování oběti pod falešnou identitou.
- Monitorování zařízení obětí prostřednictví spyware a keyloggerů.
- Zveřejňováním informací ze života oběti.
- Kontaktování rodiny či přátel oběti.

Kyberstalkingu se lze bránit ochranou svých osobních dat na internetu, zabezpečením svých sociálních sítí, užíváním silných hesel. Důležité také je dodržování bezpečného užívání internetu a uvědomění si, jaký obsah uživatel sdílí veřejně. V tomto případě se obětí může stát kterákoliv věková skupina, kdy motivem může být obtěžování či vydírání oběti, poškození oběti před společnosti či se může jednat o opětovné navázání vztahu po jeho ukončení. [59]

4.4.6 Shrnutí

Děti a dospívající mládež jsou v dnešním světě vesměs neustále online. Komunikují přes sociální sítě se svými přáteli, rodiči. Hrají různé hry, ve školách se používají počítače ve větší míře, než tomu bylo v minulosti. Dá se tedy podotknout, že děti jsou velmi ohroženou skupinou v online prostředí. Jejich malá znalost bezpečnosti, důvěřivost, zvědavost a v některých případech i strach z nich dělá snadnou kořist pro online predátory. Jaká nebezpečí na tuto skupinu na internetu číhá? U dětí se jedná především o kyberšikanu a netholismus. U kyberšikany jsou velice ohrožení kybergroomingem, kde útočník sází na jejich strach, osamění, důvěřivost a lehkou manipulaci. Senioři v naší společnosti se mohou také potýkat s kyberšikanou a netholismem, díky jejich osamělosti, a dále díky jejich důvěřivosti jsou lehce zmanipulovatelní k šíření poplašných a řetězových zpráv a v neposlední řadě mohou být zneužity podvodníky. Populace pracovně produktivního věku se mohou týkat hrozby kyberšikany, hlavně sextingu, dále kyberstalkingu, netholismu, okrajově mohou podléhat vlivu dezinformací a podvodníkům. [60]

5 BANKOVNÍ PROSTŘEDÍ

Fenoménem dnešní doby jsou mobilní telefony s přístupem k internetu a používání velkého množství aplikací. Někteří uživatelé tedy přesunuli svou aktivitu z počítačů na tablety a mobilní telefony. Každým rokem dochází k vylepšení mobilních zařízení. Integrují se baterie s dlouhou výdrží, větší a kvalitnější displeje, GPS, fotoaparáty s vysokým rozlišením, NFC čtečky či biometrie. V posledních letech se také rozmohl trh s mobilními aplikacemi, které tato vylepšení využívají. Bohužel pro uživatele, nejsou při návrhu a vývoji těchto aplikací, dodržována základní pravidla bezpečného zpracování citlivých informací, se kterými aplikace pracují. Toto způsobuje, že jejich důvěrnost, integrita či dostupnost klesá. Z tohoto plyne, že jsou mobilní aplikace potenciálními hrozbami a v některých případech i bezpečnostní rizika. Tato bezpečnostní rizika vycházejí z klasických útoků proti webovým a desktopovým aplikacím. Mezi tyto zranitelnosti můžeme zahrnout špatně zabezpečenou komunikaci klient-server, například při použití veřejné, nezabezpečené Wi-Fi sítě i mobilního hotspotu. Mezi další zranitelnosti patří lidský faktor, díky němuž může také dojít ke ztrátě našeho zařízení a tím ke ztrátě dat. Hrozbou, která může mít fatální důsledky, je samozřejmě i malware, který může být do zařízení nainstalován v podobě chtěné aplikace, otevření nedůvěryhodné aplikaci, nebo v důsledku sociálního inženýrství útočníka, jako je phishing či pharming. Mobilní aplikace mohou zpracovávat data, která poté vedou k neobvyklým útokům na vstupní body, jako je NFC, Bluetooth, fotoaparát, SMS, mikrofon, USB či QR kódy. Mezi nejzávažnější útoky na mobilní aplikace můžeme považovat ty, při kterých dochází k únikům citlivých dat, jako jsou uživatelská jména či hesla. Jelikož uživatelé v mobilních zařízeních používají i mobilní bankovnictví, je nutné, aby vývojáři, v tomto případě bankovních institucí, vyvíjeli tyto aplikace tak, aby nedocházelo k únikům dat a tím pádem, aby nedocházelo k poškození uživatele a na druhé straně k obohacení útočníka. [61]

5.1 Bankovní identita

Tato identita slouží k ověřování totožnosti uživatele v online prostředí. Nemusí se přitom jednat pouze o ověření v bankovním prostředí. Tato identita umožňuje komunikovat z domova i s úřady, či soukromými společnostmi, a to bez nutnosti vyplňovat další přihlašovací údaje. Je to vlastně digitální doklad totožnosti. Bankovní identitu tvoří uživatelské jméno. Klient si tedy místo původního klientského čísla, zvolí přihlašovací jméno, které je složené z číslic a písmen. Důležitou součástí je telefonní číslo, které musí být unikátní. Bankovní identita může být zabezpečena další aplikací, jako má k dispozici Česká spořitelna a její

aplikace George klíč. Tato mobilní aplikace nahrazuje potvrzování formou ověřovacích SMS zpráv. Potvrzování probíhá pomocí šestimístného PIN kódu také pomocí biometrických prvků. Jako je touch ID nebo Face ID. Jedná se o funkce na novějších typech mobilních telefonů iPhone, kdy dochází k ověření pomocí naskenování biometrických prvků a jejich porovnání s již naskenovaným vzorkem umístěným v databázi. Touch ID používá otiskem prstu, Face ID používá skenování obličeje. Pomocí bankovní identity je možné v mobilním bankovnictví uskutečňovat:

- Platby,
- Nastavení trvalých příkazů,
- Ověření při přihlášení do elektronického bankovnictví v PC,
- Potvrzení plateb za nákup zboží online platební kartou.
- Podepisování dokumentů v elektronickém bankovnictví,
- Odbourává nutnost osobního kontaktu s bankou,

Bankovní identita je pro bankovní sektor brána jako elektronický doklad totožnosti, což znamená, že už klient nemusí posílat kopie svých dokladů, záleží jen na něm, se kterou organizací svou bankovní identitu propojí. Pomocí bankovní identity je tedy možné, kromě bank, komunikovat také s:

- Portál občana,
- Bodový systém řidiče,
- Aplikace eRecept,
- Portály úřadů,
- Komunikace s poskytovateli energií.
- E-shopy a weby.

Jaká jsou tedy bezpečnostní pravidla a zásady při používání bankovní identity? Bankovní identita je zabezpečena stejným způsobem jako je internetové bankovnictví, což znamená, že využívá stejné technologie se stejnými bezpečnostními prvky. Nejdůležitější zásadou je opatrnost uživatele při používání mobilního bankovnictví, aby nedošlo ke krádeži citlivých dat, odcizení, ztrátě mobilního zařízení, případně svou neopatrností nenainstalovat do zařízení nebezpečnou či nedůvěryhodnou aplikaci. Pokud nebude uživatel opatrný, mohla

by být jeho bankovní identita odcizena, což by mělo fatální důsledky. Bankovní identita by se měla používat na stránkách, které jsou k tomu oprávněny. Jedná se o bankovní instituce, státní instituce a důvěryhodné soukromé společnosti, které poskytují důvěryhodné online služby. Bankovní identita tedy řeší jeden z velkých problémů, na který v kybernetickém světě můžeme narazit, a tím je vylákání přihlašovací údajů útočníkem od oběti. Dříve se tedy dalo do elektronického bankovnictví přihlásit pomocí, většinou přiděleného klientského čísla a hesla, které si uživatel sám zvolí. Tyto údaje bylo možné od oběti vylákat pomocí sociálního inženýrství, a to buď pomocí phishingu či pharmingu. Phishing je metoda, kdy útočník zašle oběti emailovou zprávu, která vypadá tak, že je odeslána z banky a naléhá na uživatele, aby se přihlásil do svého elektronického bankovnictví a zadali své přihlašovací údaje. Oběť většinou zpanikaří a zadá své přihlašovací údaje, což vede k poskytnutí těchto údajů útočníkovi. Oproti tomu pharming, je metoda, která napadá překlad DNS a při pokusu o vstup na stránku svého internetového bankovnictví, je oběť útoku přesměrována na podvrhnutou stránku útočníkem. Většinou nic netušící klient zadá své přihlašovací údaje, které má poté k dispozici útočník. Bankovní instituce poté zavedly ověřování pomocí SMS zpráv. To mělo zamezit možnost přihlášení útočníka do cizího elektronického bankovnictví, neboť bylo potřeba, svůj přístup dále ověřit pomocí vygenerované SMS zprávy, která byla doručena klientovi. Bohužel i v těchto případech je možné tuto SMS zprávu odcizit, a to buď pomocí malware, který sbírá data ze zařízení oběti, případně pomocí špionážního software – spyware, který je určen k tomu, aby sbíral uživatelská jména, hesla a ověření. Některé banky také přišly s ověřením pomocí bezpečnostních obrázků, ale jednalo se spíše o doplňkové ověření. S nástupem bankovní identity tedy začíná období vyššího zabezpečení internetového bankovnictví v mobilních zařízeních. [62], [63]

5.2 Porovnání aplikací mobilního bankovnictví

V porovnání byly zvoleny bankovní instituce, dle jejich používání. Budeme porovnávat mobilní aplikace z pohledu bezpečnosti při použití na operačním systému iOS, pro mobilní telefony iPhone. Zanalyzujeme jejich přihlašovací možnosti do aplikace, bezpečnostní ověření plateb, platba online platební kartou na internetu a jaké funkcionality nabízejí.

5.2.1 Česká spořitelna

Česká spořitelna vyvinula pro své klienty mobilní, bankovní aplikaci George. Tato aplikace umožňuje svým klientům bezpečně a pohodlně spravovat své finance přímo z mobilního

telefonu. Je dostupná zdarma v české, slovenské, anglické, německé a rumunské verzi. V mobilním telefonu s OS Android se jazyk nastavuje ručně, oproti tomu ve verzi iOS se nastavení jazyka aplikace řídí dle nastavení jazyka v telefonu. Pro použití aplikace George, je potřeba zřízení bankovní identity, chytrý telefon s aktualizovaným operačním systémem a možností připojení k internetu. Pro možnost vyšší bezpečnosti, Česká spořitelna vyvinula další aplikaci George klíč. Aby mohla být tato aplikace využita, je nutné mít obě tyto aplikace nainstalované na stejném zařízením. Pro první přihlášení je nutné uživatelské jméno a heslo, poté si klient vybere, jakou bezpečnostní metodou se chce přihlašovat. Na výběr jsou Otisk prstu (OS telefonu převezme otisk prstu, který je uložen pro odemčení mobilního zařízení), dalšími možnostmi ověření je PIN či gesto. Pro další přihlášení se již klient přihlásí dle zvolené metody. Tato aplikace uživatelům dále přináší:

- Slevový program Moneyback,
- Možnost uložení účtenek přímo k platbě,
- Upozornění na budoucí výdaje,
- George klíč,
- Automatické třídění plateb,
- Bezpečné nastavení.

Pro vyšší bezpečnost je dobré si do mobilního zařízení nainstalovat společně s mobilní aplikací George i George klíč. Díky této aplikaci klienti potvrzují své platby bezpečněji a jednodušeji. Aplikace funguje tak, že když uživatel ve svém mobilním bankovnictví zadá platbu, potvrzení této platby poté probíhá pomocí aplikace George klíč. Odpadá tedy nutnost přepisování kódů z SMS zprávy. Po zadání platby se zobrazí na telefonu oznámení pro potvrzení v aplikaci George klíč. Uživatel otevře aplikaci a potvrdí platbu tím, že zadá svůj šestimístný dodatečný PIN kód. Poté je platba odeslána. V aplikaci je možné také potvrzení plateb pomocí otisku prstu, a to v případě, že se jedná o důvěryhodné platby. Jedná se o platby, které jsou určeny příjemcům, kterým jsou platby často zasílány, či pokud se jedná o platbu nižší částky. Velkou výhodou je, že při potvrzování plateb, není nutné mít mobilní zařízení připojeno k internetu či k mobilní síti operátora. Velkou novinkou je zprovoznění potvrzení plateb kartou v e-shopech v aplikaci George klíč. Tato novinka vychází ze změny, která byla prosazena Evropskou Unií, která schválila vyšší zabezpečení plateb

po internetu dalším bezpečnostním faktorem. Česká spořitelna k tomu tedy využila svou aplikaci George klíče. Mezi další funkcionality této potvrzovací aplikace patří:

- Aplikace hlídá PIN ke kartě a její možné zneužití,
- Volání do klientského centra,
- Schválení platby až do výše 10 milionu,
- Aplikace může být na více zařízeních,
- Bezpečnostní prvek pro přihlášení do elektronického bankovnictví v PC.

Stejně jako u ostatních aplikací, i zde platí bezpečnostní desatero a jelikož se jedná o bankovnictví, platí zde tyto pravidla o to více.

1. Vždy je tedy nutné aplikaci stahovat jen z oficiálních obchodů.
2. Zvolit si bezpečný PIN pro přístup do aplikace.
3. Při použití biometrie, je nutné ověřit, že jsou na řízení uloženy pouze jeho otisky prstů.
4. Nepřipojovat se na žádných free Wi-Fi sítích.
5. Nainstalovat si aplikaci pouze do zařízení, které využívá klient.
6. Důležité je používat unikátní PIN pro přístup do aplikace než pro ostatní aplikace či zařízení.
7. Nepotvrzovat transakce, které sám uživatel nevytvořil.
8. Pravidelná aktualizace operačního systému, aplikace mobilní banky a případně nainstalovat antivirový program.
9. Při ztrátě zařízení si zvolit možnost vyhledání, zamknutí, případně z něj vzdáleně vymazat dat, pokud má klient tuto možnost.

V případě podezření na zneužití, by se měl klient obrátit na svou banku. [64], [65], [66]

5.2.2 Komerční banka

Komerční banka nabízí aplikaci Mobilní banka. Tato aplikace nabízí svým klientů vyhledávání nejbližší pobočky či bankomatu, simulaci spotřebitelských úvěrů a hypoték, kalkulačku penzijního připojištění, zablokování platební karty, rychlé zadání platby, zobrazení

transakční historie, platba pomocí QR kódu a mnoho dalšího. Pro provozování bankovní aplikace Mobilní banka, je nutné si nejprve zvolit způsob přihlášení:

- Bezpečnostní heslo – jedná se o klasické přihlášení pomocí hesla, které si uživatel sám zvolí. Tento způsob je doporučován klientům s tlačítkovými telefony. V tomto případě se používá v kombinaci bezpečnostních SMS kódů. Tedy stále nižší stupeň zabezpečení.
- Certifikát na čipové kartě – tento způsob bohužel není možný pro využití v mobilním bankovnictví, jelikož je nutné mít čtečku čipových karet a počítač s OS Windows.
- KB Klíč – jedná se o moderní metodu přihlašování do mobilní aplikace internetového bankovnictví Komerční banky.

KB Klíč se nastavuje tím způsobem, že si uživatel nastaví uživatelské jméno a šestimístný PIN kód, s kterým se potom uživatel bude přihlašovat do všech aplikací Komerční banky. Stejně tak, jako u České spořitelny, tak i u aplikace Komerční banky je možné si nastavit místo šestimístného PINu, otisk prstu či sken obličeje. Tímto klíčem je možné také provádět autorizaci platebních příkazů, provádění změn a podepisování dokumentů. Tato aplikace také funguje bez připojení k internetu. Od ledna 2021 zprovoznila Komerční banka potvrzení plateb na internetu pomocí aplikace KB Klíč. Ve své podstatě jsou KB Klíč a George klíč podobné aplikace. V obou těchto aplikacích se potvrzují platby, které uživatel provede na internetu, aplikace tedy nahrazuje potvrzení platby v podobě SMS kódu. Při platbách velmi nízkých částek či pokud je uživatel v e-shopu přihlášen, nemusí být potvrzování platby kartou na internetu vyžadováno. [67], [68]

KB Klíč se musí používat společně s aplikací pro Mobilní banku. Nejbezpečnějším způsobem použití této aplikace je nastavení si ověření pomocí biometrie, jako je Touch ID a Face ID, v případě, že telefon uživatele tuto možnost nemá, je možné se do aplikace přihlásit pomocí uživatelského jména a hesla. Tento způsob přihlášení do bankovnictví není již považován za nejbezpečnější způsob přihlášení, neboť zde není potřeba dvou faktorového ověření, např. jako je potvrzení pomocí SMS kódu. V případě napadení zařízení s touto aplikací a úniku citlivých údajů pro bankovnictví, by měl útočník plný přístup do mobilního bankovnictví oběti. Aktivaci Mobilní banky je nutné provést pomocí internetového bankovnictví v počítači, kdy je nutné aplikaci spárovat s elektronickým bankovnictvím. Velkým plusem je ale možnost zvolení si mezi aktivním a pasivním nastavením mobilní aplikace. Aktivní nastavení nabízí uživateli plně funkční bankovní aplikaci, kdy je možné provádět platby,

dostávat náhledy transakcí a další, pasivní nastavení slouží pouze jako náhled. V tomto režimu není možné z Mobilní banky platit a ani provádět další aktivity. Pro zprovoznění aplikace je nutné vše podepsat bezpečnostním prvkem, který má uživatel nastaven. Tedy buď pomocí KB Klíče či za pomoci bezpečnostního hesla. [69]

Komerční banka dále nabízí svým klientů službu ochrana Trusteer Rapport. Jedná se o nástroj na ochranu proti specifickým hrozbám, jako jsou podvržené škodlivé stránky (phishing), škodlivého malware a na zamezení pokusů o zjištění hesel pomocí nástroje keylogger. Trusteer Rapport používají uživatelé i dalších bank, jako je např. Bank of America, ING či Societé Générale. Nástroj vytváří bezpečný tunel mezi uživatelským zařízením a stránkou, na kterou se uživatel přihlašuje, analyzuje chování uživatele a stránky a případně upozorní, pokud zjistí, že je stránka podvrhnutá. [70]

5.2.3 AirBank

Banka Air Bank, nabízí svým klientům aplikaci My Air. Přes aplikaci je možné založení účtu, možnost povolení či zakázání některých funkcí, provádění plateb, přihlášení pomocí biometrie, odměny za placení kartou, oznámení o zůstatku, QR platby, a jiné. Jedinečnost této aplikace spočívá v tom, že uživatel používá pouze jednu aplikaci oproti již zmíněným aplikacím. Přes aplikaci je možné si sjednat pojištění, ukázat účty od jiných bank, a další. Při platbách se používá bezpečnostní klíč či otisk prstu, který musí být stejný jako ten, se kterým uživatel otevírá samotnou aplikaci. I v případě této mobilní aplikace, je nutno pro zprovoznění propojit účet s aplikací. Spárování je možné pomocí elektronického bankovnictví v PC. Proces je podobný, jako má Komerční banka. Uživatel si zvolí název zařízení, ve kterém má aplikaci nainstalovanou. Internetová aplikace vygeneruje registrační kód, který se poté zadá přímo v mobilní aplikaci, případně je možné vyfotit tento kód aplikaci pomocí QR čtečky. Posledním důležitým krokem, je vytvoření si bezpečného hesla. Toto heslo slouží nejen pro přihlášení, ale i pro potvrzení plateb, které jsou prostřednictvím mobilní aplikace vytvořeny. V mobilní aplikace je možné také spárovat svou kartu s aplikací Apple Pay (Google Pay). Jedná se o virtualizaci platební karty, která je v podobě tokenu naskenována v telefonu a plně nahrazuje placení platební kartou. Výhodou tohoto placení oproti placení běžnou (plastovou kartou), je virtuální token, který je při každé platbě unikátní a není tedy možné jej zneužít obchodníkem (možným útočníkem). Tuto funkcionalitu nabízejí i výše zmíněné banky. [71], [72]

Aplikace My Air je pevně svázána s mobilním zařízením uživatele. Bez této aplikace, není možné se do bankovnictví dostat. Při ztrátě zařízení je možné aplikaci od účtu odpojit a připojit k jinému zařízení. Funkcionalita bezpečný klíč uživatele přihlásí do internetového bankovnictví v PC pomocí vyfocení QR kódu. Jedná se o nejbezpečnější možnost přihlášení se do internetového bankovnictví na trhu. Pomocí bezpečnostního klíče se provádí i potvrzování plateb v internetovém bankovnictví. Stejný způsob je využit i pro potvrzení plateb na internetu. Po zaplacení již uživatel nečeká na potvrzovací SMS zprávu, ale otevře aplikaci My Air a v ní platbu potvrdí. Další výhodou je potvrzení identity volajícího v mobilní aplikaci při kontaktování bankovní instituce. Uživatel již nemusí odpovídat na bezpečnostní otázky, na místo toho potvrdí kód v aplikaci, a tímto způsobem je klient ověřen. Air Bank také nabízí možnost používat aplikaci pasivním způsobem, tedy pro kontrolu zůstatků a k potvrzování plateb. [73]

5.3 Porovnání bezpečnosti mobilních aplikací

Při porovnání a detailní analýze společnosti Scott & Rose, vyšly jako nejlepší mobilní aplikace bankovních institucí Air Bank s aplikací My Air, Komerční banka s aplikací Mobilní banka a jako třetí Moneta Money Bank s aplikací Smart Banka. S těchto tří bankovních aplikací, byla jako nejlepší vybrána aplikace Mobilní banka od Komerční banky.

