Odolnost osob vůči kybernetickým útokům

Jan Jelínek

Bakalářská práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva

Akademický rok: 2023/2024

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Jan Jelínek**
Osobní číslo:	**L21398**
Studijní program:	**B1032A020002 Ochrana obyvatelstva**
Forma studia:	**Kombinovaná**
Téma práce:	**Odolnost osob vůči kybernetickým útokům**

Zásady pro vypracování

1. Na základě provedené rešerše zpracujte teoretický vstup do dané problematiky.
2. Objasněte základní pojmy související s odolností jednotlivců vůči kybernetickým útokům.
3. Analyzujte současný stav řešené problematiky ve vybrané oblasti.
4. Navrhněte doporučení pro zvýšení odolnosti osob vůči kybernetickým útokům.

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

V Uherském Hradišti, dne: 3.5.2024

Jméno a příjmení studenta: Jan Jelínek

.....
podpis studenta

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

Seznam doporučené literatury:

1. AUGENBAUM, Scott E. *The Secret to Cybersecurity: A Simple Plan to Protect Your Family and Business from Cybercrime*. Nashville (Tennessee): Forefront Books, 2019. ISBN 978-19-4867-708-0.
2. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, 2019. ISBN 978-80-8816-834-8.
3. SEDLÁK, Petr a KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **1. prosince 2023**
Termín odevzdání bakalářské práce: **3. května 2024**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 4. prosince 2023

ABSTRAKT

Tato bakalářská práce se zaměřuje na kybernetickou odolnost jednotlivců a identifikaci slabých míst v osobní kybernetické bezpečnosti. Vzhledem k narůstajícímu počtu kybernetických útoků a pokračující digitalizaci společnosti je klíčové pochopit, jak mohou jednotlivci účinně chránit své informační systémy a data. Hlavním cílem práce je identifikovat klíčové slabiny v osobní kybernetické odolnosti a navrhnout strategie pro jejich posílení. V praktické části bylo provedeno polostrukturované dotazníkové šetření mezi oběťmi kybernetické kriminality a nestandardizovaný rozhovor s odborníkem na kybernetickou odolnost, aby se získala data pro formulaci těchto strategií. Práce analyzuje různé typy kybernetických útoků s důrazem na nejnovější hrozby.

Klíčová slova: kybernetická bezpečnost, kybernetické útoky, digitální ochrana, odolnost proti kybernetickým útokům, prevence kybernetických útoků

ABSTRACT

This bachelor's thesis focuses on cyber resilience among individuals and identifies vulnerabilities in personal cybersecurity. With the increasing number of cyberattacks and the ongoing digitalization of society, it is crucial to understand how individuals can effectively protect their information systems and data. The main goal of this thesis is to identify key vulnerabilities in personal cyber resilience and propose strategies for their strengthening. The practical part included a semi-structured questionnaire survey among victims of cybercrime and an unstandardized interview with an expert in cyber resilience to gather data for formulating these strategies. The thesis analyses various types of cyberattacks, emphasizing the latest threats.

Keywords: cybersecurity, cyberattacks, digital protection, cyber resilience, cyberattack prevention

Na tomto místě bych chtěl vyjádřit své upřímné poděkování Ing. Petrovi Svobodovi, Ph.D., za jeho odborné vedení, cenné rady a neustálou podporu při psaní této bakalářské práce. Jsem mu velmi vděčný za čas, který mi věnoval, a za motivaci, kterou mi poskytoval v průběhu celého studia. Děkuji za možnost pracovat pod jeho vedením a za vše, co jsem se díky němu naučil.

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

OBSAH

ÚVOD

Ve světě, kde technologie a internetové připojení pronikají do každého aspektu našeho osobního a profesního života, se kybernetická bezpečnost stává neodmyslitelnou součástí naší každodenní existence. Tato bakalářská práce, zaměřená na odolnost osob vůči kybernetickým útokům, přichází v čase, kdy se celosvětově zvyšuje frekvence a sofistikovanost kybernetických hrozeb, což vyvolává značné obavy o soukromí, bezpečnost a ekonomickou stabilitu.

Jako student ochrany obyvatelstva, tak i zaměstnanec Policie ČR, jsem se rozhodl propojit akademické poznatky s praktickými zkušenostmi a zaměřit se na kybernetické útoky z pohledu prevence a reakce na incidenty. Tato práce poskytuje nejen teoretické základy týkající se historie a vývoje internetu, ale také zkoumá specifické aspekty kybernetického prostoru a legislativního rámce v České republice.

Hlavním cílem této práce je na základě indukce navrhnout praktická doporučení pro zvýšení odolnosti osob vůči kybernetickým útokům. V rámci dílčích cílů bude pojednáno o souvisejících teoretických východiscích řešené problematiky. Dále budou za pomoci polostrukturovaného dotazníkového šetření mezi obětmi kybernetické kriminality identifikovány jejich slabá místa vůči hrozbám v kyberprostoru. Součástí bude také získání rad a doporučení od experta na kybernetickou odolnost osob, což bude realizováno prostřednictvím nestandardizovaného rozhovoru.

Při zpracování jsem vycházel z nejnovějších dat a výzkumů, a snažil se o komplexní přístup, který by byl přínosný jak pro akademickou obec, tak pro praktické využití v rámci bezpečnostních sil. Analýza základních principů kybernetické bezpečnosti a aktuálních hrozeb je klíčová pro formulaci doporučení, která by mohla pomoci nejen jednotlivcům, ale i organizacím chránit se proti stále sofistikovanějším útokům. Skrze interakci s odborníkem z praxe a prostřednictvím dotazníkového šetření jsem se pokusil získat ucelený obraz o stávajících ochranných opatřeních a percepci hrozeb mezi občany.

Tato práce přispívá k důležité diskusi o tom, jak můžeme lépe chránit naši digitální infrastrukturu a osobní údaje, a posiluje tak oblast kybernetické bezpečnosti v akademickém i veřejném sektoru. Přináší nový pohled na to, jak by mohly být implementovány nové metody a techniky pro zvýšení odolnosti vůči kybernetickým útokům, čímž poskytuje cenný přínos pro všechny, kdo se v této oblasti pohybují.

I. TEORETICKÁ ČÁST

1 INTERNET A KYBERPROSTOR

Obecně v povědomí veřejnosti panuje rovnice internet = kyberprostor = web, ačkoliv jsou si tato slova v mnohém podobná, není tomu tak. Můžeme velice zjednodušeně říct, že internet jako takový je součástí mnohem rozsáhlejšího kyberprostoru. (Kolouch a Bašta, 2019)

1.1 Historie internetu

Internet způsobil revoluci ve způsobu, jakým žijeme, pracujeme a komunikujeme s ostatními. Je to rozsáhlá informační a komunikační síť, která změnila svět, jak ho známe. Jak to ale všechno začalo? V následujících odstavcích si přiblížíme cestu internetu od jeho skromných počátků ve Spojených státech amerických až po vznik World Wide Webu (WWW) a jeho současnou globální přítomnost. (Ryan, 2010; Seel, 2022)

Historie internetu sahá do období studené války, kdy byla potřeba lepší komunikace mezi počítači klíčová pro vojenské a výzkumné účely ve Spojených státech. První kroky k vytvoření internetu byly učiněny v 60. letech 20. století, kdy J.C.R. Licklider z MIT představil koncept globálně propojené sítě počítačů. Tento nápad vedl k vývoji ARPANETu v roce 1969, který byl první pracující sítí používající technologii přepínání paketů, navrženou Paul Baranem a Donaldem Daviesem. (Ryan, 2010; Seel, 2022)

ARPANET rychle expandoval a v 70. letech 20. století se stal základem pro další výzkum a rozvoj sítí. V těchto letech byly položeny základy protokolů TCP/IP, které vyvinuli Vint Cerf a Bob Kahn. Tyto protokoly umožnily spojení mnoha různých sítí do jednoho sjednoceného celku, což vedlo k vytvoření skutečné "sítě sítí", kterou dnes známe jako internet. (Ryan, 2010; Seel, 2022)

V roce 1983 ARPANET přešel na používání protokolů TCP/IP a oficiálně se stal součástí větší a otevřenější sítě. V průběhu 80. let 20. století začaly vznikat první komerční poskytovatelé internetových služeb, což umožnilo rozšíření internetu do komerčního sektoru a následně k veřejnosti. (Ryan, 2010; Seel, 2022)

Velkým průlomem bylo zavedení World Wide Webu v roce 1990, který vyvinul Tim Berners-Lee ve švýcarském CERNu. Web používal hypertext k propojení dokumentů po celém internetu a zjednodušil přístup k informacím, což vedlo k rychlému rozšíření internetu mezi běžné uživatele po celém světě. (Ryan, 2010; Seel, 2022)

Dnes je internet nezbytnou součástí každodenního života, umožňuje nejen základní komunikaci, ale i složité distribuované sítě, které podporují obrovské množství aplikací, od cloudových služeb po internet věcí a mnoho dalších.

1.2 Kyberprostor

Kyberprostor nebo cyberspace je Oxfordským anglickým slovníkem definován jako: „*The space of virtual reality; the notional environment within which electronic communication (esp. via the internet) occurs*“ tedy jako prostor virtuální reality, pomyslné prostředí, v němž probíhá elektronická komunikace, a to zejména prostřednictvím internetu. (Cyberspace, c2023)

V české legislativě je pak kyberprostor definován v zákoně číslo č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) v § 2 písm. a) tohoto zákona jako: „*kybernetickým prostorem digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.*“ (ČESKO, 2014)

Nicméně obě tyto definice nejsou dostatečné a jako jednu z nejzdařilejších definic kyberprostoru uvádí dokument Cyberspace Operations: Concept Capability Plan 2016-2028.

Ten definuje kyberprostor jako prostor složený ze tří vrstev:

- Fyzické.
- Logické.
- Sociální. (Kolouch a Bašta, 2019)

Tyto vrstvy se pak dále dělí na celkem pět složek.

Fyzická vrstva obsahuje dvě složky nazvané jako „geographic component“ a fyzické síťové komponenty. Přesný překlad pojmu „geographic component“ bychom v českém jazyce hledali jen velmi těžce, ale odkazuje na síťové prvky a jejich přesné umístění ve fyzickém světě. Pojem "fyzická síťová komponenta" zahrnuje infrastrukturu neboli síťový harware, jako jsou kabely, zařízení pro řízení sítě (přepínače, směrovače) a další zařízení. (Army Training and Doctrine Command a The United States Army, 2016)

Toto rozdělení fyzické vrstvy je podstatné za účelem stanovení geopolitických hranic fyzického světa do světa virtuálního, jelikož v kyberprostoru je velmi lehké tyto hranice

téměř nezištně překračovat. (Army Training and Doctrine Command a The United States Army, 2016)

Logická vrstva obsahuje složku logických síťových komponent, tento pojem odkazuje na způsob, jakým je realizována logická komunikace mezi jednotlivými síťovými uzly, kdy v tomto případě se jedná zejména o protokoly jako je TCP/IP. Uzly mohou být například mobilní telefony a počítače. (Army Training and Doctrine Command a The United States Army, 2016)

Sociální vrstva obsahuje dvě složky nazvané jako kyberosobnost a osobnost. Kyberosobnost používá v síti konkrétní identifikátor jako je emailová adresa, IP adresa, číslo telefonu a další, osobnost je pak skutečná osoba připojená k síti. V této vrstvě pak může docházet i k situacím, kdy jednu kyberosobnost používá zároveň více osobností (rodina používající jednu emailovou adresu) a zároveň může mít jedna osobnost více kyberosobností (jeden člověk používající více emailových adres). (Army Training and Doctrine Command a The United States Army, 2016)

1.3 Internet

V českém jazyce dle školního vydání Pravidel českého pravopisu rozlišujeme dva pojmy, a to internet s malým i a Internet s velkým I, kdy internet jsou propojené počítačové sítě a Internet je celosvětová informační a komunikační síť tedy World Wide Web. (Internet)

Internet je rozsáhlý propojený systém sítí fungující celosvětově, umožňující komunikaci a poskytování datových služeb prostřednictvím různých typů sítí, včetně soukromých, veřejných, podnikových, akademických a vládních. Jeho charakteristickou vlastností je decentralizace, což znamená, že není řízen žádným centrálním orgánem. Pro komunikaci mezi zařízeními využívá internet protokoly a standardy, které určují formát, adresaci a přenos datových jednotek. (Kolouch a Bašta, 2019)

I když se pojmy internet a World Wide Web (WWW) často používají synonymicky, jsou technicky odlišné. Internet je globální síť propojených počítačů a sítí, zatímco World Wide Web je konkrétní služba využívající infrastrukturu internetu k poskytování přístupu k webovým stránkám a digitálním aplikacím. Mezi populární internetové služby patří email, VoIP (Voice over IP) a SMS (Short Message Service). (Kolouch a Bašta, 2019)

1.4 Právní prostředí Internetu v České republice

Internet jako celek nikdo nevlastní. Jedná se o soubor informačních a telekomunikačních technologií, který zahrnuje různé právní subjekty, včetně jednotlivců a organizací, jako jsou uživatelé a poskytovatelé služeb. Přestože internet jako celek nemá majitele a nepředstavuje fyzickou, ani právnickou osobu, jeho části, jako jsou počítačové sítě, mohou být vlastněny různými subjekty například poskytovateli internetových služeb nebo státy. Tyto části pak mohou být podle zákona považovány za hmotné věci. Podle § 489 občanského zákoníku se za věc považuje *"vše, co je rozdílné od osoby a slouží potřebě lidí."* (Česko, 2021) Dále, § 496 odst. 1 občanského zákoníku hmotnou věc definuje jako *"ovladatelnou část vnějšího světa, která má povahu samostatného předmětu."* (Česko, 2021) Z tohoto pohledu by se dalo teoreticky říct, že internet je hmotnou věcí dle českého práva. Avšak, otázka vlastnictví internetu jako celku je složitá, protože internet se skládá z mnoha různých částí a služeb. Smejkal (Smejkal, 2015) k tomu uvádí: *"Věc v právním slova smyslu profiluje její ovladatelnost. Internet jako celek si nelze přivlastnit, ani jej ovládat."* Navíc, internet jako celek nelze jednoduše zařadit mezi hmotné ani nehmotné věci, protože bez fyzické infrastruktury by nemohl fungovat. Internet je tedy úzce spjat s fyzickými prvky, které jsou vlastněny různými subjekty. V kontextu odpovědnosti za nezákonné činy je důležité využívat nejen národní, ale i mezinárodní právní nástroje, a diskuse o odpovědnosti musí zahrnovat jak poskytovatele služeb, tak uživatele. (Kolouch, 2016; Sedlák a Konečný, 2021)

2 LEGISLATIVA KYBERNETICKÝCH ÚTOKŮ

V České republice se vyšetřováním kybernetických trestných činů zabývá především odbor kriminální policie a vyšetřování při Policii ČR. Od 1. ledna 2023 funguje v rámci této struktury nově vytvořená jednotka s názvem Národní centrum proti terorismu, extremismu a kybernetické kriminalitě, která má působnost na celostátní úrovni. (Zločiny v době moderních technologií: Jak řeší české právo kybernetickou kriminalitu a jak se proti ní bránit?, 2023)

Před zřízením tohoto útvaru se problematikou kyberkriminality zabýval oddíl v rámci Národního centra proti organizované kriminalitě. Vzhledem k tomu, že kyberprostor přesahuje hranice států, je důležité spolupracovat mezinárodně na odhalování a boji proti těmto trestným činům. Tato spolupráce se často týká shromažďování důkazů a zatýkání či vydávání pachatelů, přičemž klíčovou platformou pro tuto spolupráci je Eurojust. V rámci boje proti kyberkriminalitě Eurojust eviduje rostoucí počet žádostí o spolupráci, jelikož kyberkriminalita patří mezi pět nejčastějších typů kriminality, s nimiž se organizace setkává. (Zločiny v době moderních technologií: Jak řeší české právo kybernetickou kriminalitu a jak se proti ní bránit?, 2023)

K detekci a potlačení vážných kybernetických trestných činů přispívá také Vojenské zpravodajství. Po novelizaci zákona o Vojenském zpravodajství, konkrétně zákona č. 289/2005 Sb., která nabyla účinnosti 1. července 2021, má tato zpravodajská služba možnost se za určitých zákonných podmínek zaměřit na detekci kybernetických útoků a hrozeb zahraničního původu, které míří proti klíčovým státním zájmům. (Zločiny v době moderních technologií: Jak řeší české právo kybernetickou kriminalitu a jak se proti ní bránit?, 2023)

Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších právních předpisů (dále jen „trestní zákoník“) se zabývá kybernetickou kriminalitou způsobem, který kategorizuje trestné činy spojené s využitím informačních a komunikačních technologií nebo těmi, které se často objevují v online prostředí, do několika skupin:

- Různé formy podvodů, včetně falešných e-shopů, inzertních podvodů, romantických podvodů a phishingu.
- Hacking, což znamená neautorizovaný přístup do systému a jeho následné zneužití.

