Univerzita Palackého v Olomouci

Fakulta tělesné kultury

Fakulta
tělesné kultury

KYBERNETICKÁ BEZPEČNOST U ŽÁKŮ ZÁKLADNÍCH ŠKOL

Diplomová práce

Autor: Bc. Jiří Odvářka

Studijní program: Ochrana Obyvatelstva

Vedoucí práce: Mgr. František Chmelík

Olomouc 2023

Bibliografická identifikace

Jméno autora: Bc. Jiří Odvářka
Název práce: Kybernetická bezpečnost u žáků základních škol

Vedoucí práce: Mgr. František Chmelík, Ph.D
Pracoviště: Institut aktivního životního stylu
Rok obhajoby: 2023
Abstrakt:

Diplomová práce pojednává o aktuálních celosvětových kybernetických hrozbách a způsobech napadení v kybernetickém prostoru.
V teoretické části se diplomová práce zaměřuje na přehledné charakterizování technik sociálního inženýrství a zasazuje je do aktuální doby.
V části praktické se diplomová práce zabývá dvěma skupinami studentů, přičemž jedna skupina se zúčastnila školení kybernetické bezpečnosti a druhá nikoliv.
Hlavním cílem diplomové práce bylo zmapovat a popsat povědomí a chování studentů v oblasti kybernetické bezpečnosti a zhodnotit dopad vzdělávací intervence na zlepšení jejich ochrany proti kybernetickým útokům.
Z výsledků práce je zřejmé, že dostatek informací v oblasti kybernetické bezpečnosti předávané prostřednictvím školních přednášek jsou klíčové pro bezpečný pohyb v kyberprostoru, přičemž zaznamenaný rozdíl u obou skupin byl největší v oblasti síťové bezpečnosti.
Výstupem je také pochopení úzce profilované problematiky, která se týká získávání dat uživatele prostřednictvím nejnovějších technik a snaha o zvýšení povědomí při pohybování se v kyberprostoru.

Klíčová slova:
phishing, baiting, pretexting, kybernetická bezpečnost, anonymita, malware, sociální inženýrství

Bibliographical identification

Author: Bc. Jiří Odvářka

Title: Cyber security and primary schools pupils

Supervisor: Mgr. František Chmelík, Ph.D.

Department: Institute of Active Lifestyle

Year: 2023

Abstract:

The diploma thesis discusses current global cyber-threats and methods of attack in cyberspace.
In the theoretical part, the thesis focuses on the clear characterization of social engineering techniques and places them in the current era.
In the practical part, the thesis deals with two groups of students, with one group participating in cyber security training and the other not.
The main goal of the thesis was to map and describe the awareness and behavior of students in the field of cyber security and to evaluate the impact of an educational intervention on improving their protection against cyber-attacks.
From the results of the work, it is clear that enough information in the field of cyber security transmitted through school lectures is key for safe movement in cyberspace, while the recorded difference between the two groups was the largest in the area of network security.
The output is also an understanding of a narrowly profiled issue that concerns the acquisition of user data through the latest techniques and an effort to increase awareness when moving in cyberspace.

Keywords:
phishing, baiting, pretexting, cyber security, anonymity, malware, social engineering

Prohlašuji, že jsem tuto práci zpracoval samostatně pod vedením Mgr. Františka Chmelíka, Ph.D., uvedl všechny použité literární a odborné zdroje a dodržoval zásady vědecké etiky.

V Olomouci dne 26. června 2023

.....

Tímto bych chtěl poděkovat vedoucímu mé diplomové práce Mgr. Františkovi Chmelíkovi, PhD. za odborné vedení, poskytnutí cenných rad a připomínek, které jsem využil při její tvorbě.

OBSAH

Obsah 7
1 Úvod 9
2 Přehled poznatků 10
2.1 Kybernetické prostředí 10
2.1.1 Rozdělení kyberprostoru 11
2.2 Kybernetická bezpečnost 11
2.3 Kybernetická kriminalita (IT crime, cybercrime) 12
2.4 Sociální inženýrství 13
2.5 Typy útočníků a lokace 14
2.5.1 Typy útočníků 15
2.5.2 Lokace útočníků 17
2.6 Kybernetická bezpečnost za éry Covid-19 17
2.7 Sociální inženýrství a jeho metody 19
2.7.1 Phishing 19
2.7.2 Pharming 26
2.7.3 Baiting 27
2.7.4 Quid Pro Quo 28
2.7.5 Tailgating 29
2.7.6 Pretexting 29
2.8 Anonymita 30
2.8.1 IP adresy a veřejný wi-fi 30
2.8.2 Man-in The-Middle Attack 30
2.8.3 Malware 31
2.8.4 Evil Twin Attacks 32
2.8.5 Způsoby zabezpečení na veřejné síti 32
2.8.6 Chování na veřejné síti 33
2.9 Vliv kybernetických hrozeb na mládež 35
3 Cíle 36
3.1 Hlavní cíl 36

3.2 Dílčí cíle 36
3.3 Výzkumné otázky 36
4 Metodika 37
4.1 Výzkumný soubor 38
4.2 Metody sběru dat 38
4.3 Statistické zpracování dat 39
5 Výsledky 40
6 Diskuse 52
7 Závěry 57
8 Souhrn 58
9 Summary 60
10 Referenční seznam 62

1 ÚVOD

Informační a komunikační technologie a s nimi často spojovaná bezpečnost není pouze trend aktuální doby, ale také téměř nutnost každého jedince porozumět principům kybernetického prostředí.

Rychle rostoucí technologická doba do určité míry usnadňuje a zrychluje práci v každodenním životě, ale s ní se pojí i vysoké kybernetické trestné činnosti a následné riziko úniku dat, které mohou být pro většinu uživatelů klíčové. Vznikají nové typy zařízení a celosvětová síť internet se neustále zrychluje.

Není tomu tak dávno, kdy připojení k internetu bylo doménou pouze dospělých lidí a v domácnosti se vyskytoval pouze jeden tzv. „rodinný počítač“. Skokem se dostáváme do doby, kdy si prakticky nikdo nedokáže představit běžný den bez zařízení, které je permanentně připojeno k internetu.

Nejvíce ohroženou skupinou, která se může stát terčem počítačové kriminality nebo jakékoli kybernetické formy napadení v kyberprostoru jsou děti. Ty už prakticky považují připojený mobilní telefon jako úplnou samozřejmost.

Ve své bakalářské práci jsem dospěl k závěru, že běžná populace není ve využívání informačních a komunikačních technologií na úrovni, které vyžadují základní znalosti z oblasti kybernetické bezpečnosti. V tomto okamžiku chci navázat svou diplomovou prací v okamžiku, kdy mým výzkumným problémem bude srovnání dvou skupin uživatelů ve věku 13-14 let, kdy jedna ze skupin projde školením pro kybernetickou bezpečnost a úkolem je tedy zjistit, zda má školení v tomto bezpečnostním směru určitý smysl či nikoli.

Svět v éře Covid-19 se neúprosně přibližuje celkové digitalizaci různých aspektů života. Stále více jsme nuceni se spoléhat na počítačové systémy, díky kterým jsme schopni komunikovat, nakupovat nebo sdílet informace a mírnit tak dopad absence sociálního kontaktu.

2 PŘEHLED POZNATKŮ

2.1 Kybernetické prostředí

Kybernetické prostředí (kyberprostor – převzato z anglického cyberspace) je souhrnný termín, který zahrnuje široké spektrum souvisejících konceptů, technologií a praktik v oblasti kybernetiky. V zásadě se jedná o virtuální svět, který se skládá z počítačových systémů, sítí, dat a aplikací propojených pomocí globálního internetu. Kybernetické prostředí je jedinečné svým rychlým rozvojem, neustálou inovací a narůstajícím dopadem na společnost, ekonomiku a politiku (Carr, 2016; Libicki, 2015).

Jednou z klíčových charakteristik kybernetického prostředí je jeho nehmotnost. To znamená, že se jedná o prostředí, které nemá fyzickou existenci, ale ovlivňuje naše každodenní životy prostřednictvím technologií a služeb, které využíváme (DeNardis, 2014). Díky této nehmotnosti může být kyberprostor vnímán jako prostor, který je nezávislý na geografických hranicích, což vytváří možnosti pro globální komunikaci a spolupráci (Zetter, 2014).

Kybernetické prostředí zahrnuje širokou škálu aktérů, od jednotlivců, firem a organizací až po státy a mezinárodní organizace. Je důležité zdůraznit, že kyberprostor je otevřený prostor, který umožňuje snadný přístup a interakci mezi aktéry, ale zároveň představuje potenciální rizika a hrozby pro uživatele a infrastrukturu (Lewis, 2014; Nakashima, 2015).

V důsledku těchto hrozeb se stává kybernetická bezpečnost klíčovou oblastí pro všechny aktéry v kyberprostoru. Kybernetická bezpečnost se zaměřuje na ochranu informačních systémů, sítí a dat před neautorizovaným přístupem, zneužitím, útoky nebo poškozením. To zahrnuje širokou škálu praktik, technologií a strategií, jako je prevence, detekce a reakce na kybernetické útoky, zajištění datového soukromí a ochrany osobních údajů, a rozvoj zákonných a politických rámců pro řešení kybernetických hrozeb (Gartzke, 2013; Morgan et al.,2017).

V rámci kybernetického prostředí je také důležité zdůraznit roli kybernetického zločinu, který představuje nelegální aktivity prováděné v kyberprostoru. Kybernetický zločin zahrnuje širokou škálu činností, jako je například krádež identity, finanční podvody, šíření malwaru, ransomware útoky, a další. V boji proti kybernetickému zločinu hraje klíčovou roli spolupráce mezi veřejným a soukromým sektorem, včetně výměny informací a zkušeností (Guitton, 2017; Kleemola, 2018).

2.1.1 Rozdělení kyberprostoru

V dokumentu Cyberspace Operations: Concept Capability Plan se kyberprostor rozděluje do třech vrstev:

1) Fyzická vrstva zahrnuje geografickou složku a fyzickou síť komponent. Geografickou složkou je myšleno konkrétní umístění síťových prvků ve fyzickém prostředí. Fyzickou síť komponent je pak myšlena infrastruktura, tedy kabely, síťové prvky a ostatní zařízení. Zatímco v kyberprostoru lze geopolitickou hranici překročit rychlostí blížící se rychlostí světla, tak v reálném světě existuje spousta omezení, která vyplývají z podstaty fyzického světa.
2) Logická vrstva sestává z komponent logické sítě, kterými jsou myšlena spojení síťových uzlů. Síťovými uzly se rozumí jakákoli zařízení připojená k počítačové síti.
3) Sociální vrstva je rozdělena na kyberosobnost a osobnost. Základním pravidlem je fakt, že jedna osobnost může mít více kybernetických osobností.

Jednodušší formou lze kyberprostor definovat jako celek, který se skládá ze služeb, dat, uživatelů a PC systémů, které se vyskytují ve virtuální prostoru. Hranice nejsou omezeny jako ve fyzickém světě, z čehož vyplývá, že nejúčinnější metodou je souhra státní správy a bezpečnostních složek na mezinárodní úrovni, které jsou podporovány vývojáři informačních a komunikačních technologií.

2.2 Kybernetická bezpečnost

Dle Itgoverance (2021) je kybernetická bezpečnost aplikování technologií, procesů a kontrol k ochraně systémů, sítí, programů, zařízení a dat před kybernetickými útoky. Základní složkou kybernetické bezpečnosti je identifikace, vyhodnocování a realizace reakcí na bezpečnostní události a incidenty.

Dle serveru vláda.cz lze kybernetickou bezpečnost charakterizovat jako celkovou ochranu sítí před kybernetickými útoky a hrozbami, aby byla zachována bezpečnost informací.

Pojem kybernetická bezpečnost se často zaměňuje s pojmem informační bezpečnost. Dle dokumentu *From information security to cyber security* se kybernetická bezpečnost a informační bezpečnost výrazně překrývá a tyto dva koncepty nejsou zcela analogické. Z dokumentu vyplývá, že kybernetická bezpečnost překračuje hranice tradiční informační bezpečnosti a zahrnuje nejen ochranu informačních zdrojů, ale i dalších aktiv, včetně člověka samotného. V kybernetické

bezpečnosti má tento faktor další rozměr a tím je člověk jako potenciální cíl kybernetického útoku, a to včetně nevědomé účasti na kybernetickém útoku. Tento faktor má etické důsledky pro společnost, protože ochranu určitých zranitelných skupin, např. dětí, lze považovat za společenskou odpovědnost.

Vzhledem k celosvětovému rozvoji informačních a komunikačních technologií se dostávají tyto technologie do popředí a jsou terčem zpravodajských služeb po celém světě. Bohatý rozvoj technologií s sebou nese plnou řadu výhod, ale i sním spjatá rizika a stále nové hrozby, které jsou monitorovány právě bezpečnostními institucemi.

Alazaba a Broadhursta (2013) Educating children about the risks of the digital environment: a case study of the ThinkUKnow program je článek, který zkoumá vzdělávací program pro děti, který se zaměřuje na rizika spojená s digitálním prostředím, včetně hackingu, ransomware a obsahu na deepwebu. Je vytvořený britskou agenturou pro ochranu dětí CEOP (Child Exploitation and Online Protection Centre). Cílem programu je vzdělávat děti, rodiče a učitele o rizicích spojených s používáním internetu a poskytovat praktické rady a podporu pro bezpečnější online chování. Některé z hlavních zjištění studie zahrnují:

i. Děti, které se zúčastnily programu *ThinkUKnow*, měly lepší povědomí o rizicích spojených s používáním internetu a byly schopny identifikovat potenciálně nebezpečné situace.
ii. Vzdělávací materiály byly považovány za atraktivní a zajímavé pro žáky, což přispělo k jejich angažovanosti a učení.
iii. Rodiče a učitelé považovali program za užitečný zdroj informací a podpory pro zlepšení kybernetické bezpečnosti ve školním prostředí.

2.3 Kybernetická kriminalita (IT crime, cybercrime)

V posledních letech se kyberkriminalita stala jednou z nejrychleji rostoucích oblastí kriminality. Nové technologie přináší nové příležitosti právě v oblasti kyberkriminality a stávají se stále sofistikovanějšími. V důsledku toho se jednotlivci, korporace i vlády ocitají tváří v tvář mnoha hrozbám kybernetické kriminality, které začínají na nejjednodušším způsobu narušení soukromí a sahají až po různé typy hackingu či ransomware.

Někteří z kybernetických útočníků páchající tyto trestné činy používají tzv. DeepWeb, ke kterému běžný uživatel nemá přístup a často nemá zdání o jeho existenci. O samotné téma

DeepWeb jsem se zajímal ve své bakalářské práci, kde jsem na základě anketního šetření dospěl k závěru, že téměř 87 % respondentů DeepWeb nenavštívilo a z toho 74 % nemá tušení o významu DeepWebu, čímž jsem dospěl k závěru, že je třeba se o tuto problematiku zajímat a snažím se touto cestou dostat tohle téma do povědomí.

Důvodem je separace tzv. SurfaceWebu („všem známé WWW – World Wide Web“) a DeepWeb, kde právě druhý jmenovaný není přístupný z „*mainstreamových*“ vyhledávačů jako je Google, Seznam, Bing a další.

Pro přístup do DarkWebu (místní část DeepWebu, kde se vyskytuje ohnisko nelegálních činností) je zapotřebí specializovaný nástroj se sofistikovanými technikami směrování a šifrování, kde nejznámější z nich je prohlížeč nazývaný Tor. Na tomto místě kyberzločinci provádějí nelegální elektronické obchody (e-commerce), tvz. „praní“ špinavých peněz, prodávají kompromitované bankovní informace nebo se zde jednoduše šíří různé programy (malware) využívající metody sociálního inženýrství.

2.4 Sociální inženýrství

Sociální inženýrství je termín, který je nejčastěji užíván pro manipulační techniku, která využívá lidské chyby a tím získání určitých informací. Nejedná se tedy o překonávání technických prostředků, ale o samotného uživatele. Neinformovaní a nezkušení uživatelé jsou cílem těchto bezpečnostních incidentů, avšak úspěšné útoky postihují i odborníky v oblasti IT. Dle serveru safetydetectives.com bylo v roce 2018 toto číslo na hodnotě 83 procent.

Útočníci využívají vysoce sofistikované metody, které se vyvíjí ruku v ruce s nejnovějšími technologiemi. Ani kryptoměny hýbající světem se těmto typům útoků nevyhnuly. Nebezpečná a zároveň nejrozšířenější forma, která vešla do povědomí má název phishing, která vychází ze způsobu lidského rozhodování. V psychologii též známá jako kognitivní chyba úsudku a této metodě se budu více věnovat v pozdějších kapitolách. Útočník využívající techniky sociálního inženýrství se nazývá sociotechnik. Útočníci používají jak online, tak offline nástroje k tomu, aby přiměli nic netušící uživatele ke kroku, který ohrožuje jejich bezpečnost.

Podle zprávy *The Human Factor* od společnosti *Proofpoint* z roku 2019 využívá celých 99 % kybernetických útoků techniky sociálního inženýrství, aby uživatele donutilo k instalaci malwaru.

Obrázek 1.

Sociální inženýrství

Zdroj: SafetyDetectives (2022)

Poznámka. První zmínky o sociálním inženýrství se datují na počátek 20. století. Využívaly se principy tehdejší doby.

2.5 Typy útočníků a lokace

Kybernetičtí útočníci jsou útočníci útočící na počítačový systém. Je důležité vědět, kterému typu útočníka uživatel čelí a podle toho také jednat a připravit se na něj. Důležitým parametrem je také taxonomie útočníků dle motivace. Tím se dá minimálně teoreticky odhadnout, čeho může být útočník schopen a někdy i doba trvání útoku. Také lokace útočníka hraje významnou roli, která je pro útočníka z pohledu logické lokace daleko přijatelnější a otvírá více možností k útoku.

Existují také různé programy, které dané kroky automatizují a není zapotřebí přítomnost fyzického útočníka. Často se jedná o uživatelsky přívětivé programy, které jsou jednoduché k nastavení a lze díky nim napáchat velké množství škody. Jedná se o nástroje útočné, které nejsou v kybernetickém prostoru novinkou, ale slouží „testerům“ pro kontrolu bezpečnosti a náchylnost k napadení konkrétních systémů. Nyní si své místo našly i v nelegálních činnostech. Prostřednictvím různých serverů lze daný program stáhnout volně bez jakéhokoli ověření či platby a útočníkem se tedy může stát prakticky kdokoliv.

Článek "*Understanding Cybersecurity Attackers and Their Motivations*" rozděluje motivaci útočníku na 4 základní typy:

1) Finanční zisk: Jednou z hlavních motivací kybernetických útočníků je finanční zisk. Tyto útoky zahrnují krádeže citlivých finančních údajů, vydírání prostřednictvím ransomwaru, podvody při elektronickém bankovnictví a další. Kyberzločinci často využívají slabiny v kyberbezpečnosti a nedostatek povědomí uživatelů k získání přístupu k citlivým údajům a finančním prostředkům.
2) Politický aktivismus a náboženské přesvědčení: Někteří útočníci jsou motivováni politickým nebo náboženským aktivismem. Hacktivisté mohou provádět kybernetické útoky s cílem upozornit na konkrétní politickou nebo sociální otázku nebo náboženské přesvědčení. Tyto útoky mohou zahrnovat DoS (Denial of Service) útoky nebo únik citlivých informací.
3) Špionáž a průmyslová sabotáž: Kyberšpionáž a průmyslová sabotáž jsou dalšími motivacemi pro kybernetické útočníky, zejména ty, kteří jsou podporováni státem. Účelem těchto útoků je získat přístup k důvěrným informacím, které mohou být použity k získání konkurenční výhody nebo k narušení operací protivníků. To může zahrnovat únik obchodních tajemství, vojenských plánů nebo citlivých politických informací.
4) Osobní motivace a pomsta: Někteří kybernetičtí útočníci mohou být motivováni osobním zájmem nebo touhou po pomstě. Například nespokojený zaměstnanec může provést útok proti svému zaměstnavateli s cílem způsobit škodu nebo dosáhnout odplaty. Tyto útoky mohou zahrnovat sabotáž systémů, zneužití přístupových práv nebo únik citlivých informací.

