VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

PROBLEMATIKA KYBERNETICKÝCH ÚTOKŮ Z POHLEDU STUDENTŮ STŘEDNÍ POLYTECHNICKÉ ŠKOLY V ČESKÝCH BUDĚJOVICÍCH

Autor práce: Marek Šmucr

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: RNDr. Růžena Ferebauerová

Katedra: Katedra právních oborů a bezpečnostních studií

2024

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 6, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Marek Šmucr

Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: České Budějovice

Název bakalářské práce: Problematika kybernetických útoků z pohledu studentů Střední polytechnické školy v Českých Budějovicích

Název bakalářské práce v anglickém jazyce: Problematics of Cyber Attacks from the Perspective of Polytechnic High School's Students in Czech Budweis

Katedra: Katedra právních oborů a bezpečnostních studií

Vedoucí bakalářské práce (jméno a příjmení, včetně titulů):

RNDr. Růžena Ferebauerová

Datum zadání bakalářské práce (měsíc, rok): duben 2023

Cíl bakalářské práce:

Hlavním cílem bakalářské práce je zjistit, jaké mají studenti zkušenosti s kybernetickými útoky, identifikovat nejčastější formy těchto útoků a navrhnout opatření umožňující bezpečnější chování mladistvých na internetu.

Vedlejším cílem je analyzovat současný stav a trendy vývoje kybernetických útoků oproti minulosti, a vyhodnotit proč meziročně v České republice přibývá o 20 % více kybernetických útoků.

Student: Marek Šmucr	3.5.2023 *datum*	 *podpis*
Vedoucí práce: RNDr. Růžena Ferebauerová	3.5.23 *datum*	 *podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	22.5.2023 *datum*	 *podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	23.5.2023 *datum*	 *podpis*
Rektor: doc. Ing. Jiří Dušek, Ph.D.	23.5.2023 *datum*	 *podpis*

Prohlašuji, že jsem bakalářskou práci vypracoval(a) samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí(ho) a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucí bakalářské práce RNDr. Růženě Ferebauerové za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

ŠMUCR, M. Problematika kybernetických útoků z pohledu studentů Střední polytechnické školy v Českých Budějovicích: bakalářská práce. České Budějovice: Vysoká škola evropských a regionálních studií, 2024. 71 s. Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová

Klíčová slova: kybernetické útoky, kybernetická bezpečnost, kyberprostor, prevence, střední škola

Bakalářská práce se zabývá problematikou kybernetických útoků zaměřených na dospívající mládež, konkrétně na studenty Střední školy polytechnické v Českých Budějovicích. V první části bakalářské práce jsou vysvětleny klíčové pojmy v oblasti kybernetických útoků. Dále práce poskytuje ucelený přehled preventivních opatření, která mohou být možným zdrojem pomoci pro oběti, ať už se jedná o online platformy, či osobní kontakt. Součástí práce je i trestněprávní legislativa týkající se kybernetických útoků. V praktické části práce jsou prezentovány výsledky dotazníkového šetření, jež si kladlo za cíl získat názory a postoje studentů Střední polytechnické školy v Českých Budějovicích na tuto problematiku.

ABSTRACT

ŠMUCR, M. The Issue of Cyber Attacks from the Perspective of Students of the Secondary Polytechnic School in České Budějovice: bachelor thesis. České Budějovice: University of European and Regional Studies, 2024. 71 s. Bachelor thesis supervisor: RNDr. Růžena Ferebauerová

Key words: cyber attacks, cyber security, cyberspace, prevention, secondary school

The bachelor thesis deals with the issue of cyber attacks that target our teenagers, specifically the students of the Secondary Polytechnic School in České Budějovice. In the first part of the bachelor thesis, the key terms associated with cyber attacks are explained. Furthermore, the work offers a comprehensive overview of preventive measures in relation to possible sources of help for victims, whether through online platforms or the personal contact. The work also includes criminal legislation that is connected with cyber attacks. The practical part of the work presents the results of a questionnaire survey, the aim of which was to obtain the opinions and attitudes of the students of the Secondary Polytechnic School in České Budějovice on this issue.

Obsah

Úvod

Informační a komunikační technologie jsou dnes již běžnou součástí našich životů. Téměř každá domácnost v České republice má přístup k internetu a většina z nás vlastní nějaké elektronické zařízení, skrze nějž je možné vstoupit do kybernetického světa. Tato obrovská počítačová síť, známá jako internet, poskytuje prostor pro množství činností, z nichž mnohé jsou nezákonné a spadají pod pojem kyberkriminalita. Děti a dospělí vyrůstající v současné době žijí obklopeni těmito technologiemi. Přesun kriminality z reálného světa do virtuálního prostředí navíc urychlilo i onemocnění covid-19. Šíření tohoto viru způsobilo v roce 2020 globální pandemii.