Z hlediska bezpečnosti je nejdůležitějším faktorem analýza bezpečnosti mobilního bankovnictví. Jelikož se uživatelé přesouvají do prostředí mobilních zařízení, je jasné, že se na toto prostředí více zaměřují i útočníci. Proto i v poslední době přibývá více útoků na tyto platformy. Při analýze bylo zkoumáno 8 základních, hodnotících parametrů, které souvisí s bezpečností, každopádně se nedá konstatovat, že banka, která má parametrů méně, je méně bezpečná. Banky implementují nejčastěji přihlášení pomocí PINu či biometrie, specializované nástroje, které zajišťují ochranu proti malware či jiným hrozbám. Komerční banka, jako první banka začala svým klientům poskytovat bezpečnostní ochranu Trusteer Mobile, kterou implementoval do své aplikace již v roce 2016. Banka využívá tým penetračních testerů, kteří ověřují zranitelnosti aplikace, kteří i při testech deaktivují ochranu aplikace, aby bylo možné do aplikace proniknout a vyzkoušet další testy. Velice zajímavou funkcionalitu nasadila do aplikace Raiffeissen Bank a Moneta Money Bank, kteří nabízejí možnost skrytí citlivých dat. Z pohledu bezpečnosti a zkoumání osmi bezpečnostních prvků, nejhůře dopadla Sberbank, která obsahuje pouze jeden bezpečnostní prvek. Na opačné straně žebříčku se

umístila aplikace Raiffeissen Bank, která obsahuje sedm z osmi bezpečnostních faktorů. Následuje ji Air Bank, která má šest z osmi.

Pro zajímavost zde uvedu pořadí, mnou zkoumaných bankovních aplikací, dle analýzy firmy Scott & Rose:

1. Raiffeissen Bank 7 z 8,
2. Air Bank – 6 z 8,
3. Komerční banka – 6 z 8,
4. Česká spořitelna – 5 z 8,
5. mBank – 5 z 8. [74]

6 PRÁVNÍ ASPEKTY KYBERNETICKÉ BEZPEČNOSTI

Legislativa kybernetické bezpečnosti se opírá o:

1. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů, č. 181/2014 Sb.
2. Směrnice Evropského parlamentu a Rady Evropské Unie 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Směrnice NIS).
3. Vyhláška o kybernetické bezpečnosti.
4. Vyhláška o významných informačních systémech a jejich určujících kritériích, č. 317/2014 Sb.
5. Nařízení vlády o kritériích pro určení prvku kritické infrastruktury, č. 432/2010 Sb.
6. Vyhláška o kritériích pro určení provozovatele základní služby, č. 437/2017 Sb.
7. Vyhláška o některých požadavcích pro zápis do katalogu cloud computingu č. 316/2021 Sb.
8. Vyhláška o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci, č. 315/2021 Sb.

6.1 Zákon o kybernetické bezpečnosti

Vstoupil v platnost dne 29. srpna 2014, s účinností dne 1. ledna 2015. Tento zákon upravuje práva a povinnosti osob, pravomoc působnost orgánů veřejné moci v oblasti kybernetické bezpečnosti. Zákon zpracovává příslušné předpisy Evropské Unie a dále upravuje zajišťování bezpečnosti elektronických komunikací a informačních systémů. Cíle zákona jsou:

- Určit základní stupeň bezpečnostních opatření.
- Zdokonalit detekci bezpečnostních incidentů.
- Zahájit hlášení o bezpečnostních incidentech.
- Inovovat systém opatření na bezpečnostní incidenty.
- Uspořádat provoz dohledových pracovišť.

Poslední novelizace tohoto zákona vznikla vešla v účinnost dne 1. září 2021.

6.2 Směrnice Evropského parlamentu a Rady EU

Směrnice NIS má za cíl synchronizovat právní úpravu členských států Evropské Unie v oblasti bezpečnosti sítí a informačních systémů. Dále má směrnice za cíl nastolit jednotný standard úrovně kybernetické bezpečnosti pro zlepšení funkcionalit trhu uvnitř EU. Určité

povinnosti, které směrnice NIS ukládá, jsou v České republice již řešeny v rámci zákona o kybernetické bezpečnosti, a jeho prováděcími předpisy. Ve směrnici NIS je také řešeno rozšíření subjektů, které budou mít stanoveny povinnosti v oblasti ochrany a prevence v případě kybernetických, bezpečnostních incidentů. Jedná se zejména o provozovatele základní služby a poskytovatele digitálních služeb, čímž se rozumí poskytovatelé internetových vyhledávačů, cloud computingu a online tržišti. Tyto požadavky, které směrnice NIS vyžaduje, je uveden v novele zákona o kybernetické bezpečnosti č. 205/2017 Sb., která vešla v účinnost dne 1. srpna 2017.

6.3 Vyhláška o kybernetické bezpečnosti

Jedná se o již zmíněnou vyhlášku, která zpracovává Směrnici NIS a dále upravuje:

- Obsah a strukturu bezpečnostní dokumentace.
- Obsah a rozsah bezpečnostních opatření.
- Kategorie, typy a hodnocení důležitosti bezpečnostních incidentů.
- Náležitosti a formu oznámení bezpečnostního incidentu.
- Náležitosti zprávy o provedení proti opatření a jeho výsledku.
- Předlohu oznámení kontaktních údajů a jeho formu.
- Postup při likvidaci provozních údajů, dat, informací a jejich kopií.

Nová verze vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb., byla zveřejněna ve Sbírce zákonů, která nese označení *Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.*

6.4 Vyhláška č. 317/2014 Sb.

Tato vyhláško o významných informačních systémech a jejich určujících kritériích byla přijata dne 19. prosince 2014. Vyhláška stanuje významné informační systémy a kritéria pro jejich určení. Pro lepší určení, zda je daný informační systém významný, vešla v roce 2020 v platnost novela této vyhlášky. Kompletní vyhláška vejde v platnost 1. ledna 2023, přičemž nabytí účinnosti je rozděleno do tří fází.

6.5 Nařízení č. 432/2010 Sb.

Toto nařízení se zabývá aspekty o kritériích pro určení prvku kritické infrastruktury, které je platné od 30. prosince 2010. Toto nařízení definuje kritéria pro správné určení prvku kritické infrastruktury, přičemž v příloze je definováno 9 odvětví, včetně jednotlivých kritérií, které určují prvek kritické infrastruktury.

6.6 Vyhláška č. 437/2017 Sb.

Tato vyhláška zpracovává kritéria pro určení provozovatele základní služby. Tuto vyhlášku zpracoval Národní úřad pro kybernetickou a informační bezpečnost, která vznikla díky přispění odborné veřejnosti. Ve vyhlášce jsou zpracovávány požadavky Směrnice NIS Evropského parlamentu a Rady EU 2016/1148 ze dne 6. července 2016, která se věnuje opatření k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Evropské Unii. Vyhláška se zabývá úpravou odvětvových a dopadových kritérií, která mají za úkol určit provozovatele základní služby a vymezit významnost dopadu narušení základní služby na zabezpečení společenských nebo ekonomických činností podle § 22a odst. 1 zákona o kybernetické bezpečnosti. Tato vyhláška nabyla účinnosti 1. února 2018, přičemž dne 1. ledna 2021 došlo k účinnosti nového znění vyhlášky, které mění dvě stávající kritéria v odvětví zdravotnictví a doplňuje o další dvě nová kritéria.

6.7 Vyhláška č. 316/2021 Sb.

Tato vyhláška, která vstoupila v platnost 1. září 2021 se zabývá požadavky pro zápis do katalogu cloudu computingu. Vyhláška stanovuje vybraný soubor vstupních kritérií pro zápis poskytovatelů služeb cloud computingu do katalogu cloud computingu, který je veden Ministerstvem vnitra České republiky. Vstupní kritéria jsou rozdělena vzestupně do čtyř bezpečnostních úrovní.

6.8 Vyhláška č. 315/2021 Sb.

Tato vyhláška se zabývá bezpečnostními úrovněmi pro využívání cloud computingu orgány veřejné moci a vešla v platnost dne 1. září 2021, na základě zmocnění dle § 28 odst. 2 písm. a) zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Tato vyhláška vnáší přehledný a jednoduchý právní rámec, díky němuž orgány veřejné mocí, budou moci provádět ohodnocení významnosti informačního či komunikačního systému, který chce provozovat prostřednictvím služeb cloud computingu. [74]

II. PRAKTICKÁ ČÁST

7 DOTAZNÍK

Cílem této kapitoly bylo vytvořit dotazník, ve kterém respondenti anonymně odpovídali na otázky týkající se internetového prostředí, jejich pohybu po síti a otázek, jejichž účelem bylo vyzkoumat podvědomí o bezpečném pohybu na internetu. Součástí dotazníku byly praktické otázky, jak se respondent zachová v okamžiku, kdy mu je doručen určitý typ emailu a závěrem byl krátký vědomostní kvíz.

7.1 Skladba dotazníku

V první části dotazníku byly respondentům pokládány běžné sociální otázky zaměřené na věk, pohlaví, nejvyšší dosažené vzdělání, pracovní status a zaměření.

Druhá část dotazníku zkoumá, co uživatelé nejčastěji na internetu dělají, zdali používají antivirový program, zdali stahují software a odkud.

Třetí část se zaměřuje na bankovnictví. Respondenti byli dotazováni, zda využívají mobilní či internetové bankovnictví, zdali používají platební kartu a v jaké formě a zda čtou upozornění, které jim banky zasílají.

Další, čtvrtá část se zaměřuje na sdílení přihlašovacích údajů, případně s kým respondenti své údaje sdílí. Jaké zabezpečení uživatelé nejčastěji používají.

Pátá část dotazníku se zaměřuje na obezřetnost uživatelů ve chvíli, kdy je jim doručen email a zkoumá, jak se respondenti zachovají v případě doručení emailů, nebo při jaké příležitosti budou respondenti sdílet svá data, s kým a jaký typ dat.

V závěrečné části, respondenti vyplňovali kvízové otázky týkající se sociálního inženýrství a hrozeb na internetu.

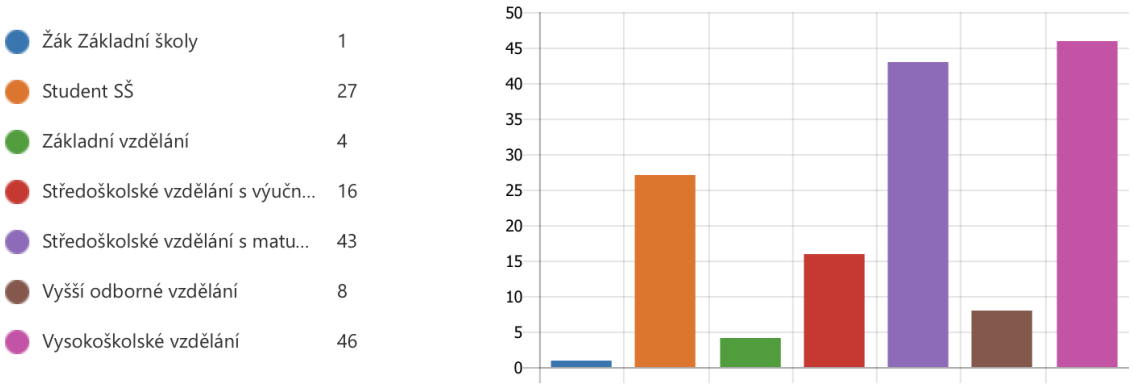
7.2 Respondenti

Na základě dotazníků bylo osloveno zhruba 300 dotazovaných, z čehož dotazník vyplnilo přibližně 50 %. Někteří z dotazovaných se nejprve ujišťovali, že se jedná o skutečnou, legitimní zprávu s odkazem, z čehož vyplývá, že toto nepatrné procento respondentů je velmi obezřetných a nedůvěřivých i vůči důvěryhodným zdrojům. Někteří respondenti dotazník nevyplnili vzhledem k nedostatku svých časových možností.

7.2.1 Diverzita respondentů

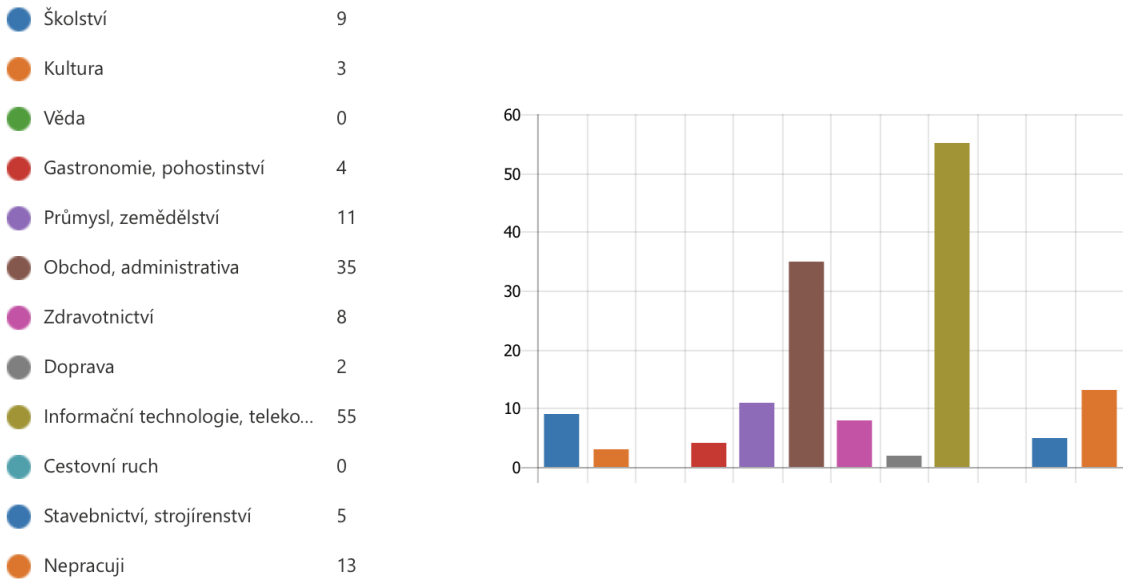
Aby byla zachována určitá diverzita, na začátku dotazníku byly definovány obecné otázky, které se týkaly těchto oblastí:

- Věk dotazovaných byl rozvržen do tří skupin. Mladiství do 20 let, dospělá, produktivní populace 20–49 let a populace nad 49, což čítalo většinou populaci s dětmi. Celkově 64 % dotazovaných spadalo do skupiny 20-49 let, 23 % bylo ve věku do 20 let a 13 % ve věku nad 49 let.
- Pohlaví respondentů bylo rozděleno do tří skupin. Žena s procentuálním podílem 52 %, muž s podílem 47 % a jiné s podílem 1 %.
- Nejvyšší dosažené vzdělání bylo respondenty označeno následovně: 46 respondentů má vysokoškolské vzdělání, 41 respondentů středoškolské vzdělání zakončené maturitní zkouškou, 27 respondentů jsou studenti střední školy.



Obrázek 6. Nejvyšší dosažené vzdělání respondentů [zdroj dotazník]

- Pracovní status dle dotazníku byl v rozložení: 57 % respondentů jsou zaměstnanci, 23 % respondentů má status studenta, 16 % respondentů jsou podnikatelé, 2 % respondentů jsou v důchodu a nezaměstnaní jsou obsaženi také ve 2 %.
- U pracovního zaměření byla skladba respondentů v rozložení: Informační technologie a telekomunikace 38 %, Obchod a administrativa 24 %, 9 % respondentů uvedlo, že nepracuje, 7 % pracuje Průmyslu a zemědělství, 6 % pracuje ve Školství. Dále zde byla v menší míře zastoupena Kultura, Gastronomie a pohostinství, Zdravotnictví, Doprava a Stavebnictví.

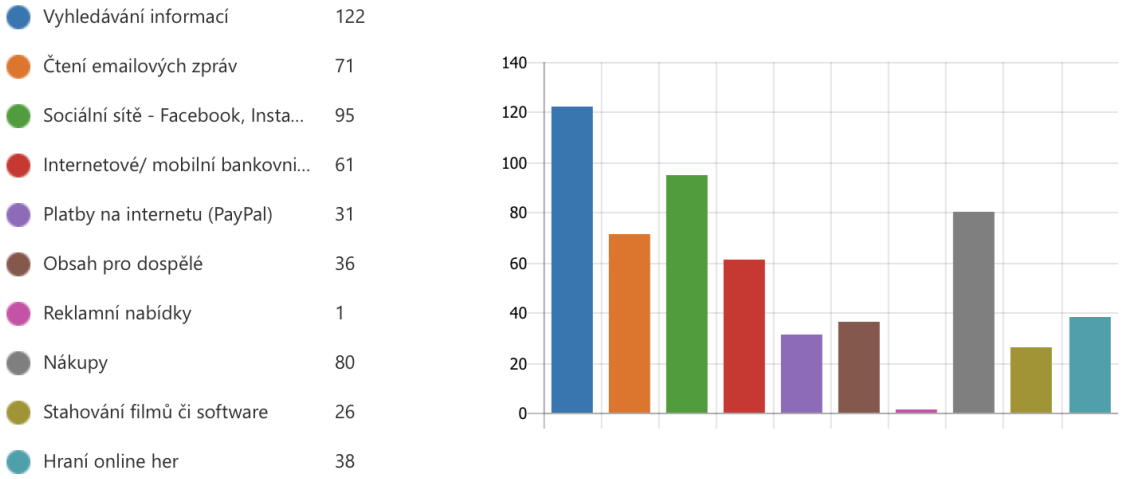


Obrázek 7. Rozložení pracovního zaměření respondentů [zdroj dotazník]

7.2.2 Průzkum pohybu a bezpečnost respondentů v digitálním prostředí

Na otázku, která se zabývala zjištěním, co uživatelé nejčastěji na internetu dělají bylo odpovězeno nejčastěji takto:

Většina respondentů, 84 % na internetu vyhledávají informace. 65 % respondentů se věnuje sociálním sítím, jako je Facebook, Instagram apod. Jako třetí nejčastější odpověď respondenti uváděli Nákupy v procentuálním zastoupení 54 %. V závěsu bylo čtení emailových zpráv, internetové a mobilní bankovnictví a hraní online her.