2.5.1 Typy útočníků

V kybernetickém prostoru existují různé typy útočníků, ale já se zaměřím na první čtyři nejrozšířenější typy, kteří mají různé schopnosti, pomocí kterých útoky realizují. Jsou jimi boti, amatéři, hackeři a profesionálové. S každým typem útočníků se může běžný uživatel dostat relativně snadno do kontaktu.

Boti

Boti jsou sofistikované počítačové programy, které mají za úkol provádět různé činnosti, nejčastěji související se sběrem, analyzováním nebo zpracováním dat. Tyto programy jsou navrženy tak, aby fungovaly na předem upravených serverech s nepřetržitým provozem, což jim umožňuje pracovat efektivně a kontinuálně bez nutnosti lidského zásahu. Boti mají jasně definovanou automatizaci, což znamená, že dokážou automaticky provádět úkoly podle předem

stanovených parametrů a pravidel. Díky své schopnosti nezávislého provádění činností mohou být boti použiti pro širokou škálu účelů, jako je sledování webových stránek pro změny obsahu, sběr informací pro výzkumné účely, nebo dokonce provádění automatických testů na webových aplikacích.

Je důležité poznamenat, že boti mohou být použiti jak pro legitimní, tak pro nelegitimní účely. V rukou kyberzločinců se boti mohou stát nástroji pro šíření malware, provádění DDoS útoků, nebo pro krádeže citlivých dat. Proto je důležité, aby se organizace a jednotlivci věnovali řádnému zabezpečení svých systémů a síťových prostředí, aby minimalizovali riziko zneužití botů pro nekalé účely.

Amatéři

Jedná se o fyzické osoby tvořící především „technologické nadšence“, kteří jeví zájem o danou problematiku. Je to nejpočetnější skupina útočníků a považuje se za nejméně nebezpečnou. Prostřednictvím webových stránek na internetu je pro většinu uživatelů jednoduché se s daným útočným programem seznámit a základní funkce aktivovat. Přispívají tomu také čím dál více rozšířená „tutoriálová“ videa a textové návody, které jsou k dispozici v různých jazycích častokrát včetně češtiny. Mnohdy pouze zkouší, zda jejich nabyté informace lze reálně využít u vhodné příležitosti. Je znám případ, kdy student střední školy využil tuto metodu pro získání informací o připraveném testu od učitele. Dostáváme se tedy na hranici nelegálního jednání, které si student často nemusí uvědomovat.
Předcházet tomuto způsobu napadení lze relativně snadno. Základní princip spočívá v dodržování kyberbezpečnostních zásad, kterým se budu dále věnovat v následujících kapitolách.

Hackeři

Hackeři představují nejnebezpečnější skupinu útočníků, kteří mají rozsáhlé odborné znalosti v oblasti výpočetní techniky a dokáží je efektivně využít. Tato skupina často zahrnuje studenty informačních technologií, programátory a další odborníky, kteří přesně rozumí problematice a funkcionalitě každého kroku útoku. Hackeři jsou schopni principiálně nastavit tzv. "ohýbání" útočných metod, aby je přizpůsobili svým potřebám a dosáhli zamýšlených cílů. Díky svým pokročilým dovednostem mohou překonat různé bezpečnostní opatření a získat přístup k citlivým informacím nebo systémům. Ochrana proti hackerům vyžaduje pokročilá kyberbezpečnostní opatření a neustálé monitorování hrozeb. To zahrnuje pravidelné aktualizace softwaru, silná hesla, šifrování dat, zabezpečení síťových spojení a vzdělávání uživatelů v oblasti kyberbezpečnosti. Je důležité si uvědomit, že i když hackeři představují vážné riziko, stále je možné se proti nim bránit dodržováním osvědčených bezpečnostních postupů a zásad.

Profesionálové

Poslední skupinou, kterou zde uvedu, jsou počítačoví profesionálové. Tito experti se vyznačují bohatými zkušenostmi z praxe a provádějí cílené útoky jak samostatně, tak v rámci organizovaných skupin. Motivace pro jejich činnost se různí, ale nejčastěji se jedná o různé vládní organizace a světové tajné služby, které mají jasně definované cíle.

Technologická vybavenost těchto profesionálů je na nejvyšší úrovni a jejich možnosti bývají často neomezené. Nicméně, pro běžného uživatele je pravděpodobnost setkání s útočníky tohoto typu velmi nízká, protože se zaměřují na hodnotné cíle a nezajímají se o méně důležité subjekty. Tato skupina se tedy valné většiny uživatelů prakticky netýká.

Přesto je důležité zmínit tuto skupinu útočníků, aby jedinci zabývající se kybernetickou bezpečností nezískali pocit absolutního bezpečí. Je nezbytné být si vědom rizik a pokračovat v dodržování kyberbezpečnostních opatření, aby byla zajištěna co nejvyšší úroveň ochrany.

2.5.2 Lokace útočníků

Podstatnou roli v přístupu ke sdíleným prostředkům hraje také odlišná fyzická a logická lokace, což znamená, že základním principem je informace, která nese údaje o tom, kdo má kde a jaký přístup k počítačovým sítím. Tato rozmanitost a různorodost přístupových údajů ztěžuje a komplikuje útoky, čímž zvyšuje úroveň zabezpečení.

2.6 Kybernetická bezpečnost za éry Covid-19

Je evidentní, že dnešní svět je naprosto odlišný od toho, ve kterém jsme žili před pár lety. Pandemie Covid-19 přinesla doslova „vlnu“ změn, která ovlivňuje všemožné aspekty našeho života. Ani kybernetická bezpečnost těmto změnám neunikla a vznikly nové „příležitosti“, které jsou útočníky často napadány. Například postupný přechod na tzv. „home office“ otevřel nové příležitosti různým typům útočníků. Je to nejistota a strach populace, která přináší nové příležitosti pro kybernetické zločince, kteří využívají formy jako phishing nebo různé druhy malwaru (ransomware a další).

Dle serveru *Comparitech* jsou kybernetické útoky řazeny do vzorců, které po určitou dobu zachovávají svůj trend. Ale vzhledem k neustále se vyvíjejícímu technologickému vývoji, ani studie z roku 2019 nevykreslují přesný obraz hrozeb, kterým čelíme nyní. Existuje naštěstí několik serverů, které zhodnocují současnou situaci, aby se populace mohla do jisté míry připravit na postpandemické kybernetické prostředí.

Podle *Emanuela Cleavera* hovořícím na *House meeting on illegal digital activities* byl zaznamenán v online kriminalitě do června 2020 až 75% nárůst denních kybernetických útoků od začátků pandemie. Nejedná se ale o nejvyšší nárůst v průběhu roku. Na úplném začátku pandemie se kybernetická kriminalita zvýšila čtyřnásobně.

V srpnu 2022 byla publikována zpráva společnosti Malwarebytes (2022) o reportu, kde pětina dotázaných společností na otázky o kybernetické bezpečnosti přiznala, že došlo k narušení bezpečnosti, které bylo důsledkem akcí zaměstnance pracujícího z domova.

Tento výsledek není natolik překvapivý, protože 18 % dotázaných organizací uvedlo, že jejich zaměstnanci nepovažují kybernetickou bezpečnost za prioritu. Následných 5% organizací považuje své zaměstnance za bezpečnostní riziko z důvodu ignorování kyberbezpečnostních praktik.

The UK's Action Fraud National Fraud & Cyber Crime Reporting Centre sleduje počet podvodů souvisejících s Covid-19. Do února 2021 zjistila, že bylo hlášeno více než 6000 případů podvodů kybernetické kriminality související s pandemií, přičemž oběti přišly o 34,5 milionu liber. Do července 2020 byla přitom tato částka na třikrát menší hodnotě.

Platforma *Zoom* pro videokonference se v době koronavirové stala bezesporu jedna z nejpopulárnějších. Snaha společnosti *Zoom Video Communications* o co největší flexibilitu využití při videokonferencích za doby pandemie nesla s sebou i četná rizika.

Kladení menšího důrazu na bezpečnostní záplaty a méně kvalitní zálohy byl přesně ten důvod, proč se do poloviny dubna roku 2020 objevily k prodeji na DarkWebu podrobnosti o 530 000 účtech platformy Zoom. Dalším krokem útočníků na platformě Zoom byl mimořádně velký počet registrací s falešnými údaji s vidinou škodlivých útoků přes tuto platformu.

Dle společnosti Microsoft se každou sekundu na celém světě uskuteční 921 hackerských útoků, přitom až 98 % z nich jde předejít prostřednictvím několika relativně jednoduchých kroků, kterým se budu dále věnovat.

Společnost ESET uvádí, že rok 2020 se nesl ve znamení „krádeže identity". Během tohoto roku vznikla řada podvodných inzerátů nabízejících „výhodné" půjčky.

České republice probíhá dle Jiří Burýšek (2022) útok následovně:

Osoba žádající o půjčku odpoví na inzerát s žádostí. Následně podvodník žádá o osobní údaje žadatele, které uživatel pošle a vzápětí následuje požadavek o vyfocení občanského průkazu s obhájením, že se jedná o kontrolu, zda žadatel není v exekuci.

Poté podvodník žádá uživatele o odeslání 1 Kč na „ověřovací účet jeho společnosti" s konkrétním variabilním symbolem, aby bylo zřejmé, že platbu odeslal konkrétní uživatel. Ve

skutečnosti se však za oponou rozehrává neuvěřitelný sled událostí. Podvodník využije zaslání dokladů, zašle je bance a založí si účet na dané jméno žadatele.

Pro aktivaci účtu banka požaduje právě aktivační platbu 1 Kč se specifickým variabilním symbolem, pomocí které potvrdí, že si účet zakládá tento skutečný člověk. Podvedený uživatel si myslí, že zasílá platbu někomu, kdo mu poskytne půjčku. Ve skutečnosti ale posílá platbu bance, která právě založila účet na jméno daného uživatele a podvodník k němu má kompletní přístup. Podvedený nemá tušení, že na jeho jméno byl založen účet a půjčku žádnou nedostane, protože žádná neexistuje.

Jde tedy čistě o zneužití osobních údajů, protože tento „digitální otisk“ má skutečně obrovskou cenu a mnoho lidí nemá ponětí, jak důležité může být své osobní údaje držet v soukromí.

2.7 Sociální inženýrství a jeho metody

2.7.1 Phishing

Phishing je typ útoků sociálního inženýrství, který se nejčastěji užívá k odcizení uživatelských dat (přihlašovací údaje, čísla kreditních karet aj.). Může k němu dojít např. když útočník, který se vydává za důvěryhodnou entitu, naláká oběť k provedení žádoucích kroků (otevření přílohy e-mailu, www odkazu nebo různých aplikací, nejčastěji s příponou „.exe“). Následující interakce aplikuje škodlivý kód, který provede předpřipravenou automatizovanou činnost, která může vést k instalaci malwaru, zamrznutí systému nebo např. úniku uživatelských dat.

Útok může mít kritické následky, které mohou vést k neoprávněným nákupům, krádežím finančních prostředků nebo krádeži identity.

Mimo jiné se phishing často používá v podnikových či vládních sítích jako součást většího útoku, tzv. APT (Advanced Persistent Threat, pokročilá perzistentní hrozba). Reálně se jedná o typ síťového útoku, při kterém je vytýčen konkrétní cíl a použití pokročilých technologií se analyzuje a monitoruje po dobu týdnů, měsíců nebo i několik let. Tento útok často končí až v momentě, kdy se dosáhne požadovaného výsledku nebo k neúspěšnému výsledku. Málo kdy tento útok končí předčasně.

Dle serveru *mobilizujeme.cz* přišla společnost ESET, která se zabývá kybernetickou bezpečností s aktuální statistikou pro květen roku 2022. Ta obsahuje data, která udávají, že od začátku roku 2022 byl v porovnání s rokem minulým, nárůst phishingových útoků až o neuvěřitelných 440 %. Útoky se nevyhýbají žádným sférám, kde dle serveru *it-market.cz* tvoří

největší část útoky proti finančnímu sektoru (23,6 %). Hned v závěsu jsou útoky proti webmailu a poskytovatelům softwarových služeb. Oproti roku předešlému se také zvýšil útok na kryptoměnové burzy.

Phishing a kryptoměny

Společnost *Avast Software s.r.o.* v roce 2021 provedla analýzu zaměřenou na kryptoměnové podvody. Z výsledků analýzy vyplývá, že nejčastějšími cíli „krypto-podvodů" jsou jednoznačně USA, Brazílie a Nigérie. Podvody se však ve velké míře vyskytují také ve Velké Británii, Rusku, Francii a České republice.

Podle *Finexu (2022)* jsou kryptoměny elektronicky vytvořené digitální měny s reálnou hodnotou, která je dána nabídkou a poptávkou a dlouhodobě lineárně roste. K roku 2021 se udává, že na celém světě existuje 100 milionů uživatelů kryptoměn, což je důvod, proč se kryptoměny stávají velmi atraktivním cílem kybernetické kriminality. Kryptoměny lze jednoduše charakterizovat jako číslo v databázi, avšak zabezpečení kryptoměn záleží na každém uživateli.

Na úvod je důležité zmínit, že existuje několik způsobů, jak ukládat kryptoměny. Mezi tyto způsoby se řadí správcovské peněženky, softwarové peněženky, papírové peněženky a hardwarové peněženky. Každý z těchto způsobů má své vlastní výhody a nevýhody, a je na uživatelích, aby si vybrali ten nejvhodnější způsob pro svoje potřeby a zabezpečení.

Správcovské peněženky

Tento typ peněženky je spravován jinou entitou, kterou může být například kryptoměnová burza. Princip fungování správcovské peněženky lze přirovnat k tradičnímu bankovnímu účtu, ke kterému má uživatel po autorizaci přístup a může své prostředky spravovat. Výhodou této peněženky je částečné zabezpečení, které poskytuje služba, a uživateli tak nabízí určitou záruku a pojištění. Avšak, pokud se jedná o podvodnou službu nebo tato zkrachuje, uživatel může přijít o své finanční prostředky.

Je důležité si uvědomit, že se jedná o účet jako každý jiný, a jeho autentifikace je chráněna pouze do té míry, jak ji uživatel sám chrání. Phishing je nejčastějším způsobem útoku napadající správcovské peněženky. Jako příklad uvedu kryptoměnovou burzu Binance se sídlem na Maltě, která podle serveru *entuzio.cz* je největší a zároveň nejrychleji rostoucí burzou na světě. Útočníci vytvoří falešnou webovou stránku, která připomíná zmíněnou kryptoburzu Binance, která se od originálu liší na první pohled pouze malými detaily. Může se často jednat o mírně odlišné typy písma, odstíny barev, avšak základním rozdílem je jiná URL adresa, která je pro rozpoznání phishingových podvodů klíčová.

Softwarové peněženky

Jedná se o typ aplikace spravující soukromé klíče majitelů kryptoměn. Výhodou softwarových peněženek je jejich uživatelská přívětivost a přehled nad vlastními kryptoměnami. Slabou stránkou této metody uchování prostředků je riziko napadení zařízení, ze kterého peněženku uživatel spravuje. Častým typem útoků u této peněženky je ransomware, který inicializuje peněženku formou zašifrování a pro jeho dešifrování vyžaduje výkupné. Dalším riziko představuje také škodlivý kód (Trojský kůň), který si do systému zavede tvz. backdoor (zadní vrátka), pomocí kterého do systému mohou proniknout další útočníci.

Papírové peněženky

Nejjednodušší řešení představuje papírová peněženka, která nemá digitální podobu a uživatel si svůj unikátní klíč musí zapsat fyzicky na papír. Velkou výhodou je finanční nenáročnost a absence rizika kybernetického napadení. Rizika spojená s tímto řešením zahrnují zapomenutí, ztrátu nebo krádež papíru s unikátním klíčem.

Hardwarové peněženky

Hardwarové peněženky jsou považovány za nejbezpečnější metodu uchování kryptoměn. Jedná se o samostatná fyzická zařízení, často ve formě USB klíčenek, která obsahují zašifrovaný unikátní kód pro přístup ke kryptoměnám. Běžně se k těmto peněženkám dodává odolná ocelová tabulka pro obnovu klíče, která odolá i vysokým teplotám. Unikátní klíč je třeba do tabulky vyřezat.

Výhodou hardwarových peněženek je vysoká úroveň zabezpečení; prolomení takového zabezpečení je možné pouze pro profesionální hackery za předpokladu dlouhodobého fyzického přístupu k zařízení. Lze tedy předpokládat, že i v případě krádeže USB klíčenky bude mít majitel dostatek času na přesměrování kryptoměn pomocí unikátního kódu zaznamenaného na odolné ocelové tabulce a znehodnocení původního klíče. Tato varianta je považována za poměrně bezpečnou, a tak je pravděpodobné, že i po ztrátě hardwarové peněženky zůstanou kryptoměny netknuté. Nevýhodou je vyšší pořizovací cena takových peněženek.

Obrázek 2.

HW peněženka Ledger

Zdroj: 2Mac (2020)

Phishing kryptoburzy

Příklady bezpečnostních tipů pocházejí přímo ze serveru *Binance.cz*, konkrétně z jejich sekce *"support",* sloužící pro klienty služby. Tyto rady jsou poskytovány klientům této platformy jako doporučení pro zajištění jejich bezpečnosti při používání kryptoměn.

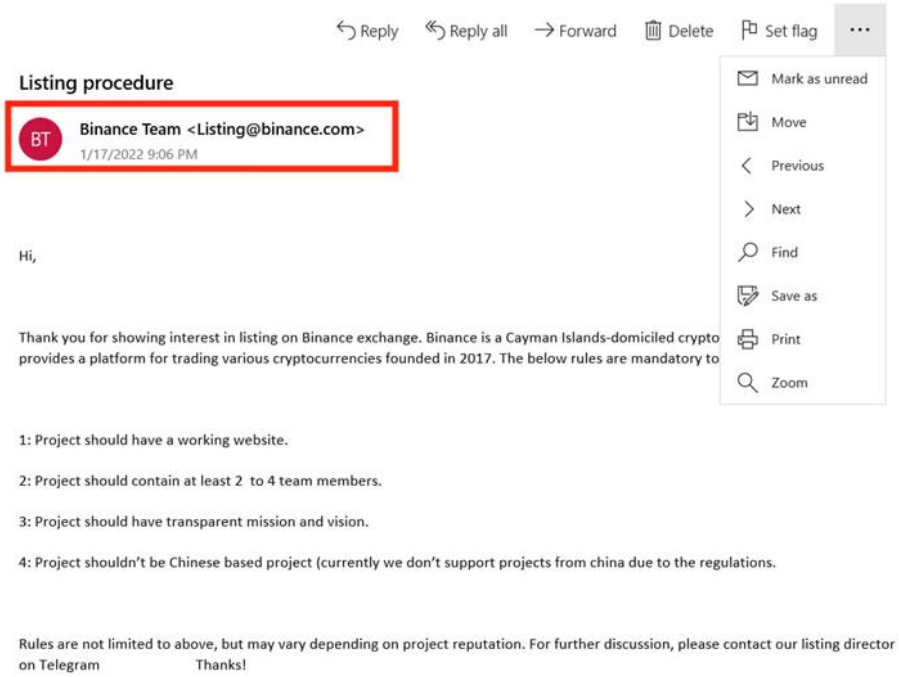
Příklad č.1

Tento phishingový e-mail se snaží vytvořit dojem, že pochází z oficiálního upozornění od služby Binance. Přestože doména může vypadat legitimně, e-mail ve skutečnosti nepatří této burze a nebyl odeslán z oficiálního e-mailového serveru.