Dnešní doba nám umožňuje ovládat základní prvky IT jediným kliknutím či stiskem tlačítka. Zatímco tak můžeme odeslat zprávu či například potvrdit nákup, stejně jednoduše se můžeme dostat do kontaktu s podvodníkem, pedofilem či nebezpečným programem, který získá neoprávněný přístup k naším údajům. Problematika počítačové kriminality se v posledních letech stala jedním z nejdiskutovanějších témat ovlivňujících naši společnost. Pachatelé spoléhají na to, že jejich činy mohou být uskutečněny prakticky anonymně a z jakéhokoli koutu světa, bez nutnosti fyzické přítomnosti.

Od roku 2011 sleduje Policie České republiky trestné činy v kyberprostoru. Z nejnovějších statistik, zveřejněných k 13. 1. 2023, vyplývá, že v roce 2011 bylo evidováno celkem 1 502 skutků, zatímco v roce 2022 jejich počet stoupl na alarmujících 18 554, což představuje meziroční nárůst o více než 94,9 %.

Zvláště znepokojivé je, že mladí lidé tráví velký podíl svého volného času na sociálních sítích, jež se pro ně staly přirozeným prostředím pro interakci a komunikaci. Toto prostředí však může být i velmi nebezpečné, zejména pro děti a mladistvé, kteří mohou být nezkušení, důvěřiví, a proto náchylnější ke kybernetickým útokům. V posledních letech dochází k nárůstu těchto útoků prostřednictvím sociálních sítí, které často vedou i k finančním újmám. Z pozice příslušníka Policie České republiky je zřejmé, že kyberkriminalita je stále na vzestupu, proto se jedná o mimořádně aktuální téma, jež si zaslouží zvýšenou pozornost.

1 Cíl a metodika bakalářské práce

V první kapitole bakalářské práce jsou představeny cíle a zvolená metodika. Hlavním cílem práce je zjistit, jaké zkušenosti mají středoškolští studenti s kybernetickými útoky, identifikovat nejčastější formy těchto útoků a navrhnout opatření umožňující bezpečnější chování mladistvých na internetu. Vedlejším cílem práce je analyzovat současný stav a trendy vývoje kybernetických útoků oproti minulým letům a vyhodnotit, proč meziročně v České republice přibývá 20 % kybernetických útoků.

Teoreticko-metodická část vychází z rešerše aktuálních pramenů a témat týkajících se kybernetické bezpečnosti. Autor dále využívá své profesní a praktické zkušenosti jako příslušník Policie České republiky, neboť při výkonu svého zaměstnání stále častěji zaznamenává, že se mladiství stávají oběťmi kybernetických útoků vedoucích k finančním ztrátám.

Součástí empirické části je dotazníkové šetření, jež si klade za cíl prověřit znalosti studentů v oblasti kybernetických útoků. Pro tyto účely byla zvolena kvantitativní výzkumná metoda dotazníkového šetření. Tato metoda nabízí několik výhod, zejména možnost oslovit větší počet respondentů a následně zobecnit výsledky na širší veřejnost.

Před samotným rozdáním dotazníků vybraným respondentům byla prověřena srozumitelnost a funkčnost dotazníku na menším vzorku respondentů, kteří poté nebyli zahrnuti do hlavního výzkumného souboru.

Před distribucí dotazníků byli respondenti informováni o účelu šetření a o tom, že poskytnuté údaje budou využity pouze pro účely této bakalářské práce. Struktura dotazníku byla navržena na základě dvou předem definovaných hypotéz:

H1: Studenti na Střední polytechnické škole v Českých Budějovicích mají vysokou úroveň znalosti o kybernetických útocích a jsou obeznámeni se všemi riziky spojenými s kyberprostorem.

H2: Škola se snaží o rizicích, která jsou spojená s užíváním internetu, své studenty co nejvíce informovat.

Po nashromáždění dat z dotazníků bude provedena jejich analýza a výsledky budou následně prezentovány ve formě grafů a tabulek. Tyto výsledky budou sloužit jako základ pro další diskuzi a závěry této bakalářské práce.

2 Vymezení základních pojmů

Pro jasnější pochopení problematiky kybernetických útoků je klíčové nejprve objasnit několik základních pojmů spojených s touto oblastí. Mezi tyto důležité pojmy patří počítačový systém, kybernetický prostor, internet a kybernetická kriminalita.