- Blagging, tedy podvodné žádosti o peníze, často skrze falešné profily jako jsou například CEO podvody.
- Mravnostní delikty, které zahrnují ohrožení výchovy mládeže, dětskou pornografii a navazování nevhodných kontaktů.
- Trestné činy proti autorskému právu, jako je nelegální sdílení hudby, filmů a softwaru.
- Násilné činy a zločiny z nenávisti, včetně vydírání, vyhrožování a nebezpečného pronásledování. (Zločiny v době moderních technologií: Jak řeší české právo kybernetickou kriminalitu a jak se proti ní bránit?, 2023; Sedlák a Konečný, 2021)

Trestní zákoník specificky vyzdvihuje tři hlavní oblasti trestných činů, které přímo souvisí s poškozením informačních systémů, sítí a dat:

- Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230).
- Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231).
- Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232). (Česko, 2009)

Tyto činy obvykle zahrnují hackování, odposlech a manipulaci s daty. Trestným činem je rovněž tvorba a šíření virů a jiných zařízení určených k neoprávněnému průniku do systémů.

Kybernetická kriminalita dále zahrnuje trestné činy, které se nevyznačují primárně kybernetickým charakterem, ale jsou spáchány prostřednictvím kyberprostoru. (Zločiny v době moderních technologií: Jak řeší české právo kybernetickou kriminalitu a jak se proti ní bránit?, 2023)

Mezi tyto činy patří:

- Šíření pornografie (§ 191).
- Výroba a jiné nakládání s dětskou pornografií (§ 192).
- Navazování nedovolených kontaktů s dítětem (§ 193b).
- Neoprávněné opatření, padělání a pozměnění platebního prostředku (§ 234).
- Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi (§ 270).

- Hanobení národa, rasy, etnické nebo jiné skupiny osob (§ 355).
- Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod (§ 356).
- Šíření poplašné zprávy (§ 357).
- Pomluva (§ 184).
- Vydírání (§ 175). (Česko, 2009)

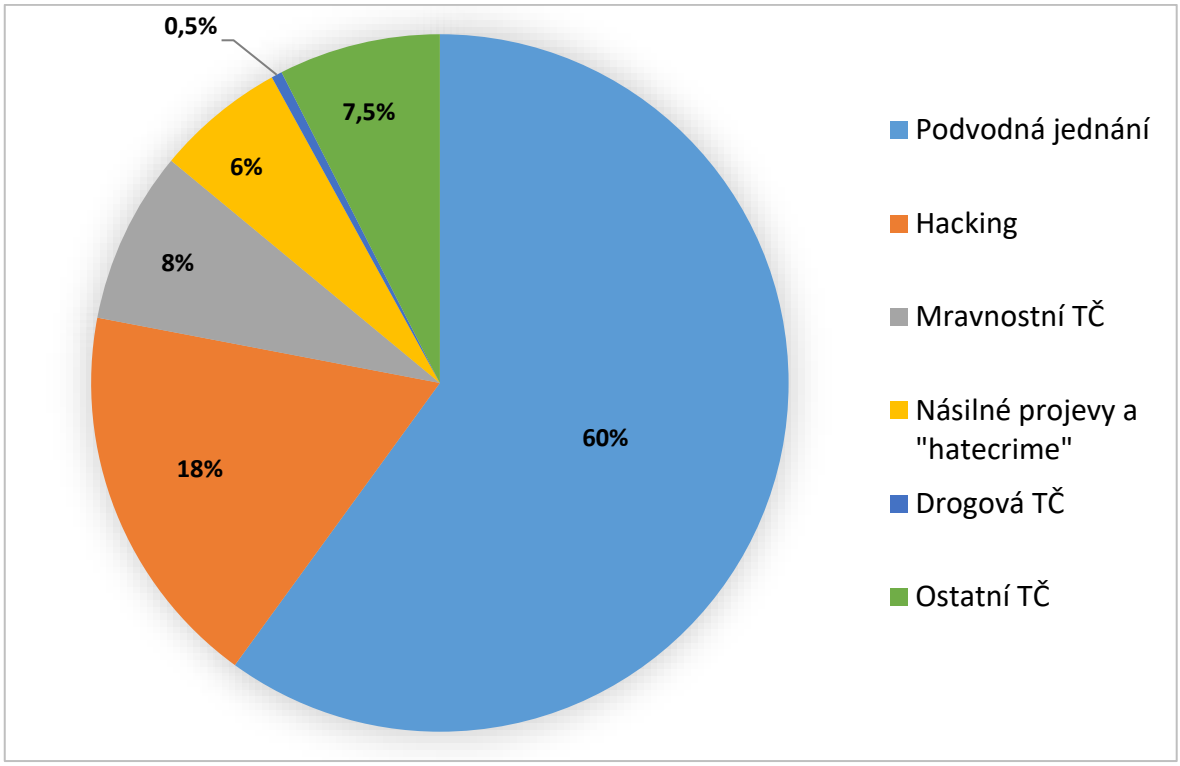
Podle statistik z let 2021 a 2022 byly mezi soukromými osobami nejčastějšími kybernetickými podvody neoprávněný přístup a poškození dat, což ukazuje, že v kyberprostoru převládají majetkové trestné činy, včetně různých podvodů a porušení autorských práv. (Zločiny v době moderních technologií: Jak řeší české právo kybernetickou kriminalitu a jak se proti ní bránit?, 2023)

2.1 Zpráva o činnosti státního zastupitelství za rok 2022

Ze zprávy o činnosti státního zastupitelství za rok 2022, která byla vydána k 22. červnu 2023 vyplývá, že v roce 2022 došlo k výraznému zvýšení počtu trestných činů realizovaných prostřednictvím internetu a dalších digitálních sítí. Byl zaznamenán přechod od tradičních metod páchání trestných činů k jejich provádění ve virtuálním světě, zejména v oblastech majetkové a hospodářské kriminality, trestných činů proti mravnosti, trestných činů zaměřených proti dětem, a trestných činů motivovaných rasovými, národnostními či jinými formami nenávisti. (Nejvyšší státní zastupitelství, 2023)

Co se týče specificky kyberkriminality, tedy vyjma výše zmíněných oblastí, nejčastějším typem trestného činu byl neautorizovaný přístup k počítačovým systémům a informačním nosičům, jak je definováno v § 230 trestního zákoníku. (Nejvyšší státní zastupitelství, 2023)

Pozoruje se stálý růst kyberkriminality, hlavně ve formě útoků zaměřených na získání přístupových údajů k internetovému bankovnictví, rozsáhlých útoků založených na falešné identitě, podvodných investic, zejména do kryptoměn, a podvodů cílených na prodejce na online inzertních platformách. Paralelně se v kyberprostoru objevují i jiné formy trestné činnosti, včetně trestných činů motivovaných rasovými, národnostními či jinými formami nenávisti takzvaných hate crimes, dětské pornografie, obchodu s narkotiky a psychotropními látkami a porušení autorského práva a souvisejících práv. (Nejvyšší státní zastupitelství, 2023)



Obrázek 1 složení kybernetické kriminality v roce 2022 (zdroj: Nejvyšší státní zastupitelství, 2023)

Na Obr. 1 je patrné složení kybernetické kriminality v ČR v roce 2022 a vychází z dat poskytnutých Policií České republiky.

V období roku 2022 byl zaznamenán rostoucí trend využívání virtuální měny Bitcoin a dalších kryptoměn pro trestnou činnost, odlišně od předchozích let, kdy se takové incidenty objevovaly spíše vzácně. Aktuálně jsou virtuální měny běžně využívány pachateli pro účely trestné činnosti. Z mezinárodních zdrojů a zkušeností vyplývá, že v roce 2022 pokračovalo porušování autorských práv na internetu, včetně streamování filmů, hudby a videoher. Tato kriminalita je však obtížně odhalitelná a prokazatelná, což má za následek její malou reprezentaci v oficiálních statistikách kyberkriminality. (Nejvyšší státní zastupitelství, 2023)

Signifikantní část kyberkriminality tvoří opakovaně páchání trestných činů, například prostřednictvím podvodných telefonátů, kdy se pachatelé vydávají za bankovní pracovníky nebo policisty. Mezi další projevy patří phishingové útoky, z nichž jako zvláště rizikové vyplynuly reverzní inzertní podvody cílící na vylákání citlivých údajů skrze falešné webové stránky. Zaznamenány byly i útoky založené na padělání webových stránek bank a jejich propagace prostřednictvím vyhledávačů. (Nejvyšší státní zastupitelství, 2023)

Obecným problémem v boji proti kyberkriminalitě je její anonymní a mezinárodní povaha, což ztěžuje odhalení fyzické polohy pachatelů. Kriminalita v této sféře pokračuje ve

vzestupu, přičemž podvody a s nimi související trestné činy představují v oblasti majetkové kriminality významný a pro vyšetřovatele klíčový problém. (Nejvyšší státní zastupitelství, 2023)

V oblasti podvodů se jako nejfrekventovanější trestný čin objevuje podvod (§ 209), přičemž mnoho případů je založeno na neznalosti nebo nedbalosti obětí. Obětmi se stávají osoby z různých věkových, profesních a sociálních skupin. Trestná činnost má často mezinárodní rozměr a je pravděpodobně organizována skupinami pachatelů s podobným modus operandy, přičemž nejčastěji pochází ze zemí jako Ukrajina, Rusko, Polsko, nebo Čína, kam směřují i zisky z těchto trestných činů. (Nejvyšší státní zastupitelství, 2023)

Identifikace a dopadení pachatelů je komplikované, zejména když cílové účty, na které jsou prostředky převedeny, často leží mimo území České republiky, což vede k nízké míře objasnění těchto případů. Přesto bylo několik pachatelů odhaleno. Na začátku roku 2022 byla schválena celková koncepce rozvoje kapacit státního zastupitelství v boji proti kyberkriminalitě. (Nejvyšší státní zastupitelství, 2023)

3 KYBERNETICKÉ ÚTOKY

Server it-slovnik.cz definuje pojem kybernetického útoku jako: *„Kyberútok je jakýkoliv pokus zničit, změnit, ukrást majetek nebo získat neoprávněný přístup i neautorizované použití majetku pomocí počítačové techniky a počítačové sítě.“* (Co je to kyberútok?, c2008-2024)

Kybernetický útok lze chápat jako nelegální činnost prováděnou v kyberprostoru, která škodí jinému člověku nebo organizaci. Ne všechny tyto činy musí být trestné, ale všechny nějak zasahují do normálního života obětí. Útoky mohou být v různých fázích od plánování po samotné provedení. Zatímco každý kybernetický trestný čin je považován za útok, ne každý útok musí být nutně trestným činem. Některé mohou spadat pod jiné právní kategorie nebo dokonce nemusí porušovat žádné zákony, pokud jde například o neetické chování. Účinnost útoku se hodnotí podle toho, jak ovlivní základní složky kybernetické bezpečnosti, což zahrnuje lidi, procesy a technologie. Je důležité tyto složky neustále vylepšovat a přizpůsobovat, aby se zabránilo útokům, detekovaly se a reagovalo na ně. (Kolouch, 2016; Sedlák a Konečný, 2021)

Abychom správně pochopili, co znamená kybernetický útok, měli bychom se podívat na vysvětlení podle zákona o kybernetické bezpečnosti. Podle § 7 tohoto zákona se rozlišují dva klíčové termíny:

- Kybernetická bezpečnostní událost.
- Kybernetický bezpečnostní incident. (Kolouch, 2016)

Kybernetickou bezpečnostní událostí je *"událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací."* (Česko, 2014) V zásadě je to situace, kdy ještě nedošlo k žádnému skutečnému poškození, ale existuje skutečná hrozba nějakého narušení. (Kolouch, 2016)

Kybernetický bezpečnostní incident je definován jako *"narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události."* (Česko, 2014) To znamená, že incident představuje skutečné narušení bezpečnosti, které má negativní dopad na informační nebo komunikační systémy. (Kolouch, 2016)

3.1 Kybernetické útoky v České republice

V průběhu roku 2023 bylo v České republice zaznamenáno 69 685 případů, kdy klienti bank padli za oběť podvodným útokům a celková škoda dosáhla výše 1,35 miliardy korun. Průměrná škoda na jednoho klienta tak činila 19 357 Kč. Díky zlepšené efektivitě nástrojů používaných k odhalování podvodů banky dokázaly výrazně zredukovat celkovou způsobenou škodu e-šmejdů. Nejvyšší částka, která byla zachráněna pro jednoho klienta v historii sledování kybernetických podvodů, činila 13 milionů korun. Česká bankovní asociace aktivně bojuje proti e-šmejdům a již druhým rokem uspořádala rozsáhlou edukační kampaň #nePINdej!. (Česká bankovní asociace, 2024)

Kyberbezpečnost má pro banky klíčový význam, ty proto investují významné finanční prostředky do vývoje pokročilých technologií a provádějí rozsáhlé osvětové kampaně jako je výše uvedená kampaň #nePINdej!. Tyto strategické opatření směřují k redukci škod způsobených kybernetickými útoky na klienty. Zatímco v prvním pololetí roku 2023 průměrná škoda na klienta činila necelých 22 000 korun, ve druhém pololetí téhož roku klesla průměrná škoda na klienta na 19 000 korun. (Česká bankovní asociace, 2024; Pidrmnaová, 2022)

Statistiky Policie ČR naznačují, že za rok 2022 byl nárůst kyberútoků nejmenší od roku 2017, v roce 2022 bylo zaznamenáno 19 592 nahlášených případů, což představuje nárůst o 5,5 % ve srovnání s rokem 2021. Nicméně, zároveň se významně zvýšila důmyslnost a sofistikovanost kyberútoků. (Česká bankovní asociace, 2024)

3.2 Nejčastější kybernetické útoky

Statistiky jsou nejčastěji vedeny u útoků, kde jsou ve hře peníze, nejedná se však ani zdaleka o jediné kybernetické útoky, ke kterým v kyberprostoru dochází. Pouze některé z nich jsou vedeny na jednotlivce za účelem zbohatnutí. Mezi nejčastější kybernetické útoků patří:

Malware známý také jako škodlivý software, představuje jakýkoliv program nebo soubor navržený s úmyslem poškodit počítač, síť nebo server. Hlavními zástupci jsou trojský kůň, virus, záznam úhozů, červ. (Lutkevich, 2022, Monnappa K A, 2018)

Útok typu **Denial-of-Service** (DoS) je forma kybernetického útoku, jehož cílem je znepřístupnit počítač nebo jiné zařízení pro jeho uživatele tím, že naruší běžný provoz zařízení. Útoky DoS obvykle pracují na principu zasypání cílového zařízení požadavky do té míry, že se normální provoz nemůže udržet, což vede k odmítnutí služby pro další

uživatele. Charakteristickým rysem útoku DoS je jeho spuštění z jednoho počítače. **Distributed Denial-of-Service** (DDoS) je varianta útoku DoS, která je realizována z mnoha rozptýlených zdrojů, například skrze botnet. (The Investopedia team, 2023)

Phishing je druh kriminální sociální manipulace, která využívá online digitální média. Nejčastěji se phishing provádí prostřednictvím emailu, ale může být realizován jakýmkoli elektronickým komunikačním kanálem, včetně webových stránek, okamžitých zpráv, textových zpráv přes mobilní telefon, a dokonce hlasových hovorů. (Grimes, 2024; Augenbaum, 2019)

Spoofing je metoda, pomocí které se kybernetický útočník maskuje za důvěryhodný nebo známý zdroj jako jsou banky, operátoři či technická podpora. Existuje mnoho forem spoofingu, včetně falšovaných emailů, maskování IP adres, falšování DNS, manipulace s GPS, napodobení webových stránek a padělaných telefonních hovorů. Tímto způsobem je útočník schopen komunikovat s cílem a získat přístup k jejich systémům nebo zařízením s cílem ukrást informace, vymámit peníze nebo nainstalovat malware či jiný škodlivý software na zařízení. (Lenaerts-Bergmans, 2022)

Útok typu **code injection** je obecný výraz pro druhy útoků založené na vložení kódu, který je poté aplikací interpretován nebo spuštěn. (Monnappa K A, 2018) Tyto útoky využívají nedostatečné zabezpečení při zpracování nedůvěryhodných dat. Obvykle jsou umožněny díky nedostatku správné validace dat na vstupu a výstupu. Rozdíl mezi code injection a command injection spočívá v tom, že možnosti útočníka jsou omezeny pouze možnostmi jazyka, do kterého byl kód injektován. Pokud útočník dokáže do aplikace vložit a spustit kód PHP, jsou jeho limity dány pouze schopnostmi PHP. Command injection pak využívá existující kód k vykonání příkazů, obvykle v rámci uživatelského rozhraní. (Zhong a Rezos, 2024)

V případě **Supply chain attacks** útočníci vyhledávají nezabezpečené síťové protokoly, nechráněné serverové infrastruktury a nebezpečné programovací praktiky. Prostřednictvím nich pronikají do systémů, modifikují zdrojové kódy a vkládají malware do aktualizací. Vzhledem k tomu, že software je vytvářen a distribuován důvěryhodnými dodavateli, jsou tyto aplikace a aktualizace podepsány a certifikovány. Při útocích na dodavatelský řetězec softwaru obvykle dodavatelé netuší, že jejich aplikace nebo aktualizace jsou při uvedení na veřejnost infikovány škodlivým kódem. Tento škodlivý kód poté běží s těmi samými oprávněními a důvěrou jako samotná aplikace. (Dansimp, 2024)

DNS tunelování je metoda útoku na Domain Name System (DNS), která spočívá v zakódování dat jiných protokolů nebo programů do dotazů a odpovědí DNS. Tato technika obvykle zahrnuje datové balíčky, které se mohou připojit k cílovému DNS serveru, což útočníkovi umožňuje ovládat aplikace a vzdálený server. DNS tunelování obvykle vyžaduje přístup k externí síťové konektivitě kompromitovaného systému – je nutné najít cestu k internímu DNS serveru s přístupem k síti. Útočníci musí rovněž ovládat server a doménu, které mohou sloužit jako autoritativní server pro provádění spustitelných programů datových balíčků a tunelování na straně serveru. (Dizdar, 2023)

Útoky na zařízení v **internetu věcí (Internet of Things - IoT)**, IoT zařízení jsou vytvářena tak, aby odpovídala obecným požadavkům, a proto často postrádají přísná bezpečnostní protokoly. Útočníci využívají tuto slabost k proniknutí do systému skrze některé z méně zabezpečených IoT zařízení. Útoky na IoT představují kybernetické útoky, které s využitím IoT zařízení získávají přístup k citlivým datům uživatelů. Útočníci obvykle na zařízení nainstalují škodlivý software, poškodí zařízení nebo získají přístup k dalším osobním datům, nebo celé síti. (Aqsa, 2024)

3.3 Příklady aktuálních kybernetických útoků

V této části budou představeny dva příklady kybernetických útoků vedených proti občanům České republiky v roce 2024. Tyto kybernetické útoky byly nahlášeny na Policii České republiky a následující dva texty jsou popisy skutku ze záznamu o zahájení úkonů trestního řízení, pro ochranu osobních údajů budou cenzurovány písmeny „XXX“ veškeré informace, podle kterých by bylo možné identifikovat oběti.