Phishingový e-mail přesvědčuje uživatele, aby na platformě Telegram kontaktovali falešné pracovníky platformy Binance. Poté následuje žádost o vložení kryptoměny do jejich blockchainu (repozitáře kryptoměn). Tyto typy e-mailů obvykle obsahují velké množství příliš pozitivních zpráv (jako jsou například levné nabídky tokenů nebo rozdávání kryptoměn).

Obrázek č. 3

Neoficiální e-mailový server



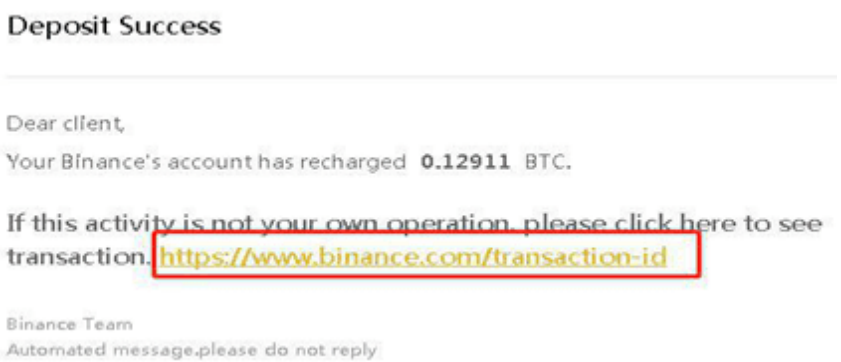
Zdroj: *Binance (2022)*

Příklad č.2

Tento phishingový e-mail nabádá uživatele, aby kliknul na škodlivý odkaz, po kterém má dojít k získání 0,129 BTC. Lze očekávat, že po rozkliknutí se aktivuje škodlivá webová aplikace, která bude schopna při nejmenším monitorovat kroky uživatele nebo bude následovat žádost o přihlášení do falešného webového portálu *Binance*.

Obrázek č.4.

Škodlivý odkaz

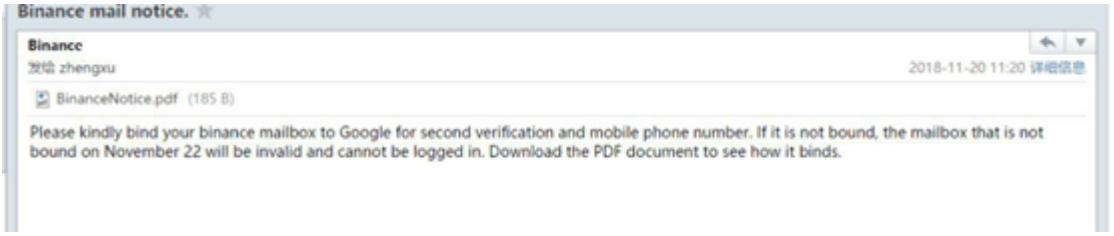


Zdroj: *Binance (2022)*

Příklad č.3

Tento druh e-mailu nabádá uživatele ke stažení škodlivého souboru ve formátu PDF, který obsahuje škodlivý software (malware). E-mail může být často rozpoznán i podle struktury, rozložení textu, hovorového nebo i nespisovného jazyka a gramatických chyb.

Obrázek č.5 Malware



Zdroj: *Binance (2022)*

Příklad č.4

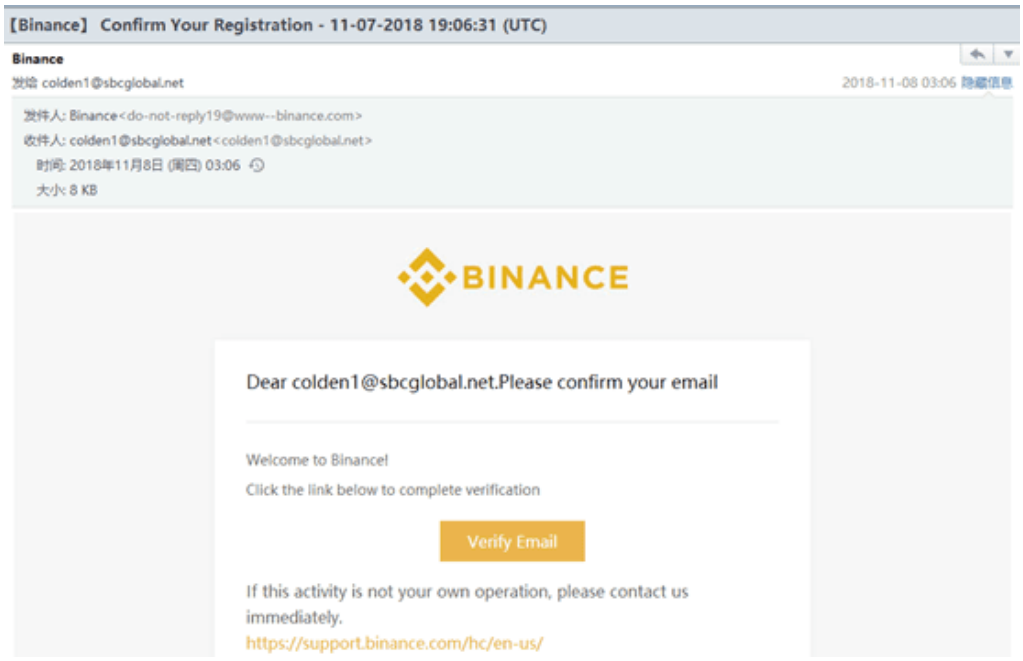
Poslední varianta, kterou zde uvedu, je považována za nejpočetnější. Jedná se o typ emailu, který útočník vytvořil se záměrem získat přístup ke skutečnému e-mailovému účtu, heslu a záložnímu klíči pro dvoufaktorové ověření.

Pod logem Binance se nachází e-mail cíleného uživatele, který má nabýt dojmu, že se jedná o ověření jeho vlastního Binance účtu. Ve vyobrazeném políčku odesílatele se nachází sice Binance doména, ale nepřesná.

Tento phishingový útok byl odeslán z do-not-reply19@www--binance.com, která používá podobnou doménu. Jedná se o nejčastější způsob, kterými se snaží útočníci vydávat za danou platformu.

Obrázek č.5

Two-factory



Zdroj: Binance (2022)

Po následné interakci na tlačítko „Ověřit e-mail“ si lze všimnout podvodné URL adresy, která je https://www--binance.com/binance/login.php. Nepozorný či nezkušený uživatel vyplní své přihlašovací údaje pro oficiální Binance účet a útočníkovi se do databáze uloží potřebná data, s kterými může dále interagovat.

Pokud uživatel využívá dvoufaktorové ověření, web jej požádá o záložní klíč a tím se provedl poslední nezbytný krok, pro přihlášení. Z podstaty věci se web přesměruje do „hluchého místa“, odkud dále nelze pokračovat. Útočník získal všechny potřebné informace.

Jak rozpoznat phishing?

1) Obecné nebo chybějící oslovení: Phishingové e-maily často postrádají specifické oslovení a obsahují pouze obecný pozdrav. Organizace při komunikaci se svými klienty totiž často nastaví e-mail tak, aby obsahoval oslovení jména.
2) Chybný pravopis a gramatika: Phishingové e-maily mohou obsahovat zvláštní nebo chybný pravopis, gramatické chyby či neobvyklé formulace. Tyto chyby mohou být indikátorem podvodného e-mailu.
3) Kontrola URL adresy: Je důležité pečlivě zkontrolovat URL adresy odkazů uvedených v e-mailu. Odkaz by měl směřovat na oficiální stránky organizace, nikoli na podvodné nebo

neznámé webové stránky. Pokud si nejste jisti, zda je odkaz legitimní, neklikejte na něj a místo toho navštivte webovou stránku organizace přímo zadaním její adresy do prohlížeče.

4) Nevěrohodné nabídky nebo naléhavost: Phishingové e-maily často obsahují příliš výhodné nabídky nebo vyžadují okamžitou akci ze strany příjemce. Buďte opatrní, pokud e-mail vyzývá k rychlému jednání nebo nabízí příliš dobře znějící výhody.
5) Neobvyklé e-mailové adresy odesílatele: Zkontrolujte e-mailovou adresu odesílatele a ujistěte se, že patří důvěryhodné organizaci. Phishingové e-maily mohou používat podobné, ale mírně odlišné e-mailové adresy nebo domény, které se snaží napodobit legitimní odesílatele.

2.7.2 Pharming

Pharming je technologicky pokročilejší forma phishingu. Při zadání webové adresy do prohlížeče jsou uživatelé nevědomky přesměrováni na falešnou webovou stránku, která vzhledově velmi připomíná (a mnohdy je nerozpoznatelná) originální stránku. V důsledku toho mohou být jakékoli informace poskytnuté na falešném webu, jako jsou například čísla účtů nebo hesla, odcizeny.

Princip pharmingu spočívá v napadení DNS serveru a nahrazení IP adresy originální webové stránky alternativní, podvodnou adresou. Podle zprávy společnosti Kaspersky z roku 2021 je 83 % případů napadení formou pharmingu zaměřeno na finanční sektor. To ukazuje, jak vysoký je zájem útočníků o citlivé finanční informace a jak důležité je být ostražitý při používání webových stránek s finančními službami.

Dle portálu Lupa má pharming dvě podoby. První podoba je značně efektivní, avšak pro útočníka velice obtížná, což omezuje její užití. Druhá podoba je pro útočníka jednodušší, nicméně také s nižší spolehlivostí. Pharming je způsob napadení DNS serveru (seznam internetových domén a daných IP adres). Podaří-li se útočníkovi jednu z cílených adres změnit (typicky internetové bankovnictví), po zadání potřebné adresy do prohlížeče dostane uživatel alternativní webovou stránku, která je často vypracovaná natolik detailně, že ji téměř nelze rozeznat. „Zlatým pravidlem“ je kontrola URL adres, ovšem nyní se potýkáme s metodou, která svou adresu zachovává. Jsou tedy velmi malé šance, že uživatel na daný podvod příjde. Jedinou přijatelnou metodou uživatele je kontrola certifikátu pro šifrování dat. Ten není útočník schopen padělat, ale lze navodit pocit z pohledu uživatele, že bez podrobného průzkumu se zdá být vše v pořádku.

Druhou podobu lze nazvat jako „lokální pharming“. V tomto případě útok neprobíhá přes DNS server, ale je cíleno na konkrétní PC s operačním systémem Windows. Ten obsahuje soubor „hosts“, který má stejný princip fungování, jako právě zmíněný server DNS, který obsahuje seznam IP adres a adekvátní domény. Podaří-li se útočníkovi v souboru provést změny a připsat adresu své falešné stránky (např. internetové bankovnictví), pak se jedná o stejný výsledek jako v případě předešlém. V praxi to znamená, že i po zadání korektní adresy URL se zobrazí alternativní stránka útočníka.

První metoda není závislá na cílových zařízeních, ale je zapotřebí „prolomit“ ochranu DNS serveru. Zároveň DNS servery tvoří páteřní sítě internetu, a tak jsou velice často vysoce chráněny. Jedná se tedy o způsob pro velice zdatné útočníky. Z toho důvodu se využívá především metoda druhá.

Druhá metoda vyžaduje přístup pro zápis dat do systému. Tedy e-mail nebo webová stránka touto funkcionalitou nedisponují. Přichází tak na řadu nejčastěji Trojský kůň, který často bývá maskován jako doplněk softwaru. Může být zaslán e-mailem v příloze, v odkaze

ke stažení nebo být přibalen u oficiální aplikace. Po úspěšné změně souboru „hosts“ následují výše zmíněné útoky.

Pokud tedy porovnáme obě výše zmíněné metody, kterými může útočník postupovat, tak v obou případech je zapotřebí uživatelská interakce a s patřičnou znalostí lze do jisté míry tomuto napadení předcházet. Z porovnání vychází, že pharming je nebezpečnější metoda než phishing a lze ní oklamat i zkušeného uživatele. Webové prohlížeče často obsahují nejrůznější formy ochran proti různým druhům kybernetických útoků, ale často není zaručena detekce, jelikož musí být web označen za škodlivý a tento proces často trvá příliš dlouho.

Ochrana proti pharmingu na úrovni DNS serverů není v moci uživatele, ale u lokálního napadení je důležitá prevence a sice antivirový program, který má pravidelně aktualizovanou databázi. Dochází ke kontrole jak elektronické pošty, tak stažených souborů z webu. Dojde-li k archivaci viru do souborů (rar, zip), antivirový program přichází na řadu v reálné době jeho extrahování.

2.7.3 Baiting

Jedna z relativně jednoduchých technik napadení zařízení je tzv. baiting. Spočívá v nastražení přenosného paměťového média (CD, flashdisk, paměťová karta), které oběť najde a z něhož spustí škodlivý kód. Tato metoda se opírá o zvědavost jednotlivce.

Nebezpečí spočívá již v samotném připojení přenosného média, a často není nutné přímé otevření souboru. Pro útočníka je výhodou finanční nenáročnost, když jsou náklady pouze na přenosné médium, které často ani není nutné pořizovat, jelikož spousta organizací je rozdává jako reklamní nebo propagační předměty.

Nejnáročnější částí této techniky je umístění média blízko oběti a následná motivace k připojení k osobnímu zařízení. Lidská kreativita ovšem nezná mezí, a útočníci tak přicházejí se stále novějšími a propracovanějšími způsoby, jak dosáhnout svého cíle. Originální médium může být například vyměněno na pracovním stole, v restauraci, po školení či během nepozornosti nebo obědové přestávky - záleží na konkrétní situaci. Útočník často má možnost osobního kontaktu s cíleným zařízením a může jej sám připojit.

Podle *Passcamp (2021)* je znám případ, kdy se útočník vydával za poctivého nálezce ztraceného média, a následně jej několik pracovníků firmy připojilo ke svým osobním zařízením. Poté byl škodlivý software schopen získat administrátorská oprávnění a spustit formátování všech dostupných disků.

Nejsilnější defenzívou odolávající baitingu je vzdělávání se a umění předvídat. Vzdělávání sebe i druhých je obecně nejsilnější obranou metodou proti sociálnímu inženýrství.

2.7.4 Quid Pro Quo

Baiting má také variantu, která se více zaměřuje na finanční motivaci oběti. Aktuální éra kryptoměn tomuto způsobu podvodu napomáhá, neboť u podvodů s decentralizovanou měnou nelze hledat nápravu u žádného úřadu.

V USA je rozšířený podvod spojený se správou sociálního zabezpečení (SSA) a její databází čísel, která mohou být zneužita k napáchání značných škod. Útočníci se vydávají za zaměstnance SSA, kteří předstírají problém se svým pracovním počítačem a žádají oběť o číslo jejího sociálního zabezpečení pro ověření identity. Následně vytvoří záminku, že je nutné ověřit identitu, jinak bude problém řešitelný pouze na pobočce.

Obdobný podvod spočívá v nabídce "pomoci" s žádostí o novou kartu sociálního zabezpečení, avšak jde ve skutečnosti o krádež osobních údajů. Tento způsob podvodu využívá finanční motivace oběti a snahu vyhnout se osobnímu jednání na pobočce, což usnadňuje útočníkovi získání citlivých informací.

2.7.5 Tailgating

Tento typ útoku spočívá v tom, že útočník sleduje cíl s oprávněným přístupem do systému, například zaměstnance s autorizací do firemní sítě. Útočník následuje stejnou cestu jako cíl při vstupu do systému a získává tak přístup do chráněné oblasti.

Jedním z nejznámějších případů tohoto druhu útoku je *Twitter Bitcoin Scam* z roku 2020, o kterém informoval například portál *vas-hosting (2021)*. Útočníci získali přístup k interním nástrojům sociální sítě Twitter, což jim umožnilo měnit jakýkoliv registrovaný e-mail a resetovat heslo k účtu. Celkem bylo napadeno 130 účtů, mezi nimiž byly cíleně napadeny účty osobností jako Elon Musk, Kayne West, Joe Biden nebo Barack Obama.

Útočníci poté zneužili tyto účty k provedení podvodu, který sliboval, že každá částka přijatá v bitcoinech bude zdvojnásobena a daná osoba tak přispěje na charitu. Výsledkem bylo snížení akcií Twitteru o 4 % za jediný den (snižování pokračovalo celkem 8 dní) a následovala pokuta ve výši 115 tisíc dolarů pro útočníky.

2.7.6 Pretexting

Jedná se o metodu podobnou phishingu, ale s větším zaměřením na individualizaci. Sociotechnik se pečlivěji připravuje na konkrétní oběť, například prostřednictvím různých scénářů, které mu pomohou z oběti vyžádat potřebné informace. Prvním krokem je navázání interakce s obětí, následuje přesvědčení druhé strany o nutnosti poskytnout více osobních informací (občanský průkaz, pas nebo jiný dokument) pro autorizaci. Jde tedy o krádež identity, která bývá často zneužita na půjčkových webech.

Možnosti zneužití závisí na množství informací o dané osobě nebo organizaci. Typickým příkladem může být firma, která si najímá externí síťovou bezpečnostní agenturu. S dostatečnými informacemi není obtížné vydávat se za auditora a fyzicky vstoupit do soukromých prostor firmy.

Phishingové útoky využívají strachu a naléhavosti. Funguje zde sociální konformita, tedy přizpůsobení se při jednání pod tlakem.

Podle článku z roku 2016 s názvem *Investice do prevence útoků a kontroly škod v kybernetické bezpečnosti* vyplývá, že investice uživatelů a poskytovatelů softwaru jsou výrazně nevyvážené. Článek se zabývá vysokými investicemi do kontroly škod, avšak nedostatečnou prevencí útoků.

2.8 Anonymita

Návrh internetového prostředí se nenesl v duchu anonymity, ale funkcionality. Pro vzájemnou komunikaci mezi zařízeními slouží IP adresy, které lze lokalizovat. Jako příklad lze uvést poskytovatele internetového připojení (provider), který může snadno lokalizovat a analyzovat konkrétní IP adresy svých zákazníků v databázi. Z mého pohledu je anonymita na internetu jednou ze základních důležitých znalostí moderního člověka. Myslím si, že každý uživatel by měl mít pojem o tom, jak se vyvarovat běžných chyb týkající se anonymity.

2.8.1 IP adresy a veřejný wi-fi

Domácí komunikační uzly, jako jsou routery nebo switche, mají schopnost sledovat tok dat v místní síti. Často je využívána nejrychlejší a nejkratší cesta, která se mění pouze v nucených případech. Tím se stává tento uzel snadno odposlouchatelným. Pokud lze identifikovat datový tok a zdroj, je možné odhadnout úmysly a zájmy uživatele. Zvláště rizikovými místy pro internetové připojení jsou veřejná místa, jako například restaurace, kavárny či školy. V následujícím textu se zaměřím na několik častých způsobů napadení na veřejných Wi-Fi sítích.

2.8.2 Man-in The-Middle Attack

Při přístupu k internetu prostřednictvím Wi-Fi naváže zařízení spojení s routerem nebo serverem, který poté přiřadí zařízení IP adresu a připojí ho k internetu. Útok *Man-in-the-Middle* nastává, když se útočník dostane mezi uživatelské zařízení a nejčastěji router. Data prochází přes útočníka a pokračují dál. Tento útok lze popsat jako monitorování datového toku s následným filtrováním informací, které jsou pro útočníka zajímavé. Kyberzločinci používají specializovaný software pro "odposlech" datového provozu.