2.1 Počítačový systém

Počítač je komplexní technický systém skládající se z hardwaru (fyzických komponentů, jako jsou procesory, paměť, periferie) a softwaru (programů a operačního systému), který umožňuje zpracovávání dat, provádění výpočtů a vykonávání úloh podle instrukcí uživatele. Počítačový systém může být samostatnou funkční jednotkou (pracující samostatně, např. osobní počítač, notebook, smartphone aj.), nebo může jít o soubor několika vzájemně propojených počítačových systémů (např. počítačová síť).[1]

2.2 Kybernetický prostor

Pro pojem kybernetický prostor (často označovaný také jako kyberprostor nebo anglicky cyberspace) existuje mnoho různých interpretací. V zásadě by se dalo říci, že se jedná o virtuální sféru, v níž probíhají kybernetické aktivity a interakce uživatelů oddělené od reálného světa. Definic virtuálního prostoru je mnoho. Kybernetický prostor je dle zákona o kybernetické bezpečnosti definován jako *„digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy a službami a sítěmi elektronických komunikací.“*[2]

Podle Koloucha *„kyberprostor představuje ono pomyslné pískoviště, na kterém se pohybujeme, ale zároveň se jedná o klíčový prvek v definici kybernetické kriminality. Aby bylo možné definovat kyberprostor, je nezbytně nutné vymezit pojem internet, který právě s kyberprostorem bezprostředně souvisí.“*[3]

Na základě dostupných definic je možné konstatovat, že kybernetický prostor nemá pevný začátek ani konec a tvoří ho samy informační a komunikační technologie. Uživatelé se zde mezi sebou dorozumívají, sdělují si informace, vzdělávají se nebo hrají hry. Toto vše je možné díky globálně propojené síti nazývané internet. Kybernetický prostor, jako ostatně vše, má své klady i zápory, jakými jsou např. nelegální aktivity páchané v různých směrech.

[1] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 57–58.
[2] ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In Sbírka zákonů, Česká republika. 2014, částka 75.
[3] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 42.

2.3 Internet

Internet představuje jeden z nejvýznamnějších vynálezů současnosti, který ovlivnil každodenní život lidí po celém světě. Bez internetu by kyberprostor nemohl fungovat. I když přesná definice internetu není jednoznačná, můžeme si ho představit jako globální síť spojující miliony počítačů a zařízení a umožňující komunikaci, sdílení informací a poskytování různých služeb.

Smejkal uvádí: *„Internet je soustavou sítí a podsítí, serverů, různých forem datových komunikací a k nim připojených počítačů; organizačně jsou to provozovatelé jednotlivých sítí a podsítí, případně propojovacích bodů (peeringových center), poskytovatelé připojení (Internet provideři), poskytovatelé služeb a obsahu (service a content providers), uživatelé apod.“*[4]

Lapáček uvádí, že „*internet je cosi, kam když připojíte svůj počítač, stanou se pro něj a tedy i pro vás dostupnými úplně všechny počítače připojené jako ten váš. Můžete tedy například vést debatu s lidmi po celém světě – a vůbec není důležité, kde zrovna jsou, jaký mají počítač a jestli je u nich zrovna den nebo noc.“*[5]

Fungování internetu lze přirovnat k síti skládající se z mnoha menších sítí spojených protokoly IP (Internet Protocol). Toto propojení umožňuje přenos dat, komunikaci a poskytování služeb mezi různými subjekty na celém světě. Klíčovou roli v této síti hrají poskytovatelé internetových služeb (ISP), jejichž úkolem je zajistit konektivitu mezi jednotlivými uzly sítě a umožnit tak spojení a komunikaci. Internet se skládá z komplexního ekosystému, který zahrnuje routery, servery, datová centra a mnoho dalších prvků. Ty společně tvoří síť umožňující lidem a zařízením přistupovat k informacím a službám online. Jelikož se mnoho útoků v současné době odehrává právě v kyberprostoru, je velice důležité rozumět fungování internetu. Ten hraje klíčovou roli v rozvoji a šíření kybernetických hrozeb.[6]

[4] LAPÁČEK, J. *Poznáváme Internet: rychle hotovo*!. Brno: Computer Press, 2007, str. 5.
[5] SMEJKAL, V. *Kybernetická kriminalita*. Plzeň, s. 58.
[6] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 78.

2.4 Kybernetická kriminalita

V úvodu této podkapitoly je důležité vymezit, co znamená pojem kriminalita. Obecná kriminalita představuje nejvýznamnější část celkové kriminality, o čemž svědčí její podíl na ní. Obecná kriminalita zahrnuje jak formu násilného jednání, tak i formy nenásilné, které svojí společenskou nebezpečností významně ovlivňují veřejné mínění občanů o své bezpečnosti. Řešení obecné kriminality vyžaduje odbornou znalost pracovníků, a to jak po stránce právní a po stránce kriminalistiky, tak i z hlediska základních znalostí psychologie, zdravotnictví apod.[7]

Do oblasti obecné kriminality zařazujeme všechny trestné činy, které dělíme na:

- násilně trestnou činnost,
- mravnostní trestnou činnost,
- majetkovou trestnou činnost.