3.3.1 Příklad č. 1

Neznámý pachatel vystupující jako Š. Š. v době od 20:45 hod. do 22:00 hod. dne 16.03.2024 z blíže neznámého místa kontaktoval poškozeného T.N. v úmyslu neoprávněně se obohatit na úkor jiné osoby, vylákal pod legendou nákupu běžeckého pásu na portále Facebook v sekci Marketplace, po domluvě odkázal poškozeného na stránky jevící se jako oficiální stránky kurýrní služby Balíkovna, kde instruoval poškozeného k vyplnění bankovních údajů ke svému bankovnímu účtu číslo XXX vedeného u Raiffeisenbank a zaslání QR kódů, které přijdou do RB klíče, poté provedl dvě platby z bankovnímu účtu poškozeného číslo XXX ve prospěch dosud nezjištěného příjemce, čímž měla být poškozenému T.N. způsobena škoda na majetku v celkové výši 120.000,- Kč. (Policie České republiky, 2024)

Na tomto příkladu lze vidět, že neznámý pachatel kontaktuje svou oběť prostřednictvím aplikace Messenger za účelem koupě běžeckého pásu, kde se domluvili na koupi a pachatel žádá o zaslání zásilky prostřednictvím kurýrní služby, na kterou zároveň zasílá fiktivní hypertextový odkaz, který oběť přesměruje na webovou stránku vypadající jako oficiální stránka kurýrní služby. Zde je oběť instruována k vyplnění veškerých přístupových údajů do internetového bankovnictví, poté je oběť ze strany pachatele instruována k zaslání QR kódů, které přijdou do klíče mobilního bankovnictví. Poté oběť okamžitě přichází o 120.000 Kč ze svého bankovního účtu, jelikož pachatel získal absolutní kontrolu nad bankovním účtem oběti. Tento skutek je kvalifikován pod paragrafy 209, 230 a 234 trestního zákoníku.

3.3.2 Přiklad č. 2

Neznámý pachatel inzeroval v blíže neupřesněné době z blíže nezjištěného místa přes aplikaci Facebook blíže nespecifikovanou nabídku na investici do krypto měn, na kterou reagoval P.K., který zde zadal své osobní údaje včetně svého telefonního čísla XXX a emailu XXX, kdy byl následně dne 22.01.2024 kontaktován z blíže nezjištěného místa osobou vystupující jako Veronika Krásná a to z telefonního čísla XXX, která mu uvedla, aby zaslal počáteční vklad ve výši 5.000,- Kč na číslo bankovního účtu XXX, pod variabilním symbolem XXX, kdy toto P.K. učinil za účelem obchodování, přičemž byl následně kontaktován z blíže nezjištěného místa osobou vystupující jako XXX, který s ním komunikoval přes aplikaci Whatsapp z telefonního čísla XXX, kdy mu sdělil, aby si do svého mobilního telefonu nainstaloval aplikaci AnyDesk, Kraken a dále mu zaslal odkaz na aplikaci https://trd.orbid.org/, kde mu zřídil přístupové údaje a následně P.K. zaslal na jeho bankovní účet číslo XXX vedený u bankovní instituce AirBank částku ve výši 608,39,- Kč, která měla být ziskem z investice v aplikaci Kraken, kdy mu dále uvedl, že je nutné zaslat další finanční částku jako investici, která je potřebná k výběru zisku ve výši okolo 42.000,- Kč, přičemž také P.K. navedl, aby se přihlásil do svého internetového bankovnictví a povolil neznámý pachateli přes aplikace AnyDesk přístup do svého mobilního telefonu, což P.K. učinil, kdy si následně neznámý pachatel zaslal se souhlasem P.K. z jeho bankovního účtu částku ve výši 35.000,- Kč na bankovní účet č. XXX, přičemž po této transakci přestal neznámý pachatel s poškozeným P.K. komunikovat, kdy má telefonní číslo nedostupné, přičemž do současné doby P.K. nezaslal žádný zisk ani nevrátil investovanou částku, čímž P.K. vznikla škoda ve výši 39.391,61,- Kč. (Policie České republiky, 2024)

Na tomto příkladu lze vidět, že oběť kontaktuje neznámého pachatele na základě inzerátu na investice do kryptoměn zveřejněného jako reklama na sociální síti Facebook, kde oběť zadá

své telefonní číslo a email. Poté je v řádu několika hodin kontaktována ze strany pachatele, kdy po představení investičního produktu se společně domluví na počáteční investici ve výši 5000 Kč, kde pachatel oběti ukáže, jak ono investování funguje a jak výhodné je, po krátkém čase zašle pachatel poškozenému na bankovní účet určitou částku, kterou prezentuje jako výdělek z investic (v tomto případě se jedná o lákavý 12% výdělek z původní částky 5000 Kč), čímž oběť navnadí k další větší investici, po zaslání peněz ovšem pachatel přestává komunikovat a oběť tak přijde o své investované peníze. Tento skutek je kvalifikován pod paragrafy 209, 230 a 234 trestního zákoníku.

3.4 Ochrana proti kybernetickým útokům

Vzhledem k narůstajícím kybernetickým hrozbám je klíčové, aby si jednotlivci byli vědomi rizik a používali efektivní metody pro zvýšení své ochrany v digitálním světě. Tyto metody jsou založeny na aktuálních osvědčených postupech a zahrnují široké spektrum opatření od technických řešení až po osobní zvyky a chování. Vzhledem k dynamické povaze kybernetických hrozeb je nezbytné, aby se jednotlivci neustále vzdělávali a adaptovali své bezpečnostní praktiky podle nejnovějších trendů a doporučení v oblasti kybernetické bezpečnosti. (Augenbaum, 2019; Plotkin, 2020)

Aktuálně osvědčenými postupy a metodologiemi jsou:

Pravidelné aktualizace a správa záplat

Software a operační systémy často obsahují bezpečnostní chyby, které mohou být zneužity hackery. Pravidelné aktualizace zajišťují opravy těchto chyb. Nastavením automatických aktualizací na Windows, macOS, Androidu a iOS je zajištěno, že zařízení obdrží nejnovější zabezpečovací opravy bez potřeby manuálního zásahu. (Augenbaum, 2019; Plotkin, 2020)

Používání silných hesel a správce hesel

Silná hesla jsou základem ochrany online identit. Správce hesel pomáhá udržet bezpečné a unikátní heslo pro každou službu bez nutnosti všechny držet v paměti. Použití kombinace velkých a malých písmen, čísel a speciálních znaků v heslech. Aplikace jako LastPass nebo 1Password mohou generovat a uchovávat hesla. (Augenbaum, 2019; Plotkin, 2020)

Dvoufaktorová autentizace (2FA)

2FA přidává další vrstvu zabezpečení tím, že vyžaduje druhý prvek ověření kromě hesla, což komplikuje přístup útočníkům. Nastavení 2FA na emailu, sociálních sítích a bankovních

účtech, obvykle pomocí SMS, emailu nebo autentizační aplikace jako Google Authenticator. (Augenbaum, 2019; Plotkin, 2020)

Opatrnost při klikání na odkazy a přílohy

Phishingové útoky a škodlivé softwary jsou často šířeny prostřednictvím infikovaných emailů nebo webových odkazů. Je nutné rozpoznávat podezřelé emaily nebo webové stránky a vyhnout se otevírání příloh nebo klikání na odkazy od neznámých odesílatelů. (Augenbaum, 2019; Plotkin, 2020)

Zabezpečení domácí sítě

Wi-Fi sítě jsou častým cílem útoků, zabezpečení těchto sítí může zabránit neoprávněnému přístupu. Řešením může být například změna výchozího jména sítě (SSID) a hesla, použití šifrování WPA3 a deaktivace funkce WPS na routeru. (Augenbaum, 2019; Plotkin, 2020)

Pravidelné zálohování dat

Zálohování je klíčové pro obnovu dat po útocích jako je ransomware. Použitím externích pevných disků nebo cloudových služeb jako je Google Drive nebo Dropbox pro pravidelné zálohování důležitých souborů. (Augenbaum, 2019; Plotkin, 2020)

Použití bezpečnostního softwaru

Antivirus a anti-malware programy detekují a eliminují potenciální hrozby před tím, než způsobí škodu. Řešením může být například instalace a pravidelná aktualizace programů jako Kaspersky, Norton nebo McAfee. (Augenbaum, 2019; Plotkin, 2020)

II. PRAKTICKÁ ČÁST

4 POLOSTRUKTUROVANÝ DOTAZNÍK

V rámci metodologie bakalářské práce byla použita metoda kvalitativního výzkumu ve formě dotazníkového šetření, kdy původně byl vytvořen polostrukturovaný dotazník ve fyzické (papírové formě). Dotazník byl koncipován jako anonymní, aby se zajistila objektivita a bezpečnost údajů poskytnutých respondenty. Tento krok byl zvolen s cílem usnadnit přístup pro respondenty, kteří byli požádáni o vyplnění dotazníku při příjmu oznámení na obvodním oddělení ve Zlíně v období podzimu a zimy roku 2023 až do jara roku 2024, dotazníku se zúčastnilo celkem 83 osob. Všichni respondenti byli poškozenými ve smyslu kyberkriminality. Po dokončení fáze sběru dat bylo však nezbytné zajistit, aby byly informace zpracovány efektivně a systematicky. S tímto cílem byly ručně všechny odpovědi převedeny z papírových dotazníků do digitální podoby, a to konkrétně do Google Formulářů. Tento krok umožnil automatizované generování datového souboru, což výrazně zjednodušilo další analýzu odpovědí. Google Formuláře následně vytvořily excelovskou tabulku, která poskytla ucelený přehled shromážděných dat.

Excelovská tabulka byla důkladně prozkoumána a analyzována, přičemž hlavní zjištění a statistiky byly začleněny do hlavního textu bakalářské práce. Kompletní datový soubor byl přiložen jako příloha práce, čímž byla zajištěna transparentnost výzkumného procesu a umožněn přístup k datům pro další potenciální výzkum v této oblasti. Tento postup zajišťuje snadnou verifikaci výsledků a podporuje reprodukovatelnost výzkumu v oblasti kybernetické bezpečnosti.

Dotazník měl za hlavní cíl získat hlubší pochopení o tom, jak poškození vnímají a řeší hrozby z kyberprostoru. V dnešním světě, kde digitální technologie pronikají do všech aspektů našeho života, se stává kybernetická bezpečnost nezbytnou součástí naší každodenní existence. Tento dotazník byl navržen tak, aby shromáždil důležité údaje o úrovni povědomí respondentů o kybernetických hrozbách, o preventivních opatřeních, která lidé podnikají, a o jejich zkušenostech s kybernetickými útoky. Účelem tohoto průzkumu je poskytnout ucelený pohled na aktuální stav kybernetické odolnosti mezi veřejností. Odpovědi z dotazníku posloužily jako základ pro analýzu, která umožnila identifikovat klíčové oblasti, kde byla a bude potřeba zvýšit povědomí a zlepšit ochranná opatření proti kybernetickým útokům.

4.1 Otázky v dotazníkovém šetření

Je klíčové pochopit nejen aktuální stav povědomí a připravenosti respondentů, ale také identifikovat oblasti, kde je možné provést zlepšení. Každá otázka v dotazníku byla pečlivě navržena s konkrétní motivací, která podporuje tento hlavní cíl:

Otázka č. 1: Pohlaví

Motivací za zahrnutím otázky o pohlaví je možnost analyzovat, zda existují významné rozdíly v povědomí a přístupu ke kybernetické bezpečnosti mezi muži a ženami. Tato informace může pomoci vytvořit cílenější vzdělávací programy.

Otázka č. 2: Věk

Zjištění věkové skupiny respondentů umožňuje zkoumat, jak se povědomí a chování týkající se kybernetické bezpečnosti liší v různých věkových kohortách. To může napomoci k rozvoji generací specifických preventivních opatření.

Otázka č. 3: Nejvyšší dosažené vzdělání

Otázka je zaměřena na zjištění souvislosti mezi úrovní vzdělání a povědomím o kybernetické bezpečnosti, což může ukázat, zda vzdělávací systém efektivně informuje o digitální bezpečnosti.

Otázka č. 4: Zkušenosti s informačními technologiemi

Zkoumání úrovně IT zkušeností umožňuje odhadnout, jak dobře jsou respondenti vybaveni k rozpoznání a reakci na kybernetické hrozby.

Otázka č. 5: Považujete se za informovaného v oblasti kybernetické bezpečnosti?

Tato otázka poskytuje přehled o subjektivním vnímání vlastního povědomí o kybernetické bezpečnosti, což je důležité pro hodnocení potřeby vzdělávacích zásahů.

Otázka č. 6: Jaké typy kybernetických útoků znáte?

Identifikace znalostí o různých typech útoků je klíčová pro posouzení úrovně informovanosti respondentů a identifikaci oblastí, které vyžadují zvýšenou osvětu.

Otázka č. 7: Z jakých zdrojů čerpáte informace o kybernetické bezpečnosti?

Zjištění preferovaných zdrojů informací pomůže v optimalizaci distribuce osvětových materiálů o kybernetické bezpečnosti.

Otázka č. 8: Jaká preventivní opatření proti kybernetickým útokům používáte?

Tato otázka odhaluje, jaké konkrétní kroky podnikají jednotlivci ke zvýšení své ochrany, což je zásadní pro identifikaci populárních a potenciálně nedostatečných opatření.

Otázka č. 9: Jak jste reagovali, když jste se stali cílem kybernetického útoku?

Odpovědi na tuto otázku poskytují přehled o běžných reakcích a strategiích obětí kybernetických útoků, což může napomoci k formulaci doporučení pro efektivní řešení incidentů.

Otázka č. 10: Na jaký typ Vašich osobních nebo pracovních dat nebo systémů zaútočil kybernetický útočník?

Zkoumání specifických cílů útoků pomáhá identifikovat nejvíce zranitelná místa v kybernetické ochraně respondentů.

Otázka č. 11: Jakou škodu či újmu Vám způsobil kybernetický útok?

Analýza rozsahu a typu způsobené škody poskytuje důležité informace o dopadech kybernetických útoků na jednotlivce.