Jedním z populárních softwarů nese název Wireshark, který se využívá k analýze provozu v počítačových sítích (řešení problémů v sítích, vývoj komunikačních protokolů či studium síťové komunikace). Tento software si našel uplatnění i v kyberkriminálních činnostech, jako je právě zmíněný útok *Man-in-the-Middle*. Pokud se útočník dostane na cílovou síť, kterou chce odposlouchávat, dokáže i méně zkušený jedinec dosáhnout požadovaného výsledku s trochou samostudia. Silnou stránkou této metody je schopnost dešifrovat autentifikační servery, ke kterým se uživatel přihlašuje za přítomnosti SSL certifikátu.

Následující kroky jsou nezbytné pro tento proces:

1) *Náhled do komunikace:*

Existuje několik způsobů, jak nahlédnout do komunikace, ale princip spočívá v nahrávání celé komunikace do souboru, který software rozumí.

2) *Zachycení kryptografického materiálu:*

Součástí získaných dat jsou symetrické šifrovací klíče, které se u dané komunikace používají.

3) *Záznam provozu:*

Při zaznamenávání provozu dokážeme dešifrovat pouze obsah, ke kterému máme odpovídající šifrovací klíče.

4) *Dešifrování komunikace:*

Posledním krokem zbývá kombinovat kryptografická data s dešifrovacími klíči. Při pokračování v odposlouchávání provozu je veškerý obsah, ke kterému máme symetrické šifrovací klíče, dešifrován v reálném čase.

Princip sledování datových paketů, tedy analýza provozu zařízení na síti, se nazývá sniffing. Jedná se o velmi účinnou metodu síťového napadení, prostřednictvím které je útočník schopen získat prakticky jakékoli informace, včetně citlivých dat, jako jsou přihlašovací údaje nebo informace o kreditních kartách.

2.8.3 Malware

Pokročilou technikou napadení je infikování Wi-Fi sítě škodlivým softwarem (malwarem). Po připojení uživatele k Wi-Fi síti malware infikuje jeho zařízení. Někteří útočníci napadají samotný směrovač, který po připojení zasílá uživateli falešná vyskakovací okna s žádostí o aktualizaci softwaru, při kterém se po odsouhlasení malware nainstaluje.

Scénář poté pokračuje podle očekávání: krádež citlivých informací, smazání souborů nebo dokonce vyřazení zařízení z provozu. Zásadním problémem pro uživatele je anonymita malwaru, který je často schopen se připojit k systémovému procesu, a tudíž vypadá jako legitimní pro operační systém.

2.8.4 Evil Twin Attacks

Evil Twin Attack, který je do češtiny volně překládán jako *Útok zlého dvojčete* je obzvlášť nebezpečný typ útoku, při kterém kyberzločinec nastaví osobní nezabezpečený Wi-Fi hotspot s jediným cílem: krádež uživatelských dat. Základním pravidlem těchto útoků je získání věrohodného názvu a přimět uživatele se k síti připojit. Nejčastěji podle lokality kyberzločinec vybírá název, který souvisí s blízkými a známými podniky, jako jsou restaurace, kavárny nebo posilovny. Pro tuto techniku jsou charakteristické i útoky založené na DNS serveru, které jsem zmínil v minulých kapitolách. Útočník nahradí adresu serveru alternativní adresou, a uživatel následně nabývá dojmu, že se jedná o oficiální webovou stránku, nebo je oběť donucena navštívit konkrétní napadenou nešifrovanou stránku.

2.8.5 Způsoby zabezpečení na veřejné síti

I když nelze veřejnou Wi-Fi síť zabezpečit úplně, svá data můžete chránit několika způsoby. Nejlepší ochranou je být informovaný a znalý. S rychle rostoucím technologickým vývojem není snadné mít přesné povědomí o všech nástrahách v kyberprostoru, ale můžeme alespoň dodržovat základní bezpečnostní pravidla, jako například:

Navštěvování pouze webových stránek s SSL certifikátem

Webové adresy mohou mít zabezpečené (https) nebo nezabezpečené (http) připojení k webu. Avšak webová stránka s SSL certifikátem (https) není zárukou bezpečného webu. Útočníci na svých webových stránkách také využívají SSL certifikáty, ale podle *Comparitech (2022)* jsou útoky výrazně redukovány, protože dešifrování informací na zabezpečených webových stránkách je i pro samotné administrátory náročnou činností a vyžaduje vyšší odbornou znalost v dané problematice. Na druhou stranu, webové stránky bez SSL certifikátu (http) mají tu nevýhodu, že data jsou přenášena v prostém textu, což je zranitelné pro útoky typu Man-in-the-Middle, při kterém by útočník nemusel vynakládat žádné další úsilí.

Podle *ITPro* (2022) jsou nejbezpečnější veřejné sítě ty, které provádí v reálném čase kontrolu HTTPS pomocí tzv. strojového učení. Prostřednictvím tohoto přístupu dochází k pokročilé detekci hrozeb založené na chování uživatele.

Web *ITPro* (2022) provedl v první vlně Covid-19 průzkum, který poukázal na fakt, že dvě třetiny všech napadených zařízení malwarem byly infikovány prostřednictvím šifrovaných připojení. Z neznámých důvodů byla nejvíce zacílenou zemí Velká Británie.

Použití VPN

Stále větší popularitu nabývá tzv. VPN (Virtual Private Network – Virtuální privátní síť). Jde o software, který vytváří chráněné síťové připojení při využívání veřejných sítí. VPN dokáže šifrovat internetový provoz a také „maskovat" online identitu. Šifrování probíhá v reálném čase a útočníkům značně komplikuje sledování online aktivity. VPN skrývá IP adresu uživatele tím, že ji přesměrovává na speciálně konfigurovaný vzdálený server provozovaný VPN hostitelem. V praxi to znamená, že VPN se stává zdrojem dat a ISP (poskytovatel internetového připojení) ani třetí strana nemá přístup k informacím o tom, ke kterým internetovým stránkám uživatel přistupuje nebo která data odesílá a přijímá.

Server *Entuzio (2020)* přichází s testem nejlépe hodnocených VPN aplikací pro rok 2022, kde se na nejvyšších příčkách umístily produkty jako: NordVPN, PureVNP, CyberGhost VPN nebo ExpressVPN. Výběr hostingu je klíčovou vlastností, kterou by měl uživatel pečlivě zvážit, protože se na trhu vyskytují i takové VPN hostingy, které mají za cíl přesně opačnou funkci než tu, se kterou ji uživatel pořizuje. Je proto dobré brát v potaz historii nebo recenze zákazníků při výběru hostingu.

Mimo anonymitu je velkým benefitem také způsob fungování, prostřednictvím kterého je možné si vybrat stát, z kterého chce uživatel přistupovat. Jedná se tedy o způsob, kterým lze zpřístupnit funkce daných služeb, které jsou v konkrétní zemi zakázány.

Využití mobilních dat

Připojení k internetu prostřednictvím mobilních dat je obvykle bezpečnější než používání veřejných Wi-Fi sítí, protože data jsou šifrována operátorem. Na cestách je proto vhodné zvážit využití mobilních dat namísto veřejných Wi-Fi sítí, abyste svá data udrželi v bezpečí. Mobilní data poskytují větší kontrolu nad vaším připojením, neboť provoz není zranitelný vůči rizikům, kterým čelíte na veřejných Wi-Fi sítích, jako jsou útoky typu man-in-the-middle nebo špatně zabezpečené sítě.

2.8.6 Chování na veřejné síti

V této části diplomové práce se zaměřím na několik důležitých bodů, které by měli uživatelé zvážit po připojení k veřejné Wi-Fi síti. Tyto rady mohou pomoci snížit riziko kybernetických útoků a zvýšit online bezpečnost.

1) Omezte přístup k citlivým údajům: Pokud jste připojeni k veřejné Wi-Fi síti, vyvarujte se přihlašování k účtům spojeným s vašimi financemi, jako je internetové bankovnictví. Zároveň zkontrolujte, které aplikace mají přístup, k jakým datům a případně upravte jejich oprávnění.
2) Navštěvujte pouze nezbytné stránky s SSL certifikátem: Když jste na veřejné síti, omezte navštěvování pouze na stránky, které jsou v daný moment nezbytné. Upřednostňujte ty, které disponují SSL certifikátem, což naznačuje, že vaše data jsou šifrována při přenosu mezi vaším zařízením a webovým serverem.
3) Odhlašujte se z účtů: Pokud používáte různé typy účtů, nezapomeňte se po jejich použití odhlásit. Tímto způsobem minimalizujete čas, který potřebuje malware k napadení vašeho účtu.
4) Nepoužívejte stejná hesla na různých webech: Je důležité používat jedinečná hesla pro různé účty a webové stránky. Pokud útočník získá přístup k jednomu webu, existuje vysoká pravděpodobnost, že bude schopen použít stejné přihlašovací údaje na jiných webových stránkách.
5) Dbejte na upozornění prohlížečů: Moderní webové prohlížeče často analyzují webové stránky ještě před jejich navštívením a varují vás před potenciálně nebezpečnými stránkami. Neignorujte tato varování a věnujte jim náležitou pozornost.
6) Nastavte zařízení tak, aby se automaticky nepřipojovalo k veřejným Wi-Fi sítím: Tímto způsobem zamezíte nechtěnému připojení k neznámým a potenciálně nebezpečným sítím.
7) Aktualizujte software a operační systém: Ujistěte se, že váš operační systém, webový prohlížeč a všechny aplikace jsou aktualizovány na nejnovější verzi. Aktualizace často obsahují záplaty a opravy bezpečnostních chyb, které mohou zlepšit ochranu vašeho zařízení.
8) Používejte VPN službu: Virtuální privátní sítě (VPN) vytvářejí šifrovaný tunel mezi vaším zařízením a VPN serverem, což ztěžuje odposlech a sledování vašich online aktivit. Používání VPN může poskytnout další vrstvu bezpečnosti při připojení k veřejné Wi-Fi síti.
9) Zabezpečte své zařízení: Ujistěte se, že váš počítač, tablet nebo smartphone je chráněn heslem nebo jiným zabezpečením, jako je biometrická autentizace. Tímto způsobem zabráníte neoprávněnému přístupu k vašemu zařízení, pokud by bylo ztraceno nebo odcizeno.
10) Zvažte použití dvoufaktorové autentizace: Dvoufaktorová autentizace (2FA) poskytuje další vrstvu bezpečnosti pro vaše účty tím, že vyžaduje nejen heslo, ale také druhý faktor, jako je SMS kód nebo biometrická data. Tímto způsobem i když útočník získá vaše heslo, stále nebude moci získat přístup k vašemu účtu bez aplikačního kódu, který přichází většinou ve formě SMS nebo do bezpečnostní mobilní aplikace.

2.9 Vliv kybernetických hrozeb na mládež

Dokument *The Importance of Cybersecurity Education in School* se zabývá a zdůrazňuje potřebu výuky kybernetické bezpečnosti současně s uvědoměním si do jaké míry je obzvlášť mládež náchylná kybernetickým útokům. Dokument také poukazuje na potřebu kontinuálního vzdělávání v této oblasti už od útlého věku. Důležitým bodem je také fakt, že rodiče často nevědí, co jejich děti na internetu dělají, a tak se děti často stávají terčem mnohých podvodníků a útočníků. Dokument se také zmiňuje o jedincích, kteří jsou technologicky zdatní už v mladém věku a tím jsou např. vlastní zařízení nebo smartphony rodičů vystaveny riziku zneužití z důvodu prozkoumávání internetu bez jakýchkoli omezení nebo dohledu. Podle průzkumu tohoto dokumentu existuje celá řada výhod, pokud je škola schopna plně uplatňovat kybernetické vzdělávání. Podstatným faktem je zjištění, že dospělí jsou méně ochotni utrácet peníze a čas za různé druhy seminářů nebo programů o kybernetické bezpečnosti, a proto je důležité, aby se škola stala centrem znalostí a vystavovala by otázky o kybernetické bezpečnosti komunitě. Dokument také dává najevo, že oblast týkající se bezpečnosti, ve které studenti prokázali nejvyšší míru znalostí jsou kyberšikana nebo některé části sdílení osobních údajů.

Dokument *Relevance of Cybersecurity Education at Pedagogy Levels in Schools* se zaměřuje na roustoucí význam vzdělávání v oblasti kybernetické bezpečnosti zejména u dětí a mládeže. Autor zdůrazňuje potřebu využívání internetu v každodenním životě jako neodmyslitelnou část. Důležité je uvědomování si rizik spojené s jeho používáním. Za důležitou část článku považuji zaměření se na to, jak stále mladší děti mají přístup k internetu a stávají se schopnějšími v používání různých technologických zařízení, na kterých je komplikované sledovat jejich aktivitu. Článek také obsahuje stále se rozvíjející závislost na mikrotransakcích, které obsahují hry a aplikace a popisuje jejich jednoduché provedení.

Dokument *Cyber Security Education for Children Through Gamification: Challenges and Research Perspectives* se zaměřuje na vzdělávání dětí v oblasti kybernetické bezpečnosti pomocí tzv. gamifikace. Jedná se o efektivní způsob vzdělávání dětí, jejich motivace a angažovanost učení prostřednictvím herních prvků a principů. Jsou zde popsány vhodné designy her, doporučené věkové skupiny a genderové rozdíly v přístupu ke gamifikovanému vzdělávání. Dále dokument diskutuje o možnostech spolupráce mezi vzdělávacími institucemi a herními vývojáři z důvodu implementace těchto dvou odvětví.

3 CÍLE

3.1 Hlavní cíl

Zmapovat a popsat povědomí a chování studentů v oblasti kybernetické bezpečnosti a zhodnotit dopad vzdělávací intervence na zlepšení jejich ochrany proti kybernetickým útokům.

3.2 Dílčí cíle

1) Popsat různé typy kybernetických útoků a jak se jim lidé mohou vyhnout.
2) Provést průzkum mezi studenty na téma kybernetická bezpečnost a zjistit jejich povědomí a chování v této oblasti.
3) Na základě výsledků průzkumu přispět k optimalizaci strategií vedoucích ke zlepšení kybernetické bezpečnosti studentů.

3.3 Výzkumné otázky

1) Jak se liší povědomí a chápání kybernetické bezpečnosti mezi studenty, kteří prošli intervencí, a těmi, kteří nebyli součástí intervence?
2) Jak se liší návyky a chování studentů v oblasti kybernetické bezpečnosti (např. frekvence změny hesel, způsoby práce s hesly) mezi třídami s intervencí a bez intervence?
3) Jaký je vliv intervence na schopnost studentů identifikovat a reagovat na různé typy kybernetických útoků?

4 METODIKA

Můj výzkum byl realizován na Základní škole Jana Železného v Prostějově, kde již několik let působím jako trenér atletické přípravky. Během svého působení na škole jsem využil plánovaného školení Policie České republiky, které bylo zaměřeno na téma týkající se kybernetické bezpečnosti, kterého se účastnili někteří učitelé a žáci. Tuto příležitost jsem využil a oslovil učitele informatiky, zda bych mohl provést srovnávací studii mezi dvěma třídami – jednou, která prošla školením, a druhou, která školení neměla. Školení trvalo čtyři vyučovací hodiny, přičemž přibližně dvě třetiny času byly věnovány přednášce o ideálních návycích v kyberprostoru, nakládání s osobními daty, zabezpečení osobních zařízení, přístupu a autorizaci v internetovém prostředí. Zbývající čas byl věnován diskusi se studenty, kteří měli možnost klást otázky týkající se dané problematiky.

Praktickou část mého výzkumu jsem uskutečnil v říjnu 2021 prostřednictvím anketního šetření, které jsem aplikoval na obě třídy, a to papírovou formou. Vzhledem k tomu, že jsem výzkum prováděl během své pedagogické praxe, měl jsem s žáky několik hodin času na diskusi o tématu kybernetické bezpečnosti, což mi umožnilo získat co nejobjektivnější odpovědi na otázky v anketě.

Skupina, která prošla intervencí byla 8.B a bylo zde 25 studentů a z toho 12 chlapců a 13 dívek. Skupina, která intervencí neprošla byla 8.A, a to s počtem 26 studentů v poměru 15 chlapců a 11 dívek.

Otázky v anketním šetření neměly vzájemnou návaznost, a studenti byli vyzváni, aby odpovídali podle svých vlastních preferencí. Kvůli relativně malému počtu respondentů a velkému množství otázek nebyly statisticky signifikantní rozdíly mezi jednotlivými skupinami považovány ve většině případů za významné. Nicméně odpovědi na zásadní otázky týkající se bezpečnosti přinesly užitečné informace a poznatky.

Doplňující otázky do diskuse byly v obou třídách totožné a jednalo se o skupinový rozhovor, kde jsem si kladl za cíl zjistit od studentů co nejvíce informací, které neobsahovala anketa. Jednalo se o otázky, které měly doplňující charakter ankety.

V rámci anketního šetření jsem se zaměřil na následující klíčové oblasti:

1) Povědomí žáků o nejčastějších hrozbách spojených s kybernetickou bezpečností a sociálním inženýrstvím.
2) Schopnost žáků identifikovat a reagovat na potenciální hrozby, jako jsou phishingové e-maily, falešné webové stránky a manipulativní techniky.

3) Úroveň znalostí a dovedností žáků v oblasti nejlepších postupů pro kybernetickou bezpečnost, jako je používání silných a jedinečných hesel, dvoufaktorové autentizace a opatrné sdílení osobních informací online.

Na základě získaných dat jsem vyhodnotil a porovnal úroveň povědomí a dovedností žáků z obou tříd v oblasti kybernetické bezpečnosti. Toto srovnání mi poskytlo cenné informace o efektivitě školení PČR a o potřebách a zranitelnostech žáků, což může přispět k dalšímu rozvoji vzdělávacích programů v oblasti kybernetické bezpečnosti.

4.1 Výzkumný soubor

Výzkumný soubor mého výzkumu se skládal ze dvou skupin studentů. První skupina obsahovala 25 respondentů, zatímco druhá skupina měla 26 respondentů. Hlavním rozdílem mezi těmito skupinami bylo, že jedna skupina absolvovala školení o kybernetické bezpečnosti poskytnuté Policií České republiky, zatímco druhá skupina takovou intervencí neprošla.

Tento rozdíl v expozici školení umožnil srovnávat úroveň povědomí, znalostí a dovedností žáků v oblasti kybernetické bezpečnosti a sociálního inženýrství. Cílem bylo zjistit, zda školení poskytované Policií ČR přispívá k lepšímu chápání a přístupu k řešení potenciálních kybernetických hrozeb.

4.2 Metody sběru dat

Pro sběr dat jsem zvolil metodu anketního šetření, které bylo realizováno na základní škole v Prostějově. Výzkum probíhal během vyhrazených hodin informatiky, kdy se žáci mohli plně soustředit na vyplňování ankety.

Anketní šetření obsahovalo 15 otázek, které pokrývaly různé aspekty kybernetické bezpečnosti, včetně základního povědomí o hrozbách, schopnosti identifikovat potenciální rizika a aplikaci nejlepších postupů pro ochranu osobních informací.

Respondenti byli vyzváni, aby odpovídali na otázky upřímně a podle svého nejlepšího uvědomění. Bylo zdůrazněno, že neexistují žádné správné nebo špatné odpovědi a že jejich účast na výzkumu je důležitá pro získání objektivních výsledků a zlepšení povědomí o kybernetické bezpečnosti.