Kybernetickou kriminalitu můžeme rozdělit do dvou hlavních kategorií. V první kategorii je výpočetní technika prostředkem k provádění nelegálních aktivit, zatímco v té druhé je samotným cílem páchání trestné činnosti.[8] Problém spočívá v tom, že jednotliví autoři a právní předpisy používají různé pojmy k označení těchto aktivit. Mezi tyto pojmy patří informační kriminalita, elektronická kriminalita, softwarová trestná činnost, počítačová trestná činnost, computer-related crime, počítačová kriminalita, kybernetická trestná činnost, kyberkriminalita a další.[9]

Jirovský uvádí, že *„tato kriminalita může být namířena přímo proti počítačům, jejich hardwaru, softwaru, datům, sítím apod., nebo v ní vystupuje počítač pouze jako nástroj pro páchání trestného činu, případně počítačová síť a k ní připojená zařízení jsou prostředím, v němž se taková činnost odehrává.“*[10]

Dle ustanovení zákona č. 40/2009 Sb., trestního zákoníku, ve znění pozdějších právních předpisů jsou identifikovány tři hlavní skutkové podstaty majetkových trestných činů v oblasti kybernetické kriminality. Tyto skutkové podstaty zahrnují:

- neoprávněný přístup k počítačovému systému a nosiči informací (§ 230),
- opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231),

[7] *Odbor obecné kriminality* [online]. [cit. 2023-09-24]. Dostupné z WWW: https://www.policie.cz/clanek/uskpv-ook-odbor-obecne-kriminality.aspx.
[8] SMEJKAL, V, SOKOL, T., VLČEK, M. *Počítačové právo*. Praha: C.H. Beck, 1995, s. 44–47.
[9] GŘIVNA, T, POLČÁK R. *Kyberkriminalita a právo*. Praha: Auditorium, 2008, s. 32.
[10] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, s. 19.

- poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232).

Dále jsou zaznamenávány trestné činy, při nichž pachatel záměrně zvolil kyberprostor jako prostředek k páchaní trestných činů, což může mít významný dopad na společnost. Mezi tyto trestné činy patří:

- šíření pornografie (§ 191),
- výroba a jiné nakládání s dětskou pornografií (§ 192),
- navazování nedovolených kontaktů s dítětem (§ 193b),
- 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).[11]

2.5 Kybernetický útok

Kybernetický útok je záměrný akt, při němž jedna nebo více osob neoprávněně proniká do informačních systémů, sítí, počítačových zařízení a dat nebo je poškozuje. Takové aktivity se mohou zaměřovat na zcizení osobních údajů, zpronevěru nebo třeba na vytváření dětské pornografie a její šíření.

Jirásek a kol. definují kybernetický útok, jako *„útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků.“*[12]

Tyto útoky mohou zahrnovat různé techniky a metody, jako jsou malware, phishing, DoS (Denial of Service) či DDoS útok, které mají za cíl potlačení funkčnosti jednoho či více počítačových systémů, případně poskytovaných služeb.[13]

[11] NGSS. *Zločiny v době moderních technologií: Jak řeší české právo kybernetickou kriminalitu a jak se proti ní bránit?* [online]. [cit.2023-10-08]. Dostupné z WWW: https://www.ngss.cz/clanek/zlociny-v-dobe-modernich-technologii-jak-resi-ceske-pravo-kybernetickou-kriminalitu-a-jak-se-proti-ni-branit-2023-05-16.
[12] JIRÁSEK, P., NOVÁK, L., POŽÁR J. *Výkladový slovník kybernetické bezpečnosti.* [online]. 2. aktualiz. vyd. Praha: AFCEA, © 2015, s. 59. Dostupný z WWW: https://afcea.cz/cesky-slovnik-pojmu-kyberneticke-bezpecnosti/.
[13] KOLOUCH, J., BAŠTA, P. *Cybersecurity*, Praha, 2019, s. 78–79.

Na základě výše uvedených informací je tedy možné kybernetický útok definovat jako jakékoli protiprávní jednání útočníka v kyberprostoru směřující proti zájmům jiné osoby. Toto jednání nemusí mít vždy podobu trestného činu, podstatné je, že narušuje běžný způsob života poškozeného.[14]

[14] KOLOUCH, J., BAŠTA, P. *Cybersecurity*, Praha, 2019, s. 78–79.

3 Formy podvodného jednání

S postupujícím vývojem informačních a komunikačních technologií (dále jen IT) získávají pachatelé prostor pro stále nové a inovativní způsoby protiprávního jednání. Tato kapitola se bude věnovat různým formám podvodných praktik v IT prostředí, ať už se jedná o ty nejběžnější, či méně známé metody. Cílem této kapitoly je detailně popsat jednotlivé podvodné praktiky, odlišit je od sebe a ukázat, jak mohou být propojeny. Následně bude popsáno, jakým způsobem mohou ovlivnit uživatele IT prostředí a jak lze efektivně reagovat na nové, obdobné varianty těchto podvodů, které se mohou objevit.

Pro jasnější porozumění této problematice bude uvedeno několik konkrétních příkladů a případových studií ilustrujících, jak tyto útoky probíhají v praxi. Znalost spektra podvodných praktik a konkrétních příkladů zvyšuje schopnost se před těmito hrozbami uchránit, vyvarovat se jim nebo jim vhodně předcházet. Pro dosažení takového cíle je nutné se detailně seznámit s jednotlivými podvodnými praktikami a pochopit, jak mohou ovlivnit bezpečnost a integritu IT prostředí.