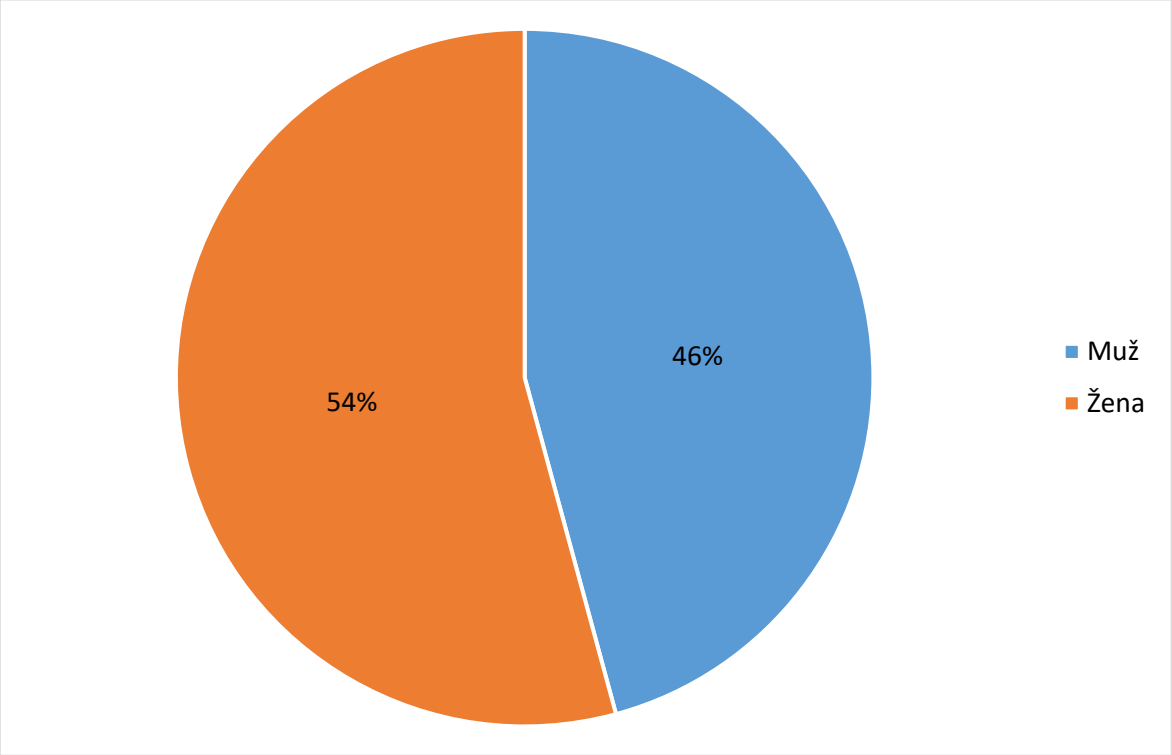
Otázka č. 12: Jaká z následujících možností by podle Vás nejvíce pomohla zvýšit odolnost osob vůči kybernetickým útokům?

Tato otázka je zásadní pro identifikaci opatření, která jsou považována za nejúčinnější v očích veřejnosti, a může napomoci k prioritizaci preventivních a vzdělávacích iniciativ.

Každá otázka v dotazníku je nezbytnou součástí širšího úsilí o pochopení a zlepšení kybernetické odolnosti, a to jak na individuální, tak na kolektivní úrovni.

4.2 Výstupní data z jednotlivých otázek dotazníkového šetření

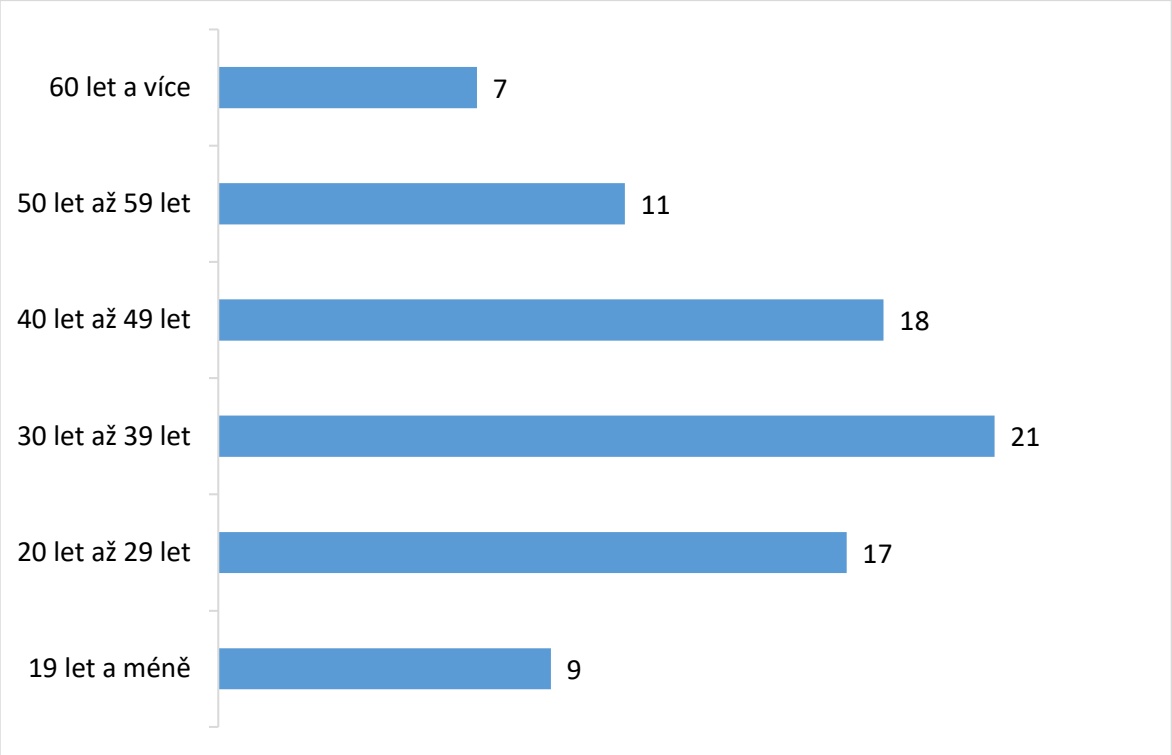
Otázka č. 1: Pohlaví



Obrázek 2 Pohlaví (zdroj: vlastní)

V rámci demografické analýzy respondentů dotazníku zaměřeného na odolnost osob vůči kybernetickým útokům bylo zjištěno, že z celkového počtu 83 účastníků průzkumu bylo 45 žen, což představuje 54,22 %, a 38 mužů, což tvoří 45,78 %. Tato data naznačují relativně vyvážené zastoupení pohlaví mezi respondenty, což umožňuje provést komplexní analýzu odpovědí s ohledem na genderovou perspektivu. Přítomnost obou pohlaví v téměř rovném poměru je důležitá pro zajištění, že zjištění a doporučení vyplývající z analýzy dotazníku jsou relevantní a aplikovatelné na širokou populaci.

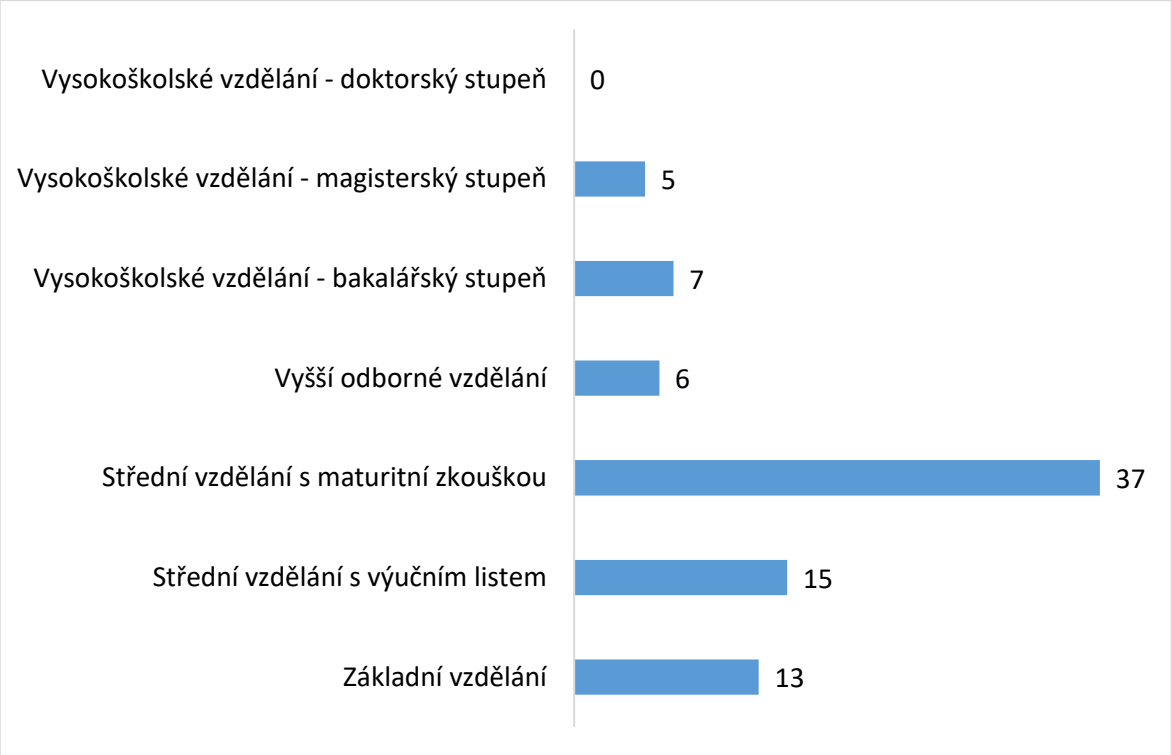
Otázka č. 2: Věk



Obrázek 3 Věk (zdroj: vlastní)

V rámci analýzy věkového rozložení respondentů dotazníku zaměřeného na odolnost vůči kybernetickým útokům bylo identifikováno následující rozdělení mezi jednotlivými věkovými skupinami. Z celkového počtu 83 účastníků bylo 9 respondentů (10,84 %) ve věku 19 let a méně, skupina ve věku 20 až 29 let tvořila 17 respondentů (20,48 %), největší zastoupení měla věková kategorie 30 až 39 let s 21 respondenty (25,30 %). Skupina 40 až 49 let představovala 18 respondentů (21,69 %), respondentů ve věku 50 až 59 let bylo 11 (13,25 %), a skupina 60 let a více čítala 7 respondentů (8,43 %).

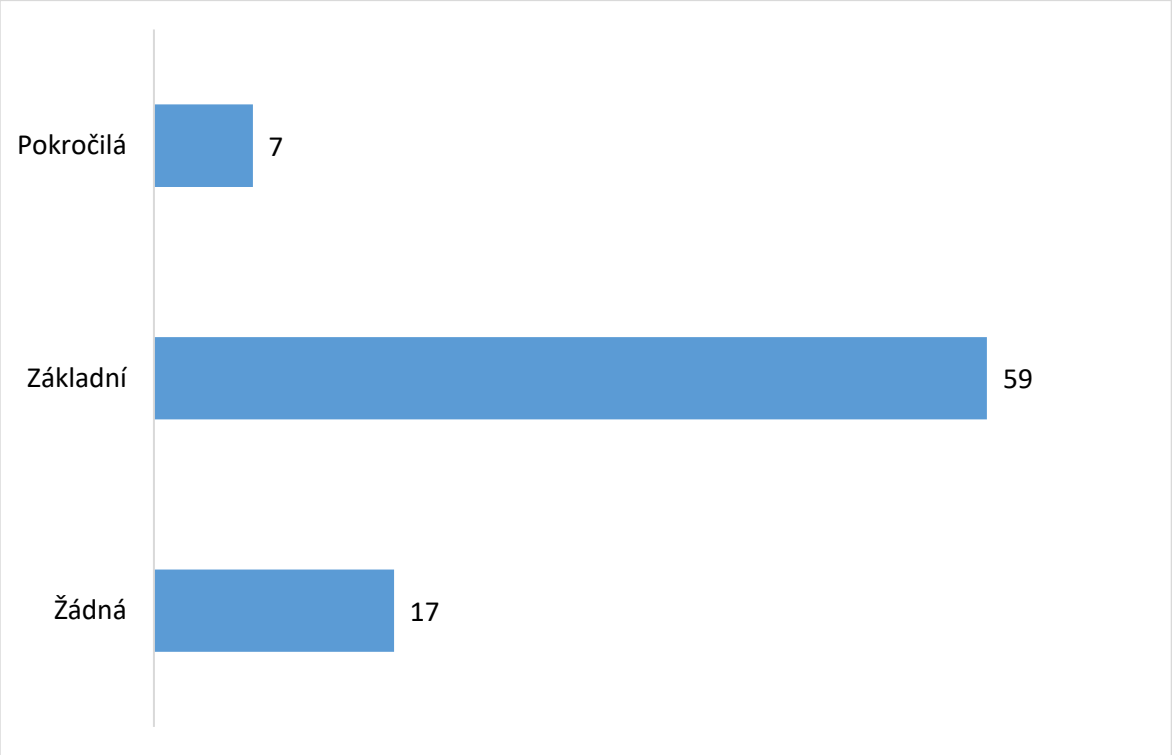
Otázka č. 3: Nejvyšší dosažené vzdělání



Obrázek 4 Nejvyšší dosažené vzdělání (zdroj: vlastní)

V analýze dosaženého vzdělání mezi respondenty dotazníku byly zaznamenány následující údaje: z celkového počtu 83 respondentů 13 respondentů (15,66 %) uvedlo, že dosáhlo základního vzdělání, skupina s dokončeným středním vzděláním s výučním listem čítala 15 osob (18,07 %), velkou část respondentů tvořilo 37 jedinců (44,58 %) s maturitou, vyšší odborné vzdělání mělo 6 účastníků (7,23 %), vysokoškolské vzdělání na bakalářském stupni dosáhlo 7 respondentů (8,43 %), magisterský stupeň vysokoškolského vzdělání byl zaznamenán u 5 respondentů (6,02 %), a žádný z respondentů nedosáhl vysokoškolského vzdělání v doktorském stupni. Tyto údaje reflektují rozmanitost vzdělávacích úrovní mezi účastníky dotazníku a poskytují ucelený přehled o vzdělávacím spektru respondentů.

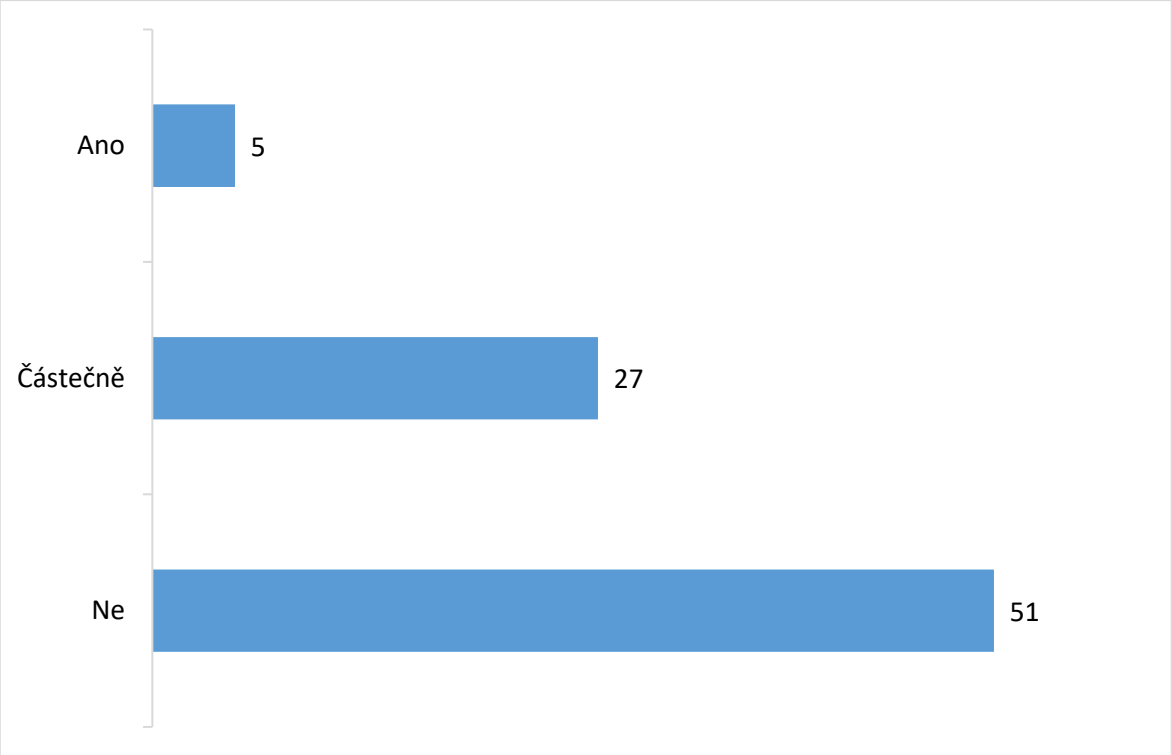
Otázka č. 4: Zkušenosti s informačními technologiemi



Obrázek 5 Zkušenosti s informačními technologiemi (zdroj: vlastní)

Z celkového počtu 83 respondentů průzkumu o IT zkušenostech 59 (71,08 %) své dovednosti hodnotilo jako základní, 7 (8,43 %) uvedlo pokročilé znalosti, a 17 (20,48 %) respondentů deklarovalo, že nemá žádné zkušenosti s informačními technologiemi.