Obrázek 8. Nejčastější činnost respondentů na internetu [zdroj dotazník]

Z dotazníku také vyplynulo, že 68 % dotázaných používá na svém zařízení antivirový program. Mezi nejčastěji používanými byly:

- Avast – 28 %,
- Windows Defender – 13 %,
- ESET – 7 %,
- AVG – 5,5 %,
- V menším měřítku zde byl zastoupen Symantec, Kaspersky, NOD32 či Spybot,
- A 8 % respondentů neznalo název antivirového programu, který používá.

Při otázce, zda respondenti používají antivirový program i v mobilním zařízení, odpovědělo 33 % respondentů, kteří jej používají i v počítači, že ano. Ve skupině uživatelů, kteří nemají zabezpečený svůj počítač, 3 % mají antivirový program alespoň v mobilním zařízení.

Respondenti byli také dotazováni, zdali a jak do svého zařízení stahují software.

- 55 % dotázaných, stahuje software do svého zařízení z oficiálních internetových stránek vydavatele.
- 20 % stahuje z úložišť typu uložto.
- A 7 % stahuje prostřednictvím BitTorrentu.
- Zbývajících 17 % dotázaných software nestahuje.

Dle další otázky za software platí pouze 31 % respondentů, 36 % využívá pouze free verze a 16 % dotazovaných přiznalo, že nelegálně stahuje software i jejich licence. U otázky, zda respondenti stahují filmy a z jakých zdrojů, byly odpovědi v tomto rozložení:

- Ano, z legitimních webů, kde za stažení platím – 32 %.
- Ano, z BitTorrentu – 8 %.
- Ne, filmy sleduji online – 37 %.
- Ne – 23 %.

7.2.3 Průzkum využívání bankovních služeb

U respondentů bylo zjišťováno, zda vlastní bankovní účet. Ze všech dotázaných, 97 % respondentů bankovní účet vlastní a z toho 95 % využívá služby internetového či mobilního bankovnictví. Co týká otázky ohledně využívání platební karty, respondenti odpověděli následovně:

- 77 % uvedlo, že platební kartu používá často,
- 8 % využívá platební kartu, jednou týdně,
- 12 % používá k platbám spíše hotovost,
- 3 % bankovní kartu nevlastní.

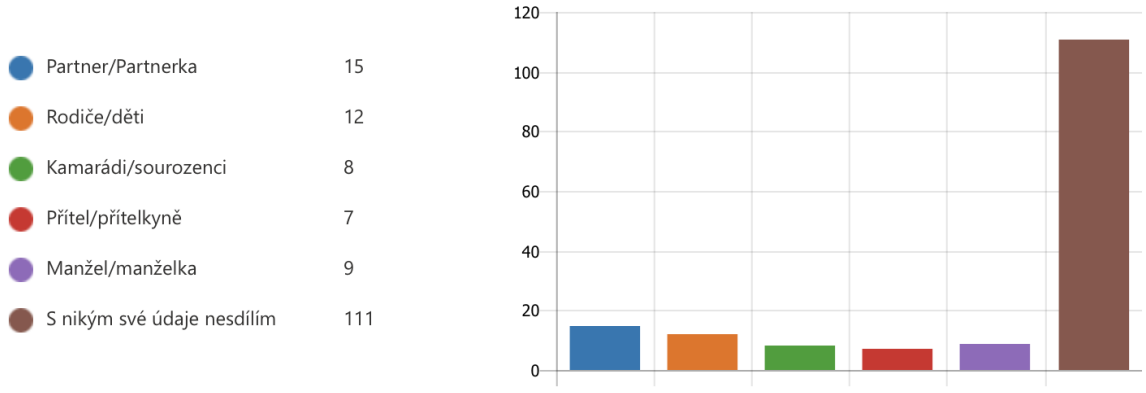
Při otázce, zda respondenti využívají platební kartu bezkontaktně, prostřednictvím mobilního telefonu pomocí ApplePay, GooglePay či GarminPay, 64 % respondentů odpovědělo, že tuto službu využívá.

Další otázka se týkala informace, zda uživatelé čtou upozornění z bank, které jsou uživatelům zobrazovány ve formě zpráv v internetovém bankovnictví. 27 % respondentů uvedlo, že tyto zprávy nečte.

7.2.4 Sdílení přihlašovacích údajů a zabezpečení účtů

Dotazníkový průzkum této části byl zahájen otázkou: „Sdílíte s někým Vaše přihlašovací údaje?“ 80 % respondentů své údaje nesdílí, oproti 20 % uživatelů, kteří své údaje sdílí. Další otázka měla za úkol zjistit, s kým respondenti své přihlašovací údaje sdílí. Z respondentů, kteří uvedli, že své údaje sdílí, bylo pořadí, s kým následující:

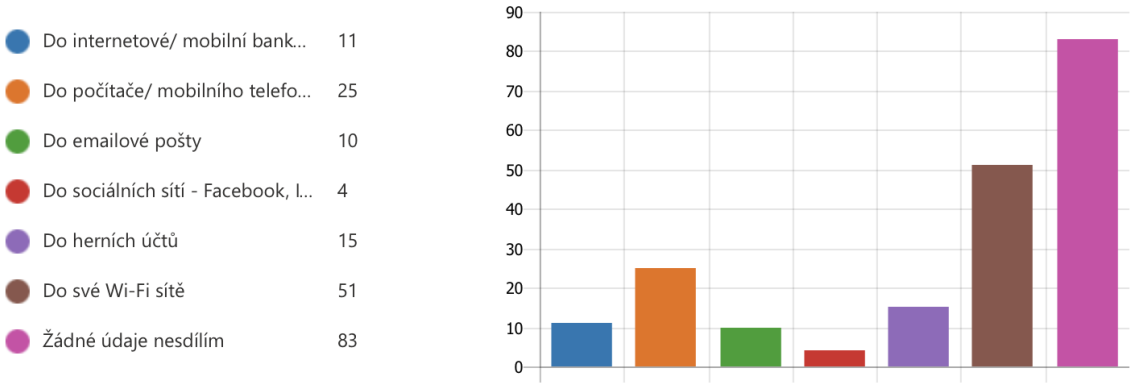
- Partner/partnerka s podílem 30 %,
- Rodiče/děti s podílem 24 %,
- Kamarádi/sourozenci 16 %,
- Manžel/manželka 16 %,
- Přítel/přítelkyně 14 %.



Obrázek 9. S kým respondenti sdílí své přihlašovací údaje [zdroj dotazník]

Při otázce „Jaké přihlašovací údaje sdílíte?“, respondenti nejčastěji odpověděli, že své přihlašovací údaje nesdílí. Ti, jenž své údaje sdílí, odpovídali následovně:

- Do své Wi-Fi sítě sdílí 44 %,
- Do svého zařízení – počítač či mobilní telefon 21 %,
- Do herních účtů 13 %,
- Do internetového či mobilního bankovnictví 10 %,
- Do emailového účtu 8 %,
- Do svých sociálních účtů 4 %.



Obrázek 10. Kam respondenti sdílí své přihlašovací údaje [zdroj dotazník]

Další sada otázek se týkala bezpečnosti hesel. Tedy jakým způsobem mají respondenti zabezpečené své účty, zda duplikují stejná hesla, používají dvou faktorové zabezpečení, generátor hesel apod.

Na otázku, zda respondenti používají stejná hesla, byla nejčastější odpověď „Ano, používám kombinaci více hesel.“ Tuto odpověď označilo 62 % dotázaných. 15 % dotázaných uvedlo, že používá výhradně jiná hesla do každého účtu. U 15 % respondentů byla odpověď, že zřídka mají stejná hesla a 8 % uživatelů používá výhradně stejné heslo.

Odpovědi na otázku, zda respondenti používají dvou faktorového zabezpečení, měla následující výsledek:

- 70 % respondentů používá dvou faktorové zabezpečení běžně.
- 15 % respondentů toto zabezpečení nepoužívá.
- A 15 % dotazovaných neví, co dvou faktorové zabezpečení znamená.

Při dotazování, jakou délku znaků hesla respondentů obsahují byly odpovědi velmi uspokojivé. Nejběžnější délka hesel u dotazovaných byla 8-11 znaků, a to u 67 %. Doporučenou délku hesla, tedy 12 a více znaků, používá 28 % respondentů a 5 % respondentů mají své účty zabezpečeny hesly o délce 4–7 znaků.

Co se týká zastoupení abecedy, čísel a speciálních znaků, odpovídali respondenti takto:

- 54 % dotazovaných používá při sestavování hesla malá, velká písmena, číslice i speciální znaky.
- 43 % používá malá, velká písmena a číslice.
- A pouze 4 % dotazovaných využívá jen malá, velká písmena.

Přičemž 70 % respondentů odpovídalo, že používají password managera a 38 % z nich, používá i generátor hesel. Generátor hesel používají i respondenti, kteří password managera nepoužívají, jejich zastoupení je s podílem 6 %.

7.2.5 Obezřetnost uživatelů u emailových zpráv

Tato sada otázek v dotazníku, testovala chování respondentů, při doručování emailových zpráv. Jakým způsobem se zachovají, jaké emaily otevírají, zda si ověřují důvěryhodné zdroje odesílatelů, anebo bez váhání otevřou jakýkoliv email, a tím se vystavují potenciálnímu riziku.

První otázka v této sadě zkoumala, zdali respondenti otevírají emaily ze spamového filtru ve své emailové schránce. Zde byla odpověď celkem jednoznačná, 86 % uvedlo, že je neotvírají, 10 % email otevřou pouze, pokud je předmět zprávy zajímavý, 3 % otevřou takový email omylem a pouze jeden dotázaný tyto emaily otevírá vždy.

Obdobná otázka se týkala otevírání zpráv ze složky hromadné či jiné v emailových schránkách. Kdy 50 % respondentů email otevřou, pokud je předmět zprávy zajímavý, 41 % dotazovaných tyto zprávy neotvírají, 5 % email otevře vždy a 4 % email otevře pouze omylem.

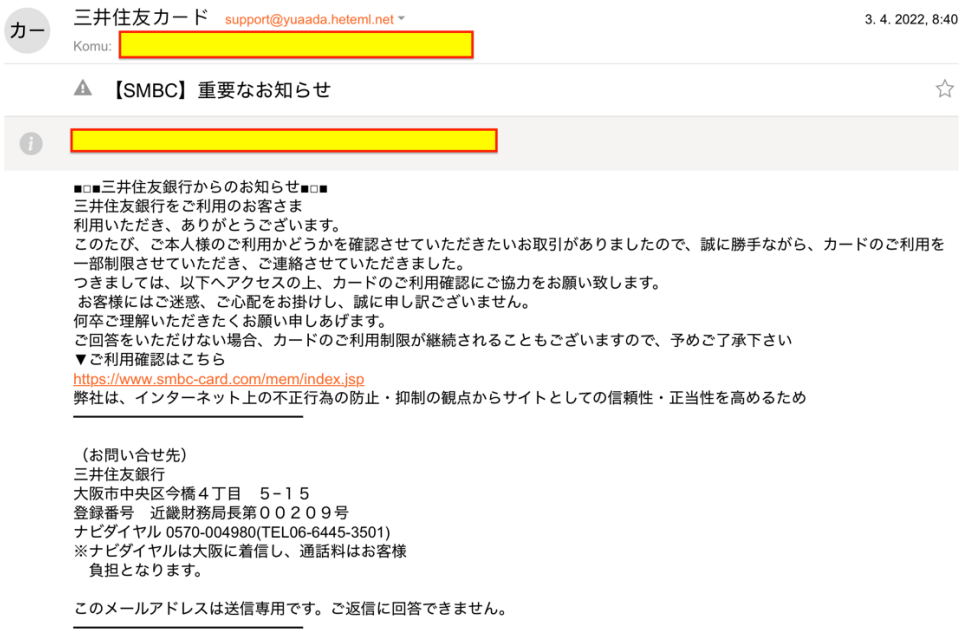
Další otázka měla za úkol zjistit, zda dotazovaní otevírají přílohy v emailu i od neznámých uživatelů. Odpovědi byly následující:

- Ano, vždy – 1,5 %,
- Ano, občas, když je předmět zajímavý – 5,5 %,
- Ano, omylem – 5 %,
- Pouze po ověření odesílatele – 34,5 %,

- Ne, přílohy od neznámých odesílatelů neotvírám – 53,5 %.

Dále byly v dotazníku uvedeny skutečně obdržené emaily od různých zdrojů, kdy měli respondenti za úkol určit, jak by se zachovali v případě doručení takového emailu do jejich emailové schránky.

První vybraný email nesl známky phishingového emailu a byl na české poměry velice nepovedený. Byl psát čínskými znaky, odesílatel byl taktéž v této znakové sadě, odkazem nevyjímaje.

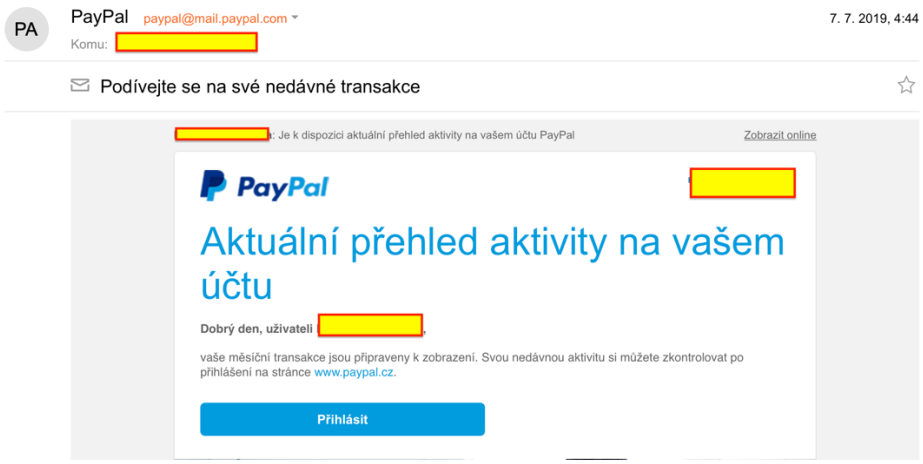


Obrázek 11. Phishingová zpráva s odkazem [zdroj vlastní]

Hypotetické chování uživatelů bylo následující:

- 57 % respondentů označilo email jako podvodný, email by smazali bez kliknutí na odkaz.
- 24 % dotazovaných by si emailu vůbec nevšímalo.
- 18 % označilo email jako spam a nahlásilo by jej.
- 1 % by email otevřelo, na odkaz by klikl, měli pocit, že se jedná o legitimní email.

Druhý email byl legitimní a byl doručen od odesílatele paypal@mail.paypal.com, ve kterém byl uveden legitimní odkaz na stránky www.paypal.cz.

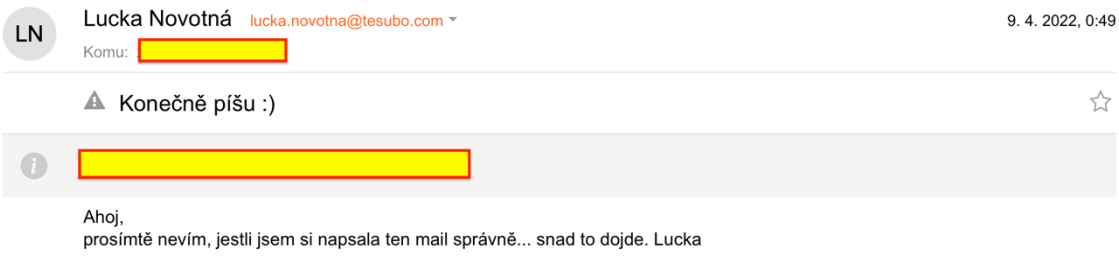


Obrázek 12. Legitimní email od společnosti PayPal [zdroj vlastní]

U tohoto emailu se dotazovaní zachovali následovně:

- 35 % by si emailu nevšímalo.
- 32 % email označilo jako podvodný, nikam by neklikli.
- 23 % označilo email jako legitimní, na odkaz by bez váhání klikli.
- A 10 % označilo email za spamovou zprávu.

Další email byl trochu těžší na rozluštění, o jakou kategorii emailu se jedná, neboť byl email psán češtinou, používal emotikony, nenesl s sebou žádnou přílohu a ani v něm nebyl žádný odkaz, na který by uživatel mohl kliknout. Jediné, co by mohlo vykazovat nějaké známky nežádoucího emailu, byl čas doručení ve spojení s emailovou adresou, která budí dojem firemního, uživatelského emailu. Tyto zprávy jsou poslední dobou hojně rozšířeny a putují sítí.



Obrázek 13. Spamová zpráva [zdroj vlastní]

V tomto případě respondenti označili email následovně:

- 37 % by si emailu nevšímalo.
- 25,5 % respondentů by na email odpovědělo, neboť se domnívalo, že se jedná o legitimní email.
- 21,5 % dotázaných označilo email za podvodný.
- A 16 % správně označilo, že se jedná o spam.

Další email, byl klasický phishingový email s přílohou ve formě zipu, která zřejmě nesla nějaký bonuse ve formě malware. Jednalo se o celkem povedený email, ale po důkladném prostudování je zde vidět špatná diakritika u některých slov. U tohoto emailu respondenti odpovídali nejčastěji takto:

- Kliknu na přiloženou přílohu pro více informací – 5 %.
- Nahlásím email jako spam – 20 %.
- Pokusím se nejprve ověřit pravost emailu – 35 %.
- Email smažu a nikam klikat nebudu – 40 %.

Přiložený email vypadal takto:


Odpovědět Odpovědět všem Předat dál Rychlé zprávy

po 28. 4. 2014 10:59

Ambraa Jaroslav <debt@vlevy.cz>

Výše pohledávky na vašem účtu #1151215389217520

Komu [redacted]

Zpráva smlouva_943140E481F1215A.zip (24 kB)

Vážený zákazníku,

Jsme velmi rádi, že jste vyuziváli produktu z naší banky.
Dovolujéme Vás upozornit, že k 25.04.2014 dlužné částky na osobní účet ve vysi #1151215389217520 8438.92 Kč. Nabízíme vám dobrovolně uhradit pohledávku v plné výši do 16.05.2014.

Dobrovolné uhrazeni pohledávky a dodrženi smlouvy #943140E481F1215A umožňuje Vám:
1) Dodržet pozitivní úvěrovou historii
2) Vyhnout se soudním sporům, placení poplatků a jiných soudních nákladů.

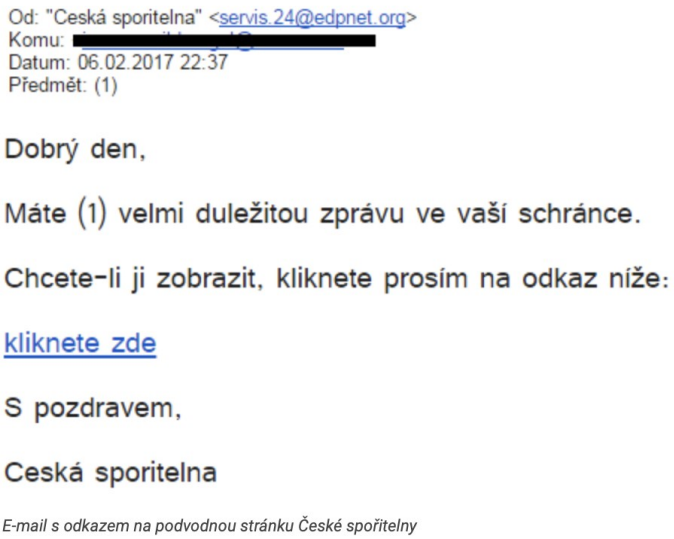
V případě prodlení uhrady pohledávky 8438.92 Kč v souladu s platnými právními předpisy, jsme oprávněni zahájit právní sankci na základe pohledávky.