Páchat IT podvody, potažmo kyberkriminalitu, je oproti běžné fyzické krádeži či loupeži výhodnější z důvodu nižšího rizika fyzické újmy, mnohonásobně vyššího zisku, nižšího trestního postihu a nižší naděje na odhalení a odsouzení.[15]

3.1 Elektronické obchodování

Formy podvodného jednání se stávají stále populárnějšími, což platí zejména v oblasti internetového obchodování. Tyto podvody se provádějí jak prostřednictvím internetových inzercí, bazarů, aukčních a slevových portálů či různých e-shopů, tak často i prostřednictvím přímých nabídek, které dorazí přes elektronickou komunikaci, například e-mailem. Charakter těchto podvodných jednání je často obdobný. Jedná se o různé typy klamných nabídek zboží, zvířat, služeb, zaměstnání, půjček a dalšího. Společným prvkem bývá lákavá nabídka a neobvykle nízká cena. Samotný podvod může mít různé podoby, od nedodání zboží či služby přes doručení poškozeného či padělaného zboží až po únik citlivých osobních údajů.[16]

3.1.1 Internetové inzerce a bazary

V naší zemi je jedním z nejznámějších a nejčastěji zneužívaných internetových bazarů pro provádění kybernetických podvodů Bazoš.cz. Existuje však celá řada dalších

[15] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, s. 30.
[16] SMEJKAL, V. *Kybernetická kriminalita*. Plzeň, s. 133.

podobných online bazarů a portálů, mezi něž patří například sBazar.cz, Hyperinzerce.cz a Facebook Marketplace (www.facebook.com). Na těchto platformách se často objevují lákavé nabídky zboží a služeb, u kterých může být značně komplikované rozpoznat podvodný inzerát již na první pohled. Registrace na internetovém bazaru za účelem podvodného obchodování a následné vytvoření podvodného inzerátu jsou velmi snadné a vyžadují pouze základní uživatelské znalosti. Jednoduché uskutečnění podvodu je jedním z hlavních důvodů, proč jsou tak rozšířené. Stačí napsat text inzerátu, přidat obrázek zboží, nastavit nízkou cenu a čekat na potenciální zájemce.

Kazuistika

K podvodu však může dojít i ze strany kupce, který se ozve na vytvořený inzerát. Podvodník se přihlásí jako zájemce o koupi a zpočátku vše působí standardně. Když však dojde na placení zboží, podvodný zájemce nabídne poslání peněz na účet skrz platební bránu známých společností a zašle odkaz na falešné internetové stránky společnosti, nerozeznatelné od těch opravdových. Rozdíl je v tom, že tyto stránky nebyly vytvořeny firmami, za něž se vydávají, ale právě těmito podvodníky. Všechny údaje o platební kartě se tak dostanou k podvodníkovi a ten poté vytvoří v mobilní aplikaci kopii platební karty, z níž může okamžitě čerpat peníze poškozeného.[17]

3.1.2 Podvodné e-shopy

Elektronický obchod, známý také jako e-shop, představuje digitální ekvivalent tradičních kamenných obchodů a funguje na internetu. Zásadním rozdílem je, že se vše odehrává virtuálně. E-shopy nabízejí zboží, které kupující vkládá do virtuálního nákupního košíku, kde si následně může zobrazit celkové množství produktů a jejich cenu. Tyto platformy často podporují vyhledávání zboží podle různých parametrů, jako jsou cena, značka, kategorie aj.

U každého produktu lze nalézt informace o dostupnosti zboží, hodnocení od ostatních zákazníků nebo je možné porovnat ho s jinými produkty. K dokončení objednávky je zapotřebí zadat doručovací adresu, zvolit způsob doručení a platby. Zákazník poté obdrží potvrzení o objednávce na zadaný e-mail. Mezi známé, důvěryhodné e-shopy patří například Alza.cz, Mall.cz nebo CZC.cz. Přes všechny tyto pozitivní aspekty elektronického obchodování existují i stinné stránky v podobě různých

[17] HRDINA, R. *Podvody na internetových bazarech* [online]. [cit. 2023-10-12]. Dostupné z WWW:https://www.policie.cz/clanek/podvody-na-internetovych-bazarech.aspx.

podvodných aktivit. Ty mohou zahrnovat falešné e-shopy, phishing útoky, neoprávněné používání platebních karet a mnoho dalších.