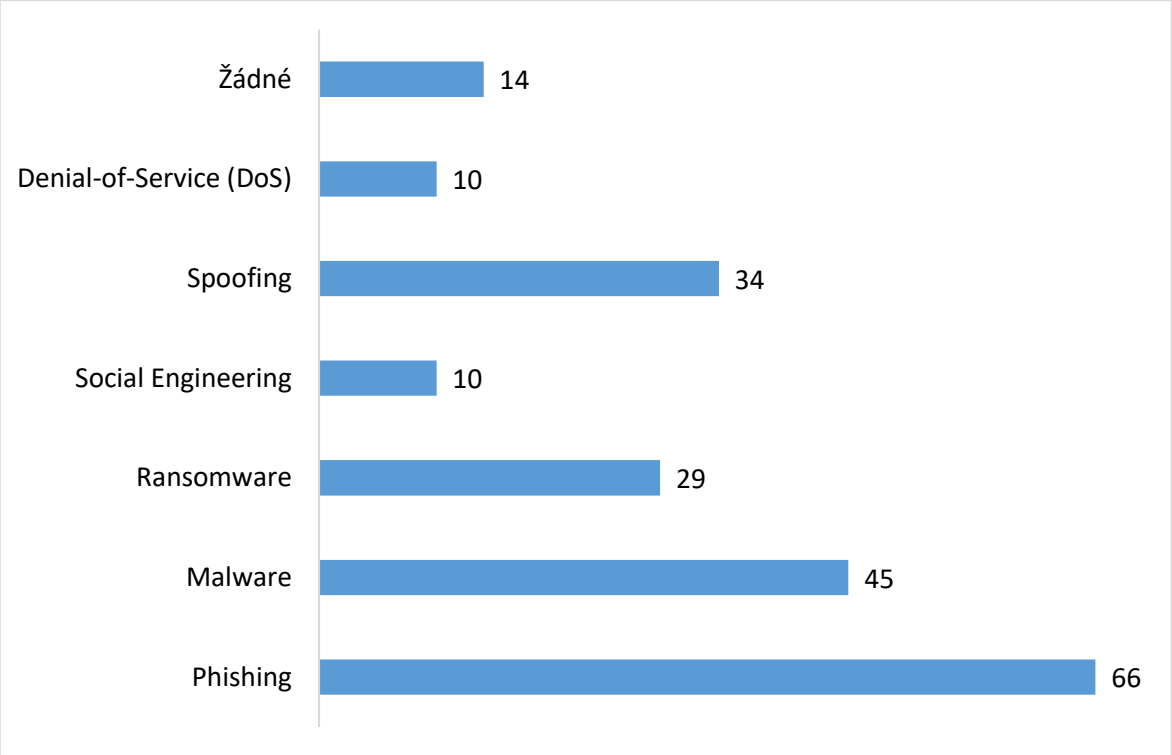
Otázka č. 5: Považujete se za informovaného v oblasti kybernetické bezpečnosti?



Obrázek 6 Považujete se za informovaného v oblasti kybernetické bezpečnosti? (zdroj: vlastní)

Z celkového počtu 83 respondentů se v oblasti kybernetické bezpečnosti považovalo za informované pouze 5 (6,02 %) osob. Větší část, 27 (32,53 %), se identifikovala jako částečně informovaná, což ukazuje na určitou míru povědomí o této problematice. Nicméně, dominantní většina, 51 (61,45 %) respondentů, se považovala za neinformované, což signalizuje značný prostor pro zlepšení v edukaci a osvětě veřejnosti v této klíčové oblasti.

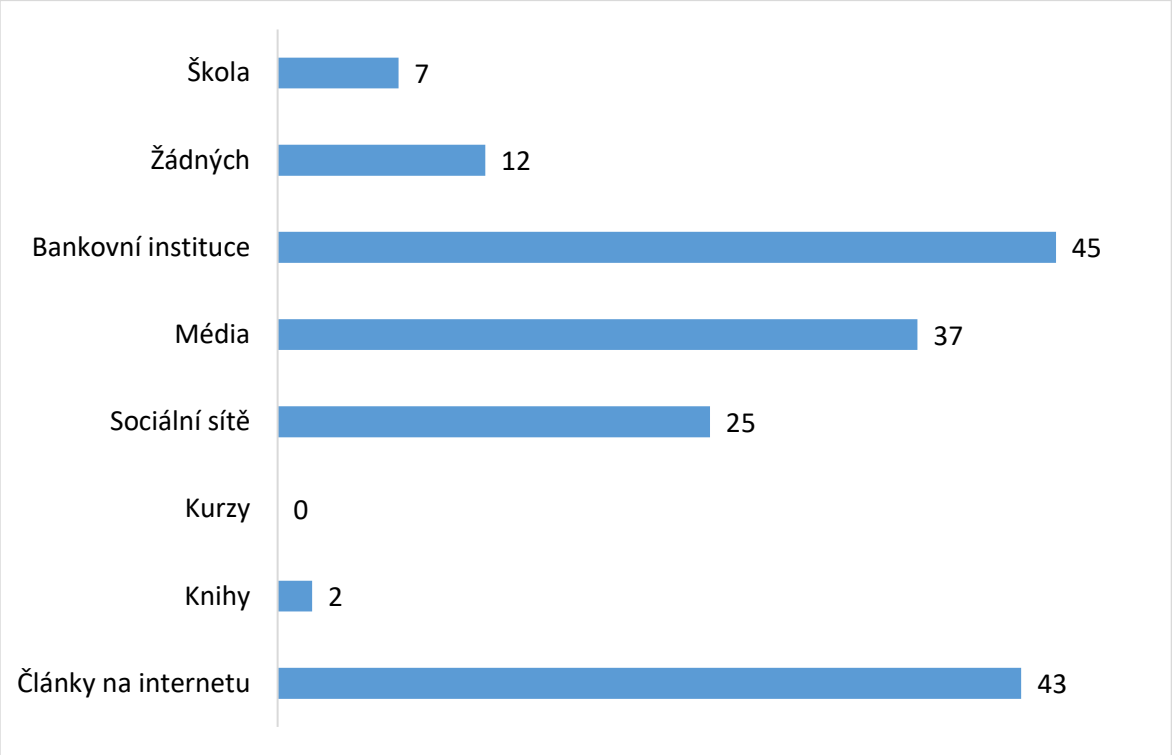
Otázka č. 6: Jaké typy kybernetických útoků znáte?



Obrázek 7 Jaké typy kybernetických útoků znáte? (zdroj: vlastní)

Z 83 respondentů nejvíce, 66 (79,52 %), identifikovalo phishing jako známý typ kybernetického útoku, což naznačuje vysoké povědomí o této hrozbě. Malware byl uveden 45 (54,22 %) účastníky, zatímco ransomware znalo 29 (34,94 %) respondentů. Méně známé útoky jako social engineering a Denial-of-Service (DoS) byly rozpoznány pouze 10 (12,05 %) účastníky. Spoofing byl znám 34 (40,96 %) respondentům. Celkem 14 (16,87 %) respondentů nebylo obeznámeno s žádným z vybraných typů kybernetických útoků.

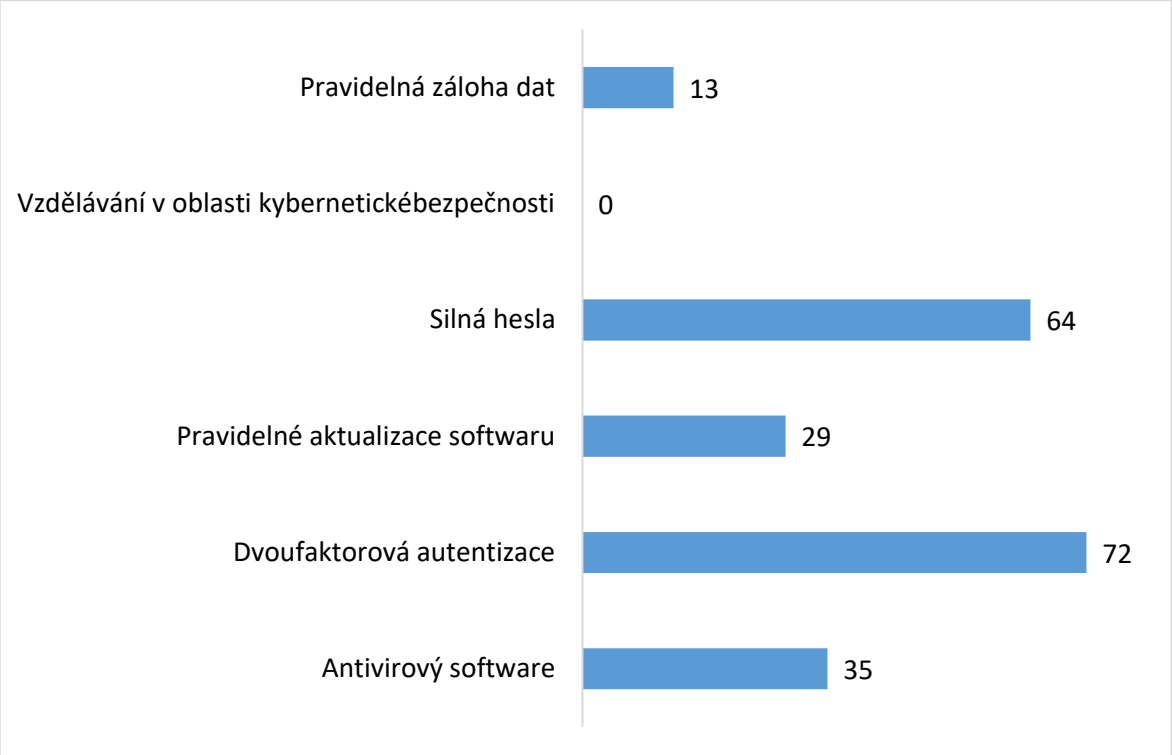
Otázka č. 7: Z jakých zdrojů čerpáte informace o kybernetické bezpečnosti?



Obrázek 8 Z jakých zdrojů čerpáte informace o kybernetické bezpečnosti? (zdroj: vlastní)

Z 83 respondentů nejčastěji, 45 (54,22 %) získávalo informace o kybernetické bezpečnosti od bankovních institucí, což bylo následováno 43 (51,81 %) osobami, které četly články na internetu. Média byla zdrojem pro 37 (44,58 %) respondentů a sociální sítě pro 25 (30,12 %) z nich. Oproti tomu knihy 2 (2,41 %) a vzdělávací instituce (škola) 7 (8,43 %) byly méně využívané zdroje. Celkem 12 (14,46 %) respondentů uvedlo, že nečerpají informace o kybernetické bezpečnosti z žádného z těchto zdrojů.

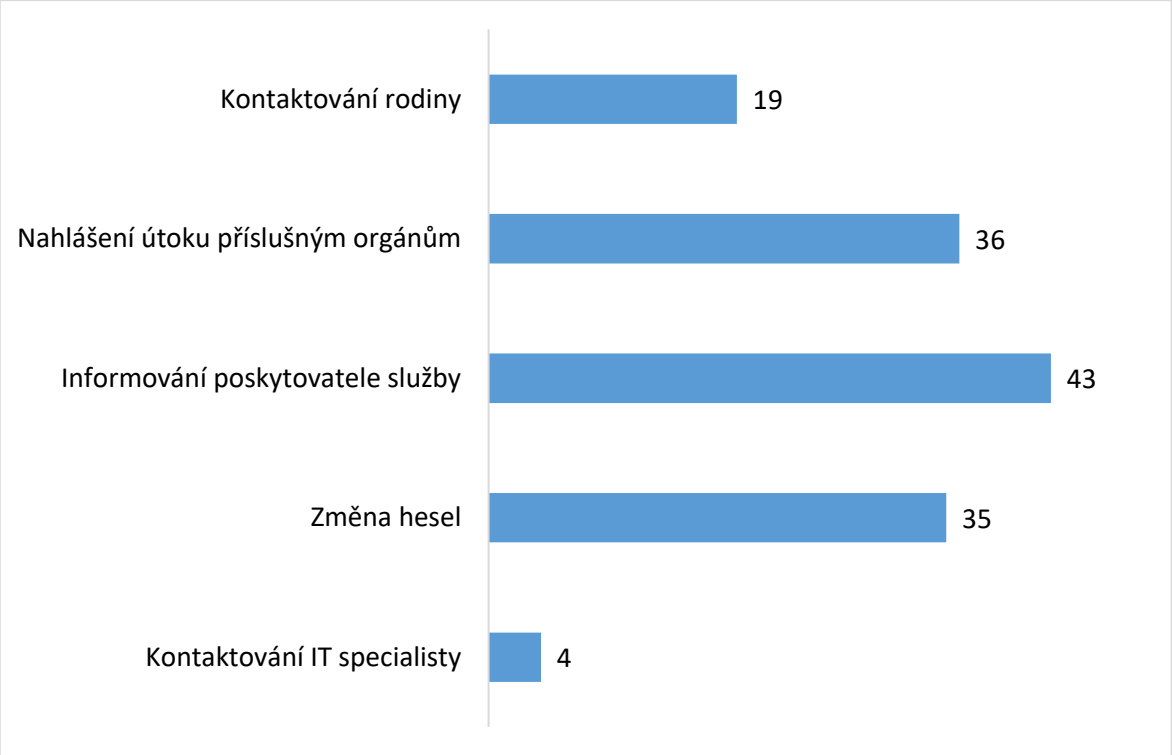
Otázka č. 8: Jaká preventivní opatření proti kybernetickým útokům používáte?



Obrázek 9 Jaká preventivní opatření proti kybernetickým útokům používáte? (zdroj: vlastní)

Nejčastějším preventivním opatřením proti kybernetickým útokům mezi 83 respondenty byla dvoufaktorová autentizace, což upřednostnilo 72 (86,75 %) účastníků. Toto bylo následováno používáním silných hesel 64 (77,11 %) a antivirovým softwarem 35 (42,17 %). Pravidelné aktualizace softwaru 29 (34,94 %) a zálohy dat 13 (15,66 %) byly rovněž používány, ale v menší míře. Zajímavé je, že vzdělávání v oblasti kybernetické bezpečnosti nebylo vybráno jako preventivní opatření žádným z respondentů.

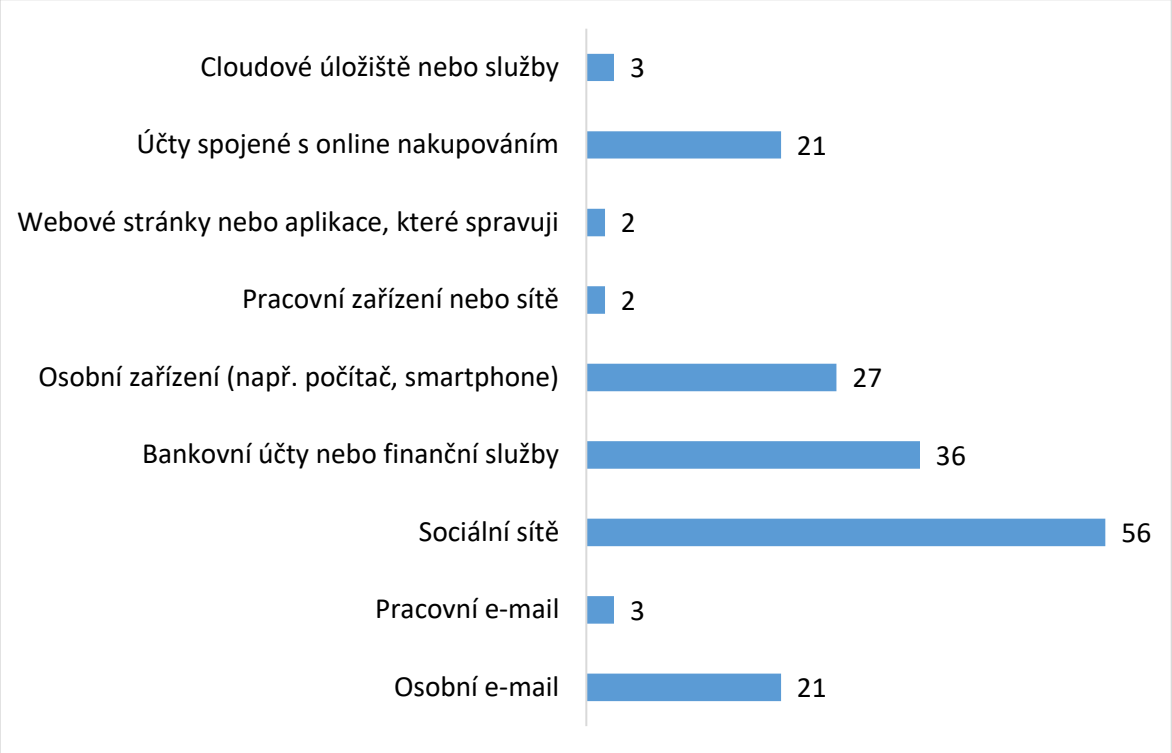
Otázka č. 9: Jak jste reagovali, když jste se stali cílem kybernetického útoku?



Obrázek 10 Jak jste reagovali, když jste se stali cílem kybernetického útoku? (zdroj: vlastní)

Když se respondenti dozvěděli, že se stali terčem kybernetického útoku, nejčastěji informovali poskytovatele služby, což učinilo 43 (51,81 %) z nich. Další často podnikaným krokem bylo nahlášení útoku příslušným orgánům 36 (43,37 %) a změna hesel 35 (42,17 %). Kontaktování rodiny bylo další reakcí s 19 (22,89 %), zatímco kontaktování IT specialisty bylo méně časté s 4 (4,82 %).