Kopie smlouvy a platební údaje jsou připojeny k tomuto dopisu jako soubor "smlouva_943140E481F1215A.zip"

S pozdravem,
Vedoucí odboru vymahani pohledávek
Ambraa Jaroslav
+420 602 730 232

Obrázek 14. Phishingová zpráva s nakaženou přílohou [7]

U dalšího email, který měl také známky phishingu s odkazem, který vedl na podvrženou stránku pomocí techniky pharming, byli respondenti dotazování, jak by se zachovali vůči odkazu uvnitř zprávy. Zpráva byla velice povedená, ale v některých slovech byla špatná diakritika a odesílatel nebyl legitimní s emailovou adresou banky.


Od: "Ceská sporitelna" <servis.24@edpnet.org>
Komu: [redacted]
Datum: 06.02.2017 22:37
Předmět: (1)

Dobrý den,

Máte (1) velmi duležitou zprávu ve vaší schránce.

Chcete-li ji zobrazit, kliknete prosím na odkaz níže:

kliknete zde

S pozdravem,

Ceská sporitelna

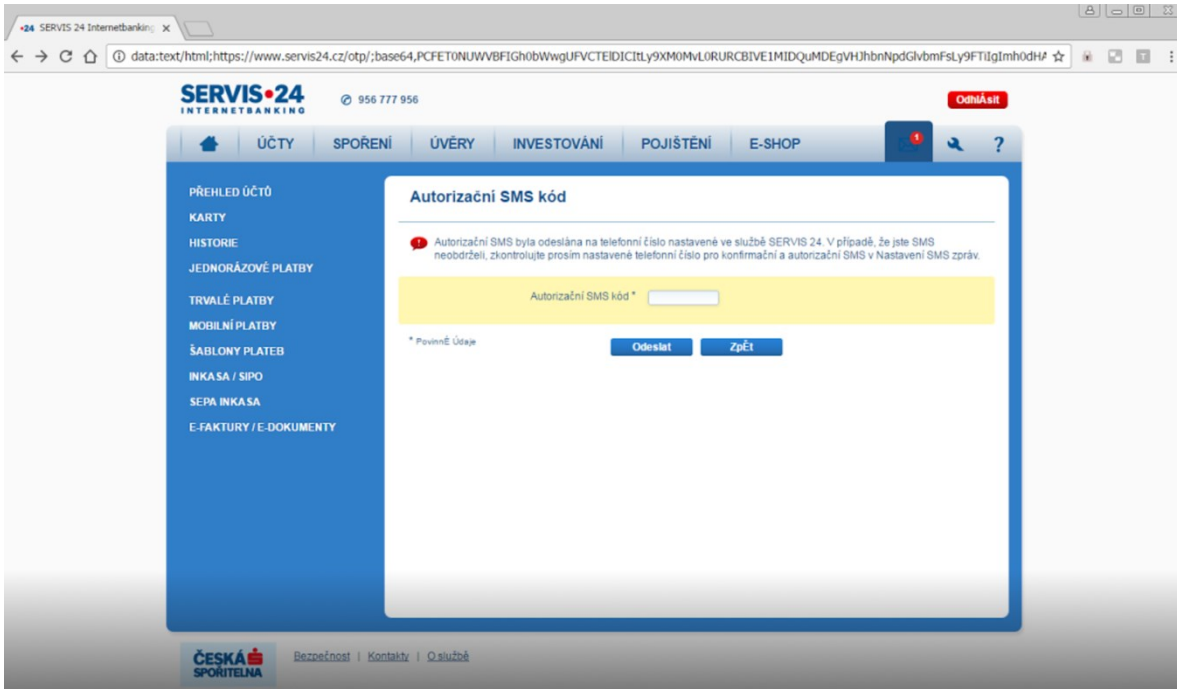
E-mail s odkazem na podvodnou stránku České spořitelny

Obrázek 15. Phishingová zpráva s odkazem na podvrženou stránku banky [44]

V tomto případě respondenti odpovídali následovně:

- Kliknu na odkaz, jedná se o legitimní email – 4 %.
- Mám dojem, že se jedná o spam, tak jej jako spam označím – 15 %.
- Mám dojem, že se jedná o podvodnou zprávu, a proto ji nahlásím bance – 46 %.
- Email smažu – 35 %.

Další otázka se týkala odkazu a pozornosti respondentů, jak by se zachovali při přesměrování na podvodnou stránku banky, v našem případě na stránku České spořitelny.



Obrázek 16. Podvodná stránka z phishingového emailu – metoda Pharming [44]

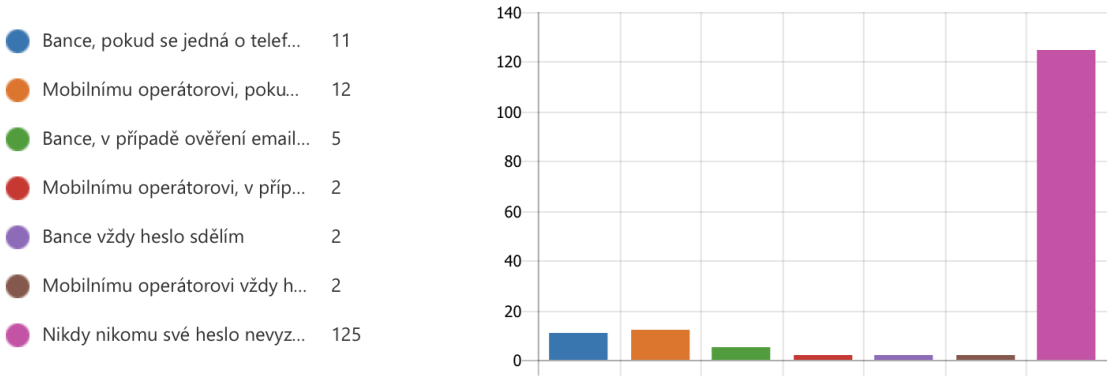
Na první pohled stránka vypadá velice povedeně. Při druhém pohledu je ovšem zřejmé, že adresa URL je nesmyslná, někde je špatná diakritika. I přesto, že by na odkaz kliklo pouze 4 % dotazovaných, byly odpovědí na otázku: „Pokud jste v předchozí odpovědi klikli na email, zobrazila se Vám tato stránka. Jak se zachováte?“ následující:

- Do kolonky zadám autorizační kód, který mi přišel na telefon, jedná se o legitimní stránku banky – 5 %.
- Nic zadávat nebudu, jedná se o spam – 9 %.
- Mám dojem, že se jedná o podvodnou stránku, a proto jí nahlásím bance – 17 %.
- Stránku zavřu křížkem a nic dalšího dělat nebudu – 6 %.
- V předchozí otázce jsem na odkaz neklikl – 63 %.

V další otázce byly respondenti vyzváni, aby si představili situaci, kdy jsou vyzváni k potvrzení či sdělení hesla. Jaké instituci by své heslo pro ověření sdělili? V tomto případě se respondenti chovali velmi obezřetně a v 86 % by své heslo nikdy nikomu neřekli. Ve 14 % případů, respondenti své odpovědi rozvrhli následovně:

- Bance, pokud se jedná o telefonní hovor – 32 %.
- Mobilnímu operátorovi, pokud se jedná o telefonní hovor – 35 %.
- Bance, v případě ověření emailem – 15 %.

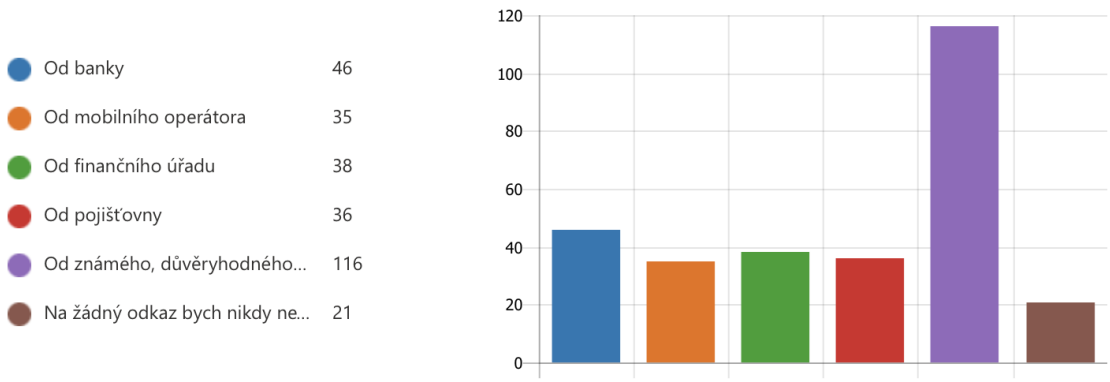
- Mobilnímu operátorovi, v případě ověření emailem – 6 %.
- Bance by své heslo vždy sdělilo 6 % respondentů.
- Mobilnímu operátorovi vždy heslo sdělí také 6 % respondentů.



Obrázek 17. Jaké instituci by respondenti sdělili své heslo [zdroj dotazník]

Další otázka studovala, jak se respondenti zachovají v případě, že jim přijde email, který obsahuje odkaz. V jakém případě by na takový odkaz klikli?

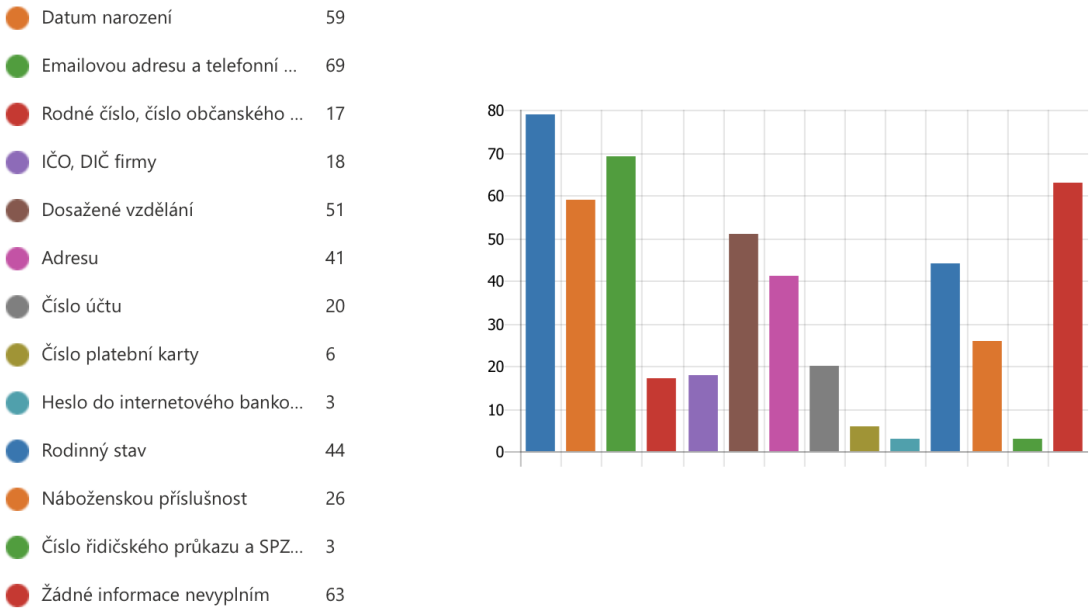
- 15 % by kliklo na odkaz od banky.
- 12 % respondentů by kliklo na odkaz od mobilního operátora.
- 13 % od finančního úřadu.
- 12 % od pojišťovny.
- 40 % respondentů by kliklo na odkaz od známého, důvěryhodného zdroje.
- 7 % by nikdy na žádný odkaz nekliklo.



Obrázek 18. Jaké instituci by respondenti klikli na odkaz v emailu [zdroj dotazník]

Dále byli respondenti vystaveni hypotéze, jak by se zachovali v situaci, kdy jim banka zašle dotazník. Jaké údaje by bance v dotazníku vyplnili? Žádné informace by neposkytlo 43 % dotazovaných, ze zbývajících 57 %, by se respondenti podělili o své údaje následovně:

- Jméno a příjmení – 18 %,
- Datum narození 13 %,
- Emailovou adresu a telefonní číslo – 16 %,
- Rodné číslo, číslo občanského průkazu – 4 %,
- IČO, DIČ firmy – 4 %,
- Dosažené vzdělání – 12 %,
- Adresu bydliště – 9 %,
- Číslo účtu – 4,5 %,
- Číslo platební karty – 1,5 %,
- Heslo do internetového bankovnictví – 1 %,
- Rodinný stav – 10 %,
- Náboženskou příslušnost – 6 %,
- Číslo řidičského průkazu a SPZ vozidla – 1 %.



Obrázek 19. Jaké údaje by respondenti vyplnili do dotazníku [zdroj dotazník]

7.2.6 Znalostní kvíz z pohledu kybernetické bezpečnosti

V této sekci bylo celkem deset otázek, kdy měl respondent vždy na výběr z možností.

První otázka: Co si představíte pod pojmem PHISHING? Zde byly odpovědi celkem jednoznačné:

- Jedná se o anglický výraz pro rybaření – 3 %.
- Jedná se o podvodnou metodu, kdy příjemce obdrží nepravý email, který se snaží z uživatele vylákat údaje – 92,5 %.
- Jedná se o výraz, který se používá v případě, že někdo chytá ryby načerno – „pytlačí“ – 0,5 %.
- Výraz nemá speciální význam – 4 %.

Druhá otázka: Co si představíte pod pojmem PHARMING?

- Jedná se o anglický výraz pro farmaření – 4 %.
- Jedná se o herní výraz, kdy hráč jde sklízet svou zahrádku – 4 %.
- Jedná se o podvodnou metodu, kdy je uživatel přesměrován na podvodnou stránku, která z něj má vylákat údaje – 77 %.
- Výraz nemá speciální význam – 15 %.

Třetí otázka: Co si představíte pod pojmem WHALING?

- Jedná se o anglický výraz pro lov velryb – 8,5 %.
- Jedná se o podvodnou metodu, která se zaměřuje na vysoce postavenou osobu v určité společnosti – 68 %.
- Jedná se o výraz z českého jazyka, odvozeného od slova válet se – „něco jako gaučing“ – 2 %
- Výraz nemá speciální význam – 21,5 %

Čtvrtá otázka: Co si představíte pod pojmem TROJSKÝ KŮŇ? I v této otázce se respondenti velice dobře orientovali a jejich odpovědi byly velmi uspokojivé.

- Trojský kůň byl použit k vniknutí Řeků do Troje – 3 %.
- Je to druh koně, který pochází z Troje – 0 %.
- Jedná se o typ viru, který vypadá jako legitimní software, ale uvnitř sebe skrývá škodlivý kód – 96 %
- Výraz nemá speciální význam – 1 %.

Pátá otázka: Co si představíte pod pojmem HOAX? Tato otázka byla pro respondenty víceméně jednoznačná.

- Jedná se o zprávu, která má za úkol příjemce vystrašit a šířit paniku – 92 %.
- Je to zaručeně pravá zpráva, kterou je potřeba rozšířit – 1,5 %.
- Je to žertovná zpráva, určitý typ vtipu – 4 %.
- Výraz nemá speciální význam – 2,5 %.

Šestá otázka: Co si představíte pod pojmem WORM?

- Jedná se o postavičku z legendární hry WORMS, oblíbené v 90. letech minulého století – 5,5 %.
- Je to speciální kód, který je schopen automatického množení a rozesílání prostřednictvím počítačové sítě – 85 %.
- Jedná se o speciální typ červa, který se používá při chytání velkých ryb – 3,5 %.
- Výraz nemá speciální význam – 6 %.

Sedmá otázka: Co si představíte pod pojmem RANSOMWARE?

- Jedná se o speciální typ viru, který po napadení počítače, zablokuje jeho obsah a po uživateli vyžaduje výkupné za odblokování obsahu – 87 %.
- Je to typ žertovného programu, který se chová náhodně – 2 %.
- Je to software, který je k dispozici zdarma po určité časové období – 3 %.
- Výraz nemá speciální význam – 8 %.

Osmá otázka: Co si představíte pod pojmem COOKIE?

- Je to soubor, který si ukládají webové stránky o návštěvě uživatele – 96 %.
- Křupavé sušenky s čokoládou – 1,5 %.
- Jedná se o typ počítačového viru – 1,5 %.
- Výraz nemá speciální význam – 1 %.

Devátá otázka: Co si představíte pod pojmem ZOMBIE?

- Jedná se o označení z filmů pro nemrtvého – 25 %.
- Je to napadený počítač, ze kterého mohou být vzdáleně prováděny počítačové útoky – 64 %.
- Tímto výrazem se označuje zastaralý software – 2 %.
- Výraz nemá speciální význam – 9 %.

Desátá otázka: Co si představíte pod pojmem DARKWEB?

- Jedná se o část internetu, která není indexována a je dostupná pouze s použitím speciálního software – 69 %.
- Jedná se o internetové stránky, které jsou běžně dostupné, ale je na nich uveden nelegální obsah – 20 %.
- Je to funkcionalita webového prohlížeče, která uživateli umožňuje nastavení tmavého režimu – 3,5 %.
- Výraz nemá speciální význam – 7,5 %.

7.3 Vyhodnocení dotazníku

Celkové vyhodnocení dotazníku je zpracováno s ohledem na posouzení bezpečného chování uživatelů v internetovém prostředí, jaký kladou důraz na obezřetné chování, zda se zbytečně nevystavují riziku potenciálních hrozeb, prostřednictvím stahování nelegálního obsahu či obsahu od neznámých uživatelů, při němž dochází ke sdílení stahovaného obsahu. Do hodnocení bylo započítáno skóre za správnou identifikaci emailu a bylo kalkulováno i s chybovostí uživatelů u jednotlivých otázek. Hodnoceny byly i kvízové otázky. Vyhodnocení dotazníku bylo provedeno na třech úrovních, a to z pohledu věkových skupin, nejvyššího dosaženého vzdělání a z pohledu pracovního zaměření.