Kromě samotné ankety jsem se také rozhodl provést několik krátkých rozhovorů s vybranými žáky, aby bylo možné získat hlubší a podrobnější informace o jejich zkušenostech, názorech a postoji v oblasti kybernetické bezpečnosti. Tyto rozhovory mi umožnily lépe

pochopit, jak žáci vnímají a reagují na kybernetické hrozby, a také identifikovat potenciální oblasti pro zlepšení v jejich znalostech a dovednostech.

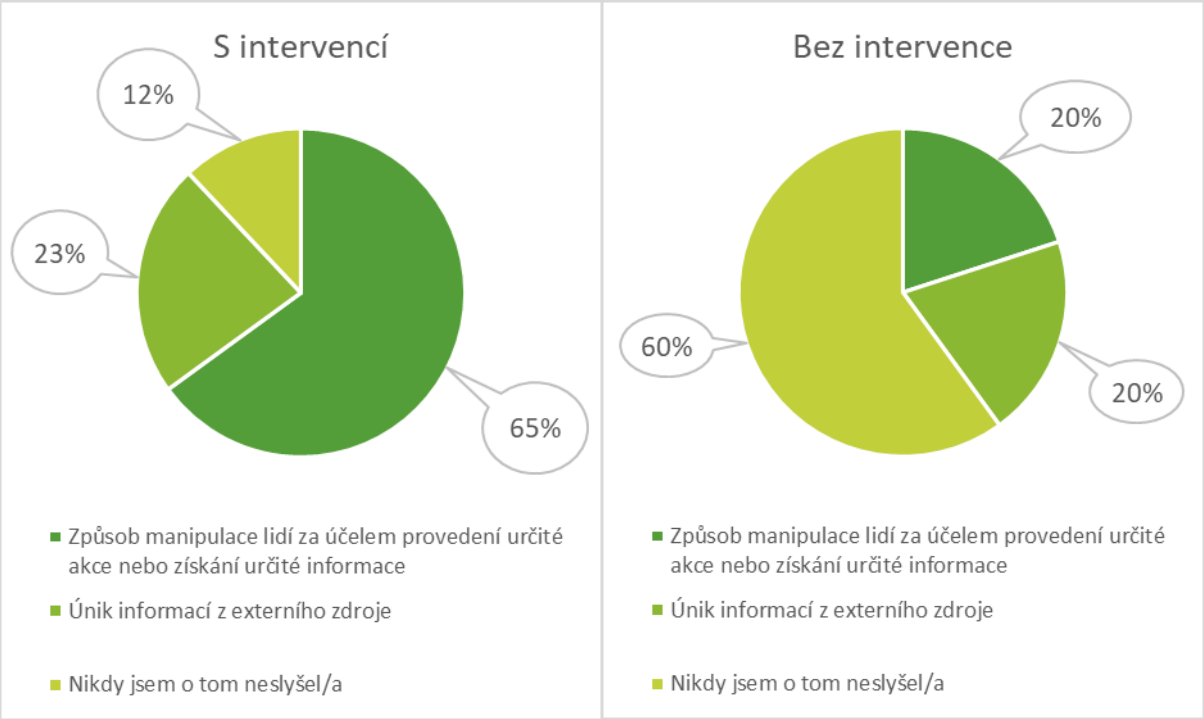
4.3 Statistické zpracování dat

Data z online ankety vytvořené pomocí Formulářů Google byla vyhodnocena pomocí software IBM SPSS a byly zde spočítány základní deskriptivní charakteristiky. K dalším analýzám – pro hodnocení rozdílů v relativních četnostech získaných odpovědí – bylo využito χ^2 testu (Campbell, 2007; Richardson, 2011) v prostředí online kalkulátoru MedCalc (MedCalc Software, 2022). Statistická významnost byla posuzována na hladině $\alpha = 0{,}05$.

5 VÝSLEDKY

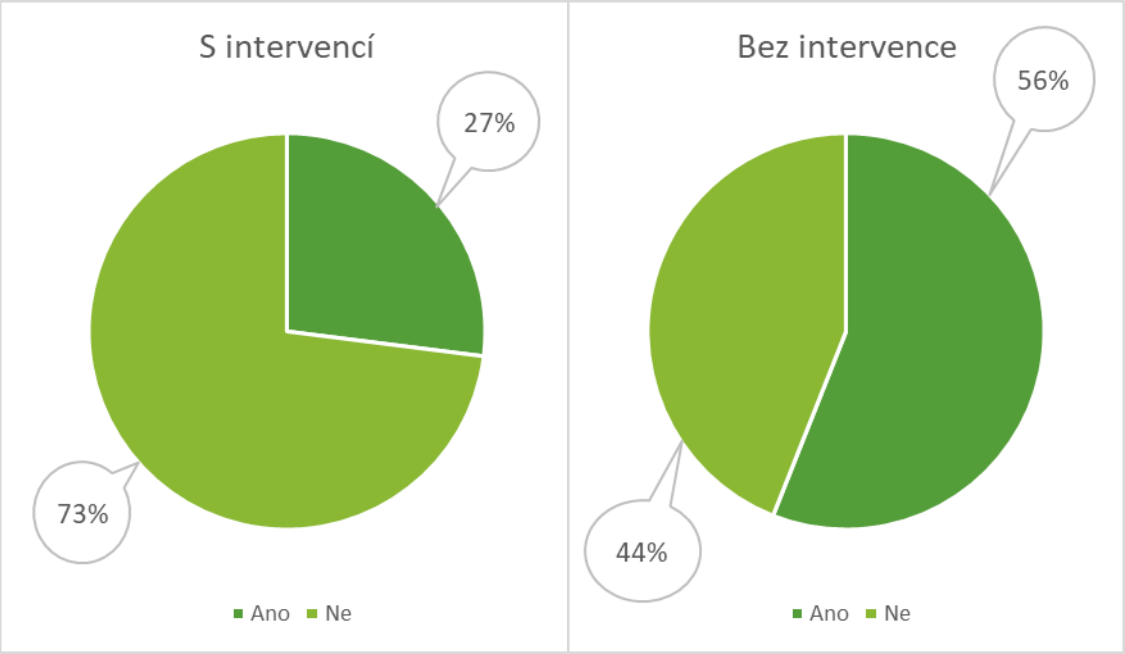
Shromáždění těchto dat a jejich následná analýza umožňuje identifikovat klíčové rozdíly mezi studenty, kteří prošli školením o kybernetické bezpečnosti a těmi, kteří ne. Výsledky poskytují důležité informace pro další vývoj vzdělávacích programů a opatření zaměřených na zvýšení povědomí o kybernetické bezpečnosti mezi širokou veřejností.

Vyhodnocení otázky 1: *„Co podle vás znamená pojem sociální inženýrství?“*



V odpovědích na otázku číslo 1: „Co podle vás znamená pojem sociální inženýrství?“ jsme zjistili mezi sledovanými třídami statisticky signifikantní rozdíl ($Z = 3,75$; $p = 0,04$). Z analýzy jednotlivých variant odpovědí vyplynulo, že žáci ze třídy, která prošla intervencí, častěji odpověděli správně ($\chi^2 = 10,38$; $p < 0,01$) než žáci ze třídy, kde intervence neproběhla. Žáci ze třídy, kde intervence neproběhla, významně četněji ($\chi^2 = 12,57$; $p < 0,01$) uvedli, že o tomto pojmu nikdy neslyšeli. Četnost třetí varianty odpovědi (nesprávné) se mezi třídami významně nelišila ($\chi^2 = 0,07$; $p = 0,80$).

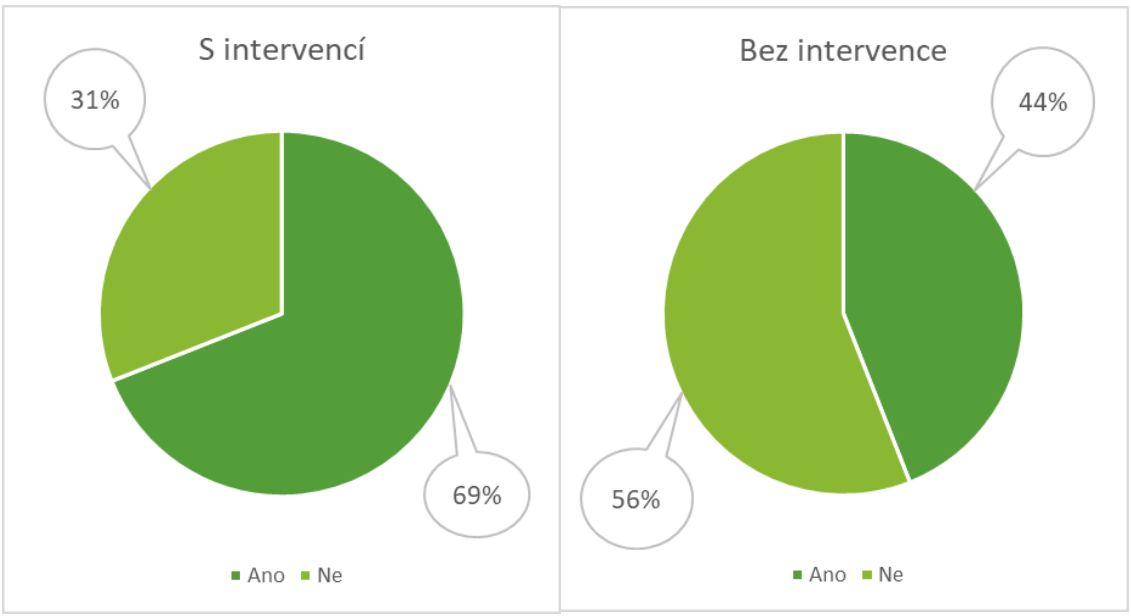
Vyhodnocení otázky 2: *„Využíváte ke správě svých osobních dat připojení k internetu přístupné na veřejných místech? (kavárny, restaurace, fitness)“*



Poznámka. Připojení na veřejnou wi-fi síť neznamená, že se útoky nedají minimalizovat.

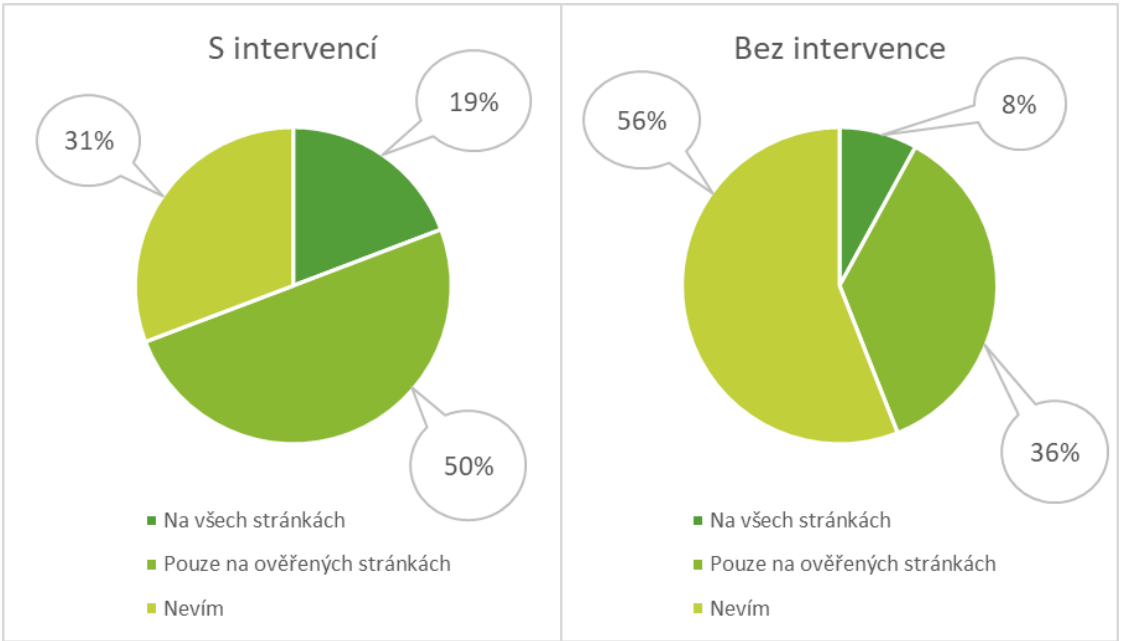
V odpovědích na otázku číslo 2: *„Využíváte ke správě svých osobních dat připojení k internetu přístupné na veřejných místech?“* byl zjištěn statisticky signifikantní rozdíl mezi sledovanými třídami ($Z = 2,09$; $p = 0,04$). Žáci, kteří prošli školením o kybernetické bezpečnosti, se významně méně spoléhají na veřejná Wi-Fi připojení pro správu svých osobních dat ($\chi^2 = 4,34$; $p = 0,04$).

Vyhodnocení otázky 3: *„Kontrolujete si URL adresu navštívené webové stránky?“*



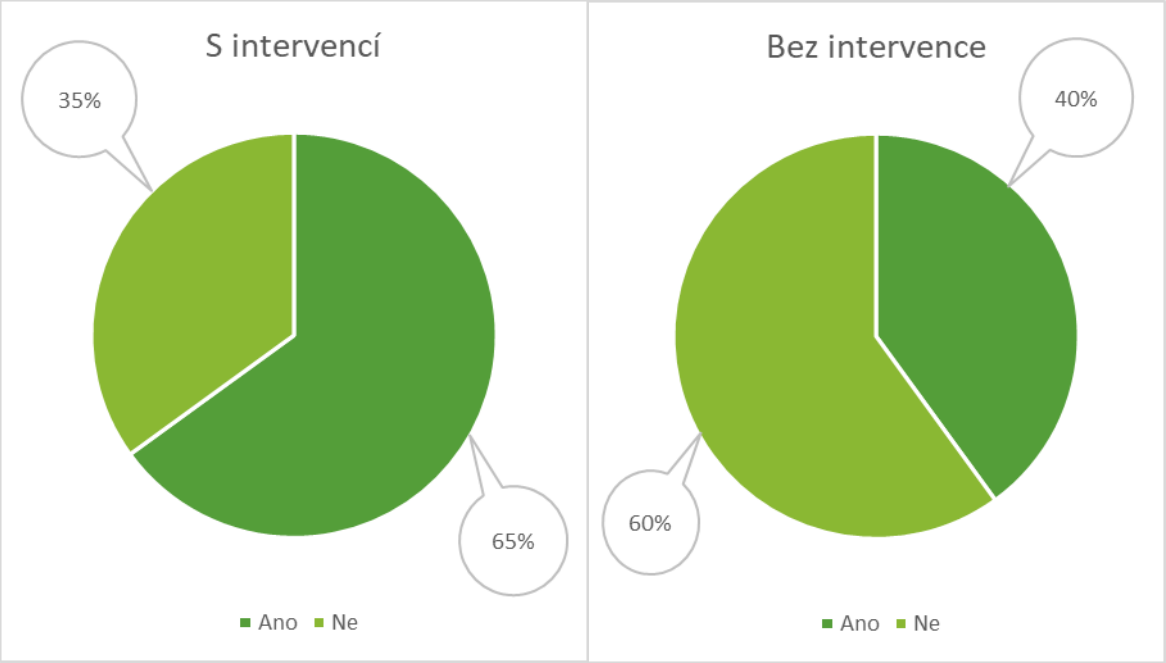
V odpovědích na otázku číslo 3: *„Kontrolujete si URL adresu navštívené webové stránky?“* nebyl nalezen statisticky signifikantní rozdíl mezi třídou, která absolvovala školení o kybernetické bezpečnosti, a třídou, která školení neprošla (Z = 1,80; p = 0,07).

Vyhodnocení otázky 4: *„Registrujete se na stránkách bez ověřeného certifikátu?“*



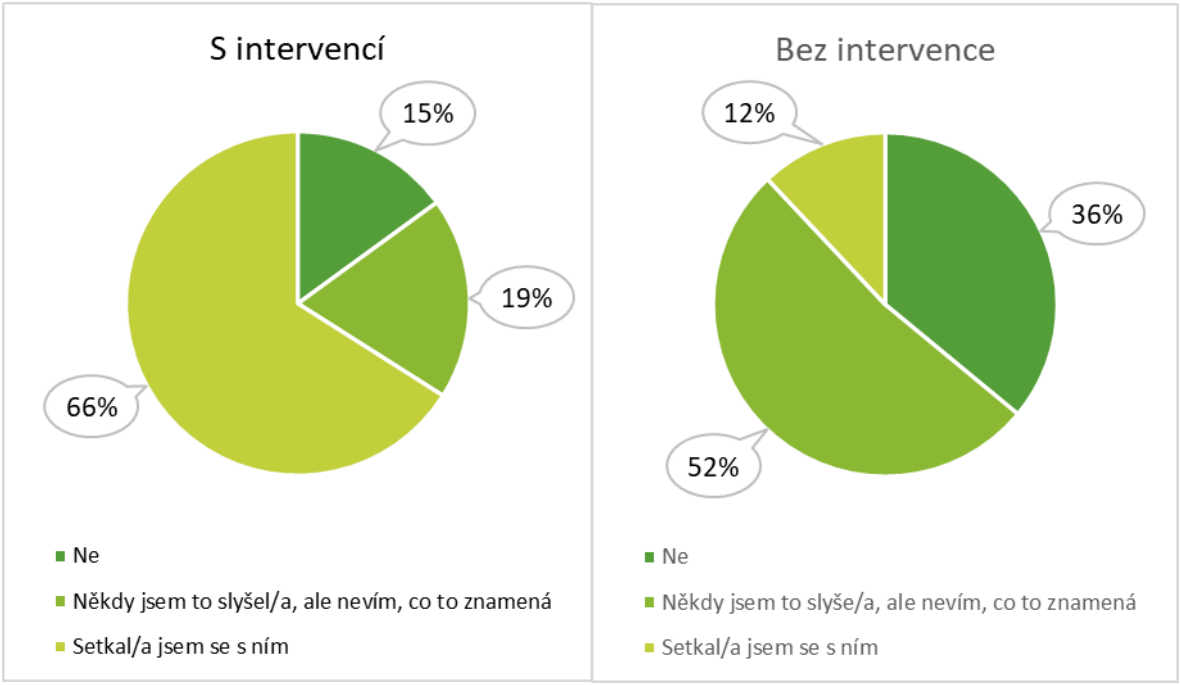
V odpovědích na otázku číslo 4*: „Registrujete se na stránkách bez ověřeného certifikátu?“* jsme nezjistili statisticky signifikantní rozdíl mezi skupinou studentů, kteří absolvovali školení o kybernetické bezpečnosti, a skupinou, která školení neprošla (Z = 1,88; p = 0,06).