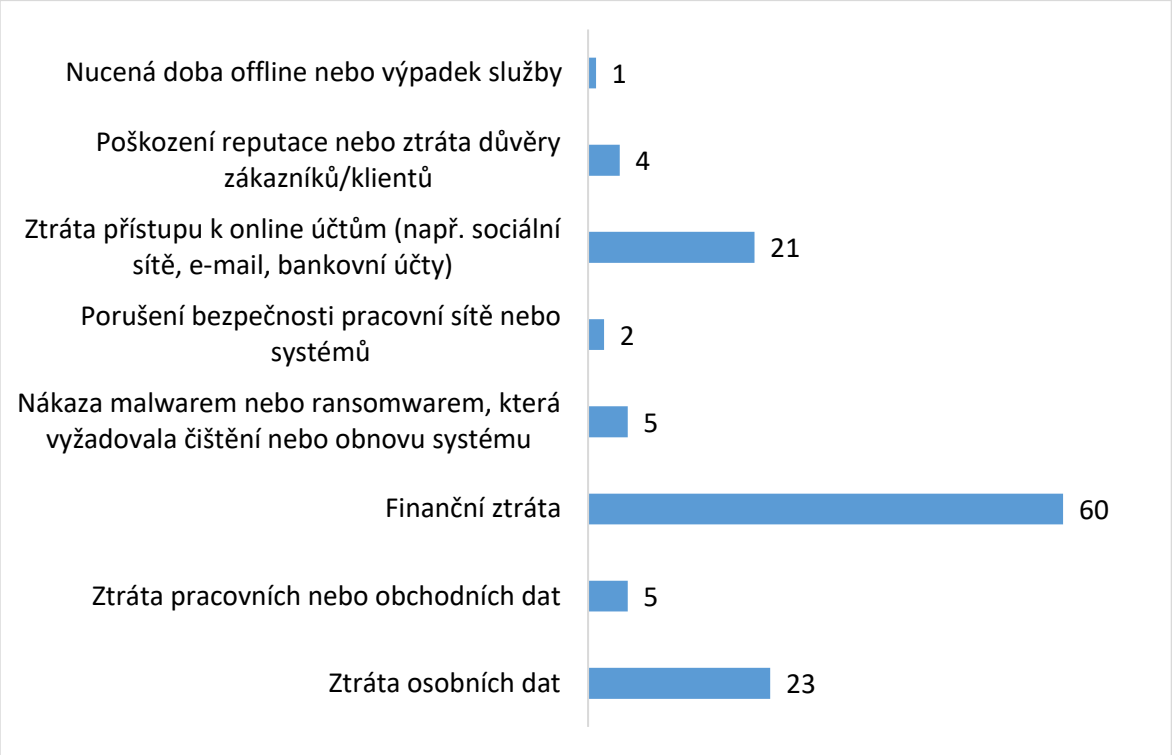
Otázka č. 10: Na jaký typ Vašich osobních nebo pracovních dat nebo systémů zaútočil kybernetický útočník?



Obrázek 11 Na jaký typ Vašich osobních nebo pracovních dat nebo systémů zaútočil kybernetický útočník? (zdroj: vlastní)

Z 83 respondentů byly jako nejčastější cíle kybernetických útoků identifikovány sociální sítě 56 (67,47 %), což poukazuje na vysokou úroveň ohrožení těchto platforem. Bankovní účty nebo finanční služby následovaly s 36 (43,37 %), což zdůrazňuje finanční motivy mnoha útoků. Osobní zařízení byla také značně zasažena 27 (32,53 %), stejně jako osobní emaily a účty spojené s nakupováním 21 (25,30 %). Méně často byly jako cíle uváděny cloudová úložiště a pracovní emaily 3 (3,61 %), webové stránky nebo pracovní zařízení 2 (2,41 %).

Otázka č. 11: Jakou škodu či újmu Vám způsobil kybernetický útok?



Obrázek 12 Jakou škodu či újmu Vám způsobil kybernetický útok? (zdroj: vlastní)

V průzkumu mezi 83 respondenty byla nejčastější škodou finanční ztráta 60 (72,29 %), dále následovala ztráta osobních dat 23 (27,71 %) a ztráta přístupu k online účtům 21 (25,30 %). Malware nebo ransomware, spolu se ztrátou pracovních dat, postihly 5 (6,02 %) respondentů. Poškození reputace nebo ztráta důvěry zákazníků se objevila u 4 (4,82 %), zatímco porušení bezpečnosti pracovní sítě či systému 2 (2,41 %) a nucená doba off-line nebo výpadek služby byly ještě méně časté 1 (1,20 %).

Otázka č. 12: Jaká z následujících možností by podle Vás nejvíce pomohla zvýšit odolnost osob vůči kybernetickým útokům?

Obrázek 13 Jaká z následujících možností by podle Vás nejvíce pomohla zvýšit odolnost osob vůči kybernetickým útokům? (zdroj: vlastní)

Za nejlepší z vybraných možností, která by nejvíce pomohla zvýšit odolnost osob vůči kybernetickým útokům považovalo 83 respondentů spuštění veřejných informačních kampaní zaměřených na zvyšování povědomí o kybernetických hrozbách 32 (38,55 %), následovanou rozvojem a integrací kurikul o kybernetické bezpečnosti do školních osnov na všech úrovních vzdělávání 16 (19,28 %), organizováním pravidelných workshopů a školení o kybernetické bezpečnosti pro veřejnost 14 (16,87 %), poskytováním online kurzů a zdrojů zdarma pro samostudium kybernetické bezpečnosti 13 (15,66 %), vytvářením a distribucí interaktivních vzdělávacích materiálů a her zaměřených na kybernetickou bezpečnost 8 (9,64 %) a nakonec bez jediného výběru možnosti podpory výzkumu a vývoje v oblasti vzdělávacích nástrojů pro kybernetickou bezpečnost.

5 NESTANDARTIZOVANÝ ROZHOVOR

Rozhovor s policistou z oddělení kybernetické kriminality Policie ČR byl navržen tak, aby poskytl náhled do světa boje proti kyberkriminalitě z pohledu odborníka, charakteristiku kyberkriminality v ČR, mezinárodní spolupráci, prevenci a ochranu, vzdělávání veřejnosti, očekávané trendy a výzvy, radu pro veřejnost, zdroje pro oběti, a osobní motivaci a zkušenosti. Tyto otázky mají za cíl objasnit, jak Policie ČR přistupuje k řešení kybernetických hrozeb a jaké strategie považuje za nejúčinnější ve snaze chránit veřejnost.

Cílem rozhovoru s policistou z oddělení kybernetické kriminality byl nejen poskytnout pohled na boj proti kyberkriminalitě, ale také nabídnout veřejnosti praktické rady pro zvýšení jejich kybernetické bezpečnosti. Expert sdílel své postřehy o nejúčinnějších preventivních opatřeních a způsobech, jak se chránit před běžnými hrozbami, čímž přispívá k většímu povědomí a lepší připravenosti občanů čelit kybernetickým útokům.

5.1 Otázky a odpovědi rozhovoru

Otázka č. 1: Jak se jmenujete a kde pracujete?

Odpověď: Mé jméno je nprap. Stanislav Cholasta a pracuji jako zaměstnanec Policie ČR přesněji jako vyšetřovatel na oddělení analytiky a kybernetické kriminality ve Zlíně.

Otázka č. 2: Jak jste se dostal k práci v oblasti kybernetické kriminality u Policie ČR a co vás na této specializaci nejvíce zajímá?

Odpověď: Od začátku své kariéry jsem působil na obvodním oddělení Policie ČR, kde jsem se setkával s nejrůznějšími formami kriminality. S ohledem na to, že v posledních letech je zřetelný nárůst kybernetické kriminality, která se stává čím dál tím větším problémem, bylo pro mě přirozenou volbou zaměřit se na tento druh kriminality.

Otázka č. 3: Jaké typy kybernetických útoků jsou v České republice nejčastější a jak se vyvíjejí v čase?

Odpověď: Nejčastěji se setkáváme s kybernetickou kriminalitou zaměřenou na lidi, kteří podlehli podvodnému investování na kryptoburzách, a s phishingem, kdy se pachatelé snaží získat přístupové údaje k internetovému bankovnictví obětí. S časem lze pozorovat, že metody pachatelů se stávají sofistikovanějšími.

Otázka č. 4: Jaká je úspěšnost Policie ČR při objasňování kybernetické kriminality a existuje rozdíl v tom, jaká kyberkriminalita má větší šanci na objasnění?

Odpověď: Úspěšnost Policie ČR v objasňování kybernetické kriminality je podstatně nižší než u tradiční kriminality. Podle mého názoru je větší šance na objasnění těch případů kyberkriminality, při kterých je možné v rámci šetření vyžádat informace od subjektů podléhajících českému právnímu systému.

Otázka č. 5: Jak Policie ČR spolupracuje s mezinárodními organizacemi a policiemi jiných států v boji proti kyberkriminalitě?

Odpověď: Policie ČR spolupracuje v boji proti kyberkriminalitě i na mezinárodní úrovni. Tato spolupráce je klíčová, jelikož pachatelé často využívají služby a platformy zahraničních společností. V některých případech umožňují mezinárodní dohody vyžádání potřebných informací, avšak v jiných případech může být vyžádání těchto informací komplikované, pokud příslušné mezinárodní smlouvy neexistují.

Otázka č. 6: Můžete zmínit některý z případů kybernetické kriminality, na kterém jste pracoval a který měl významný dopad nebo vás osobně zasáhl?

Odpověď: Velmi mě zasáhl případ, kdy organizovaná skupina provozovala podvodnou webovou stránku nabízející obchodování s kryptoměnami. Stopy vedly k mnoha poškozeným, kteří byli využiti pro podvody. Tento případ ukázal, jak rozsáhlá a organizovaná může kyberkriminalita být.

Otázka č. 7: Jaké jsou podle vaší zkušenosti nejefektivnější metody prevence proti kybernetickým útokům pro jednotlivce i organizace?

Odpověď: Neustálá osvěta a informovanost o rizicích a metodách ochrany proti kyberkriminalitě jsou klíčové. Je důležité osvětlovat tuto problematiku od dětství až po starší generaci. Možnosti osvěty zahrnují mediální kampaně, kurzy a přednášky.

Otázka č. 8: Existuje podle vás oblast, ve které je potřeba ze strany státu zapracovat na vzdělávání svých občanů?

Odpověď: Určitě ano, ve všech. Obecně lze říct, že stát při řešení otázky kybernetické kriminality zaspal a nyní je několik let pozadu v kanceláři vtipkujeme až o 10 letech, ale ono to není daleko od pravdy. Do vzdělávacích osnov se dostávají otázky kyberkriminality a finanční gramotnosti velice pozvolna a jakmile se tam dostanou je zde otázka, zda tomu rozumí samotní pedagogové. Je zřejmé, že samotný stát na to nestačí a je nutné, aby se do prevence kyberkriminality zapojili i soukromé subjekty jako můžeme sledovat například

u bankovních institucí, které varují své zákazníky před podvody při každé návštěvě pobočky či internetové platbě, tak to má být a určitě se jedná o správnou cestu.

Otázka č. 9: Jaké vzdělávací programy nebo iniciativy Policie ČR podporuje nebo provádí pro zvýšení povědomí o kybernetické bezpečnosti mezi občany?

Odpověď: Policie ČR se snaží informovat veřejnost o případech kyberkriminality a upozorňovat na potenciální rizika. Podporujeme také organizace, které se zabývají prevencí kyberkriminality. Jednou z největších společných akcí Policie ČR a České bankovní asociace je vzdělávací kampaň „#nePINdej!“.

Otázka č. 9: Jaké nové trendy a výzvy v oblasti kybernetické kriminality očekáváte v nadcházejících letech a jak se na ně Policie ČR připravuje?

Odpověď: Očekávám, že v blízké budoucnosti bude stále důležitější role umělé inteligence v oblasti kybernetické kriminality. Předpokládá se, že vývoj v této oblasti bude rychlý a policie bude muset přizpůsobit své metody a prostředky.

Otázkač. 10: Jakou radu byste dal každému, kdo chce zlepšit svou kybernetickou bezpečnost?

Odpověď: Mám jich hned několik. Důležité je ověřovat si, s kým komunikujete po telefonu nebo přes internet a být opatrný při sdílení osobních informací. Je za potřebí používat „selský rozum“, například jestli se zdá být příležitost k investici až moc dobrá pravděpodobně je a bude se často jednat o podvod. Dále pokud nám antivirus nebo internetový prohlížeč říká, že se jedná o nebezpečnou stránku, pravděpodobně je. Poměrně nebezpečné jsou například veřejné Wi-Fi sítě, těmto by se měla veřejnost také vyhýbat.

Otázka č. 11: Kam by se měli obrátit lidé v ČR, pokud se stanou obětí kybernetického útoku?

Odpověď: V případě stání se obětí kybernetického útoku je klíčové vyhledat odbornou pomoc, například u poskytovatele dané služby. K dispozici jsou specializované webové stránky (např. www.e-bezpeci.cz), telefonní linky, a v neposlední řadě je možné se obrátit na Policii ČR, která poskytne odbornou pomoc nebo směřuje k dalším odborníkům.

Otázka č. 12: Co vás nejvíce motivuje ve vaší práci a jak se vyrovnáváte s psychickou náročností řešení případů kybernetické kriminality?

Odpověď: Motivuje mě rozmanitost a dynamika problematiky kyberkriminality a samozřejmě možnost úspěšně dopadnout pachatele. Po náročné práci je pro mě důležité najít čas na relaxaci a trávení volného času s rodinou nebo v přírodě.

5.2 Závěry z rozhovoru

Tento rozhovor poskytl ucelený pohled na situaci kybernetické kriminality v České republice z perspektivy zkušeného specialisty a zdůraznil význam prevence, osvěty a mezinárodní spolupráce v boji proti této neustále se vyvíjející hrozbě.

Z rozhovoru s panem Stanislavem Cholastou z OAKK Zlín o kybernetické kriminalitě v České republice vyplývá několik klíčových závěrů:

Charakteristika a vývoj kyberkriminality: V České republice se nejčastěji setkáváme s podvodným investováním na kryptoburzách a phishingem. Tyto metody se stávají stále sofistikovanějšími, což zvyšuje potřebu neustálého vzdělávání a adaptace ochranných strategií.

Výzvy v objasňování kyberkriminality: Objasňování kybernetické kriminality je složitější než u tradiční kriminality, přičemž větší šance na úspěch mají případy, kde je možné získat informace od subjektů podléhajících českému právnímu systému.

Mezinárodní spolupráce: Boj proti kyberkriminalitě vyžaduje úzkou mezinárodní spolupráci, neboť pachatelé často využívají zahraniční služby a platformy. Existence mezinárodních dohod je klíčová pro úspěch v této oblasti.

Prevence a osvěta: Klíčovými metodami prevence proti kybernetickým útokům jsou neustálá osvěta a informovanost veřejnosti. Je důležité cílit na všechny věkové skupiny a využívat různé platformy pro šíření osvěty.

Budoucí trendy a výzvy: V oblasti kybernetické kriminality se očekává rostoucí role umělé inteligence, což představuje nové výzvy pro bezpečnostní síly. Příprava na tyto trendy vyžaduje inovace a adaptaci stávajících metod.

Důležitost osobní ochrany a zdrojů pomoci: Důležitá je opatrnost při online komunikaci a využívání dostupných zdrojů pro pomoc v případě stání se obětí kybernetického útoku.

6 NÁVRH NA ZLEPŠENÍ SITUACE

Z dotazníkového šetření je zřejmé, že kybernetické útoky si nevybírají mezi pohlavími a jejich terčem jsou jak muži, tak ženy, z mé osobní zkušenosti mohu říct, že ženy se stávají terčem kybernetických útoku častěji zato muži přicházejí o mnohem více peněz. Co se týče věkového rozložení tak celkem logicky nejčastějším terčem kybernetických útoků jsou lidé v produktivním věku, ale nejzranitelnější skupinou jsou lidé nad 60 let, kteří dospívali v zcela odlišné době, takto to skutečně je i v praxi, kdy lidé nad 60 let mají problém s rozpoznáním legitimnosti informací zveřejňovaných v kyberprostoru a jejich chybné rozhodnutí si často nepřipouštějí ani poté co se stali terčem kybernetického útoku. Jakmile lidé vlastní mobilní telefon anebo počítač, považují svou zkušenost s informačními technologiemi za základní, toto si dovolím tvrdit, že v dnešní době již dávno neplatí a pouhé užívání něčeho, čemu téměř nerozumím, ze mě nedělá zkušeného s informačními technologiemi, toto platí v podstatě i o informovanosti v oblasti kybernetické bezpečnosti, pouhé povědomí o existenci něčeho z nás nedělá informované, pokud neznáme konkrétní příklady či případy.

Z výsledků můžeme pozorovat, že slovo phishing nebo jak lidově slýcháme „fišing“ je téměř každému známé, ale jen pouze zlomek lidí dokáže pojem převést do reálného světa a definovat jeho význam či jak by takový phishing vlastně mohl vypadat. Za jako velice efektivní informační kampaň musím vyzdvihnout a je to i patrné z výsledků snahu bankovních institucí o osvětu svých klientů, kdy značnou měrou ba dokonce největší přispívají k povědomí veřejnosti o nebezpečnosti kybernetických útoků a vynalézavosti útočníků, tato snaha je očividně funkční a má velký dosah. Dvoufaktorová autentizace ve společnosti se silnými hesly se u široké veřejnosti ukazuje jako nejčastější ochranný mechanismus proti kybernetickým útokům, je to z velké části způsobeno povinností pro uživatele ze strany poskytovatelů dané služby, toto lze do budoucna považovat za krok právním směrem, nicméně z praxe je zřejmé, že toto nestačí a pokud oběti svým útočníkům tyto údaje předají tak se stávají neefektivními. Nejčastějším motivátorem kybernetických útočníků je finanční zisk, toto je patrné i z výsledků, kdy drtivá většina přijatých oznámení na Policii ČR od obětí kybernetických útoků obsahuje určitou ztrátu ať už finanční nebo citovou.