7.3.1 Vyhodnocení dle věkové skupiny respondentů

Tabulka 2. Vyhodnocení odpovědí respondentů – věk [zdroj vlastní]

Vyhodnocení dotazníku s ohledem na bezpečné chování uživatelů v internetovém prostředí - rozřazení dle věku respondentů.				
Vybranné otázky dotazníku, které mají za úkol vyzkoumat, která skupina se na internetu pohybuje bezpečněji.	**Předmět zkoumání u dané otázky a její vliv (pozitivní/negativní) na bezpečnost.**	**Skupina do 20 let - 33 respondentů**	**Skupina 20 - 49 let - 94 respondentů**	**Skupina nad 49 let - 18 respondentů**
Používáte antivirový program?	Kladná odpověď - ANO	70%	64%	**83%**
Software do svého zařízení...?	Bezpečnostní pochybení - stahování z BitTorrent - negativní dopad.	**24%**	5%	0%
Stahování filmů.	Stahování z BitTorrentu - negativní dopad.	**12%**	10%	0%
Za software...?	Nelegální stahování software - negativní dopad.	**42%**	27%	6%
Čtete zprávy a upozornění z banky?	Negativní dopad - nečte.	27%	26%	**33%**
Sdílíte s někým Vaše přihlašovací údaje?	Negativní dopad - sdílí přihlašovací údaje.	**24%**	19%	11%
Jaké přihlašovací údaje sdílíte?	Žádné údaje uživatelé nesdílí - pozitivní dopad.	51%	54%	**72%**
Používáte stejná hesla k přihlášení do více účtů?	Použití stejných/podobných hesel - negativní dopad.	**6% / 72%**	**8,5% / 61%**	5,5% / 50%
Používáte dvoufaktorové zabezpečení?	Nepoužívání 2FA zabezpečení/nevím, co to je - negativní dopad.	9% / 6%	**18% / 13%**	**17% / 44%**
Kolik znaků mají průměrně Vaše hesla?	4-7 znaků - negativní dopad.	**6%**	5%	0%
Kolik znaků mají průměrně Vaše hesla?	Více jak 12 znaků - pozitivní dopad	**51%**	23%	11%
Otevíráte emaily ze spamového filtru?	ANO - bezpečnostní riziko - negativní dopad.	21%	10%	**22%**
Otevíráte přílohy i od neznámých odesílatelů?	ANO - bezpečnostní riziko - negativní dopad.	12%	9%	**28%**
Chování uživatele v případě doručení určitých emailů.	Všechny emaily správně identifikované - pozitivní dopad.	9%	10%	**17%**
Chování uživatele v případě doručení určitých emailů.	Špatná identifikace emailů - chybovost - negativní dopad.	21%	15%	**22%**
Jaké instituci heslo pro ověření sdělíte?	Uživatel heslo sdělí - negativní dopad.	**24%**	10,5%	11%
V jakém případě byste klikli na odkaz v emailu?	Uživatelé, kteří na odkaz vždy kliknout - negativní dopad.	**42%**	29%	33%
V jakém případě byste klikli na odkaz v emailu?	Uživatelé nikdy na odkazy v emailech neklikají - pozitivní.	6%	15%	**17%**
Které údaje bance vyplníte?	Uživatelé bance žádné údaje nesdělí -pozitivní dopad.	21%	45%	**67%**
Závěrečný kvíz.	Všechny odpovědi správně - pozitivní dopad.	**45%**	37%	28%
	Celkové skóre	**-9 bodů**	**3 body**	**4 body**

Při hodnocení dle věkových skupin, bylo zjištěno, že se nejobezřetněji na internetu chovají lidé nad 49 let, v těsném závěsu byli lidé z věkové skupiny 20-49 let a nejnebezpečněji se v internetovém prostředí pohybují lidé do 20 let. Každá pozitivně vnímaná otázka z pohledu bezpečnosti, byla při nejlepším výsledku hodnocena +1 bodem, při negativním výsledku -1 bodem. U otázek vnímaných negativním způsobem, bylo hodnocení opačné. Detailní výsledky jsou uvedeny v tabulce.

7.3.2 Vyhodnocení dle nejvyššího dosaženého vzdělání

Tabulka 3. Vyhodnocení odpovědí respondentů – vzdělání [zdroj vlastní]

Vyhodnocení dotazníku s ohledem na bezpečné chování uživatelů v internetovém prostředí - rozřazení dle nejvyššího dosaženého vzdělání.				
Vybranné otázky dotazníku, které mají za úkol vyzkoumat, která skupina se na internetu pohybuje bezpečněji.	**Předmět zkoumání u dané otázky a její vliv (pozitivní/negativní) na bezpečnost.**	**Základní vzdělání - 5 respondentů**	**Středoškolské vzdělání - 86 respondentů**	**Vysokoškolské vzdělání - 54 respondentů**
Používáte antivirový program?	Kladná odpověď - ANO	**100%**	66%	67%
Software do svého zařízení...?	Bezpečnostní pochybení - stahování z BitTorrent - negativní dopad.	**20%**	14%	0%
Stahování filmů.	Stahování z BitTorrentu - negativní dopad.	**20%**	12%	4%
Za software...?	Nelegální stahování software - negativní dopad.	20%	27%	**30%**
Čtete zprávy a upozornění z banky?	Negativní dopad - nečte.	20%	**28%**	26%
Sdílíte s někým Vaše přihlašovací údaje?	Negativní dopad - sdílí přihlašovací údaje.	**40%**	20%	17%
Jaké přihlašovací údaje sdílíte?	Žádné údaje uživatelé nesdílí - pozitivní dopad.	40%	55%	**59%**
Používáte stejná hesla k přihlášení do více účtů?	Použití stejných/podobných hesel - negativní dopad.	20% / 40%	**7% / 63%**	6% / 63%
Používáte dvoufaktorové zabezpečení?	Nepoužívání 2FA zabezpečení/nevím, co to je - negativní dopad.	0% / 20%	**16% / 16%**	17% / 11%
Kolik znaků mají průměrně Vaše hesla?	4-7 znaků - negativní dopad.	**40%**	5%	2%
Kolik znaků mají průměrně Vaše hesla?	Více jak 12 znaků - pozitivní dopad	**40%**	34%	19%
Otevíráte emaily ze spamového filtru?	ANO - bezpečnostní riziko - negativní dopad.	**60%**	15%	7%
Otevíráte přílohy i od neznámých odesílatelů?	ANO - bezpečnostní riziko - negativní dopad.	**40%**	13%	7%
Chování uživatele v případě doručení určitých emailů.	Všechny emaily správně identifikované - pozitivní dopad.	**20%**	11%	9%
Chování uživatele v případě doručení určitých emailů.	Špatná identifikace emailů - chybovost - negativní dopad.	**40%**	20%	19%
Jaké instituci heslo pro ověření sdělíte?	Uživatel heslo sdělí - negativní dopad.	**40%**	15	9%
V jakém případě byste klikli na odkaz v emailu?	Uživatelé, kteří na odkaz vždy kliknout - negativní dopad.	**60%**	34%	28%
V jakém případě byste klikli na odkaz v emailu?	Uživatelé nikdy na odkazy v emailech neklikají - pozitivní.	**20%**	12%	15%
Které údaje bance vyplníte?	Uživatelé bance žádné údaje nesdělí -pozitivní dopad.	0%	42%	**46%**
Závěrečný kvíz.	Všechny odpovědi správně - pozitivní dopad.	40%	35%	**43%**
	Celkové skóre	**-3 body**	**-6 bodů**	**9 bodů**

U hodnocení dle nejvyššího dosaženého vzdělání se nejméně bezpečně v internetovém prostředí pohybují jedinci se středoškolským vzděláním. Tato skupina nedosáhla v nastaveném hodnocení ani jednoho plusového bodu, spíše se jejich odpovědi držely v neutrální hladině s inkriminací k negativně hodnoceným odpovědím. Nejstabilnější odpovědi měla skupina respondentů, jenž má vysokoškolské vzdělání jako nejvyšší dosažené, tato skupina se na internetu chová nejobezřetněji.

7.3.3 Vyhodnocení dle pracovního zaměření

U vyhodnocení dotazníků dle pracovního zaměření, byl zvolen bodový systém 0–6 bodů, kdy celkové pořadí, dle nejbezpečnějšího chování bylo následují:

- Obchod a administrativa,

- Informační technologie a telekomunikace,
- Průmysl a doprava,
- Školství a kultura, společně se zdravotnictvím,
- Nepracující,
- Gastronomie a pohostinství.

Tabulka 4. Vyhodnocení odpovědí respondentů – pracovní obor [zdroj vlastní]

Vyhodnocení dotazníku s ohledem na bezpečné chování uživatelů v internetovém prostředí - rozřazení dle pracovního zaměření								
Vybranné otázky dotazníku, které mají za úkol vyzkoumat, která skupina se na internetu pohybuje bezpečněji.	**Předmět zkoumání u dané otázky a její vliv (pozitivní/negativní) na bezpečnost.**	**Nepracující - 13**	**IT a Telekomunikace - 55**	**Školství a Kultura - 12**	**Gastronomie a pohostinství - 4**	**Průmysl a Doprava- 18**	**Obchod a Administrativa - 35**	**Zdravotnictví - 8**
Používáte antivirový program?	Kladná odpověď - ANO	69%	71%	75%	50%	66%	63%	62%
Software do svého zařízení...?	Bezpečnostní pochybení - stahování z BitTorrent - negativní dopad.	15%	9%	17%	0%	11%	6%	0%
Stahování filmů.	Stahování z BitTorrentu - negativní dopad.	0%	15%	8%	0%	5%	9%	0%
Za software...?	Nelegální stahování software - negativní dopad.	30%	35%	33%	25%	17%	20%	13%
Čtete zprávy a upozornění z banky?	Negativní dopad - nečte.	60%	24%	17%	25%	17%	29%	25%
Sdílíte s někým Vaše přihlašovací údaje?	Negativní dopad - sdílí přihlašovací údaje.	7%	22%	33%	25%	11%	8%	62%
Jaké přihlašovací údaje sdílíte?	Žádné údaje uživatelé nesdílí - pozitivní dopad.	69%	53%	50%	25%	56%	69%	25%
Používáte stejná hesla k přihlášení do více účtů?	Použití stejných/podobných hesel - negativní dopad.	15% / 54%	4% / 69%	8% / 50%	25% / 25%	0% / 78%	11% / 57%	12,5% / 50%
Používáte dvoufaktorové zabezpečení?	Nepoužívání 2FA zabezpečení/nevím, co to je - negativní dopad.	7,5% / 30%	13% / 0%	8% / 50%	0% / 25%	28% / 0%	20% / 29%	25% / 12,5%
Kolik znaků mají průměrně Vaše hesla?	4-7 znaků - negativní dopad.	8%	0%	17%	0%	11%	6%	0%
Kolik znaků mají průměrně Vaše hesla?	Více jak 12 znaků - pozitivní dopad	38%	45%	25%	25%	11%	6%	37%
Otevíráte emaily ze spamového filtru?	ANO - bezpečnostní riziko - negativní dopad.	23%	15%	17%	0%	11%	11%	13%
Otevíráte přílohy i od neznámých odesílatelů?	ANO - bezpečnostní riziko - negativní dopad.	15%	5%	25%	25%	17%	8,50%	25%
Chování uživatele v případě doručení určitých emailů.	Všechny emaily správně identifikované - pozitivní dopad.	0%	9%	8%	25%	11%	14%	13%
Chování uživatele v případě doručení určitých emailů.	Špatná identifikace emailů - chybovost - negativní dopad.	23%	18%	17%	25%	17%	20%	25%
Jaké instituci heslo pro ověření sdělíte?	Uživatel heslo sdělí - negativní dopad.	23%	11%	25%	50%	6%	11%	13%
V jakém případě byste klikli na odkaz v emailu?	Uživatelé, kteří na odkaz vždy kliknout - negativní dopad.	23%	38%	33%	50%	33%	23%	38%
V jakém případě byste klikli na odkaz v emailu?	Uživatelé nikdy na odkazy v emailech neklikají - pozitivní.	8%	11%	25%	0%	11%	17%	13%
Které údaje bance vyplníte?	Uživatelé bance žádné údaje nesdělí -pozitivní dopad.	38%	33%	50%	25%	39%	60%	37%
Závěrečný kvíz.	Všechny odpovědi správně - pozitivní dopad.	30%	51%	25%	0%	17%	46%	13%
	Celkové skóre	**52 bodů**	**66 bodů**	**53 bodů**	**49 bodů**	**58 bodů**	**70 bodů**	**53 bodů**

7.4 Shrnutí a přínosy výzkumu

Obecné vyhodnocení dotazníku ukázalo, že počítačová gramotnost populace v České republice je uspokojivá až na určité nedostatky, které vykazují spíše jednotlivci z řad mladší a starší generace.

Nejčastější činností, která je na internetu provozována je vyhledávání informací, v některých případech s inkriminací k nelegálnímu stahování filmů či software s nejvyšší obsazeností u věkové skupiny do 20 let se základním vzděláním, bude se tedy jednat spíše o studenty. Znepokojivý je ovšem fakt, že toto chování vykazují i lidé, kteří jako svůj pracovní obor uvedli Informační technologie, Telekomunikace a Školství. Bohužel, ale pouze třetina respondentů používá antivirový program v mobilním zařízení, oproti počítači, kde jej používá téměř 70 % respondentů.

U sdílení přihlašovací údajů, téměř čtvrtina respondentů uvedla, že své údaje sdílí, a to nejčastěji s partnerem, rodiči či s dětmi. Nejčastěji sdílné přihlašovací údaje jsou do počítače či mobilního telefonu a do internetového či mobilního bankovnictví.

Co se týká politiky hesel, 70 % respondentů využívá výhradně slabší hesla, a to i díky faktu, že svá hesla používají výhradně stejné či jako kombinace hesla s jedním, stejným základem. Třetina respondentů nepoužívá dvou faktorové zabezpečení a někteří bohužel ani nevědí, o co se jedná.

Pozitivním hlediskem je fakt, že respondenti měli určité podvědomí o možných hrozbách, které se k nim mohou dostat formou emailové komunikace, či o vybraných termínech z oblasti kybernetické bezpečnosti. Na druhou stranu, necelá polovina respondentů by otevřela přílohu v emailu od neznámého odesílatele, i když někteří po až po ověření.

Znepokojující je fakt, že by až třetina respondentů sdělila či potvrdila své heslo některým institucím, jako je banka nebo mobilní operátor, a to jak emailem, tak i telefonicky. V polovině případů, by respondenti dokonce bez váhání klikli na odkaz v emailu od banky, mobilního operátora, finančního úřadu či pojišťovny. Při zjišťování, jaká data by respondenti sdíleli, by pouze třetina nesdělila žádné instituci žádná data prostřednictvím formuláře zaslaného na email.

Přínosem dotazníkového šetření je výzkum počítačové gramotnosti, podvědomí veřejnosti o možných kybernetických hrozbách, dále šetření, jakým způsobem nakládají se svou bezpečností, daty, a jaké vykazují chování ve chvíli, kdy jim je doručen podezřelý email. Mnoho respondentů bylo s dotazníkem velmi spokojeni, kdy si chválili jeho skladbu, možnost otestování svého vlastního chování, a dokonce uvědomění si, že se nechovají v některých situacích příliš bezpečně. Někteří respondenti dokonce přemýšlí o změně politiky hesel a více se o problematiku kybernetické bezpečnosti začali zabývat a vyslovili přání si poté celou práci přečíst.

8 ANALÝZA INFORMOVANOSTI VEŘEJNOSTI

Jakým způsobem je širší veřejnost informovaná o možných hrozbách a jsou tyto informace dostačující? Dle dotazníkového průzkumu, 85 % respondentů odpovědělo, že na internetu vyhledávají informace. Vyhledávají, ale i informace z oblasti kybernetické bezpečnosti, nebo je toto spíše dominantou lidí, kteří se pohybují v sektoru informačních technologií? Jakým způsobem je možné najít informace o kybernetických hrozbách? Pokud si uživatel do vyhledávače zadá kybernetická bezpečnost, naskytne se mu možnost zjišťovat informace z tisíců dostupných internetových stránek.

8.1 Národní úřad pro kybernetickou bezpečnost

Mezi prvními se při zkoumání zobrazily stránky Národního úřadu pro kybernetickou a informační bezpečnost – NÚKIB. Na těchto stránkách je uživatel informován o aktuálních hrozbách a zranitelnostech. Stránky jsou velmi často aktualizovány a jsou zde doplňovány nové články. NÚKIB vydává i varování na základě světových konfliktů a krizí. Jsou zde podrobnosti o novém malware, podvodných telefonátech či emailech. [76]

8.2 Ministerstvo vnitra České republiky

Na stránkách Ministerstva vnitra České republiky jsou mimo témat terorismu či extremismu, řešeny i otázky kybernetických hrozeb, které jsou zde celkem solidně popsány. Jsou zde dokumenty k aktuálním kybernetickým hrozbám, závěry z konference Kybernetické výzvy a hrozby – CYBER a doporučení, které z těchto rizik vyplývají. Dále je zde možné nalézt nepřeberné množství dokumentů jako jsou bezpečnostní politika, prezentace francouzského ministerstva vnitra a další. Při ohledání stránky s bezpečnostním výzkumem, se dostaví zklamání, stránka je prázdná a žádný výzkum na ní, bohužel pro uživatele není. Velice povedený je ovšem projekt Safer Internet, který cílí na vzdělávání dětí v oblasti kybernetické bezpečnosti a upozorňuje na novinky v zabezpečení aplikací a změny podmínek pro užívání, dále upozorňuje na podvodné chování na internetu apod. [77], [78]

Součástí internetových stránek MVCR je i odkaz na stránky Policie ČR, kde mohou uživatele nalézt podobné informace jako na stránkách MVCR.

8.3 Bankovní instituce

Bankovní instituce v tomto ohledu mají lepší dosah pro osvětu, kterou mohou šířit směrem ke svým klientům. Dle dotazníkového šetření, bylo zjištěno, že 97 % respondentů vlastní

bankovní účet a 92 % dotazovaných aktivně využívá internetové či mobilní bankovnictví, jejímž prostřednictví banky mohou komunikovat se svými klienty. Po analýze bylo zjištěno, že banky využívají této platformy k informování klientů. V některých případech se zpráva zobrazí přímo bez jejích otevření klientem, v jiných případech je informace o možné hrozbě ve formě zprávy od banky. Dle dotazníku vyšlo, že zprávy z banky čte 73 % klientů. Při bližším šetření, bylo zjištěno, že potíž je spíše v tom, že banky na své klienty chrlí nepřeberné množství informací a zasílají svým klientům prostřednictvím těchto zpráv i marketingové nabídky. Uživatele jsou poté zahlceni nepotřebnými informacemi, a díky tomu si nevšimnou důležitého bezpečnostního upozornění, čímž se mohou vystavit riziku a podlehnout podvodnému jednání ze strany útočníka.

Většina bank má na svých stránkách i jistý typ blogu, kde se snaží své klienty vzdělávat na téma kybernetické bezpečnosti a možných hrozeb, včetně znaků, jak podvodnou zprávu odhalit. Mezi aktuální hrozby v poslední době, na které banky nejčastěji upozorňují, jsou podvodné emailové zprávy – phishing, podvodné telefonáty – vhishing či podvodné bazarové inzeráty. [79], [80], [81]

8.4 Shrnutí informovanosti o kybernetické bezpečnosti

Na internetu je velké množství informací, a když uživatel vyhledává určitou informaci, musí chvíli pátrat, než najde to, co opravdu hledal. A právě toto se ukazuje jako problém v oblasti kybernetické bezpečnosti. Na spojení „Kybernetická bezpečnost“, lze najít nepřeberné množství článků o hrozbách, které již nejsou aktuální, různé druhy školení, které nabízejí firmy jiným firmám, či jednotlivcům, testování zaměstnanců, studijní obory, zákon o kybernetické bezpečnosti a mnoho dalšího. Ve své podstatě neexistuje ucelený přehled, který by uživatelům poskytoval veškeré informace na jednom místě. Kdo by se ve svém volném čase dobrovolně zabýval hledáním informací o kybernetických hrozbách, když většina uživatelů a firem si stále myslí, že toto téma se jich přece netýká, že jsou malé ryby a proč by právě jim chtěl někdo uškodit? Každý den se setkáváme s podvodnými zprávami, poplašné a řetězové zprávy se šíří sociálními sítěmi jako laviny a uživatelé tyto dezinformace čtou a přeposílají si je v hojném množství, bohužel bez ověření pravosti dané zprávy. Informovanost ve firmách je o něco lepší, i když se stále setkáváme s informacemi, že lepší zabezpečení, vývoj aplikací prodražuje. Většina lidí si myslí, že se jich problém s bezpečností netýká do doby, než se něco stane, a to může být mnohdy již pozdě.

8.5 Šíření osvěty o kybernetické bezpečnosti

Osvětu o kybernetické bezpečnosti a jakým způsobem se chránit proti možným útoků je nutné mezi lidmi lépe šířit. Jakým způsobem uživatele zaujmout, aby místo hraní her, nebo sledování videí na sociálních sítí, si našli pár minut a přečetli si informace o aktuálních hrozbách? Pokud tyto informace nebudou jako hlavní titulek na zpravodajských, internetových stránkách, jen malé procento lidí si tyto informace aktivně vyhledá. V dnešním digitálním světě je proto potřeba vytvořit takovou kampaň, která uživatele zaujme, a to bez rozdílu věku. V dnešní době mají největší dosah sociální sítě, a je na nich prakticky každý. Profilů, které na bezpečnostní hrozby upozorňují je na sociálních sítí také velké množství, ale pokud si je uživatel sám, dobrovolně nevyhledá, informace se k němu nedostanou.