Kazuistika

V roce 2019 tři muži nabízeli k prodeji elektroniku přes internetové bazary a fiktivní e-shopy (ejabko.eu; imarketo.eu; gmzone.cz; techtronic.cz; best-elektro.cz), které sami založili. Přestože zájemci za objednané zboží zaplatili, nikdy ho neobdrželi a peníze jim nebyly vráceny. Během půl roku tito pachatelé podvedli celkem 650 osob z celé České republiky, a způsobili tak škodu za téměř 5 miliónů korun. K přijímání plateb za objednané zboží užívali účty založené na různé osoby bez jejich vědomí nebo užívali účty osob (tzv. bílých koní), které jim umožnily přijetí platby a posléze ji převedly na kryptoměny do bitcoinových peněženek pachatelů.[18]

3.2 Phishing

Phishing, anglický výraz odvozený od slova „fishing“ (rybaření), představuje jednu z nejzákeřnějších a nejrozšířenějších kybernetických hrozeb v dnešní době. Tato hrozba se projevuje různorodými způsoby, ale nejběžnější formou je e-mailová zpráva zaslaná oběti. V této zprávě se nachází odkaz vedoucí na podvodnou webovou stránku, která bývá klíčem k úspěchu útočníka.[19]

Podvodné webové stránky často naprosto přesně kopírují vzhled oficiálních stránek renomovaných institucí, jako jsou banky, e-commerce platformy nebo sociální sítě. To běžným uživatelům ztěžuje rozpoznání podvodu. Mnoho lidí má tendenci věřit, že pokud webová stránka vypadá jako oficiální, musí to být v pořádku. Avšak právě toto přesvědčení činí phishing tak úspěšným. Klíčovou součástí phishingových útoků je schopnost útočníků vytvářet falešné webové stránky, dokonale imitující vzhled a obsah legitimních stránek. To může zahrnovat kopírování grafického designu, loga, či dokonce URL adresy. Stránky často vyzývají uživatele k zadání citlivých údajů, jako jsou hesla, čísla kreditních karet nebo sociálního zabezpečení.

Jak vyplývá z meziroční zprávy Národního úřadu pro kybernetickou a informační bezpečnost z roku 2022, v roce 2021 se na území České republiky ukázaly jako nejpoužívanější vektory kybernetických útoků právě phishing, spear phishing a podvodné

[18] KORMOŠOVÁ, I. *Podvody na internetu* [online].[cit. 2023-10-11]. Dostupné z WWW: https://www.policie.cz/clanek/podvody-na-e-shopech.aspx.
[19] DVOŘÁK, M. *Phishing, pharming a jejich právní postih.* Trestněprávní revue, číslo 34. 2018, s. 84 [online]. [cit. 2023-10-11]. Dostupné z WWW: http://www.beck-online.cz.

e-maily. Během roku 2022 se s pokusy o phishing či úspěšnými útoky setkalo až 92 % respondentů. Co se týče spear phishingových e-mailů (tedy podvodných e-mailů cílených na konkrétní osobu), bylo jejich cílem 49 % dotázaných. Podvodné e-maily zasáhly až 89 % respondentů, zatímco vishing (voice phishing, tedy phishing prováděný přes telefonní hovor) byl zaznamenán u 20 % z nich. Tento nárůst je mírný, avšak neméně důležitý.[20]

Aby bylo možné bránit se phishingu, je důležité kontrolovat e-mailové adresy odesílatele, a to i tehdy, pokud e-mail vypadá důvěryhodně. Phishingové e-maily často obsahují gramatické nebo pravopisné chyby, což může být známkou podvodu. Uživatelé by nikdy neměli otevírat podezřelé odkazy nebo stahovat soubory, pokud si nejsou naprosto jisti jejich pravostí. V případě jakéhokoli podezření ohledně legitimnosti příchozí zprávy je nezbytné provést její ověření. Nejsnadnějším způsobem je kontaktovat odesílatele prostřednictvím jiného komunikačního kanálu. Například pokud uživatel obdrží e-mail od banky se žádostí o aktualizace hesla, měl by zavolat na oficiální číslo své banky a ověřit si, že je takový e-mail skutečný.[21]

Kazuistika

V roce 2012 se na sociální síti Facebook nacházel odkaz na phishingovou stránku novamaturita.kvalitne.cz nabízející okamžité výsledky státních maturit. I když se prokazatelně jednalo o podvod, během 24 hodin tyto stránky navštívilo 2632 uživatelů, kteří provedli celkem 4145 zobrazení.[22]

Velký phishingový útok začal v průběhu prosince 2014 (konkrétně v období Vánoc) a pokračoval v lednu 2015. Tento útok byl rozdělen do dvou fází. V první fázi byly uživatelům zaslány e-mailové zprávy s přáním veselých Vánoc prostřednictvím elektronické pohlednice. V druhé fázi byly v průběhu ledna zasílány zprávy o potvrzení objednávky na elektroniku. Ve zprávě bylo uživateli sděleno, že si zakoupil zboží (např. tiskárnu, harddisk, fotoaparát atp.), které zaplatil předem platební kartou, a že v příloze nalezne fakturu. Oba dva útoky měly společný prvek, a to malware obsažený v příloze

[20] *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022* [online]. [cit. 2023-10-15]. Dostupné z WWW:https://nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2022.pdf

[21] AVAST. *Phishing* [online]. [cit. 15.10.2023]. Dostupné z WWW: https://www.avast.com/cs-cz/c-phishing.