Jak výsledky ukazují, tak lidé ke zvyšování povědomí o kybernetické bezpečnosti považují za klíčové veřejné informační kampaně a integraci kybernetické bezpečnosti do školních osnov na všech úrovních studia v této částí práce se ve třech částech pokusím předložit rady

a návrhy, jak by se současná situace mohla zlepšit, a to zejména v integraci kybernetické bezpečnosti do školních osnov.

6.1 Obecné rady

V dnešní digitálně propojené době je ochrana proti kybernetickým útokům nezbytná nejen pro podniky, ale i pro jednotlivce. Přestože se technologie stále vyvíjí a poskytuje nové příležitosti pro osobní i profesní růst, s sebou přináší i nové hrozby v podobě kybernetických útoků, které mohou ohrozit naše osobní údaje, finanční zabezpečení, a dokonce i naši fyzickou bezpečnost. V následujících odstavcích poskytnu čtyři praktické rady, které může veřejnost využít ke zvýšení své odolnosti vůči těmto digitálním hrozbám. Tato doporučení jsou zaměřena na posílení základních aspektů kybernetické bezpečnosti a měla by sloužit jako základní průvodce pro každého, kdo chce chránit své digitální prostředí.

Používejte silná hesla a správce hesel: Každá osoba by měla používat silná, jedinečná hesla pro různé online účty. Doporučuje se kombinovat velká a malá písmena, číslice a speciální znaky. Uchovávání hesel v bezpečném správci hesel může pomoci spravovat tyto údaje bez rizika jejich zapomenutí.

Efektivita silných hesel je přímo závislá na naší schopnosti udržet je v soukromí a nevydávat je třetím stranám, bez ohledu na zdánlivou legitimnost jejich požadavků. Jakmile totiž sdělíme svá hesla jiným osobám, i když se zdá jejich žádost opodstatněná, oslabujeme tím jejich ochranný potenciál. Tím pádem se hesla stávají znehodnocenými a my efektivně eliminujeme jakoukoliv ochranu, kterou byla hesla designována poskytovat. Toto zásadní porušení bezpečnostních protokolů následně umožňuje útočníkům volný přístup k našim citlivým a cenným datům.

Používejte dvoufaktorovou autentizaci: Kdekoliv je to možné, měli byste aktivovat dvoufaktorovou autentizaci (2FA). Tato bezpečnostní vrstva vyžaduje druhý prvek ověření k přihlášení, což ztěžuje potenciálním útočníkům přístup k vašim účtům, i když se jim podaří získat vaše heslo.

Podobně jako se silnými hesly je to i s dvoufaktorovou autentizací, která představuje klíčovou vrstvu zabezpečení, významně zvyšující ochranu přístupu k účtům tím, že vyžaduje dvě nezávislé formy ověření identity uživatele. Tento bezpečnostní mechanismus však ztrácí svou účinnost, pokud dojde k sdílení autentizačních kódů s třetími stranami. Předání těchto kódů jakýmkoli způsobem vede k podstatnému oslabení zabezpečení, neboť umožňuje

útočníkům obejít obě úrovně ochrany a získat přístup k chráněným datům. Je tedy nezbytné, aby uživatelé chránili své autentizační kódy stejně pečlivě jako svá hesla.

Aktualizujte své software a operační systémy: Pravidelné aktualizace softwaru a operačních systémů zajistí, že vaše zařízení obsahuje nejnovější bezpečnostní opravy a ochranu proti známým hrozbám. Automatické nastavení aktualizací může pomoci udržet vaše systémy vždy aktuální.

Buďte obezřetní vůči phishingovým útokům: Vždy pečlivě kontrolujte emaily a odkazy před kliknutím na ně. Phishingové útoky často využívají zdánlivě legitimní emaily nebo zprávy k získání citlivých informací, jako jsou hesla nebo bankovní údaje. Naučte se rozpoznávat podezřelé znaky, jako jsou gramatické chyby, nesprávné adresy URL a nevyžádané žádosti o informace.

Výše uvedené rady byly konzultovány s nprap. Stanislavem Cholastou, kdy tento s radami souhlasí a v podstatě podobné myšlenky předává z pravidla podvedeným v kybernetických podvodech. Nicméně při konzultaci zdůraznil důležitost a užitečnost zálohování osobních dat. Z tohoto důvodu byla přidána ještě jedna a poslední rada:

Pravidelné zálohování dat: Pro zajištění ochrany osobních i pracovních dat před ztrátou způsobenou kybernetickými útoky, jako je ransomware, je nezbytné pravidelně zálohovat důležité soubory. Zálohy by měly být prováděny na více médiích, včetně externích pevných disků a cloudových úložišť. Doporučuje se zálohovat data v pravidelných intervalech, ideálně pomocí automatizovaného softwaru, který zjednoduší proces a minimalizuje riziko lidské chyby. Pro zvýšení bezpečnosti je důležité udržovat alespoň jednu zálohu oddělenou a izolovanou od hlavní sítě, aby byla ochráněna před síťovými útoky.

6.2 Aplikace intuitivního myšlení v praktickém rozhodování

Použití zdravého rozumu při ochraně proti kybernetickým útokům je klíčové. Zde je několik způsobů, jak mohou jednotlivci aplikovat zdravý rozum ve své kybernetické ochraně:

Nevěřte všemu, co vidíte nebo čtete: Kybernetičtí útočníci často používají sofistikované phishingové techniky, které mohou vypadat velmi přesvědčivě. Vždy důkladně ověřujte pravost emailů, zpráv a webových stránek před tím, než zadáte jakékoliv osobní údaje nebo stahujete soubory.

Zvažte rizika a důsledky: Před kliknutím na jakýkoliv odkaz nebo otevřením přílohy se zamyslete nad možnými důsledky. Neživte zvědavost na úkor bezpečnosti. Pokud něco

vypadá podezřele nebo příliš dobře, aby to byla pravda, pravděpodobně to tak je. Je zásadní, že pokud náš antivirový program identifikuje nějaký soubor nebo webovou stránku jako nebezpečnou, měli bychom tuto informaci považovat za důvěryhodnou. Pokud tedy dojde k varování od antivirového programu, existuje vysoká pravděpodobnost, že objekt skutečně představuje riziko. V případě, že někdo tvrdí opak, tedy že identifikovaná hrozba je ve skutečnosti bezpečná, je nezbytné pečlivě zvážit důvěryhodnost a odbornost této osoby nebo zdroje informací.

Mějte na paměti, že nikdo není imunní: Často lidé předpokládají, že jsou příliš malými, aby byli cílem kybernetických útoků. Tento přístup může vést k nedostatečné ochraně. Kybernetické hrozby jsou všudypřítomné a mohou zasáhnout každého. Dokonce lze předpokládat, že čím zranitelnější cíl je tím spíše se stane terčem kybernetického útoku.

Používejte technologie s rozvahou: Zvažte, jaké informace sdílíte online, a buďte opatrní, když používáte aplikace a služby, které mohou shromažďovat vaše data. Nastavení soukromí a bezpečnosti by mělo být přizpůsobeno tak, aby chránilo vaše informace, aniž by to omezilo vaši online aktivitu.

Aplikací těchto základních principů selského rozumu do vašeho každodenního digitálního života můžete významně snížit riziko stát se obětí kybernetického útoku a chránit svoje osobní a finanční informace.

6.3 Integrace kybernetické bezpečnosti do školních osnov

Je zcela zásadní zajistit, aby učitelé a vyučující byli pravidelně vzděláváni v oblasti kybernetické bezpečnosti. To je klíčové pro úspěšné začlenění této tematiky do školních osnov na všech úrovních vzdělávání. Pravidelné vzdělávání učitelů zajišťuje, že jsou aktuálně informováni o nejnovějších trendech, technologiích a hrozbách, což je umožňuje efektivně předávat tuto znalost studentům. Několik klíčových aspektů pro vzdělávání učitelů v kybernetické bezpečnosti zahrnuje:

- Profesionální rozvojové programy: Organizování pravidelných školení a workshopů, které učitelům poskytnou nejen teoretické znalosti, ale také praktické dovednosti v oblasti kybernetické bezpečnosti. To může zahrnovat jak základní, tak pokročilé kurzy zabezpečení, v závislosti na jejich předchozím vzdělání a potřebách.
- Přístup k aktuálním zdrojům: Učitelé by měli mít snadný přístup k nejnovějším zdrojům a materiálům, které mohou využít ve svých hodinách. To zahrnuje odborné

články, online kurzy, video tutoriály a další vzdělávací nástroje aktualizované s nejnovějšími informacemi o kybernetických hrozbách a ochranných strategiích.

- Síťování a komunitní spolupráce: Podpora vytváření profesních sítí mezi učiteli, kde mohou sdílet zkušenosti, učební strategie a osvědčené postupy. Tím se podporuje spolupráce a sdílení znalostí v oblasti kybernetické bezpečnosti.
- Certifikace a další kvalifikace: Nabídka možností pro učitele získat certifikáty a další kvalifikace v oblasti kybernetické bezpečnosti, což může pomoci zvýšit jejich kredibilitu a efektivitu při výuce této důležité oblasti.
- Zpětná vazba a hodnocení: Implementace systémů pro zpětnou vazbu, které učitelům umožní vyhodnotit účinnost své výuky a zjistit oblasti, které vyžadují další zlepšení nebo aktualizaci.

Vytvořením podpůrného a dynamického vzdělávacího prostředí pro učitele, kde se pravidelně setkávají s novými informacemi a metodami v oblasti kybernetické bezpečnosti, můžeme zlepšit celkovou efektivitu školního vzdělávacího programu a lépe připravit studenty na výzvy spojené s digitálním světem.

Poté by byla možná integrace kurikula kybernetické bezpečnosti do školních osnov na všech úrovních vzdělávání. Ta by měla být přizpůsobena věkovým skupinám a vzdělávacím potřebám, od základních škol až po vysoké školy. Tento přístup by zajišťoval, že každá věková skupina získává relevantní a praktické informace, které odpovídají jejich schopnostem a digitálnímu prostředí. Níže je navrženo, jak by mohl vypadat tento rozsáhlý vzdělávací program rozdělený podle úrovní vzdělání:

Základní školy

- Základní pojmy kybernetické bezpečnosti – vysvětlení základních pojmů jako jsou kyberprostor, internet, osobní údaje a hesla.
- Bezpečné chování na internetu – naučit děti rozpoznávat bezpečné a nebezpečné aktivity online, včetně bezpečného používání sociálních médií a her.
- Základy ochrany osobních údajů – učení o důležitosti ochrany osobních informací a jak správně nakládat s hesly.

Střední školy

- Rozpoznání a reakce na kybernetické hrozby – detailní vysvětlení běžných kybernetických hrozeb jako je phishing, malware a sociální inženýrství.
- Praktická bezpečnostní opatření – poučení o využívání antivirového softwaru, firewallu, dvoufaktorové autentizace a bezpečných online návyků.
- Etické a právní aspekty kybernetické bezpečnosti – diskuse o etice v kyberprostoru, přehled základních právních rámců ochrany dat.

Vysoké školy a univerzity

- Pokročilé strategie kybernetické ochrany – výuka o šifrování, síťové bezpečnosti, pokročilých bezpečnostních protokolech a strategiích ochrany proti kybernetickým útokům.
- Simulace a studie případů – použití simulačních nástrojů a analýza reálných případových studií pro hlubší pochopení kybernetických útoků a ochranných taktik.
- Formulace kybernetických strategií a řízení rizik – kurzy navržené k tvorbě a zavádění účinných strategií pro kybernetickou bezpečnost a metod pro efektivní řízení rizik v digitálním prostředí.

Metodika začlenění a výuky

- Adaptace obsahu na věkovou úroveň – ujistěte se, že výukový materiál je přizpůsoben schopnostem a pochopení každé věkové skupiny.
- Interaktivní a praktické učení – zahrnutí aktivit, které podporují aktivní učení, jako jsou kvízy, interaktivní hry a projektové práce zaměřené na kybernetickou bezpečnost.
- Spolupráce s odborníky a průmyslem – pravidelné zapojení externích odborníků a organizování workshopů a seminářů vedených praktiky z oboru.
- Průběžná aktualizace kurikula – udržování aktuálnosti vzdělávacích materiálů v reakci na neustále se měnící kybernetické prostředí a hrozby.

Tento přístup k integraci kybernetické bezpečnosti do školních osnov na všech úrovních vzdělávání zajišťuje, že studenti jsou vybaveni potřebnými znalostmi a dovednostmi k ochraně sebe a svého digitálního prostředí před kybernetickými hrozbami.

6.4 Kurz pro veřejnost

V dnešní digitálně propojené době je pochopení a aplikace základů kybernetické bezpečnosti klíčové pro každého jednotlivce i organizaci. Tento dvoudenní kurz byl designován tak, aby účastníkům byl poskytnut komplexní přehled o nejčastějších kybernetických hrozbách a způsobech, jak se proti nim účinně bránit. Kurz kombinuje teoretické vzdělávání s praktickými aktivitami a je vhodný pro široké spektrum účastníků, od běžných uživatelů internetu po IT profesionály.

Cíle kurzu

Účastníkům bude přiblíženo, jak rozpoznat běžné typy kybernetických útoků a jejich projevy. Bude demonstrována aplikace praktických technik pro zabezpečení osobních a firemních zařízení. Dále bude vysvětleno, jak vytvářet a udržovat bezpečné síťové prostředí a jak efektivně reagovat na kybernetické incidenty a minimalizovat jejich dopady.

Struktura kurzu

Den 1.: Základy kybernetické bezpečnosti a prevence útoků

Během prvního dne by se účastníci měli naučit základní pojmy a principy kybernetické bezpečnosti. Toto zahrnuje porozumění nejčastějším hrozbám jako jsou malware, phishing a ransomware. Budou se věnovat analýze reálných případů kybernetických útoků a naučí se rozpoznávat potenciální hrozby. Dále se zaměří na zabezpečení osobních zařízení, kde se naučí, jak správně konfigurovat operační systémy a aplikace pro maximální bezpečnost. Naučí se také vytvářet a spravovat silná hesla pomocí správců hesel.

Sekce 1.: Úvod do kybernetické bezpečnosti

- Představeny budou základní pojmy kybernetické bezpečnosti, včetně vysvětlení termínů jako malware, phishing, ransomware.
- Analýza reálných případových studií kybernetických útoků.

Sekce 2.: Zabezpečení osobních zařízení a hesel

- Budou prezentovány metody pro zabezpečení operačních systémů (Windows, macOS, Linux) a mobilních zařízen. Bude zdůrazněna důležitost silných hesel a použití správců hesel.
- Nastavení správce hesel a demonstrace vytváření silných hesel budou účastníkům ukázány.

Sekce 3: Identifikace a prevence phishingových útoků

- Jak rozpoznat pokusy o phishing a sociální inženýrství.
- Účastníci dostanou příklady emailů a zpráv a pokusí se identifikovat znaky phishingu v interaktivní simulaci.

Den 2: Obranné strategie a reakce na incidenty

Druhý den kurzu se bude věnovat pokročilým obranným strategiím a reakcím na kybernetické incidenty. Účastníci se dozví, jak zabezpečit domácí a firemní sítě, včetně nastavení firewallů a bezpečnostních konfigurací Wi-Fi. Budou prakticky pracovat s antivirovým softwarem a naučí se, jak detekovat a eliminovat malware. Závěrečná část bude věnována plánování reakcí na incidenty, kde se účastníci naučí vytvářet efektivní komunikační a reakční plány pro různé typy kybernetických útoků. Tento den bude završen simulací reálného kybernetického útoku, kde účastníci aplikují své nově získané dovednosti v praxi.

Sekce 4.: Zabezpečení domácích a firemních sítí

- Budou objasněny základy síťového zabezpečení, význam firewallů, bezpečnostní nastavení Wi-Fi sítí.
- Bude nastavena zabezpečená domácí síťová konfigurace a bude demonstrováno použití síťových monitorovacích nástrojů.

Sekce 5.: Ochrana proti malwaru a ransomware

- Prevence proti malwaru, nástroje a strategie pro detekci a eliminaci malwaru.
- Ukázka instalace a konfigurace antivirového software, analýza a čištění infikovaného systém.

Sekce 6.: Reakce na kybernetické incidenty

- Jak vytvořit a implementovat plán reakce na incidenty, komunikace během a po incidentu.
- Simulace reakce na kybernetický útok, včetně komunikace s podporou a právními službami, bude provedena ve formě role-play.

Metody výuky

Přednášky budou poskytovány zkušenými odborníky a praktiky v oblasti kybernetické bezpečnosti. Budou použity simulace útoků a reakce na ně v kontrolovaném prostředí pro testování schopností účastníků reagovat na reálné hrozby.