Nejlepší je začít se vzděláváním od základních škol, aby bylo možné vychovat generaci, která bude mít podvědomí o kybernetické bezpečnosti a hrozbách již od útlého věku. Existují dokonce školení či materiály pro učitele základních škol, které se kybernetickou bezpečností zabývají, a je možné je v již v uceleném formátu předávat žákům.

Na středních školách se již postupně uchylují k zařazení učiva na toto téma, aby učitelé své svěřence vzdělávali i v této oblasti. Není to ovšem pravidlem a jedná se spíše o dominantu škol, které jsou zaměřeny technickým směrem.

Ve firemním prostředí je vzdělávání a informovanost o něco lepší, ovšem se tato školení bere spíše jako nutnost. Většina školení také probíhá formou elearnnigu, což vede často k nepozornosti posluchače a v případě závěrečného testu, k vyhledávání informací pomocí internetu. Dalším neduhem jsou přehnané nároky na bezpečnostní politiku hesel, jenž zaměstnance nutí ke kreativitě v podobě ulehčení si zapamatování hesla, což je spíše kontraproduktivní. Poté uživatelé raději volí jednodušší hesla na zapamatování, či si je nechávají někde napsaná. Toto chování uživatelů může vést k velkému oslabení firemní bezpečnosti a k možnosti infiltrace do počítačové sítě ze strany útočníka.

Poslední, velmi opomíjenou skupinou populace jsou senioři, pro které jsou technologické vymoženosti dnešní doby velkou neznámou a díky jejich důvěřivosti, jsou ochotni sdílet jakékoliv informace bez jejich předešlého ověření. Kdo zajistí osvětu těchto uživatelů? V tomto případě by velmi pomohlo, kdyby byli uživatelé informováni ze strany své rodiny, aktivně ze strany státních institucí, bankovních institucí či ze strany sociálních sítí.

ZÁVĚR

Cílem diplomové práce bylo popsat současné metody sociálního inženýrství a jeho dopady na veřejnost v pojetí kybernetické bezpečnosti a ukázat možnosti obrany proti sociálnímu inženýrství. V práci jsou uvedeny a rozebrány útoky typu phishing, pharming, whaling, včetně podrobného popisu, jakým způsobem jsou sociotechniky využívány a na koho útočníci při svých útocích cílí. Také jsou zde uvedeny konkrétní hrozby, které se zaměřují na různé skupiny populace včetně provedení analýzy současné osvěty o kybernetických hrozbách a legislativního rámce. V práci je uvedeno, jakým způsobem se útočník snaží docílit svých cílů pro zmanipulování oběti, včetně možnosti zanesení nebezpečného malware do zařízení oběti. V práci jsou uvedeny popisy jednotlivých hrozeb, jako jsou viry, červi, ransomware, APT apod. Každý malware pracuje odlišným způsobem a je používán k dosažení různých cílů ze strany útočníka. Další část diplomové práce se zabývá hrozbami, které ohrožují jednotlivé skupiny populace. Populaci je možné z tohoto hlediska rozdělit do tří skupin, děti a mládež, produktivní, pracující populaci a seniory. Z hlediska tohoto rozdělení jsou nejohroženější skupinou děti a mládež, kterých se týkají hrozby, jako jsou kyberšikana, kybergrooming či netholismus. U skupiny v produktivním věku, jsou hrozbami většinou netholismus a internetové podvody, které cílí na vylákání informací a peněz z obětí či podlehnutí dezinformačním zprávám. Senioři jsou nejčastěji vystaveni hrozbám typu kyberšikana, dezinformacím či netholismu. Vzhledem k jejich osamělosti jsou velmi náchylní k podlehnutí této závislosti, jelikož jim digitální svět nabízí alespoň nějakou sociální interakci. Dalším cílem bylo provést šetření kybernetické gramotnosti populace v České republice včetně jeho vyhodnocení. Na základě dotazníkového šetření, bylo zjištěno, že nejméně informovaná je populace do 20 let, jedná se tedy především o děti a mládež, kteří nejčastěji podléhají neznalosti ohledně stahování software a filmů, které často uskutečňují i z nelegálních zdrojů. Nepoužívají bezpečná hesla, která sdílí a nejsou informováni o možnostech napadení ze strany sociálních inženýrů. Na druhé straně hodnocení stála skupina seniorů, kteří si více informace ověřují, nestahují žádný nelegální obsah, ale na druhou stranu nemají dobré podvědomí o kybernetických hrozbách a nedokážou správně reagovat ve chvíli, kdy obdrží nevyžádaný email. U produktivní populace je nejméně používán antivirový program, objevuje se zde i neznalost dvou faktorového zabezpečení a používání slabších hesel. Rozdělení dle vzdělání bylo na základní, do kterého spadali i žáci základních škol, středoškolské vzdělání včetně studentů středních škol a vysokoškolské vzdělání. Z pohledu kybernetické gramotnosti, nejlépe reagovali lidé s vysokoškolským vzděláním, kteří až na stahování

nelegálního obsahu či nesprávného zařazení emailu, si v průzkumu vedli dobře. Tato skupina nesdílí své osobní údaje a nereaguje na odkazy v emailových zprávách. U populace se středoškolským vzděláním je naopak běžné stahování nelegálního obsahu, sdílení informací i přihlašovacích údajů, nezajímají se o kybernetickou bezpečnost a na odkazy také občas klikají. U poslední skupiny, tedy se základním vzděláním se mezi časté neduhy zapisuje nelegální stahování software či emailů, používání slabých hesel, prohlížení si obsahu ze spamových filtrů či kliknutí na závadný obsah. Třetí rozdělení bylo dle pracovního zaměření, kdy nejbezpečnější chování na internetu prokázali respondenti, kteří se zabývají obchodem nebo administrativou. Naopak nejohroženější skupinou byli lidé se zaměřením do gastronomie, nepracující, lidé z oblasti školství a kultury či zdravotnictví. Pracovníci v informačních technologiích, telekomunikacích, dopravě a průmyslu měli průměrné znalosti. V práci byla také provedena analýza legislativy a osvěty o kybernetických hrozbách. Legislativa, až na zákon o kybernetické bezpečnosti je zaměřena spíše obecně a necílí přímo na kybernetické útoky. Posuzuje se spíše případ od případu. Osvěta směrem k populaci je více zaměřena na IT experty, kteří vědí, kde tyto informace hledat. Osvětu zaštiťuje Národní úřad pro kybernetickou bezpečnost, který informuje o aktuálních hrozbách a jejich možných dopadech. Dále Ministerstvo vnitra České republiky, Policie ČR a bankovní instituce. Jednou z otázek v dotazníkovém šetření bylo zjistit, jestli respondenti čtou zprávy z banky, neboť většina bank prostřednictvím těchto zpráv informuje i o kybernetických hrozbách, které se mohou týkat jejich klientů. Využívání těchto zpráv je ovšem i k marketingovým účelům, a proto je většina respondentů nečte. Bankovní instituce nabízejí i možné informace o jednotlivých útocích na svých stránkách. Policie ČR má k dispozici na svých stránkách velké množství testů a studijních materiálů pro širokou veřejnost, se zaměřením na základní a střední školy. V práci jsou navrženy možnosti zlepšení vzdělání s ohledem na věkové skupiny. Nejdůležitější je začít se vzděláváním už na základních školách, kde je možné vychovávat populaci, která bude mít podvědomí o kybernetických hrozbách, na jejichž základech se dá poté dále stavět. Důležité je informovat žáky o nástrahách internetu co nejdříve, aby se nestaly oběťmi sociálního či jiného útoku. Bohužel na základních školách není kybernetická bezpečnost v osnovách a chybí zde proškolený personál, který by mohl kybernetickou bezpečnost na základních školách vyučovat. Žáci se tedy k těmto informacím dostanou jen při vyvinutí své vlastní aktivity. V tomto případě by mohlo být řešením lepší proškolení učitelů základních škol a zařazení výuky o kybernetické bezpečnosti do učebních osnov. Další možností, jak lépe informovat veřejnost je prostřednictvím sociálních sítí, které by mohly informovat

o aktuálních hrozbách formou bannerů nebo oznámení, tak jak tomu bylo v době pandemie. Velmi účinným informačním médiem se mohou také stát bankovní instituce, které mají velký dosah mezi populaci, neboť v dnešní době používá internetové či mobilní bankovnictví téměř každý. Pokud budou více šířit osvětu a cílit na širší veřejnost, kterou by bylo možné zaujmout tímto tématem, zvýšilo by se tím podvědomí o kybernetických hrozbách. Přínos diplomové práce je v určení mezer ve vzdělání u populace v České republice a výstup, jakým směrem se zaměřit v případě šíření osvěty o kybernetických hrozbách. Mnoho respondentů mě po vyplnění dotazníku kontaktovalo a doptávalo se, jakým způsobem mají hledat informace o kybernetické bezpečnosti a hrozbách, jak se lépe chránit či jakým způsobem se chovat bezpečněji. Je tedy zřejmé, že pokud je téma podané zajímavým způsobem, lidé mají zájem se dále vzdělávat. Někteří respondenti uvedli, že si uvědomili, že se nechovají v kybernetickém prostředí bezpečně a že se vystavují potenciálnímu nebezpečí. Dalším přínosem bylo seznámení respondentů ze školství, kde vyhledávat informace pro studijní materiály pro žáky základních a středních škol, které mohou zařadit do svých hodin informatiky. Odezvy na poskytnuté materiály byly velmi pozitivní. Děti kvízy a hry bavily a zlepšilo to jejich podvědomí o kybernetické bezpečnosti a díky tomu budou ve výuce i nadále pokračovat.

SEZNAM POUŽITÉ LITERATURY

[1] Infografika – Nejzávažnější kybernetické hrozby v EU. *Rada Evropské unie: Generální sekretariát*[online]. 2021 [cit. 2022-04-08]. Dostupné z: https://www.consilium.europa.eu/cs/infographics/cyber-threats-eu/

[2] Hrozby: Hrozby kybernetické bezpečnosti. *ACS Office s. r. o.* [online]. 2022 [cit. 2022-04-08]. Dostupné z: https://acsoffice.cz/kyberneticka-bezpecnost/hrozby/

[3] Sociální inženýrství: Co je sociální inženýrství. *Avast* [online]. 2022 [cit. 2022-04-08]. Dostupné z: https://www.avast.com/cs-cz/c-social-engineering

[4] HÁJKOVÁ, Vladimíra. *Informační bezpečnost: Ochrana osobních údajů na internetu* [online]. 2016 [cit. 2022-04-08]. Dostupné z: https://docplayer.cz/2486770-Informacni-bezpecnost.html#show_full_text

[5] Phishing. *ESET* [online]. 2022 [cit. 2022-04-09]. Dostupné z: https://www.eset.com/cz/phishing/#jak-poznat-phishing-web

[6] 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.

[7] Spear phishing je cílený phishing, kterému se lze jen těžko bránit. *Clever Smart* [online]. 2012 [cit. 2022-04-09]. Dostupné z: https://www.cleverandsmart.cz/spear-phishing-je-cileny-phishing-kteremu-se-lze-jen-tezko-branit/

[8] DLP: Jak zabránit úniku citlivých informací. *Clever Smart* [online]. 2012 [cit. 2022-04-09]. Dostupné z: https://www.cleverandsmart.cz/dlp-jak-zabranit-uniku-citlivych-informaci/

[9] Malware. *Avast* [online]. 2022 [cit. 2022-04-09]. Dostupné z: https://www.avast.com/cs-cz/c-malware

[10] Umělá inteligence ve službách zločinu. *Computerworld* [online]. 2018 [cit. 2022-04-09]. Dostupné z: https://www.computerworld.cz/clanky/umela-inteligence-ve-sluzbach-zlocinu/

[11] Kybernetické hrozby v roce 2020 a dál. *ICTBLOG* [online]. 2020 [cit. 2022-04-09]. Dostupné z: https://www.ictblog.cz/kyberneticke-hrozby-v-roce-2020-a-dal/

[12] Internet v Česku slaví 30 let. Dnes ho používá 83 procent obyvatel. *Aktuálně.cz* [online]. 2022 [cit. 2022-04-09]. Dostupné z:

https://zpravy.aktualne.cz/ekonomika/internet-v-cesku-slavi-30-let-dnes-ho-pouziva-83-procent-oby/r~d03c50dc898511ecb5bd0cc47ab5f122/

[13] Realita je ještě podivnější než fikce, říká spisovatel a vynálezce slova kyberprostor William Gibson. *Radio Wave* [online]. 2022 [cit. 2022-04-09]. Dostupné z: https://wave.rozhlas.cz/realita-je-jeste-podivnejsi-nez-fikce-rika-spisovatel-a-vynalezce-slova-8135174

[14] CO JE INTERNET?. *IMIP* [online]. 2022 [cit. 2022-04-09]. Dostupné z: https://www.imip.cz

[15] Darkweb a Tor. *MUNI* [online]. 2022 [cit. 2022-04-09]. Dostupné z: https://kisk.phil.muni.cz/onlife/temata/vyhledavani-na-internetu/darkweb-a-tor

[16] Největší internetový černý trh přestal fungovat: Co stojí za jeho výpadkem? Jak se dostat na dark web? A co tam na vás čeká?. *Blog Avast* [online]. 2020 [cit. 2022-04-09]. Dostupné z: https://blog.avast.com/cs/pohled-do-hlubin-darknetu

[17] Jak se dostat bezpečně na Dark web z PC I mobilu?. *1T.cz* [online]. 2022 [cit. 2022-04-09]. Dostupné z: https://1t.cz/jak-se-dostat-bezpecne-na-dark-web/

[18] HARRIS, Shon, Allen HARPER, Chris EAGLE a Jonathan NESS. *Gray Hat Hacking: The Ethical Hacker's Handbook* [online]. Second Edition. 2008 [cit. 2022-04-15]. ISBN 978-00-7159-553-7.

[19] HÁK, Igor. *Moderní počítačové viry* [online]. Hradec Králové, 2005 [cit. 2022-04-15]. Dostupné z: https://viry.cz/downloadą/kniha.pdf

[20] Nejzajímavější počítačové viry - znáte je?. *CoolClub* [online]. [cit. 2022-04-15]. Dostupné z: https://club.coolpeople.cz/nejzajimavejsi-pocitacove-viry/1336.html

[21] POČÍTAČOVÉ VIRY, ČERVI A TROJSKÉ KONĚ. *Internetem bezpečně* [online]. 2018 [cit. 2022-04-15]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/malware/virus/

[22] Počítačové viry. *ÚVTMU zpravodaj* [online]. 2011 [cit. 2022-04-15]. Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/160.html

[23] Počítačový červ. *AVAST* [online]. 2020 [cit. 2022-04-15]. Dostupné z: https://www.avast.com/cs-cz/c-computer-worm

[24] Počítačové viry: Červ. *Viry* [online]. 2021 [cit. 2022-04-15]. Dostupné z: https://viry.estranky.cz/clanky/cerv.html

[25] 6 nejškodlivějších počítačových kódů. *21. Století* [online]. 2021 [cit. 2022-04-15]. Dostupné z: https://21stoleti.cz/2006/02/17/6-nejskodlivejsich-pocitacovych-kodu/

[26] What Is Stuxnet?. *McAfee* [online]. [cit. 2022-04-15]. Dostupné z: https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html

[27] První ransomware existoval už v roce 1989. Největší neplechu způsobil WannaCry. *Novinky.cz*[online]. 2017 [cit. 2022-04-15]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/prvni-ransomware-existoval-uz-v-roce-1989-nejvetsi-neplechu-zpusobil-wannacry-40038257

[28] Historie a vývoj ransomwaru: všechno to začalo s AIDS. *Lupa.cz* [online]. 2017 [cit. 2022-04-15]. Dostupné z: https://www.lupa.cz/clanky/historie-a-vyvoj-ransomwaru-vsechno-to-zacalo-s-aids/

[29] DEFINICE A TYPY MALWARU RANSOMWARE. *Glennbouchard* [online]. 2017 [cit. 2022-04-15]. Dostupné z: https://glennbouchard.com/cs/352-pengertian-dan-jenis-malware-ransomware.html

[30] Vše, co potřebujete vědět o ransomwaru a jak se před ním ochránit. *Avast blog* [online]. 2019 [cit. 2022-04-15]. Dostupné z: https://blog.avast.com/cs/co-je-ransomware

[31] Škodlivý kód WannaCry děsí i po letech, infikuje miliony systémů. *Novinky.cz* [online]. 2019 [cit. 2022-04-15]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/skodlivy-kod-wannacry-desi-i-po-letech-infikuje-miliony-systemu-40298574

[32] WannaCry impact on embedded OSs. *Honeywell* [online]. 2017 [cit. 2022-04-15]. Dostupné z: https://support.honeywellaidc.com/s/article/WannaCry-impact-on-embedded-OSs

[33] WannaCry. *Avast* [online]. 2022 [cit. 2022-04-15]. Dostupné z: https://www.avast.com/cs-cz/c-wannacry

[34] Threat Watch: New "SaveTheQueen" Ransomware Found. *Binary Defense* [online]. 2020 [cit. 2022-04-15]. Dostupné z: https://www.binarydefense.com/threat_watch/new-savethequeen-ransomware-found/

[35] Inside Out Security: A Queen's Ransom: Varonis Uncovers Fast-Spreading "SaveTheQueen" Ransomware. *Varonis* [online]. 2020 [cit. 2022-04-15]. Dostupné z: https://www.varonis.com/blog/save-the-queen-ransomware/

[36] Vyděračské viry: 10 nejvážnějších hrozeb, které představuje ransomware. *Živě.cz* [online]. 2020 [cit. 2022-04-15]. Dostupné z: https://www.zive.cz/clanky/vyderacske-viry-10-nejvaznejsich-hrozeb-ktere-predstavuje-ransomware/sc-3-a-202228/default.aspx#part=7

[37] CactusPete APT group's updated Bisonal backdoor. *SecureList by Kaspersky* [online]. 2020 [cit. 2022-04-15]. Dostupné z: https://securelist.com/cactuspete-apt-groups-updated-bisonal-backdoor/97962/

[38] Lazarus Hacking Group Strikes Again Using New Malware Variant "MATA". *CISOMAG* [online]. 2020 [cit. 2022-04-15]. Dostupné z: https://cisomag.eccouncil.org/mata-lazarus-hacking-group/

[39] Skupina Lazarus vyvíjí prostředky i pro útok na dodavatelské řetězce. *Network News* [online]. 2021 [cit. 2022-04-15]. Dostupné z: https://www.itsec-nn.com/skupina-lazarus-vyviji-prostredky-i-pro-utok-na-dodavatelske-retezce/

[40] Alert (AA21-048A):: AppleJeus: Analysis of North Korea's Cryptocurrency Malware. *Cybersecurity & Infrastructure Security Agency* [online]. 2021 [cit. 2022-04-15]. Dostupné z: https://us-cert.cisa.gov/ncas/alerts/aa21-048a

[41] JAMES, Lance. *Phishing bez záhad*. Praha: Grada, 2007. ISBN 978-80-247-1766-1.

[42] MITNICK, Kevin D. a William L. SIMON. *Umění klamu*. Gliwice: Helion, 2003. ISBN 83-7361-210-6.