Vyhodnocení otázky 5: *„Používáte na svém PC nelegální software?“*



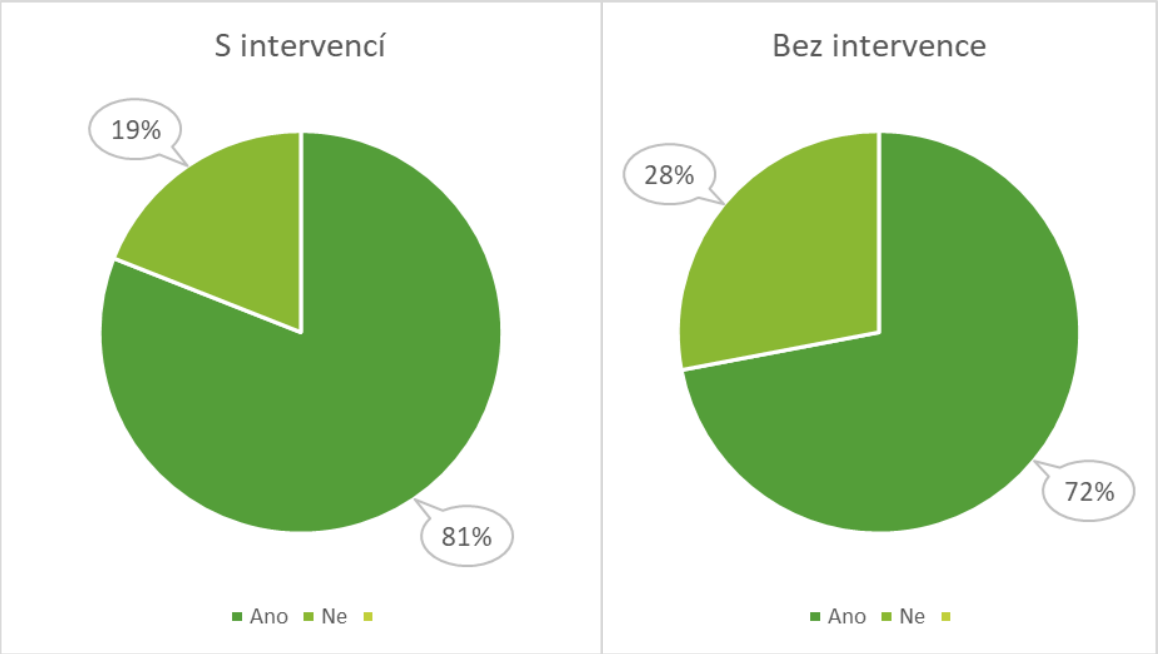
V odpovědích na otázku číslo 5: „Používáte na svém PC nelegální software?“ jsme nezjistili mezi sledovanými třídami statisticky signifikantní rozdíl (Z = 1,80; p = 0,07).

Vyhodnocení otázky 6: *„Říká vám něco pojem phishing?“*



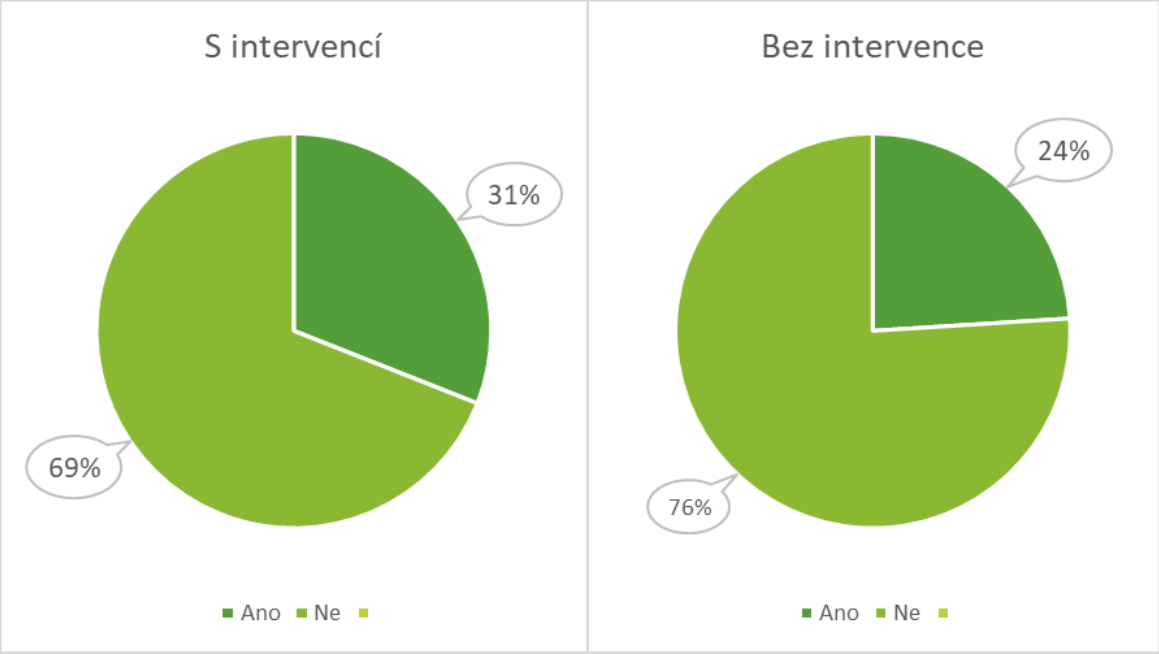
V odpovědích na otázku číslo 6: „Říká vám něco pojem phishing?“ jsme zjistili mezi sledovanými třídami statisticky signifikantní rozdíl ($Z = 3{,}42$; $p < 0{,}01$). Z analýzy jednotlivých variant odpovědí vyplynulo, že se významné rozdíly mezi třídami prokázaly v odpovědi „Setkal/a jsem se s ním“ ($\chi^2 = 14{,}75$; $p < 0{,}01$).

Vyhodnocení otázky 7: *„Používáte antivirový program?“*



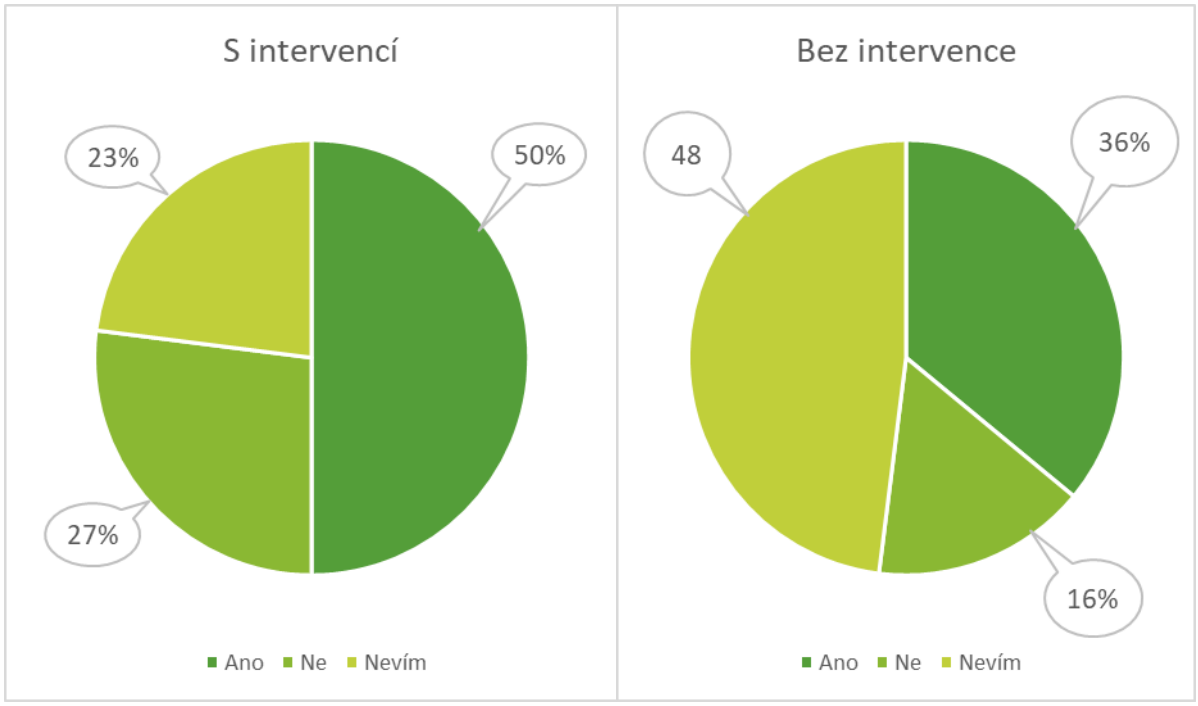
V odpovědích na otázku číslo 7: *„Používáte antivirový program?“* nebyl zjištěn statisticky signifikantní rozdíl mezi skupinou studentů, která prošla školením o kybernetické bezpečnosti, a skupinou, která školení neprošla (Z = 0,73; p = 0,47).

Vyhodnocení otázky 8: *„Používáte jiný zabezpečovací software než antivirus? (Anti-malware, VPN).“*



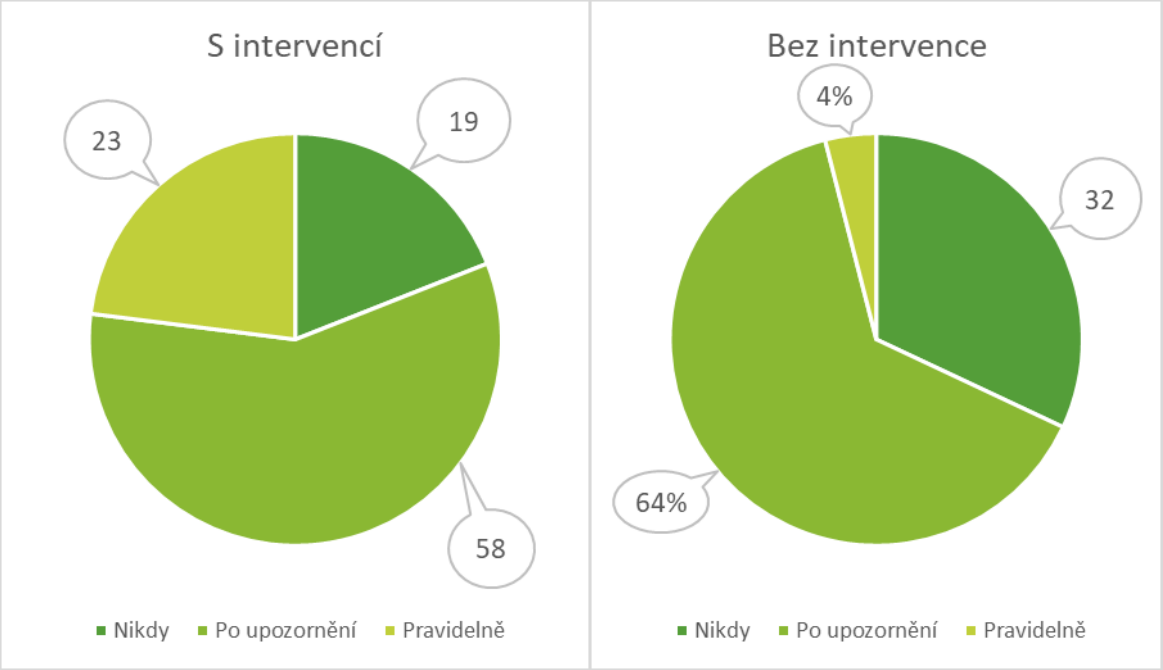
V odpovědích na otázku číslo 8: „Používáte jiný zabezpečovací software než antivirus? (Anti-malware, VPN)“ jsme nezjistili mezi sledovanými třídami statisticky signifikantní rozdíl (Z = 0,54; p = 0,59).

Vyhodnocení otázky 9: *„Máte nastavenou automatickou aktualizaci těchto programů?“*



V odpovědích na otázku číslo 9: „Máte nastavenou automatickou aktualizaci těchto programů?“ jsme nezjistili mezi sledovanými třídami statisticky signifikantní rozdíl (Z = 1,53; p = 0,13).

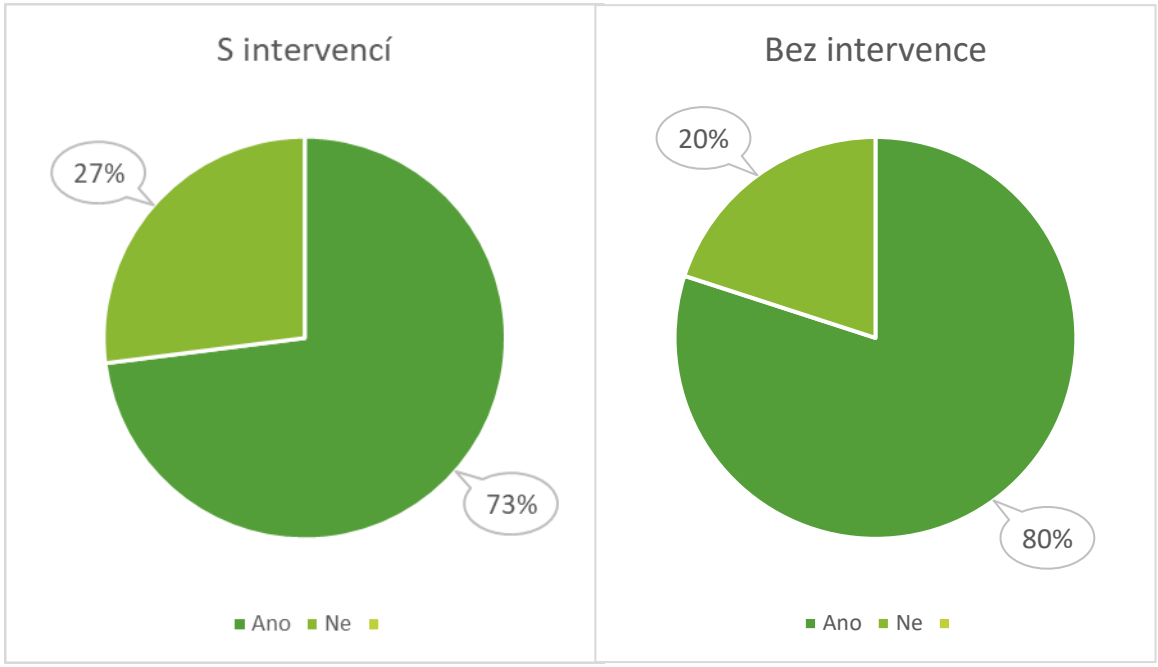
Vyhodnocení otázky 10: *„Jak často záměrně měníte svá hesla?“*



Poznámka. Tato otázka může být ovlivněna faktem, že servery často pravidelně vyžadují změnu hesel.

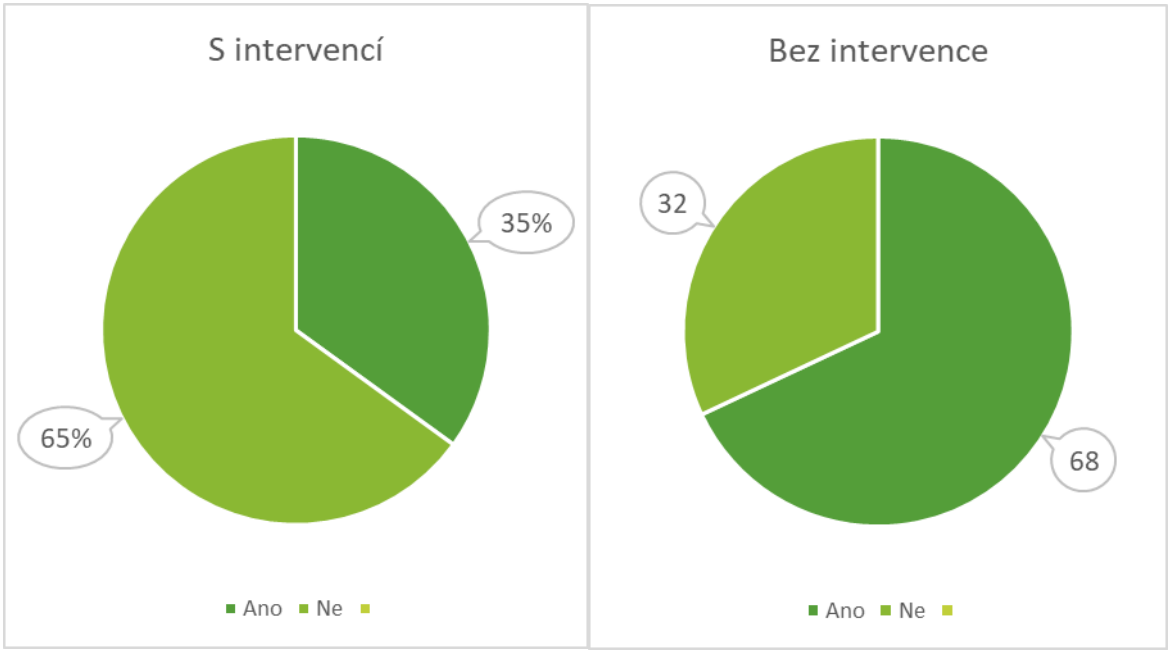
V odpovědích na otázku číslo 10: „Jak často záměrně měníte svá hesla?“ jsme nezjistili mezi sledovanými třídami statisticky signifikantní rozdíl ($Z = 1{,}78$; $p = 0{,}08$).

Vyhodnocení otázky 11: *„Při volbě hesla vždy používám kombinaci velkých a malých písmen, čísel a speciálních znaků.“*



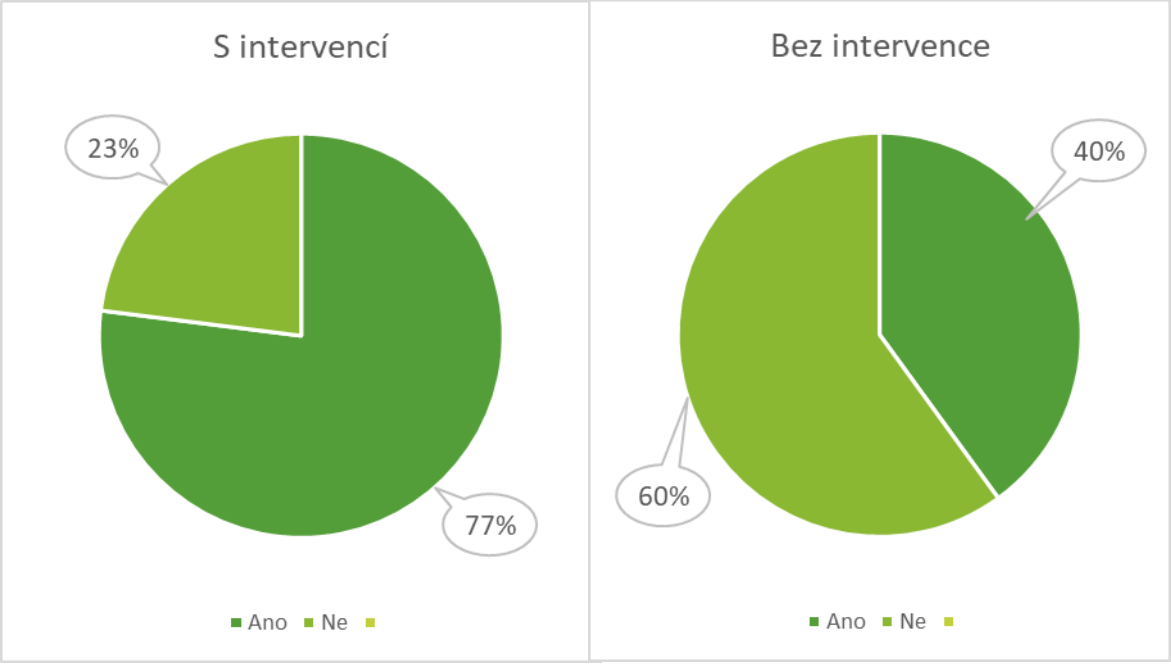
V odpovědích na otázku číslo 11: „Při volbě hesla vždy používám kombinaci velkých a malých písmen, čísel a speciálních znaků.“ jsme nezjistili mezi sledovanými třídami statisticky signifikantní rozdíl (Z = 0,58; p = 0,56).