Spolupráce s odborníky

V rámci dalšího rozvoje a zajištění kvality navrhovaného kurzu by bylo vhodné zvážit spolupráci s Národním úřadem pro kybernetickou a informační bezpečnost. Tato instituce může poskytnout odborné znalosti, aktuální informace o hrozbách a osvědčené postupy, které by kurzu dodaly na důvěryhodnosti a relevanci. Spolupráce by mohla zahrnovat řadu prvků, které by kurzu přidaly hodnotu. Například specialisté z Národního úřadu by mohli přispět svými odbornými znalostmi v rámci jednotlivých modulů kurzu prostřednictvím expertních přednášek. Dále by kurz mohl využívat nejnovější studie a reporty vydané úřadem, což by zajistilo, že vzdělávací obsah bude vždy aktuální a v souladu s nejnovějšími trendy a doporučeními v oblasti kybernetické bezpečnosti. Úřad by také mohl poskytnout přístup k simulovaným prostředím nebo reálným scénářům útoků, což by účastníkům umožnilo prakticky si vyzkoušet své dovednosti v bezpečném a kontrolovaném prostředí.

Výstup kurzu

Účastníci obdrží certifikát o absolvování kurzu, který potvrzuje získané dovednosti v oblasti obrany proti kybernetickým útokům.

ZÁVĚR

Tato bakalářská práce byla zaměřena na posouzení odolnosti jednotlivců proti kybernetickým útokům a na identifikaci jejich slabých míst v oblasti kybernetické bezpečnosti. Hlavním cílem bylo poskytnout ucelený pohled na aktuální stav kybernetické odolnosti v českém kontextu a na základě zjištění navrhnout efektivní strategie pro jejich zlepšení.

Práce kombinovala teoretické poznatky s praktickým výzkumem, včetně dotazníkového šetření a rozhovoru s odborníkem z praxe. Výsledky dotazníkového šetření odhalily, že i když má většina respondentů základní povědomí o kybernetických hrozbách, jejich schopnost efektivně reagovat na tyto hrozby je omezená kvůli nedostatku specifických znalostí a dovedností.

Jedním z klíčových zjištění je, že existuje výrazný rozdíl mezi vnímáním bezpečnostních rizik a skutečnými schopnostmi jednotlivců ochránit se. Toto zjištění podtrhuje potřebu zintenzivnění osvětových kampaní a školení zaměřených na praktické aspekty kybernetické bezpečnosti. Zlepšení vzdělávání v oblasti kybernetické bezpečnosti by mělo být realizováno prostřednictvím školních programů a veřejných iniciativ, které by měly být podporovány jak státními, tak soukromými institucemi.

V souladu s cíli práce byly navrženy návrhy na zlepšení aktuální situace, a to formou několika rad pro zvýšení kybernetické odolnosti osob, nástinem integrace kybernetické bezpečnosti do školních osnov, a to na všech stupních vzdělávání a vytvořením kurzu pro veřejnost. Závěr práce také vyzývá k lepší spolupráci mezi veřejným a soukromým sektorem v boji proti kybernetickým hrozbám a zdůrazňuje potřebu kontinuálního vývoje technologií a metod pro detekci a ochranu proti kybernetickým útokům.

Výzkum podtrhl, že navzdory existujícím opatřením zůstává kybernetická bezpečnost velkou výzvou, která vyžaduje nejen technologická, ale také sociální a vzdělávací opatření. Závěry práce poskytují strategický základ pro budoucí akce v této oblasti a navrhují směry pro další výzkum, který by mohl prohloubit pochopení této problematiky a přispět k jejímu efektivnějšímu řešení.

Práce tak přináší významný přínos do diskuse o kybernetické bezpečnosti, nabízí konkrétní návrhy pro zlepšení a posiluje povědomí o důležitosti proaktivního přístupu k ochraně digitálního prostředí, čímž naplňuje stanovené cíle.

SEZNAM POUŽITÉ LITERATURY

AQSA, Amir, 2024. *What are IOT attacks?* In: Educative [online]. [cit. 2024-03-19]. Dostupné z: https://www.educative.io/answers/what-are-iot-attacks

ARMY TRAINING AND DOCTRINE COMMAND a THE UNITED STATES ARMY, 2016. *Cyberspace Operations Concept Capability Plan 2016-2028*. 1. CreateSpace Independent Publishing Platform. ISBN 9781530413928.

AUGENBAUM, Scott E, 2019. *The Secret to Cybersecurity: A Simple Plan to Protect Your Family and Business from Cybercrime.* Nashville (Tennessee): Forefront Books. ISBN 978-19-4867-708-0.

ČESKÁ BANKOVNÍ ASOCIACE, 2024. *Češi a kyberbezpečnost 2024.* In: Česká bankovní asociace [online]. [cit. 2024-04-22]. Dostupné z: https://cbaonline.cz/cesi-a-kyberbezpecnost-2024

ČESKO, 2009. *Zákon č. 40/2009 Sb. Zákon trestní zákoník.* Online. In: Zákony pro lidi. AION CS, © 2010-2024. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40 [cit. 2024-03-12].

ČESKO, 2012. *Zákon č. 89/2012 Sb. Zákon občanský zákoník.* Online. In: Zákony pro lidi. AION CS, © 2010-2024. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181 [cit. 2024-03-11].

ČESKO, 2014. Zákon č. 181/2014 Sb. *Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).* Online. In: Zákony pro lidi. AION CS, © 2010-2024. Dostupné z: https://www.zakonyprolidi.cz/cs/2012-89 [cit. 2024-03-11].

Co je to kyberútok?, c2008-2024. In: It-slovník [online]. [cit. 2024-04-22]. Dostupné z: https://it-slovnik.cz/pojem/kyberutok

Cyberspace, c2023. In: Oxford English Dictionary [online]. [cit. 2024-04-22]. Dostupné z: https://www.oed.com/search/dictionary/?scope=Entries&q=cyberspace&tl=true

DANSIMP, 2024. *Supply chain attacks.* In: Microsoft [online]. [cit. 2024-03-19]. Dostupné z: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/malware/supply-chain-malware?view=o365-worldwide

DIZDAR, Admir, 2023. *What Is DNS Tunneling and How to Detect and Prevent Attacks.* In: Brightsec [online]. [cit. 2024-03-19]. Dostupné z: https://brightsec.com/blog/dns-tunneling/

GRIMES, Roger A., 2024. *Fighting Phishing.* 1. Wiley. ISBN 9781394249213.

Internet. In: Pravidla [online]. [cit. 2024-04-22]. Dostupné z: https://www.pravidla.cz/hledej/?qr=Internet

KOLOUCH, Jan, 2016. *CyberCrime.* Praha: CZ.NIC, z.s.p.o. CZ.NIC. ISBN 978-80-88168-15-7.

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

LENAERTS-BERGMANS, Bart, 2022. *WHAT IS A SPOOFING ATTACK?* In: Crowdstrike [online]. [cit. 2024-03-19]. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/spoofing-attacks/

LUTKEVICH, Ben, 2022. *Malware.* In: TechTarget [online]. [cit. 2024-03-19]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/malware

MONNAPPA K A, 2018. *Learning Malware Analysis.* 1. Packt Publishing. ISBN 9781788397520.

NEJVYŠŠÍ STÁTNÍ ZASTUPITELSTVÍ, 2023. *Zpráva o činnosti státního zastupitelství za rok 2022.* In: STÁTNÍ ZASTUPITELSTVÍ [online]. [cit. 2024-04-22]. Dostupné z: https://verejnazaloba.cz/wp-content/uploads/2023/06/Zpr%C3%A1va-o-%C4%8Dinnosti-2022-_textov%C3%A1-%C4%8D%C3%A1st.pdf

PIDRMNAOVÁ, Zuzana, 2022. *ZPRAVODAJSTVÍ 2022: #nePINdej!.* In: Policie České republiky [online]. [cit. 2024-04-22]. Dostupné z: https://www.policie.cz/clanek/nepindej.aspx

PLOTKIN, Robert, 2020. *Privacy, Security, and Cyberspace, Revised Edition.* 1. Chelsea House. ISBN 9781438182728.

POLICIE ČESKÉ REPUBLIKY, 2024. *Internetový podvod* [počítačový program]. 1.

RYAN, Johnny, 2010. *A History of the Internet and the Digital Future.* Reaktion Books. ISBN 978-18-6189-835-7.

SEDLÁK, Petr a Martin KONEČNÝ, 2021. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* 1. Brno: CERM, akademické nakladatelství. ISBN 978-80-7623-068-2.

SEEL, Peter B., 2022. *Digital Universe.* 2. Wiley-Blackwell. ISBN 9781119630975.

SMEJKAL, Vladimír, 2015. *Kybernetická kriminalita.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. Pro praxi. ISBN 978-807-3805-012.

THE INVESTOPEDIA TEAM, 2023. *Denial-of-Service (DoS) Attack: Examples and Common Targets.* In: Investopedia [online]. [cit. 2024-03-19]. Dostupné z: https://www.investopedia.com/terms/d/denial-service-attack-dos.asp

ZHONG, Weilin a REZOS, 2024. *Code Injection.* In: Owasp [online]. [cit. 2024-03-19]. Dostupné z: https://owasp.org/www-community/attacks/Code_Injection

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

DDoS	Distributed Denial-of-Service
DoS	Denial-of-Service
IoT	Internet of Things
Sb	Sbírky
SMS	Short Message Service
URL	Uniform Resource Locator
VoIP	Voice over IP
WWW	World Wide Web

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: DOTAZNÍK

Odolnost osob vůči kybernetickým útokům

Tento formulář je navržen s cílem shromáždit důležité informace o odolnosti osob vůči kybernetickým útokům. Jeho struktura zahrnuje několik klíčových sekcí, které nám umožňují porozumět, jak dobře jsou jednotlivci informováni o kybernetických hrozbách, jaké preventivní opatření proti nim podnikají, a jaké zkušenosti mají s případnými útoky, které je již postihly. Zaměřujeme se na základní informace o respondentech, jejich povědomí o kybernetické bezpečnosti, preventivních opatření, která implementují, a jejich zkušenosti s kybernetickými útoky, včetně způsobených škod a reakcí na tyto útoky.

* Označuje povinnou otázku

1. **Pohlaví** *

Označte jen jednu elipsu.

- ◯ Muž
- ◯ Žena

2. **Věk** *

Označte jen jednu elipsu.

- ◯ 19 let a méně
- ◯ 20 let až 29 let
- ◯ 30 let až 39 let
- ◯ 40 let až 49 let
- ◯ 50 let až 59 let
- ◯ 60 let a více

Obrázek 14 Otázky dotazníku 1 až 2 (zdroj: vlastní)

3. **Nejvyšší dosažené vzdělání** *

Označte jen jednu elipsu.

- ◯ Základní vzdělání
- ◯ Střední vzdělání s výučním listem
- ◯ Střední vzdělání s maturitní zkouškou
- ◯ Vyšší odborné vzdělání
- ◯ Vysokoškolské vzdělání - bakalářský stupeň
- ◯ Vysokoškolské vzdělání - magisterský stupeň
- ◯ Vysokoškolské vzdělání - doktorský stupeň
- ◯ Jiné: _____

4. **Zkušenosti s informačními technologiemi** *

Označte jen jednu elipsu.

- ◯ Žádná
- ◯ Základní
- ◯ Pokročilá
- ◯ Expert

Povědomí o kybernetické bezpečnosti

V sekci o povědomí o kybernetické bezpečnosti se zaměřujeme na zjištění, jak dobře jsou respondenti informováni o kybernetických hrozbách a jaké zdroje informací využívají k rozšíření svých znalostí v této oblasti. Cílem je odhalit úroveň povědomí o různých typech kybernetických útoků a pochopit, jak aktivně lidé vyhledávají informace, které by jim pomohly lépe chránit svá data a soukromí online. Tyto informace nám poskytnou přehled o tom, jak efektivně mohou být jednotlivci připraveni čelit kybernetickým hrozbám a jaké vzdělávací programy nebo zdroje by mohly být pro veřejnost nejužitečnější.

Obrázek 15 Otázky dotazníku 3 až 4 (zdroj: vlastní)

5. **Považujete se za informovaného v oblasti kybernetické bezpečnosti?** *

Označte jen jednu elipsu.

- ◯ Ano
- ◯ Částečně
- ◯ Ne

6. **Jaké typy kybernetických útoků znáte?** (Možnost výběru více odpovědí) *

Zaškrtněte všechny platné možnosti.

- ☐ Phishing
- ☐ Malware
- ☐ Ransomware
- ☐ Social Engineering
- ☐ Spoofing
- ☐ Denial-of-Service (DoS)
- ☐ Žádné
- ☐ Jiné: _____

7. **Z jakých zdrojů čerpáte informace o kybernetické bezpečnosti?** (Možnost výběru více odpovědí) *

Zaškrtněte všechny platné možnosti.

- ☐ Články na internetu
- ☐ Knihy
- ☐ Kurzy
- ☐ Sociální sítě
- ☐ Média
- ☐ Bankovní instituce
- ☐ Žádných
- ☐ Jiné: _____

Obrázek 16 Otázky dotazníku 5 až 7 (zdroj: vlastní)

Kybernetický útok

V sekci o kybernetickém útoku se soustředíme na zkušenosti respondentů s konkrétními incidenty, způsobené škody a reakce na tyto události. Cílem je získat hlubší pochopení skutečných dopadů kybernetických útoků na jednotlivce, ať už se jedná o ztrátu dat, finanční ztráty, nebo poškození systémů. Otázky jsou navrženy tak, aby odhalily, jak respondenti identifikovali útok, jaké kroky podnikli k řešení situace a jaký dopad měl incident na jejich osobní nebo profesní život. Tato sekce poskytuje klíčové informace pro pochopení, jak jsou lidé vybaveni (nebo nevybaveni) k řešení kybernetických hrozeb a jaké jsou nejčastější slabiny v jejich obraně proti kybernetickým útokům.

8. **Jaká preventivní opatření proti kybernetickým útokům používáte?** (Možnost výběru více odpovědí) *

Zaškrtněte všechny platné možnosti.

- [ ] Antivirový software
- [ ] Dvoufaktorová autentizace
- [ ] Pravidelné aktualizace softwaru
- [ ] Silná hesla
- [ ] Vzdělávání v oblasti kybernetické bezpečnosti
- [ ] Pravidelná záloha dat
- [ ] Jiné: _____

9. **Jak jste reagovali, když jste se stali cílem kybernetického útoku?** (Možnost výběru více odpovědí) *

Zaškrtněte všechny platné možnosti.

- [ ] Kontaktování IT specialisty
- [ ] Změna hesel
- [ ] Informování poskytovatele služby
- [ ] Nahlášení útoku příslušným orgánům
- [ ] Kontaktování rodiny
- [ ] Jiné: _____

Obrázek 17 Otázky dotazníku 8 až 9 (zdroj: vlastní)

10. **Na jaký typ Vašich osobních nebo pracovních dat nebo systémů zaútočil kybernetický útočník?** (Možnost výběru více odpovědí) *

Zaškrtněte všechny platné možnosti.

- [ ] Osobní e-mail
- [ ] Pracovní e-mail
- [ ] Sociální sítě
- [ ] Bankovní účty nebo finanční služby
- [ ] Osobní zařízení (např. počítač, smartphone)
- [ ] Pracovní zařízení nebo sítě
- [ ] Webové stránky nebo aplikace, které spravuji
- [ ] Účty spojené s online nakupováním
- [ ] Cloudové úložiště nebo služby
- [ ] Jiné: _____

11. **Jakou škodu či újmu Vám způsobil kybernetický útok?** (Možnost výběru více odpovědí) *

Zaškrtněte všechny platné možnosti.

- [ ] Ztráta osobních dat
- [ ] Ztráta pracovních nebo obchodních dat
- [ ] Finanční ztráta
- [ ] Nákaza malwarem nebo ransomwarem, která vyžadovala čištění nebo obnovu systému
- [ ] Porušení bezpečnosti pracovní sítě nebo systémů
- [ ] Ztráta přístupu k online účtům (např. sociální sítě, e-mail, bankovní účty)
- [ ] Poškození reputace nebo ztráta důvěry zákazníků/klientů
- [ ] Nucená doba offline nebo výpadek služby
- [ ] Jiné: _____

Obrázek 18 Otázky dotazníku 10 až 11 (zdroj: vlastní)

12. Jaká z následujících možností by podle Vás nejvíce pomohla zvýšit odolnost osob vůči kybernetickým útokům? (Zvolte jednu odpověď) *

Označte jen jednu elipsu.

- ◯ Rozvoj a integrace kurikul o kybernetické bezpečnosti do školních osnov na všech úrovních vzdělávání
- ◯ Organizování pravidelných workshopů a školení o kybernetické bezpečnosti pro veřejnost
- ◯ Poskytování online kurzů a zdrojů zdarma pro samostudium kybernetické bezpečnosti
- ◯ Spuštění veřejných informačních kampaní zaměřených na zvyšování povědomí o kybernetických hrozbách
- ◯ Vytváření a distribuce interaktivních vzdělávacích materiálů a her zaměřených na kybernetickou bezpečnost
- ◯ Podpora výzkumu a vývoje v oblasti vzdělávacích nástrojů pro kybernetickou bezpečnost

Obrázek 19 Otázka dotazníku 12 (zdroj: vlastní)

PŘÍLOHA P II: DOTAZNÍKOVÁ DATA SOUBOR .XLSX

Z důvodu obsáhlosti souboru byl soubor přiložen pouze v elektronické podobě ve formátu xlsx pod názvem Dotazníkové_šetření_data + grafy.xlsx.