[43] Příběhy sociálního inženýrství: Možná v nich také účinkujete... *MUNI* [online]. 2022 [cit. 2022-04-25]. Dostupné z: https://security.muni.cz/socialni_inzenyrstvi

[44] Techniky sociálního inženýrství. *KPCS* [online]. 2022 [cit. 2022-04-25]. Dostupné z: https://www.kpcs.cz/cs/novinky/blog/techniky-socialniho-inzenyrstvi.html

[45] What is a Whaling Attack?. *Kaspersky* [online]. 2022 [cit. 2022-04-25]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/what-is-a-whaling-attack

[46] What Is Pharming and How to Protect Yourself. *Kaspersky* [online]. 2022 [cit. 2022-04-25]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/pharming

[47] 15 top open-source intelligence tools: Find sensitive public info before the bad guys do. *CSO United States* [online]. 2021 [cit. 2022-04-26]. Dostupné z: https://www.csoonline.com/article/3445357/what-is-osint-top-open-source-intelligence-tools.html

[48] KOHOUT, Roman a Radek KARCHŇÁK. *Bezpečnost v online prostředí*. Karlovy Vary: Biblio Karlovy Vary, 2016. ISBN 978-80-260-9543-9.

[49] PRAVIDLO 3-2-1 PRO BEZPEČNÉ ZÁLOHOVÁNÍ. *Průvodce IT* [online]. 2021 [cit. 2022-04-27]. Dostupné z: https://www.pruvodce.it/blog-it-rady-a-navody/pravidlo-3-2-1-pro-bezpecne-zalohovani/

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

[51] Měřič síly hesla. *Hodza* [online]. 2021 [cit. 2022-04-27]. Dostupné z: https://hodza.net/password-meter/

[52] Jak vytvořit silné heslo - 7 zlatých pravidel. *VPN Mentor* [online]. 2021 [cit. 2022-04-27]. Dostupné z: https://cs.vpnmentor.com/blog/jak-vytvorit-silne-heslo-7-zlatych-pravidel/

[53] Anonymita a bezpečnost na internetu. *EO SECURITY* [online]. 2019 [cit. 2022-04-30]. Dostupné z: https://eo-security.cz/bezpecny-internet/?gclid=CjwKCAjwsJ6TBhAIEiwAfl4TWAj-gJD7e4UhVHsHuOyvSGyfax8O2cPoP-CFm5RU45XlZwy5RvHlyi6xoCksgQAvD_BwE

[54] ŠEVČÍKOVÁ, Anna. *Děti a dospívající online: vybraná rizika používání internetu*. Praha: Grada, 2014. Psyché (Grada). ISBN 978-80-210-7527-6.

[55] O čem se nejvíc lhalo na internetu? Přinášíme pět dezinformací roku. *Deník.cz* [online]. 2020 [cit. 2022-04-30]. Dostupné z: https://www.denik.cz/z_domova/top-pet-fakenews.html

[56] Dezinformace v online prostředí. *Vysvetli.cz* [online]. 2020 [cit. 2022-04-30]. Dostupné z: https://www.vysvetli.cz/fakenews

[57] HOAX. *Internetem bezpečně* [online]. 2018 [cit. 2022-04-30]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/hoax/#1491992524408-b2797c22-d9f471e4-e089412b-edf227c5-c79da29b-5208

[58] Kyberšikana seniorů: Co ohrožuje seniory na internetu?. *I-senior* [online]. 2022 [cit. 2022-04-30]. Dostupné z: https://www.i-senior.cz/kybersikana-senioru-co-ohrozuje-seniory-na-internetu/

[59] Kyberstalking. *Internetem bezpečně* [online]. 2018 [cit. 2022-04-30]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kyberstalking/

[60] Průzkum Avastu: Senioři čelí hrozbám v e-mailech, teenageři na TikToku. *Avast blog* [online]. 2021 [cit. 2022-04-30]. Dostupné z: https://blog.avast.com/cs/pruzkum-avastu-seniori-celi-hrozbam-v-e-mailech-teenageri-na-tiktoku

[61] Bezpečnost mobilních aplikací. *AEC* [online]. 2015 [cit. 2022-04-30]. Dostupné z: https://www.aec.cz/cz/ztisku/lukas-blaha-bezpecnost-mobilnich-aplikaci-dsm-2015.pdf

[62] Bankovní identita: Využijte snadný a bezpečný přístup k on-line službám. *CSAS* [online]. 2019 [cit. 2022-04-30]. Dostupné z: https://www.csas.cz/cs/o-nas/bezpecnost-ochrana- dat/bankovni-identita

[63] Dejte zelenou jednoduššímu přístupu k online službám. *AirBank* [online]. 2019 [cit. 2022-04-30]. Dostupné z: https://www.airbank.cz/produkty/bankovni-identita/

[64] Uživatelská příručka internetového a mobilního bankovnictví. *CSAS* [online]. 2019 [cit. 2022-04-30]. Dostupné z: https://www.csas.cz/static_internet/cs/Redakce/Ostatni/Ostatni_IE/Prilohy/up-george.pdf

[65] Jak si stáhnout a přihlásit se do mobilní aplikace George?. *CSAS* [online]. 2019 [cit. 2022-04-30]. Dostupné z: https://www.csas.cz/cs/caste-dotazy/jak-si-stahnout-a-prihlasit- se-do-mobilni-aplikace-george

[66] George klíč: Bezpečnější přihlašování i odesílání plateb. *CSAS* [online]. 2021 [cit. 2022-04-30]. Dostupné z: https://www.csas.cz/cs/mobilni-aplikace/george-klic

[67] Jak se přihlásit: Vyberte si způsob přihlašování do internetového bankovnictví. *KB* [online]. 2021 [cit. 2022-04-30]. Dostupné z: https://www.kb.cz/cs/podpora/jak-se-prihlasit

[68] KB Klíč. *KB* [online]. 2019 [cit. 2022-04-30]. Dostupné z: https://www.kb.cz/cs/pod- pora/slovnik/vyrazy-zacinajici-na-k/kb-klic

[69] Mobilní banka: Nejlepší mobilní bankovnictví, které používá více než 1 milion klientů. *KB* [online]. 2022 [cit. 2022-04-30]. Dostupné z: https://www.kb.cz/cs/mobilni-banka?os=iosx#iosx-Document-Ma-

[70] TRUSTEER RAPPORT. *KB* [online]. 2022 [cit. 2022-04-30]. Dostupné z: https://www.kb.cz/cs/bezpecnost/klient

[71] Air Bank v kapesním vydání. *AirBank* [online]. 2022 [cit. 2022-04-30]. Dostupné z: https://www.airbank.cz/produkty/mobilni-aplikace/

[72] ApplePay. *Apple* [online]. 2019 [cit. 2022-04-30]. Dostupné z: https://www.apple.com/cz/ap- ple-pay/

[73] Nastavte si aplikaci My Air jako bezpečný klíč k účtu. *AirBank* [online]. 2022 [cit. 2022-04-30]. Dostupné z: https://www.airbank.cz/bezpecny-klic-k-uctu/

[74] Z rozsáhlé analýzy mobilního bankovnictví vzešla Cena Finparády za rok 2019: Získala ji Komerční banka. *Finparada* [online]. 2020 [cit. 2022-04-30]. Dostupné z: https://finpa- rada.cz/6159-Z-rozsahle-analyzy-mobilniho-bankovnictvi-vzesla-Cena-Finpa- rady.aspx

[75] Legislativa KB. *NÚKIB* [online]. 2020 [cit. 2022-05-01]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

[76] Národní úřad pro kybernetickou a informační bezpečnost: Hrozby a zranitelnosti. *NÚKIB*[online]. 2022 [cit. 2022-05-06]. Dostupné z: https://www.nukib.cz/cs/infoservis/hrozby/

[77] DOKUMENTY - BEZPEČNOST A PREVENCE: Dokumenty – kybernetické hrozby. *MVCR* [online]. 2022 [cit. 2022-05-06]. Dostupné z: https://www.mvcr.cz/clanek/o-nas-bezpecnost-a-prevence-dokumenty-bezpecnost-a-prevence-dokumenty-kyberneticke-hrozby.aspx

[78] Safer Internet: SOCIÁLNÍ SÍTĚ. *Safer Internet* [online]. 2022 [cit. 2022-05-06]. Dostupné z: https://www.saferinternet.cz

[79] AKTUÁLNÍ HROZBY: NOVINKY Z BEZPEČNOSTI. *KB* [online]. 2022 [cit. 2022-05-06]. Dostupné z: https://www.kb.cz/cs/bezpecnost/aktualni-hrozby

[80] Podvody, které zrovna letí. *AirBank* [online]. 2022 [cit. 2022-05-06]. Dostupné z: https://www.airbank.cz/co-vas-nejvic-zajima/podvody-ktere-zrovna-leti/

[81] https://www.csas.cz/cs/zpravy-z-banky#/e14b7b/0/cz.csas.csas.aktuality.novinky.bezpecnost

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AI	Umělá inteligence (Artificial Intelligence).
IT	Informační technologie (Information Technology).
OS	Operační systém (Operating Systém).
IM	Komunikační program (Instant message).
IP	Protokol internetu (Internet Protocol).
PC	Osobní počítač (Personal Computer).
EU	Evropská Unie (European Union).
QR	Dvourozměrný, čárový kód (Quick Response).
CD	Kompaktní disk (Compact Disc).
GPS	Polohové zařízení (Global Positioning System).
NFC	Bezdrátová komunikace (Near Field Communication).
NIS	Síťový a informační systém (Network and Information Systems).
AVG	Antivirový ochránce (Anti Virus Guard).
SPZ	Státní poznávací značka.
IČO	Identifikační číslo osoby.
DIČ	Daňové identifikační číslo.
DVD	Disk digitálního videa (Digital Video Disc).
PIN	Osobní identifikační číslo (Personal Identification Number).
TLS	Kryptografický protokol pro zabezpečení (Transport Layer Security).
DNS	Protokol pro překlad názvů webových stránek (Domain Name System).
URL	Určení přesné identifikace na internetu (Uniform Resource Locator).
TCP	Protokol pro transportní vrstvu (Transmission Control Protocol).
WWW	Celosvětová komunikační síť (World Wide Web).
TOR	Program zajišťující anonymitu při pohybu na internetu (The Onion Router).
VPN	Virtuální privátní síť (Virtual Private Network).

USB	Univerzální sériová sběrnice (Universal Serial Bus).
PWS	Malware pro odcizení hesel (Password stealer).
IRC	Protokol pro textovou komunikaci (Internet Relay Chat).
MBR	Spouštěcí záznam v prvním sektoru (Master Boot Record).
SMS	Textová zpráva (Short Message Service).
API	Rozhraní pro komunikaci se software (Application Programming Interface).
DLL	Dynamicky linkovaná knihovna (Dynamic Link Library)
BAT	Spustitelný dávkový soubor (Batch File).
EXE	Spustitelný programový kód (ze slova EXEcutable).
EML	Přípona souboru emailu.
APT	Pokročilá perzistentní hrozba (Advanced Persistent Threat).
VBS	Visual Basic Script.
USA	Spojené státy americké (United States of America).
CIA	Ústřední zpravodajská služba (Central Intelligence Agency).
PCS	Systém řízení procesů (Process Control Systém).
PLC	Programovatelný logický automat (Programmable Logic Controller).
CVV	Číslicový kód pro autorizaci online plateb (Card Verification Code).
DLP	Prevence úniku dat (Data Loss Protection, Data Leak Prevention).
NBA	Systém prevence průniku (Network Behavior Analysis).
iOS	Mobilní operační systém společnosti Apple.
DDoS	Útok na internetové služby (Distributed Denial of Service Attack)
RaaS	Ransomware jako služba (Ransomware as a Service).
CIDR	Beztřídní směrování (Classless Inter Domain Routing).
SMTP	Protokol zajišťující rozesílku emailů (Simple Mail Transfer Protocol).
Wi-Fi	Komunikační standard pro bezdrátový přenos dat (Wireless Fidelity).
MVČR	Ministerstvo vnitra České republiky.

NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost.
HTTPS	Protokol zabezpečující komunikaci (Hypertext Transfer Protocol Secure).
OSINT	Zpravodajství z otevřených zdrojů (Open Source Intelligence).
C, C++	Kompilované programovací jazyky.
SCADA	Dispečerské řízení a sběr dat (Supervisory Control And Data Acquisition).
BOTNET	Velké množství infikovaných zařízení (Robot Network).
MILNET	Počítačová síť armády USA (Military Network).
USENET	Soustava vzájemně propojených uzlů (User's Network).
BITNET	Počítačová univerzitní síť (Because It's Time Network).
ARPANET	Předchůdce internetu (Advanced Research Projects Agency Network).
CAPTCHA	Označení pro automatická Turingův test, který slouží k odlišení počítačů od lidí (Completely Automated Public Turing test to tell Computers and Humans Apart).

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA PI: DOTAZNÍK SOCIÁLNÍ INŽENÝRSTVÍ

Sociální inženýrství

Dobrý den,

jmenuji se Romana Nováková a studuji pátým rokem Univerzitu Tomáše Bati ve Zlíně studijní program Informační technologie. Ráda bych Vás touto cestou požádala o vyplnění mého dotazníku Sociální inženýrství, který bude výhradně použit jako podklad pro mou Diplomovou práci a je zcela anonymní. Dotazník poslouží k výzkumu informací, které si uživatele vyměňují v kybernetickém prostoru, co na internetu nejčastěji dělají a závěrem rychlý kvíz . Vyplnění dotazníku zabere zhruba 15 minut a věřím, že Vás bude bavit.

Předem Vám velice děkuji, že jste ochotni dotazník vyplnit. A za Váš drahocenný čas. V případě dotazů, jsem k dispozici na emailu romana.novakova22@seznam.cz (mailto:romana.novakova22@seznam.cz).

* Povinné

1

Kolik je Vám let? *

- do 20 let
- 20 - 49 let
- 49 a výše

2

Jaké je Vaše pohlaví? *

- Žena
- Muž
- Jiné

3

Jaké je Vaše nejvyšší dosažené vzdělání? *

- Žák Základní školy
- Student SŠ
- Základní vzdělání
- Středoškolské vzdělání s výučním listem
- Středoškolské vzdělání s maturitou
- Vyšší odborné vzdělání
- Vysokoškolské vzdělání

4

Jaký je Váš pracovní status? *

- Zaměstnanec
- Podnikatel
- Student
- Důchodce
- Nezaměstnaný

5

Jaké je Vaše zaměření? *

- Školství
- Kultura
- Věda
- Gastronomie, pohostinství
- Průmysl, zemědělství
- Obchod, administrativa
- Zdravotnictví
- Doprava
- Informační technologie, telekomunikace
- Cestovní ruch
- Stavebnictví, strojírenství
- Nepracuji

6

Co nejčastěji děláte na internetu? (Můžete vybrat více možností) *

- [ ] Vyhledávání informací
- [ ] Čtení emailových zpráv
- [ ] Sociální sítě - Facebook, Instagram
- [ ] Internetové/ mobilní bankovnictví
- [ ] Platby na internetu (PayPal)
- [ ] Obsah pro dospělé
- [ ] Reklamní nabídky
- [ ] Nákupy
- [ ] Stahování filmů či software
- [ ] Hraní online her

7

Používáte antivirový program? Pokud ano, který? *

- ( ) Ano
- ( ) Ne

8

Jaký antivirový program používáte?

9

Používáte antivirový program i v mobilním zařízení? *

- Ano
- Ne

10

Software do svého zařízení...? (Můžete vybrat více možností) *

- Stahuji pomocí BitTorrentu
- Stahuji z oficiálních webu vydavatele
- Stahuji z uložišť jako je např. uložto
- Nestahuji

11

Za software...? (Můžete vybrat více možností) *

- [ ] Neplatím a využívám free verze
- [ ] Neplatím a stahuji software i licence
- [ ] Platím vydavateli
- [ ] Nestahuji software

12

Vlastníte bankovní účet? *

- ( ) Ano
- ( ) Ne

13

Používáte internetové či mobilní bankovnictví? *

- ( ) Ano
- ( ) Ne

14

Používáte aktivně svou platební kartu? *

- Ano, často
- Ano, jednou týdně
- Ne, platím spíše hotově
- Ne, nevlastním platební kartu

15

Používáte svou kartu bezkontaktně? Prostřednictvím mobilního telefonu - GooglePay, ApplePay či GarminPay? *

- Ano
- Ne

16

Čtete zprávy a upozornění z bank, které se zobrazují v internetovém bankovnictví? *

- Ano
- Ne

17

Sdílíte s někým Vaše přihlašovací údaje? *

- ○ Ano
- ○ Ne

18

S kým sdílíte Vaše přihlašovací údaje? (Můžete vybrat více možností) *

- ☐ Partner/Partnerka
- ☐ Rodiče/děti
- ☐ Kamarádi/sourozenci
- ☐ Přítel/přítelkyně
- ☐ Manžel/manželka
- ☐ S nikým své údaje nesdílím

19

Jaké přihlašovací údaje sdílíte? (Můžete vybrat více možností) *

- [ ] Do internetové/ mobilní bankovnictví
- [ ] Do počítače/ mobilního telefonu
- [ ] Do emailové pošty
- [ ] Do sociálních sítí - Facebook, Instagram
- [ ] Do herních účtů
- [ ] Do své Wi-Fi sítě
- [ ] Žádné údaje nesdílím

20

Používáte stejná hesla k přihlášení do více účtů? *

- ( ) Ano, výhradě používám stejné heslo
- ( ) Ano, používám kombinaci více hesel
- ( ) Ne, zřídka mám někde stejné heslo
- ( ) Ne, u všech účtů mám jiné heslo

21

Používáte dvoufaktorové zabezpečení? *

- Ano
- Ne
- Nevím co to znamená

22

Kolik znaků mají průměrně Vaše hesla? *

- 4 - 7 znaků
- 8 - 11 znaků
- 12 a více znaků

23

Při sestavování hesla používáte? *

- Pouze malá/ velká písmena
- Písmena + čísla
- Písmena + čísla + speciální znaky

24

Používáte password managera? *

- Ano
- Ne

25

Používáte generátor hesel? *

- Ano
- Ne

26

Otevíráte emaily ze spamového filtru ve Vašich emailových schránkách? *

- Ano, vždy
- Ano, občas, když je předmět zajímavý
- Ano, omylem
- Ne

27

Otevíráte emaily ze složky hromadné či ze složky ostatní ve Vaší emailové schránce? *

- Ano, vždy
- Ano, občas, když je předmět zajímavý
- Ano, omylem
- Ne

28

Otevíráte přílohy i od neznámých odesílatelů? *

- Ano, vždy
- Ano, občas, když je předmět zajímavý
- Ano, omylem
- Pouze po ověření odesílatele
- Ne, přílohy od neznámých odesílatelů neotvírám

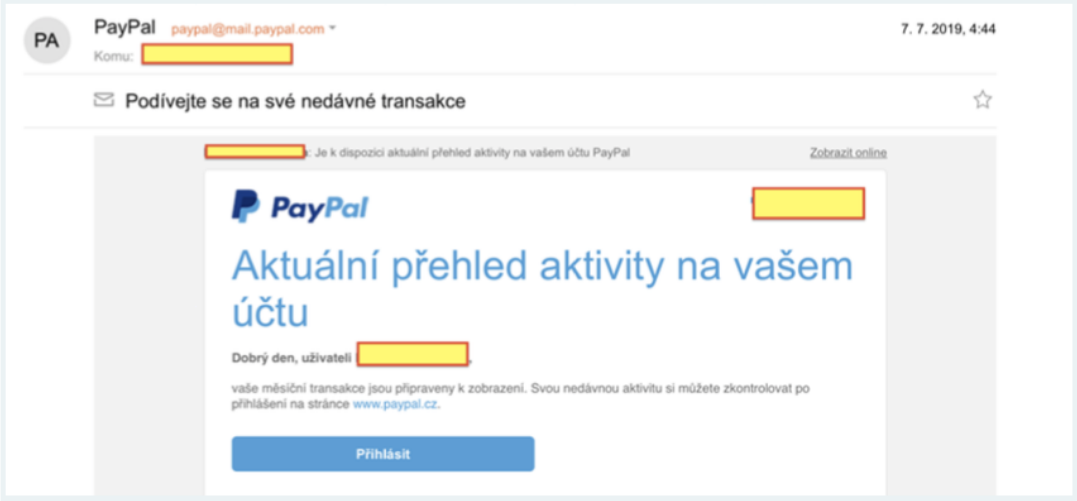
29

Jak byste se zachovali v případě doručení tohoto emailu? *

- Kliknu na odkaz, jedná se o legitimní email
- Mám dojem, že je email spam, proto jej jako spam nahlásím
- Email smažu a nikam klikat nebudu, jedná se o podvodný email
- Emailu si nebudu všímat