Vyhodnocení otázky 12: *„Používáte nebo upřednostňujete dvoufaktorové ověření?“*



V odpovědích na otázku číslo 12: „Používáte nebo upřednostňujete dvoufaktorové ověření?“ jsme zjistili mezi sledovanými třídami statisticky signifikantní rozdíl (Z = 2,36; p = 0,02). Z analýzy jednotlivých variant odpovědí vyplynulo, že se významné rozdíly mezi třídami prokázaly v odpovědi „Ano“ (χ2 = 5,45; p = 0,02), i „Ne“ (χ2 = 5,45; p = 0,02). Myslím si, že důvodem těchto odpovědí mohou být i faktory jako složitost nebo čas strávený přidáním dvoufaktorového ověření k běžně zabezpečenému účtu. Z mé debaty se studenty lze zároveň usoudit, že i u skupiny, která prošla školením se zřejmě příliš nezmění přístup uživatelských přihlášení.

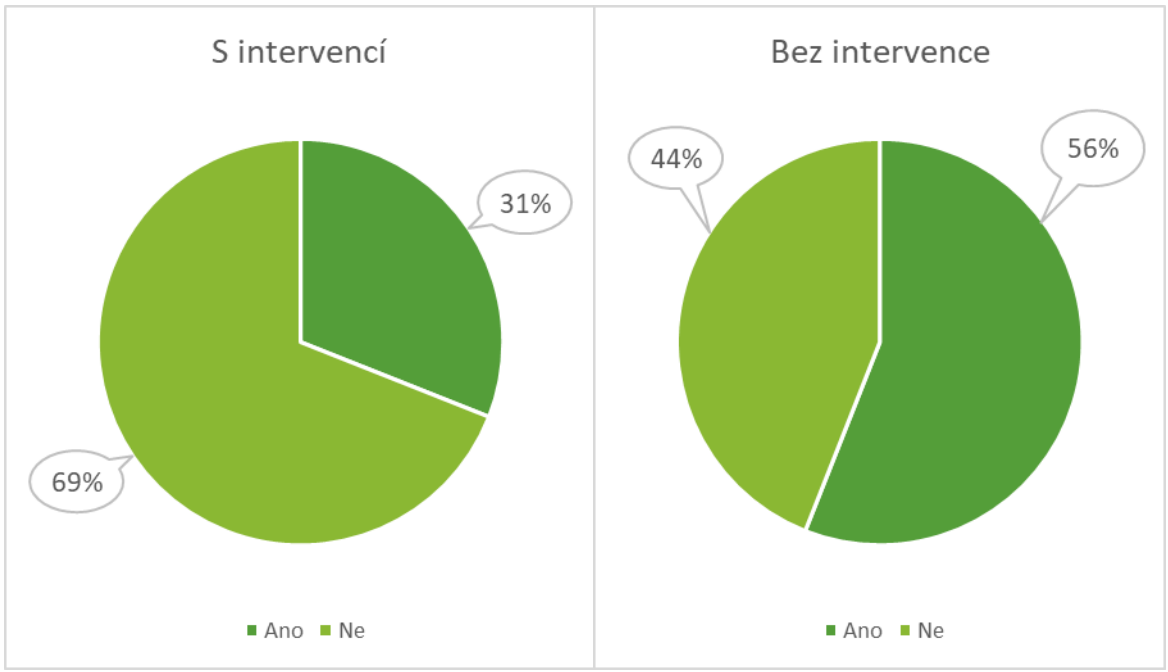
Vyhodnocení otázky 13: *„Setkali jste se někdy s emailem, který Vás odkazoval na finanční instituci a požadoval Vaše přihlášení v podobě loginu a hesla?“*



Poznámka. S podvodným e-mailem se dle zprávy FBI z roku 2020 setká v USA v průměru každá e-mailová schránky minimálně jednou denně.

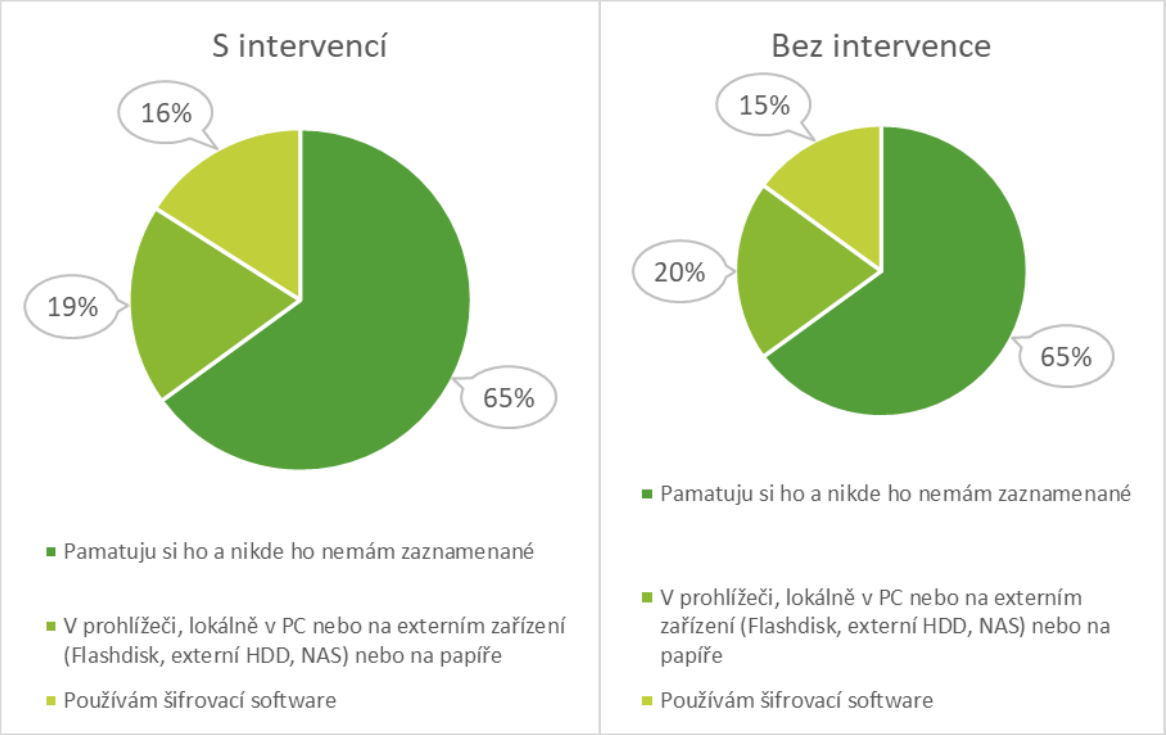
V odpovědích na otázku číslo 13: „Setkali jste se někdy s emailem, který Vás odkazoval na finanční instituci a požadoval Vaše přihlášení v podobě loginu a hesla?“ jsme zjistili mezi sledovanými třídami statisticky signifikantní rozdíl (Z = 2,65; p = 0,01). Z analýzy jednotlivých variant odpovědí vyplynulo, že se významné rozdíly mezi třídami neprokázaly v odpovědi „Ano“ (χ^2 = 7,06; p = 0,01), i „Ne“ (χ^2 = 7,06; p = 0,01).

Vyhodnocení otázky 14: *„Používáte pro přihlášení na různé stránky stejná hesla?“*



V odpovědích na otázku číslo 14: „Používáte pro přihlášení na různé stránky stejná hesla?“ jsme nezjistili mezi sledovanými třídami statisticky signifikantní rozdíl ($Z = 1,80$; $p = 0,07$). Z analýzy jednotlivých variant odpovědí vyplynulo, že se významné rozdíly mezi třídami neprokázaly v odpovědi „Ano“ ($\chi 2 = 3,45$; $p = 0,06$), ani „Ne“ ($\chi 2 = 3,18$; $p = 0,07$). V průběhu školení byly uváděny důvody, proč by uživatel neměl na stejných portálech uvádět stejná hesla a způsob, jakým byla tato problematika pojata (bezpečnost a napadení dalších účtů) lze předpokládat, že studenti s intervencí na tuto informaci reagovali.

Vyhodnocení otázky 15: *„Jak pracujete s hesly?“*



V odpovědích na otázku číslo 15: „Jak pracujete s hesly?“ jsme nezjistili mezi sledovanými třídami statisticky signifikantní rozdíl ($Z = 0,71$; $p = 0,48$).

6 DISKUSE

V průběhu analýzy výsledků ankety lze pozorovat, že studenti, kteří absolvovali školení kybernetické bezpečnosti od Policie ČR, byli v průměru o něco obezřetnější při pohybu v kyberprostoru, a to v klíčových událostech. Tito studenti byli lépe informováni o potenciálních hrozbách a velké rozdíly lze zpozorovat např. u otázky týkající se bezpečnosti sítí nebo phishingu, kterému jsem v přehledu poznatků věnoval značnou část. Nicméně je důležité podotknout, že i mezi skupinou s intervencí je spousta studentů, kteří ignorují nabyté informace. Tito studenti se mohou stále chovat riskantně a neuplatňovat zásady kybernetické bezpečnosti, což ukazuje na určitou míru neponaučitelnosti. Tato skutečnost poukazuje nejen na potřebu častějšího školení, ale také pravidelného opakování a získávání informací o kybernetické bezpečnosti, aby se zvýšilo povědomí i zájem studentů v této problematice. Je také důležité přizpůsobit přístup a obsah školení potřebám a zájmům studentům, aby bylo pro ně relevantnější a zajímavější.

První otázka: *„Co podle vás znamená pojem sociální inženýrství?*“ se ukázala ve skupině, která prošla intervencí, jako přínosná (následovala diskuse na téma sociální inženýrství). První otázka byla vstupní otázka, která má pouze znalostní charakter daného pojmu. Tento výsledek přikládám k faktu, že pojem sociální inženýrství prozatím nenabyl patřičné popularity na internetu a studenti mají tedy minimální pravděpodobnost, že na tento pojem narazí.

Druhá otázka: *„Využíváte ke správě svých osobních dat připojení k internetu přístupné na veřejných místech? (kavárny, restaurace, fitness)*. I v tomto případě proškolená skupina odpověděla ve vyšší míře, pro odpověď negativní. Dá se tedy předpokládat, že důvodem bylo právě absolvované školení, ve kterém se studenti dozvěděli, jaké jsou hrozby, které mohou na veřejných sítích zařízení napadnout. Po skončení testu u skupiny s intervencí jsem položil otázku, zda se studenti připojují na veřejných místech výjimečně.

Odpovědí byla ve většině případů „Pouze v nejnutnějších případech“ nebo „Z bezpečnostních důvodů využívám mobilní data“. Viz kapitola *Způsoby zabezpečení na veřejné síti*. Ve skupině bez intervence byly odpovědi dělené téměř napůl, přičemž lze předpokládat, že se na odpovědích podílí jak neabsolvování školení, tak fakt, že nynější doba přispívá k bohatému obsáhnutí tarifů i studentů základních škol a nemají tedy zapotřebí využívat připojení k veřejné síti. Při diskusi v této skupině jsem se setkal i se studenty, kteří byli toho názoru, že jsou data v bezpečí a nemají o ně žádný strach.

Třetí otázka: *„Kontrolujete si URL adresu navštívené webové stránky?“.* Dle mého názoru se jedná o klíčovou otázku týkající se kybernetické bezpečnosti. Jsou známy případy, kdy dokonce IT specialisté se stávají oběťmi útoků, které lze snadno odhalit právě kontrolou obyčejného řádku URL, kterým disponuje každý známý webový prohlížeč (Google Chrome, Edge,

Mozilla Firefox, Safari, Opera). V nedávném rozhovoru na tuto bezpečnost upozorňovat bezpečnostní ředitel O2 Radek Šichtanc.

Jedná se o otázku, u které se domnívám, že by se měla stát heslem pro tzv. „surfování po internetu". „Nejslabším místem IT bezpečnosti je a bude člověk. I ten opravdu zkušený". Radek Šichtanc (2022).

Na třetí otázku v anketě hlasovala proškolená skupina studentů v tomto případě kladně téměř v ¾ případů, což mě mile potěšilo, a i zde lze předpokládat, že školení mělo patřičný význam. U skupiny bez intervence byla kladná odpověď méně než poloviční a po následné diskusi se studenty jsem nabyl dojmu, že je tato hodnota ještě menší. U obou skupin jsem položil otázku, z jakého důvodu si své URL adresy nekontrolují a odpovědi byly různorodé. Nejčastější odpovědi: 1) Je to ztráta času 2) Poznám, když jsem na správné stránce 3) Nevěděl/a jsem, že je v tom rozdíl.

Dle mých průběžných výsledků mohu říct, že jsou kybernetické hrozby, o kterých uživatelé vůbec netuší.

Antivirová společnost *Norton (2022)* uvádí na serveru *Securityweek* anonymní dotazník, ve kterém zazněla totožná otázka s pouhými 28 % kladných odpovědí. Proto se tedy domnívám, že mé tvrzení o chybách z nedbalosti a nevědomosti jsou správné.

Čtvrtá otázka: *„Registrujete se na stránkách bez ověřeného certifikátu?".*

Otázka je zamýšlena tak, zda při registraci na webu studenti dbají na absenci SSL certifikátu či nikoli. U první skupiny, která prošla školením se polovina studentů rozhodla pro odpověď: „Pouze na ověřených stránkách" a ¼ studentů si je vědoma toho, že se registrují na všech stránkách, a proto jsem se rozhodl při diskusi tuto otázku dále probrat se studenty, při které jsem vyvodil závěr, že studenti, kteří se registrují na všech webových stránkách se registrují z toho důvodu, aby měli často k dispozici zdarma placený obsah a nemuseli dané služby (hry, aplikace, filmy) kupovat. Lze tedy konstatovat, že i přes znalost tohoto nebezpečí vyměňuje skupina znalých studentů peníze za bezpečnost. Zbylá větší třetina studentů neví, na kterých webových stránkách se registruje a nekontroluje nebo nemá povědomí o SSL certifikátech. U skupiny bez intervence si není více než polovina studentů jistá, na kterých stránkách se registrují a je tedy tato hodnota podle očekávání daleko vyšší než u předešlé skupiny s intervencí. Lze tedy předpokládat, že tato reálná hodnota je ještě vyšší.

Pátá otázka: „Používáte na svém PC nelegální software?". Tato otázka neměla u obou skupin signifikantní rozdíly a procentuálně převládala odpověď „Ano" u skupiny bez intervence. Tudíž jsem se pustil do diskuse se studenty a vyplynulo najevo, že převažujícím důvodem je u obou tříd placený software. Dá se tedy předpokládat, že většina respondentů si daný software stahuje ze serverů typu *Ulož.to, WebShare, Hellspy, Datoid* nebo prostřednictvím *torrentů*.

Zde je vysoké riziko nakažení zařízení malwarem, ale valná většina studentů si je vědoma přítomnosti antivirových programů, které tyto typy nákaz pomáhají minimalizovat a spoléhají na ně.

Z těchto odpovědí výsledky naznačují, že školení o kybernetické bezpečnosti nemělo významný vliv na používání nelegálního softwaru mezi žáky v obou třídách, což může být způsobeno faktory, jako je osobní zkušenost, rodinné prostředí nebo zdroje informací, které nebyly předmětem školení.

Myslím si, že vliv na odpovědi na tuto otázku jsou vysoce individualizované a uživatel je přesvědčen, že platit za jakýkoliv software není jeho povinností, a to i na úkor bezpečnostních hrozeb. Zároveň lze potvrdit, že lidé spoléhají na antivirové programy a další bezpečnostní software.

Šestá otázka: *„Říká vám něco pojem phishing?“.* Taktéž jako první otázka se jedná o otázku mající pouze znalostní charakter daného pojmu. U skupiny s intervencí se kladné odpovědi přiblížily ¾ respondentů a jsou tedy obeznámeni s tímto pojmem. Druhá skupina bez intervence se k této otázce kladně vyjádřila pouze ve výjimečných případech. Lze očekávat, že se s phishingem setkalo velké množství všech testovaných lidí, ale neprokázalo znalost v této problematice. Myslím si tedy, že dané školení v tomto ohledu přineslo pozitivní ohlasy.

Sedmá otázka: „Používáte antivirový program?“. U obou skupin se prokázala ve velké míře odpověď „Ano“ a důvodem, si myslím, je ten fakt, že se jedná o nejvíce diskutované téma, na které uživatel naráží jak v časopisech, tak na internetu. Nejedná se tedy o klíčovou bezpečnostní absenční hrozbu uživatelů.

Osmá otázka: *„Používáte jiný zabezpečovací software než antivirus? (Anti-malware, VPN)“*. V odpovědích na tuto otázku bylo až překvapivě velké množství kladných odpovědích bez ohledu na testované skupiny, které byly téměř totožné. V diskusi se na tuto otázku také přihlásili jedinci, kteří odpověděli v otázce *„Využíváte ke správě svých osobních dat připojení k internetu přístupné na veřejných místech? (kavárny, restaurace, fitness).* kladně a doplnili přítomnost služby VPN na svém zařízení. Tím velice spolehlivě minimalizovali viditelnost svého zařízení na veřejné síti a lze tedy říct, že jsou zde tací, kteří si své soukromí chrání pokročilejšími způsoby jako je zmíněná služba VPN. Více se o tuto problematiku zajímám v kapitole *Anonymita*.

Devátá otázka: *„Máte nastavenou automatickou aktualizaci těchto programů?“.* U intervenční skupiny celá polovina studentů odpověděla kladně, jelikož při školení byla jedna z dílčích úkolů si zkontrolovat na svém osobním zařízení právě aktualizace bezpečnostního softwaru. Pouze necelá ¼ studentů neměla o potřebě aktualizací u bezpečnostních programů povědomí. U skupiny bez intervence dle očekávání převažovala odpověď „Nevím“ a lze předpokládat, že si tuto potřebnou funkcionalitu na svém osobním zařízení nehlídají.

Aktualizace databází považuji za velice důležitou část prevence, a to z důvodu vzniku nových bezpečnostních hrozeb a na které vývojáři bezpečnostního softwaru odpovídají pomocí záplat. I zde tedy mělo školení určitý vliv právě v oblasti prevence.

Desátá otázka: *„Jak často záměrně měníte svá hesla?“*. Otázku na téma ohledně přihlašovacích hesel považuji za klíčovou, a ne nadarmo koluje v IT bezpečnosti rčení, že nejslabším článkem v bezpečnosti je člověk. Zde se rozdíly mezi jednotlivými třídami prokázaly po absolvování školení vyšší. V obou případech převládaly možnosti „Až po upozornění“, což je důležitá funkcionalita na webových stránkách, ale je třeba mít na paměti, že touto funkcí nedisponují všechny weby. Proto nejlepší prevence je pravidelná změna hesel. Uživatel by měl změnit heslo i na základě neočekávané aktivity na účtu, které lze na sofistikovanějších službách zobrazit. Dále je tohle množství odpovědí dle mého názoru zapříčiněno také tím, že se servery bez změny hesla při upozornění potřeby heslo změnit, odmítne uživatele přihlásit.

Důvodů, proč měnit svá hesla je hned několik, ovšem z mého pohledu je nejdůležitějším důvodem především častý únik databází z všemožných serverů, které obsahují přihlašovací údaje.

Jedenáctá otázka: „*Při volbě hesla vždy používám kombinaci velkých a malých písmen, čísel a speciálních znaků.“*

Odpovědi na tyto otázky jsou u obou skupin ze ¾ zodpovězené kladně a domnívám se, že mohou být důvodem častá „vynucení“ těchto kombinací samotnými weby. Jedná se tedy o poměrně velkou úspěšnost v odpovědích na tuto otázku. Je zapotřebí brát v potaz, že stále existují servery, které tuto kombinaci nevyžadují a představují potenciální riziko pro uživatele. Absence kombinací těchto znaků je častým terčem útoků tzv. „hrubou silou“. Jedná se o útok, který má snahu rozluštit heslo bez přítomnosti dešifrovacího klíče. V praxi to znamená, že útočník má k dispozici pouze výkonný hardware, na kterém probíhá automatizovaný útok, tedy zkoušení kombinací písmen, čísel a znaků v náhodném pořadí. Nebezpečnější alternativu představuje „slovníkový útok“ při kterém má útočník k dispozici hesla z uniklých databází.