[22] VOŘÍŠEK, L. *Phishing v praxi, aneb jak jsem nachytal české studenty* [online]. [cit. 2023-10-15]. Dostupné z WWW: https://cdr.cz/clanek/phishing-jak-jsem-nachytal-ceske-studenty-nova-maturita.

e-mailu. Konkrétně se jednalo o trojského koně (Kryptik) prezentovaného jako spořič obrazovky.[23]

3.3 Vishing

Voice phishing, známý též jako „vishing“, představuje sofistikovanou formu kybernetického útoku, při němž je oběť kontaktována prostřednictvím telefonu. Útočník se vydává za zaměstnance důvěryhodné organizace, obvykle banky, a důmyslně prezentuje důvod svého hovoru. Tak může sdělit například zdánlivé napadení bankovního účtu uživatele, což mnohdy vyvolá obavy a sníží obezřetnost oběti. Útočníci často využívají metodu známou jako „spoofing“ spočívající ve falšování identity volajícího. Dokážou tak napodobit oficiální kontakt, například infolinku banky. Celý telefonní hovor pak působí důvěryhodně a zastrašená osoba může podlehnout pokušení a poskytnout své citlivé údaje, které útočníkovi otevřou dveře k bankovnímu účtu.

Vishingové útoky se řadí k nejsložitějším typům kybernetických hrozeb, neboť útočníci využívají lidskou tendenci věřit veřejně přístupným informacím a institucím, jako jsou banky či úřady. Skrze sofistikovanou manipulaci se pachatelé snaží získat přístup k citlivým datům a finančním prostředkům. Jejich přístup často spočívá ve studiu a analýze potencionální oběti, což jim umožňuje předstírat situaci, která může vypadat jako oprávněná žádost o ověření údajů.[24]

Kazuistika

Neznámý pachatel vydávající se za zaměstnance banky telefonicky kontaktoval 22letou ženu z Litoměřicka a sdělil jí, že její bankovní účet je v ohrožení a bude zmrazen. Poškozené doporučil, aby neprodleně vyzvedla peníze z účtu a vložila je na bezpečný účet prostřednictvím QR kódu, který jí zašle. Poškozená vyzvedla peníze a vložila je přes QR kód na doporučení falešného bankéře do bankomatu na Bitcoiny.[25]

3.4 Smishing

Smishing, zkratka pro „SMS phishing“, představuje podvodnou techniku, při níž pachatelé využívají textové zprávy k získání citlivých informací od obětí. Tato metoda

[23] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 260.
[24] ESET. *Co je vishing?* [online]. [cit. 2023-12-14]. Dostupné z WWW:https://www.eset.com/cz/vishing/.
[25]KOFROVÁ, P. *Vishing* [online]. [cit. 2023-10-15]. Dostupné z WWW: https://www.policie.cz/clanek/vishing.aspx.

probíhá podobně jako vishing, avšak místo hovoru je zde klíčovou komunikační formou SMS.[26]

Typický scénář smishingu začíná odesláním SMS oběti, v níž je uvedeno, že byla zjištěna podezřelá transakce na jejím bankovním účtu. Pachatel v textu poskytne telefonní číslo, na které má oběť zatelefonovat. Zde se představí jako zaměstnanec banky, snažící se získat důvěru oběti. K přesvědčení oběti, aby poskytla citlivé údaje, jako jsou kontrolní kódy uvedené v podvodné SMS, využívá různorodé taktiky.

V moderních variantách smishingu se často objevuje odkaz přímo v SMS zprávě směřující na podvodné internetové stránky. To je pak spojeno s technikou známou jako „pharming“. Tímto způsobem pachatelé následně získávají další informace potřebné k provedení podvodné transakce.

Kazuistika

Žena z Litoměřicka, která obdržela na mobilní telefon SMS zprávu s internetovým odkazem na údajnou doručovatelskou společnost, si myslela, že se jedná o vyrovnání daní. Ve zprávě byl odkaz na webové stránky společnosti. Když poškozená tento odkaz otevřela, byla přesměrována na vyplnění klíče ke svému mobilnímu bankovnictví, jejž vyplnila a odeslala. Tímto neznámý pachatel vylákal z poškozené přístup k účtům.[27]

3.5 Pharming

Pharming představuje nebezpečnou kybernetickou taktiku zaměřenou na Domain Name System (DNS) servery. Tyto servery jsou klíčové pro překlad doménových jmen na odpovídající IP adresy, což je základní krok pro připojení k webovým stránkám.[28]

Když si chce běžný uživatel například zkontrolovat svůj bankovní účet online, otevře si webový prohlížeč a zadá adresu své banky. V tuto chvíli se může stát, že se ocitne na stránce, která vypadá jako ta pravá. Ve skutečnosti se však může jednat o falešnou stránku, na niž byl uživatel přesměrován útočníkem přes DNS. Pokud netuší, že se jedná o podvod, a zadá své přihlašovací údaje, útočník získá přístup k citlivým údajům, jako jsou jméno a heslo k internetovému bankovnictví.[29]

[26] SMEJKAL, V. *Kybernetická kriminalita*. Plzeň, s.138–139.
[27] KAMIL, M. *Smishing* [online]. [cit. 2023-10-15]. Dostupné z WWW: https://www.policie.cz/clanek/uzemni-utvary-sprava-severoceskeho-kraje-zpravodajstvi-smishing.aspx.
[28] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 263.
[29] SAK, P. *Úvod do teorie bezpečnosti*. Praha: Nakladatelství PETRKLÍČ s.r.o., 2018, s. 234–238.