30

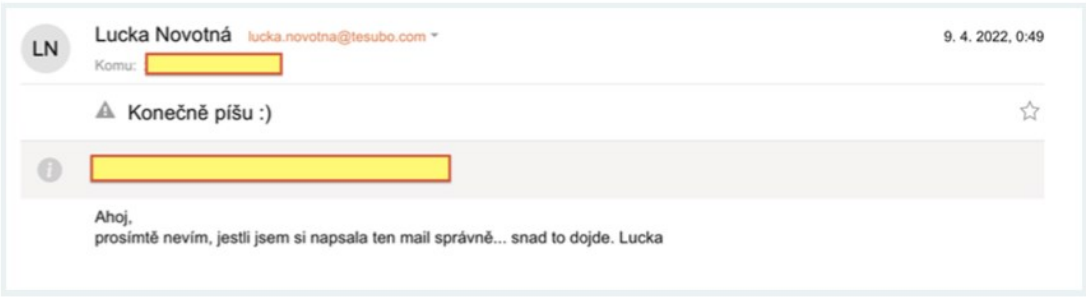
Jak byste se zachovali v případě doručení tohoto email? *



- Kliknu na odkaz, jedná se o legitimní email
- Mám dojem, že email je spam, proto jej jako spam nahlásím
- Email smažu a nikam klikat nebudu, jedná se o podvodný email
- Emailu si nebudu všímat

31

Jak byste se zachovali v případě doručení tohoto emailu? *



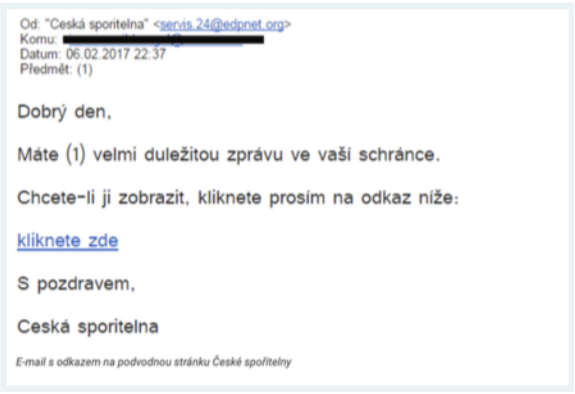
- Na email odpovím, jedná se o legitimní email
- Mám dojem, že se jedná o spam, proto jej jako spam nahlásím
- Email smažu, jedná se o podvodný email
- Emailu si nebudu všímat

32

Jak byste se zachovali v případě doručení tohoto emailu s přílohou? *

- ○ Kliknu na přiloženou přílohu pro více informací
- ○ Nahlásím email jako spam
- ○ Pokusím se nejprve ověřit pravost emailu
- ○ Email smažu a nikam klikat nebudu, jedná se o podvodný email

33



Jak byste se zachovali v případě doručení tohoto emailu? *

- ○ KLiknu na odkaz, jedná se o legitimní email
- ○ Mám dojem, že se jedná o spam, tak jej jako spam označím
- ○ Mám dojem, že se jedná o podvodnou zprávu a proto ji nahlásím bance
- ○ Email smažu

34

Pokud jste v předchozí odpovědi klikli na email, zobrazila se Vám tato stránka. Jak se zachováte? *

- Do kolonky zadám autorizační kód, který mi přišel na telefon, jedná se o legitimní stránku banky
- Nic zadávat nebudu, jedná se o spam
- Mám dojem, že se jedná o podvodnou stránku a proto ji nahlásím bance
- Stránku zavřu křížkem a nic dalšího dělat nebudu
- V předchozí otázce jsem na odkaz neklikl

35

Představte si situaci, kdy jste vyzváni k potvrzení či sdělení hesla. Jaké instituci heslo pro ověření sdělíte? (Můžete vybrat více možností) *

- [ ] Bance, pokud se jedná o telefonní hovor
- [ ] Mobilnímu operátorovi, pokud se jedná o telefonní hovor
- [ ] Bance, v případě ověření emailem
- [ ] Mobilnímu operátorovi, v případě ověření emailem
- [ ] Bance vždy heslo sdělím
- [ ] Mobilnímu operátorovi vždy heslo sdělím
- [ ] Nikdy nikomu své heslo nevyzradím

36

V jakém případě byste klikli na odkaz v emailu? (Můžete vybrat více možností) *

- [ ] Od banky
- [ ] Od mobilního operátora
- [ ] Od finančního úřadu
- [ ] Od pojišťovny
- [ ] Od známého, důvěryhodného zdroje
- [ ] Na žádný odkaz bych nikdy neklikl

37

Stahujete filmy? (Můžete vybrat více možností) *

- [ ] Ano, z legitimních webů jako je uložto.cz, prehrajto apod, kde za stažení platím
- [ ] Ano, z BitTorrentu
- [ ] Ne, filmy sleduji online
- [ ] Ne

38

Představte si situaci, že jste obdrželi dotazník od své bankovní instituce. Které údaje bance vyplníte? (Můžete vybrat více možností) *

- [ ] Jméno a příjmení
- [ ] Datum narození
- [ ] Emailovou adresu a telefonní číslo
- [ ] Rodné číslo, číslo občanského průkazu
- [ ] IČO, DIČ firmy
- [ ] Dosažené vzdělání
- [ ] Adresu
- [ ] Číslo účtu
- [ ] Číslo platební karty
- [ ] Heslo do internetového bankovnictví
- [ ] Rodinný stav
- [ ] Náboženskou příslušnost
- [ ] Číslo řidičského průkazu a SPZ vozidla
- [ ] Žádné informace nevyplním

39

Co si představíte pod pojmem PHISHING? *

- Jedná se o anglický výraz rybaření
- Jedná se o podvodnou metodu, kdy příjemce obdrží nepravý email, který se snaží vylákat z něj má vylákat údaje
- Jedná se o výraz, který se používá v případě, že někdo chytá ryby na černo - pytlačí
- Výraz nemá speciální význam

40

Co si představíte pod pojmem PHARMING? *

- Jedná se o anglický výraz pro farmaření
- Jedná se o herní výraz, kdy hráč jde sklízet svou zahrádku
- Jedná se o podvodnou metodu, kdy je uživatel přesměrován na podvodnou stránku, která z něj má vylákat údaje
- Výraz nemá speciální význam

41

Co si představíte pod pojmem WHALING? *

- Jedná se o anglický výraz pro lov velryb
- Jedná se o podvodnou metodu, která se zaměřuje na vysoce postavenou osobu v určité společnosti
- Jedná se o výraz z českého jazyka, odvozeného od slova válet se - něco jako gaučing
- Výraz nemá speciální význam

42

Co si představíte pod pojmem TROJSKÝ KŮŇ? *

- Trojský kůň byl použit k vniknutí Řeků do Troji.
- Je to druh koně, který pochází z Troje
- Jedná se o typ viru, který vypadá jako legitimní software, ale uvnitř sebe ukrývá škodlivý kód.
- Výraz nemá speciální význam

43

Co si představíte pod pojmem HOAX? *

- Jedná se o zprávu, která má za úkol příjemce vystrašit a šířit paniku
- Je to zaručeně pravá zpráva, kterou je potřeba rozšířit
- Je to žertovná zpráva, určitý typ vtipu
- Výraz nemá speciální význam

44

Co si představíte pod pojmem WORM? *

- Jedná se o postavičku z legendární hry WORMS, oblíbené v 90. letech minulého století
- Je to speciální kód, který je schopen automatického množení a rozesílání prostřednictvím počítačové sítě
- Jedná se o speciální typ červa, který se používá při chytání velkých ryb
- Výraz nemá speciální význam

45

Co si představíte pod pojmem RANSOMWARE? *

- Jedná se o speciální typ viru, který po napadení počítače, zablokuje jeho obsah a po uživateli vyžaduje výkupné za odblokování obsahu
- Je to typ žertovného programu, který se chová náhodně
- Je to software, který je uživatelům k dispozici zdarma po určité časové období
- Výraz nemá speciální význam

46

Co si představíte pod pojmem COOKIE? *

- Je to soubor, který si ukládají webové stránky o návštěvě uživatele
- Jsou to křupavé sušenky s čokoládou
- Jedná se o typ počítačového viru
- Výraz nemá speciální význam

47

Co si představíte pod pojmem ZOMBIE? *

- Jedná se o označení z filmů pro nemrtvého
- Je to napadený počítač, ze kterého mohou být vzdáleně prováděny počítačové útoky
- Tímto výrazem se označuje zastaralý software
- Výraz nemá speciální význam

48

Co si představíte pod pojmem DARKWEB? *

- Jedná se o část internetu, která není indexována a je dostupná pouze s použitím speciálního software
- Jedná se internetové stránky, které jsou běžně dostupné, ale je na nich uveden nelegální obsah
- Je funkcionalita webového prohlížeči, který uživateli umožňuje nastavení tmavého režimu
- Výraz nemá speciální význam

PŘÍLOHA PII: VYHODNOCENÍ DOTAZNÍKU

Vyhodnocení dotazníku s ohledem na bezpečné chování uživatelů v internetovém prostředí - rozřazení dle věku respondentů.				
Vybranné otázky dotazníku, které mají za úkol vyzkoumat, která skupina se na internetu pohybuje bezpečněji.	**Předmět zkoumání u dané otázky a její vliv (pozitivní/negativní) na bezpečnost.**	**Skupina do 20 let - 33 respondentů**	**Skupina 20 - 49 let - 94 respondentů**	**Skupina nad 49 let - 18 respondentů**
Používáte antivirový program?	Kladná odpověď - ANO	70%	64%	**83%**
Software do svého zařízení...?	Bezpečnostní pochybení - stahování z BitTorrent - negativní dopad.	**24%**	5%	0%
Stahování filmů.	Stahování z BitTorrentu - negativní dopad.	**12%**	10%	0%
Za software...?	Nelegální stahování software - negativní dopad.	**42%**	27%	6%
Čtete zprávy a upozornění z banky?	Negativní dopad - nečte.	27%	26%	**33%**
Sdílíte s někým Vaše přihlašovací údaje?	Negativní dopad - sdílí přihlašovací údaje.	**24%**	19%	11%
Jaké přihlašovací údaje sdílíte?	Žádné údaje uživatelé nesdílí - pozitivní dopad.	51%	54%	**72%**
Používáte stejná hesla k přihlášení do více účtů?	Použití stejných/podobných hesel - negativní dopad.	**6% / 72%**	**8,5% / 61%**	5,5% / 50%
Používáte dvoufaktorové zabezpečení?	Nepoužívání 2FA zabezpečení/nevím, co to je - negativní dopad.	9% / 6%	**18% / 13%**	**17% / 44%**
Kolik znaků mají průměrně Vaše hesla?	4-7 znaků - negativní dopad.	**6%**	5%	0%
Kolik znaků mají průměrně Vaše hesla?	Více jak 12 znaků - pozitivní dopad	**51%**	23%	11%
Otevíráte emaily ze spamového filtru?	ANO - bezpečnostní riziko - negativní dopad.	21%	10%	**22%**
Otevíráte přílohy i od neznámých odesílatelů?	ANO - bezpečnostní riziko - negativní dopad.	12%	9%	**28%**
Chování uživatele v případě doručení určitých emailů.	Všechny emaily správně identifikované - pozitivní	9%	10%	**17%**
Chování uživatele v případě doručení určitých emailů.	Špatná identifikace emailů - chybovost - negativní dopad.	21%	15%	**22%**
Jaké instituci heslo pro ověření sdělíte?	Uživatel heslo sdělí - negativní dopad.	**24%**	10,5%	11%
V jakém případě byste klikli na odkaz v emailu?	Uživatelé, kteří na odkaz vždy kliknout - negativní dopad.	**42%**	29%	33%
V jakém případě byste klikli na odkaz v emailu?	Uživatelé nikdy na odkazy v emailech neklikají - pozitivní.	6%	15%	**17%**
Které údaje bance vyplníte?	Uživatelé bance žádné údaje nesdělí -pozitivní dopad.	21%	45%	**67%**
Závěrečný kvíz.	Všechny odpovědi správně - pozitivní dopad.	**45%**	37%	28%
	Celkové skóre	**-9 bodů**	**3 body**	**4 body**

Vyhodnocení dotazníku s ohledem na bezpečné chování uživatelů v internetovém prostředí - rozřazení dle nejvyššího dosaženého vzdělání.				
Vybranné otázky dotazníku, které mají za úkol vyzkoumat, která skupina se na internetu pohybuje bezpečněji.	**Předmět zkoumání u dané otázky a její vliv (pozitivní/negativní) na bezpečnost.**	**Základní vzdělání - 5 respondentů**	**Středoškolské vzdělání - 86 respondentů**	**Vysokoškolské vzdělání - 54 respondentů**
Používáte antivirový program?	Kladná odpověď - ANO	**100%**	66%	67%
Software do svého zařízení...?	Bezpečnostní pochybení - stahování z BitTorrent - negativní dopad.	**20%**	14%	0%
Stahování filmů.	Stahování z BitTorrentu - negativní dopad.	**20%**	12%	4%
Za software...?	Nelegální stahování software - negativní dopad.	20%	27%	**30%**
Čtete zprávy a upozornění z banky?	Negativní dopad - nečte.	20%	**28%**	26%
Sdílíte s někým Vaše přihlašovací údaje?	Negativní dopad - sdílí přihlašovací údaje.	**40%**	20%	17%
Jaké přihlašovací údaje sdílíte?	Žádné údaje uživatelé nesdílí - pozitivní dopad.	40%	55%	**59%**
Používáte stejná hesla k přihlášení do více účtů?	Použití stejných/podobných hesel - negativní dopad.	20% / 40%	**7% / 63%**	6% / 63%
Používáte dvoufaktorové zabezpečení?	Nepoužívání 2FA zabezpečení/nevím, co to je - negativní dopad.	0% / 20%	**16% / 16%**	17% / 11%
Kolik znaků mají průměrně Vaše hesla?	4-7 znaků - negativní dopad.	**40%**	5%	2%
Kolik znaků mají průměrně Vaše hesla?	Více jak 12 znaků - pozitivní dopad	**40%**	34%	19%
Otevíráte emaily ze spamového filtru?	ANO - bezpečnostní riziko - negativní dopad.	**60%**	15%	7%
Otevíráte přílohy i od neznámých odesílatelů?	ANO - bezpečnostní riziko - negativní dopad.	**40%**	13%	7%
Chování uživatele v případě doručení určitých emailů.	Všechny emaily správně identifikované - pozitivní dopad.	**20%**	11%	9%
Chování uživatele v případě doručení určitých emailů.	Špatná identifikace emailů - chybovost - negativní	**40%**	20%	19%
Jaké instituci heslo pro ověření sdělíte?	Uživatel heslo sdělí - negativní dopad.	**40%**	15	9%
V jakém případě byste klikli na odkaz v emailu?	Uživatelé, kteří na odkaz vždy kliknout - negativní dopad.	**60%**	34%	28%
V jakém případě byste klikli na odkaz v emailu?	Uživatelé nikdy na odkazy v emailech neklikají -	**20%**	12%	15%
Které údaje bance vyplníte?	Uživatelé bance žádné údaje nesdělí -pozitivní dopad.	0%	42%	**46%**
Závěrečný kvíz.	Všechny odpovědi správně - pozitivní dopad.	40%	35%	**43%**
	Celkové skóre	**-3 body**	**-6 bodů**	**9 bodů**

Vyhodnocení dotazníku s ohledem na bezpečné chování uživatelů v internetovém prostředí - rozřazení dle pracovního zaměření								
Vybranné otázky dotazníku, které mají za úkol vyzkoumat, která skupina se na internetu pohybuje bezpečněji.	**Předmět zkoumání u dané otázky a její vliv (pozitivní/negativní) na bezpečnost.**	**Nepracující - 13**	**IT a Telekomunikace - 55**	**Školství a Kultura - 12**	**Gastronomie a pohostinství - 4**	**Průmysl a Doprava- 18**	**Obchod a Administrativa - 35**	**Zdravotnictví - 8**
Používáte antivirový program?	Kladná odpověď - ANO	69%	71%	75%	50%	66%	63%	62%
Software do svého zařízení...?	Bezpečnostní pochybení - stahování z BitTorrent - negativní dopad.	15%	9%	17%	0%	11%	6%	0%
Stahování filmů.	Stahování z BitTorrentu - negativní dopad.	0%	15%	8%	0%	5%	9%	0%
Za software...?	Nelegální stahování software - negativní dopad.	30%	35%	33%	25%	17%	20%	13%
Čtete zprávy a upozornění z banky?	Negativní dopad - nečte.	60%	24%	17%	25%	17%	29%	25%
Sdílíte s někým Vaše přihlašovací údaje?	Negativní dopad - sdílí přihlašovací údaje.	7%	22%	33%	25%	11%	8%	62%
Jaké přihlašovací údaje sdílíte?	Žádné údaje uživatelé nesdílí - pozitivní dopad.	69%	53%	50%	25%	56%	69%	25%
Používáte stejná hesla k přihlášení do více účtů?	Použití stejných/podobných hesel - negativní dopad.	15% / 54%	4% / 69%	8% / 50%	25% / 25%	0% / 78%	11% / 57%	12,5% / 50%
Používáte dvoufaktorové zabezpečení?	Nepoužívání 2FA zabezpečení/nevím, co to je - negativní dopad.	7,5% / 30%	13% / 0%	8% / 50%	0% / 25%	28% / 0%	20% / 29%	25% / 12,5%
Kolik znaků mají průměrně Vaše hesla?	4-7 znaků - negativní dopad.	8%	0%	17%	0%	11%	6%	0%
Kolik znaků mají průměrně Vaše hesla?	Více jak 12 znaků - pozitivní dopad	38%	45%	25%	25%	11%	6%	37%
Otevíráte emaily ze spamového filtru?	ANO - bezpečnostní riziko - negativní dopad.	23%	15%	17%	0%	11%	11%	13%
Otevíráte přílohy i od neznámých odesílatelů?	ANO - bezpečnostní riziko - negativní dopad.	15%	5%	25%	25%	17%	8,50%	25%
Chování uživatele v případě doručení určitých emailů.	Všechny emaily správně identifikované - pozitivní dopad.	0%	9%	8%	25%	11%	14%	13%
Chování uživatele v případě doručení určitých emailů.	Špatná identifikace emailů - chybovost - negativní	23%	18%	17%	25%	17%	20%	25%
Jaké instituci heslo pro ověření sdělíte?	Uživatel heslo sdělí - negativní dopad.	23%	11%	25%	50%	6%	11%	13%
V jakém případě byste klikli na odkaz v emailu?	Uživatelé, kteří na odkaz vždy kliknout - negativní dopad.	23%	38%	33%	50%	33%	23%	38%
V jakém případě byste klikli na odkaz v emailu?	Uživatelé nikdy na odkazy v emailech neklikají - pozitivní.	8%	11%	25%	0%	11%	17%	13%
Které údaje bance vyplníte?	Uživatelé bance žádné údaje nesdělí -pozitivní dopad.	38%	33%	50%	25%	39%	60%	37%
Závěrečný kvíz.	Všechny odpovědi správně - pozitivní dopad.	30%	51%	25%	0%	17%	46%	13%
	Celkové skóre	**52 bodů**	**66 bodů**	**53 bodů**	**49 bodů**	**58 bodů**	**70 bodů**	**53 bodů**