Dvanáctá otázka: „*Používáte nebo upřednostňujete dvoufaktorové ověření?“.* U odpovědí na tuto otázku se překvapivě vyšší úspěšnost prokázala u skupiny, která neprošla intervencí a sice téměř o dvojnásobek. Dle mého názoru si často uživatelé aktivují dvoufaktorové ověření až v moment, kdy se stane sám obětí napadení.

Mohu tedy konstatovat, že informace ohledně prevence zabezpečení a síly svého bezpečnostního hesla nejsou pro většinu studentů prioritní a přikládají důraz síle svého hesla. Možnosti, kterými by útočník překonal dvoufaktorové ověření (2FA) zde samozřejmě jsou, ale nelze popřít, že 2FA výrazně zabezpečuje účty prostřednictvím e-mailu nebo mobilního telefonu.

Dle společnosti Microsoft je dvoufaktorové ověření schopno zablokovat až 99,9 % automatizovaných útoků.

Třináctá otázka: *„Setkali jste se někdy s emailem, který Vás odkazoval na finanční instituci a požadoval Vaše přihlášení v podobě loginu a hesla?“.*

V odpovědích na tuto otázku se rozdíly ve skupinách prudce lišily a to tak, že ve skupině s intervencí se 77 % respondentů s tímto druhem e-mailu setkalo, kdežto ve druhé skupině to byla pouze třetina respondentů. Dle mého názoru se může jednat o důvod neznalosti daných uživatelů v problematice phishingových útoků a většina potenciálních obětí není schopna tento typ útoku analyzovat. Myslím si tedy, že zde obzvláště důležitou roli sehrálo zmiňované školení. Více jsem se věnoval této problematice v kapitole *Sociální inženýrství a jeho metody*.

Čtrnáctá otázka: *„Používáte pro přihlášení na různé webové stránky stejná hesla?“.* Zde si skupina s intervencí vedla velice dobře a to v 69 %, což určitě přisuzuji danému školení, na kterém se studenti dozvěděli důvody, proč je důležité na různých webech používat různá hesla. Skupina, která intervencí neprošla se v silnější polovině pohybuje s negativní odpovědí a usuzuji, že si nejsou tohoto rizika vědomi. Jedná se tedy o důležitou informaci týkající se osobní bezpečnosti. Důvodem tohoto bezpečnostního pravidla je především únik databází na veřejný internet a používá-li uživatel dané heslo i na jiných webech, je prokazatelně vyšší pravděpodobnost prolomení účtu právě na jiném serveru. Školení kybernetické bezpečnosti se prokázalo u této otázky jako velice přínosné.

Patnáctá otázka: *„Jak pracujete s hesly?“.* U této otázky jsou téměř shodné odpovědi u obou skupin, kde převažuje ve 2/3 odpověď „Pamatuji si ho a nikde ho nemám zaznamenané“. Myslím si, že důležitým faktorem u této otázky je lidská lenost, která je zde paradoxně ku prospěchu věci, jelikož je to nejbezpečnější způsob. Jakékoli jiné zaznamenávání hesel zvyšuje šance na únik. Nelze ovšem popřít, že znalost uživatelů není zcela dostačující i z pohledu internetových prohlížečů, při kterých uživatelé svá hesla častokrát ukládá do nezabezpečených klíčenek internetových prohlížečů bez svého vědomí.

7 ZÁVĚRY

Z výsledků práce vyplývá, že povědomí a chápání mezi studenty, kteří prošli intervencí a těmi, kteří nebyli součástí intervence, bylo zjištěno, že skupina studentů, kteří se zúčastnili školení, měla větší povědomí o rizicích připojování k internetu na veřejných místech, kontrola URL řádku nebo ověřených certifikátů. Naopak se neprokázaly významné rozdíly ve využívání nelegálního software, antivirových a doplňkového bezpečnostního software a myslím si, že tento důvod má charakter zvyku.

Návyky a chování studentů při práci s hesly se zdají být ovlivňovány jednotlivými servery, které po uživateli vyžadují změnu hesel v daných intervalech nebo po patřičné události a zároveň vyžadují podmínky kladené na složitost hesla, ale při dvoufaktorovém ověření a využívání stejných hesel na různých serverech se prokázal významný rozdíl ve prospěch školené skupiny a považuji tuto znalost za klíčovou.

Pozitivní vliv školení se prokázal i v oblasti phishingových útoků a skupina s intervencí v porovnání skupinou druhou téměř excelovala, a to především v dialozích týkajících se phishingových technik.

Závěrem tedy mohu říct, že informace v oblasti kybernetické bezpečnosti předávané ve školské instituci se zdají být ideální pro zvýšení povědomí této problematiky ve společnosti.

8 SOUHRN

Diplomová práce pojednává o aktuálních celosvětových kybernetických hrozbách a způsobech napadení v kybernetickém prostoru. Snahou v mé diplomové práci bylo poskytnout běžným uživatelům pohybujících se v internetovém prostředí potřebné informace, týkající se kybernetické bezpečnosti, se zaměřením na aktuální nejnovější trendy.

Definoval jsem jasně základní pojmy vztahující se ke kybernetické bezpečnosti, bez kterých, dle mého názoru, by čtenář nebyl schopen dále správně chápat tuto problematiku. Pojmy jako kybernetické prostředí, kybernetická kriminalita nebo sociální inženýrství byly charakterizovány a vysvětleny a důraz se také kladl na typy útočníků, jako jsou amatéři, hackeři, profesionálové a útočníky programovaní roboti nazývání jako automatizovaní boti.

Dále se práce věnuje sociálnímu inženýrství a jeho metodám, kde jsem se zaměřil vedle anonymity uživatele a bezpečnosti na síti také na možné napadení uživatele prostřednictvím phishingu v kombinaci se stále populárnějšími kryptoměnami, které se v poslední době staly terčem těchto útoků. Důležitá je prevence a kontinuální vzdělávání v oblasti kybernetické bezpečnosti.

Hlavním cílem diplomové práce bylo zmapovat a popsat povědomí a chování studentů v oblasti kybernetické bezpečnosti a zhodnotit dopad vzdělávací intervence na zlepšení jejich ochrany proti kybernetickým útokům. Dílčími cíli bylo popsat různé typy kybernetických útoků a jak se jim lidé mohou vyhnout, provést průzkum mezi studenty na téma kybernetická bezpečnost a zjistit jejich povědomí a chování v této oblasti, a nakonec na základě výsledků průzkumu přispět k optimalizaci strategií vedoucích ke zlepšení kybernetické bezpečnosti studentů.

Průzkum mezi studenty jsem prováděl na Základní škole Jana Železného v Prostějově, kde se konalo školení Policie České republiky, které bylo zaměřeno na téma týkající se kybernetické bezpečnosti. Školení trvalo čtyři vyučovací hodiny, přičemž přibližně dvě třetiny času byly věnovány přednášce o ideálních návycích v kyberprostoru, nakládání s osobními daty, zabezpečení osobních zařízení, přístupu a autorizaci v internetovém prostředí.

Praktickou část mého výzkumu jsem uskutečnil v říjnu 2021 prostřednictvím anketního šetření, které jsem aplikoval na obě třídy, a to papírovou formou. Vzhledem k tomu, že jsem výzkum prováděl během své pedagogické praxe, měl jsem s žáky několik hodin času na diskusi o tématu kybernetické bezpečnosti, což mi umožnilo získat co nejobjektivnější odpovědi na otázky v anketě. Skupina, která prošla intervencí byla 8.B a bylo zde 25 studentů a z toho 12 chlapců a 13 dívek. Skupina, která intervencí neprošla byla 8.A, a to s počtem 26 studentů v poměru 15 chlapců a 11 dívek. Data z online ankety vytvořené pomocí Formulářů Google byla vyhodnocena

pomocí software IBM SPSS a byly zde spočítány základní deskriptivní charakteristiky. K dalším analýzám – pro hodnocení rozdílů v relativních četnostech získaných odpovědí – bylo využito χ^2 testu (Campbell, 2007; Richardson, 2011) v prostředí online kalkulátoru MedCalc (MedCalc Software, 2022). Statistická významnost byla posuzována na hladině $\alpha = 0,05$.

Z výsledků práce je zřejmé, že dostatek informací v oblasti kybernetické bezpečnosti předávané prostřednictvím školních přednášek jsou klíčové pro bezpečný pohyb v kyberprostoru, přičemž zaznamenaný rozdíl u obou skupin byl největší v oblasti síťové bezpečnosti.

Z výsledků práce vyplývá, že povědomí a chápání mezi studenty, kteří prošli intervencí a těmi, kteří nebyli součástí intervence, bylo zjištěno, že skupina studentů, kteří se zúčastnili školení, měla větší povědomí o rizicích připojování k internetu na veřejných místech, kontrola URL řádku nebo ověřených certifikátů. Naopak se neprokázaly významné rozdíly ve využívání nelegálního software, antivirových a doplňkového bezpečnostního software a myslím si, že tento důvod má charakter zvyku.

Návyky a chování studentů při práci s hesly se zdají být ovlivňovány jednotlivými servery, které po uživateli vyžadují změnu hesel v daných intervalech nebo po patřičné události a zároveň vyžadují podmínky kladené na složitost hesla, ale při dvoufaktorovém ověření a využívání stejných hesel na různých serverech se prokázal významný rozdíl ve prospěch školené skupiny a považuji tuto znalost za klíčovou.

Pozitivní vliv školení se prokázal i v oblasti phishingových útoků a skupina s intervencí v porovnání skupinou druhou téměř excelovala, a to především v dialozích týkajících se phishingových technik.

Závěrem tedy mohu říct, že informace v oblasti kybernetické bezpečnosti předávané ve školské instituci se zdají být ideální pro zvýšení povědomí této problematiky ve společnosti.

9 SUMMARY

The diploma thesis discusses current global cyber threats and methods of attack in cyber space. The effort in my diploma thesis was to provide ordinary users moving in the Internet environment with the necessary information regarding cyber security, focusing on the latest trends.

I have clearly defined the basic concepts related to cyber security, without which, in my opinion, the reader would not be able to further understand this issue correctly. Concepts such as the cyber environment, cybercrime or social engineering were characterized and explained, and emphasis was also placed on the types of attackers, such as amateurs, hackers, professionals and attacker-programmed robots called automated bots.

Furthermore, the work is devoted to social engineering and its methods, where, in addition to user anonymity and security on the network, I also focused on the possible attack of the user through phishing in combination with increasingly popular cryptocurrencies, which have recently become the target of these attacks. Prevention and continuous education in the field of cyber security is important.

The main goal of the thesis was to map and describe the awareness and behavior of students in the field of cyber security and to evaluate the impact of an educational intervention on improving their protection against cyber attacks. The sub-goals were to describe the different types of cyber attacks and how people can avoid them, to conduct a survey among students on the topic of cyber security and to find out their awareness and behavior in this area, and finally, based on the results of the survey, to contribute to the optimization of strategies leading to the improvement of cyber security of students .

I conducted the survey among students at the Jan Železný Elementary School in Prostějov, where the Czech Republic Police training was held, which was focused on the topic of cyber security. The training lasted four class hours, with approximately two-thirds of the time devoted to a lecture on ideal cyberspace habits, handling of personal data, security of personal devices, access and authorization in the Internet environment.

I carried out the practical part of my research in October 2021 through a survey, which I applied to both classes, in paper form. Since I conducted the research during my teaching practice, I had several hours of time to discuss the topic of cyber security with the students, which allowed me to get the most objective answers to the survey questions. The group that underwent the intervention was 8.B and there were 25 students, of which 12 were boys and 13 were girls. The group that did not undergo the intervention was 8.A, with 26 students in the ratio of 15 boys and 11 girls. Data from an online survey created using Google Forms was

evaluated using IBM SPSS software and basic descriptive characteristics were calculated. The $\chi 2$ test (Campbell, 2007; Richardson, 2011) was used in the MedCalc online calculator environment (MedCalc Software, 2022) for further analyses—to assess differences in the relative frequencies of responses obtained. Statistical significance was assessed at the $\alpha = 0.05$ level.

From the results of the work, it is clear that enough information in the field of cyber security transmitted through school lectures is key for safe movement in cyberspace, while the difference recorded for both groups was the largest in the area of network security.

The results of the work show that awareness and understanding between students who went through the intervention and those who were not part of the intervention, it was found that the group of students who took part in the training had a greater awareness of the risks of connecting to the Internet in public places, checking the URL line or verified certificates. On the contrary, no significant differences were found in the use of illegal software, anti-virus and additional security software, and I think that this reason has the character of habit.

The habits and behavior of students when working with passwords seem to be influenced by individual servers, which require the user to change passwords at given intervals or after an appropriate event, and at the same time require conditions imposed on the complexity of the password, but with two-factor authentication and the use of the same passwords on different servers, it has been proven a significant difference in favor of the trained group and I consider this knowledge to be crucial.

The positive effect of the training was also demonstrated in the field of phishing attacks, and the intervention group almost excelled compared to the other group, especially in dialogues regarding phishing techniques.

In conclusion, I can say that the information in the field of cyber security transmitted in an educational institution seems to be ideal for increasing the awareness of this issue in society.

10 REFERENČNÍ SEZNAM

Achkoski, J., & Dojchinovski, M. (2000). *Cyber terrorism and cybercrime*. Retrieved 14. 4. 2022 from World Wide Web: https://core.ac.uk/download/pdf/35329569.pdf

Alazab, A., & Broadhurst, R. (2013). *Educating children about the risks of the digital environment: a case study of the ThinkUKnow program.* Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 7(1), Article 5.

Avast (2021). *Crypto based phishing scams*. Retrieved 12.5.2022 from the World Wide Web: https://blog.avast.com/cs/crypto-based-phishing-scams-avast

Bateman, R. (2020). *10 Best Anti-Spyware Software for 2020*. Retrieved 25. 6. 2022 from the World Wide Web: https://www.safetydetectives.com/blog/the-best-anti-spywaresoftware/

Brenner, S. (2010). *Cybercrime*: Criminal Threats for Cyberspace. California: Greenwood Publishing Group.

Binance (2022). *Examples of Phishing E-mails*. Retrieved 19.6.2022 from the World Wide Web: https://www.binance.com/en/support/faq/360020817051

Campbell, I. (2007). *Chi-squared and Fisher-Irwin tests of two-by-two tables with small sample recommendations. Statistics in Medicine, 26*(19), 3661–3675. https://doi.org/10.1002/sim.2832

Carr, J. (2016). *Inside Cyber Warfare: Mapping the Cyber Underworld*. O'Reilly Media.

DeNardis, L. (2014). *The Global War for Internet Governance*. Yale University Press.

Entuzio (2022). *TOP 13 Burzy*. Retrieved 13.6.2022 from World Wide Web: https://entuzio.cz/krypto-burzy/

Forbes (2013). *Meet The Dread Pirate Roberts*, *The Man Behing Booming Black Market Drug Website Silk Road.*

Gartzke, E. (2013). *The myth of cyberwar: Bringing war in cyberspace back down to earth*. International Security, 38(2), 41-73.

Gibson, W (1984). *Neuromancer*. USA: Ace Books.

Guitton, C. (2017). *Understanding the digital diplomacy of state actors: An international relations perspective.* Global Affairs, 3(1), 59-68

Igarapé institute (2018). *Brazil struggles with effective cyber-crime response*. Retrieved 5. 6. 2022 from the World Wide Web: https://igarape.org.br/en/brazil-struggles-witheffective-cyber-crime-response/

IntrustIT (2022). *Multi Factor Authentication*. Retrieved 17.6.2022 from the World Wide Web: https://www.intrust-it.com/multi-factor-authentication-what-the-microsoft-mfa-warning-really-means/

ITGovernance (2021). *Cyber security*. Retrieved 11.5.2022 from the World Wide Web: https://www.itgovernance.co.uk/cyber-health-check

IT Market (2022). *Phishing na nejvyšší úrovni*. Retrieved 17.6.2022 from the World Wide Web: https://www.it-market.cz/articles/phishing/phishing-na-nejvyssi-urovni-1-milion-utoku-v-1-ctvrtleti-2022

Janczewski, L. J., & Colarik, A. M. (2005). *Managerial guide for handling cyber-terrorism and information warfare*. Retrieved 5. 5. 2022 from the World Wide Web: https://www.researchgate.net/publication/294563593_Managerial_guide_for_handling_cyber-terrorism_and_information_warfare

Kolouch, J. (2016). *CyberCrime*. Praha: CZ.NIC, z. s. p. o.

Lewis, J. A. (2014). *Cybersecurity and Cyberwarfare: Preliminary Assessment of National*

Libicki, M. C. (2015). *Cyberspace in peace and war*. Naval Institute Press.

Lorents, P., & Ottis, R. (2011). *Cyberspace: Definition and implications*.

MedCalc Software. (2022). *Comparison of proportions calculator*. https://www.medcalc.org/calc/comparison_of_proportions.php

Nakashima, E. (2015). *As encryption spreads*, U.S. grapples with clash between privacy, security. The Washington Post.

NATO Public Diplomacy Division (2007). *Centre of Excellence Defence Against Terrorism*, Ankara, Turkey. Retrieved 14. 6. 2022 from the World Wide Web: https://books.google.cz/books?id=Eg7vAgAAQBAJ&printsec=frontcover&hl=cs&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Norton (2022). *SaaS App Vanity URLs Can Be Spoofed for Phishing*, Social Engineering

Passcamp (2021). *What is a baiting attack and how to prevent it?* Retrieved 20.6.2022 from the World Wide Web: https://www.passcamp.com/blog/what-is-a-baiting-attack-and-how-to-prevent-it/

Policie ČR (2020). *Kyberkriminalita*. Retrieved 5. 5. 2022 from the World Wide Web: https://www.policie.cz/clanek/kyberkriminalita.aspx

Richardson, J. T. (2011). *The analysis of 2 × 2 contingency tables--yet again*. *Statistics in Medicine, 30*(8), 890–892. https://doi.org/10.1002/sim.4116

Sanders, A. (2022). *Co je sociální inženýrství a proč je to hrozba v roce 2022?* Safetydetectives. Retrieved 14.5.2022 from the World Wide Web: https://cs.safetydetectives.com/blog/co-je-socialni-inzenyrstvi-a-proc-je-to-takova-hrozba/

Segal, A. (2016). *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. PublicAffairs.

Solove, D. J. (2011). *Nothing to Hide: The False Tradeoff between Privacy and Security*. Yale University Press.

Solms, R.V., Niekerk, J. V. (2013). *From information security to cyber security*. Retrieved 19.5.2022 from the World Wide Web: https://doi.org/10.1016/j.cose.2013.04.004

Šichtanc, R., (2022). CyberSecurity Podcast ProID

Taddeo, M., & Floridi, L. (2018). *Regulating Artificial Intelligence: A Multilayered Challenge. Springer.*

The Jargon File (2016). *Hacker slang and hacker culture*. Retrieved 9. 5. 2022 from the World Wide Web: http://catb.org/jargon/html/distinctions.html

US Army (2010). *Cyberspace Operations Concept Capability Plan 2016-2028*. Retrieved 11.5.2022 from the World Wide Web: https://irp.fas.org/doddir/army/pam525-7-8.pdf

Vláda České republiky (2021). *Kybernetická bezpečnost*. Retrieved 11.5.2022 from the World Wide Web: https://www.vlada.cz/cz/evropske-zalezitosti/umela-inteligence/kyberneticka_bezpecnost/kyberneticka-bezpecnost-192766/

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown.*