Tento typ útoku se nemusí týkat jen bankovnictví. Podvodníci mohou vytvářet různé aplikace, téměř nerozeznatelné od těch oficiálních. Přestože jsou vizuálně podobné těm pravým, skrývá se v nich nebezpečný vir, který se může dostat do mobilního zařízení uživatele a poškodit ho.

3.6 Malware

Pojem malware vznikl sloučením anglických slov „malicious software“, což lze volně přeložit jako „škodlivý software“. Tímto pojmem se označuje sofistikovaný software navržený s úmyslem narušit, poškodit nebo zneužít počítačový systém. Jeho cílem může být nejen poškození systému, ale také krádež dat a informací uložených v počítači, nebo dokonce získání neoprávněného přístupu k cílovému systému.

Existuje mnoho forem malwaru, přičemž každá z nich se vyznačuje specifickými činnostmi, které provádí. Jediná forma malwaru může kombinovat několik funkcí, jako je například schopnost šířit se prostřednictvím e-mailu či v peer-to-peer sítích a současně shromažďovat e-mailové adresy z napadeného systému.

V minulosti vzniklo mnoho pojmenování spadajících dnes pod termín „malware“. Tyto názvy vycházely z hlavních funkcí, které měly tyto škodlivé programy vykonávat. Jedná se například o adware, spyware, počítačové viry, trojské koně, keyloggery, ransomware, rootkity a počítačové červy.[30]

3.6.1 Spyware

Slovo spyware je odvozeno z anglického „spy software“, což v překladu znamená „špionážní software“. Jedná se o formu škodlivého softwaru, jehož hlavním účelem je sledovat a shromažďovat informace o činnostech uživatele na počítači, a to často bez vědomí nebo souhlasu dotyčného uživatele. Tyto informace mohou zahrnovat širokou škálu dat, včetně historie prohlížených webových stránek, klávesových údajů, osobních údajů a informací o podnikání.

Spyware může být instalován v počítači jako samostatný malware, avšak může se také šířit jako součást jiných, na první pohled nezávadných aplikací. Uživatelé často nerozpoznají přítomnost spywaru a souhlasí s jeho instalací během procesu stahování nebo instalace aplikace. Tato schopnost skrýt svou přítomnost a nebýt zjištěn je jedním

[30] OSTERHOUDT, M. *Computer Health Made Easy V.2 - Beware of the "Wares" Adware, Malware and Spyware*. Lulu Press, Inc, 2013, s. 19–20.

z důvodů, proč je spyware tak nebezpečný. Dokáže zůstat aktivní na pozadí systému, kde tajně shromažďuje data o aktivitě uživatele.[31]

3.6.2 Adware

Adware neboli reklamní software představuje kategorii programů, které si automaticky zobrazují, přehrávají nebo stahují reklamní obsah na počítači po jejich instalaci nebo v průběhu užívání tohoto softwaru. Účelem reklam může být často financování tvorby a udržování programu, což umožňuje jeho bezplatnou dostupnost pro uživatele.

Je důležité rozlišovat mezi pojmy adware a spyware. Ačkoli mohou být oba spojeny s reklamními prvky, většina adwarů nemá za úkol sledovat uživatele nebo shromažďovat jeho osobní informace. Jejich hlavním účelem je spíše poskytovat reklamní obsah, čímž podporují autory softwaru. Adware může nabývat různých forem, včetně bannerů, pop-up oken, in-text odkazů a dalších reklamních prvků. Tyto reklamy mohou být pro uživatele relevantní na základě jejich internetové aktivity. Adware hraje důležitou roli v digitálním světě tím, že umožňuje vývojářům nabízet software zdarma. Avšak nadměrné množství reklam a potenciálně otravné reklamní prvky mohou uživatele frustrovat.[32]

3.6.3 Trojský kůň

Trojský kůň, nebo jednoduše „trojan“, představuje sofistikovaný druh malwaru, který se často schovává pod maskou legitimního nebo užitečného softwaru. Na první pohled se zdá být bezpečnou aplikací, ale ve skutečnosti má zrádné záměry a cíle ohrožující bezpečnost systémů.

Trojský kůň vyniká schopností maskovat svou pravou identitu. Často se prezentuje jako užitečná aplikace či program lákající uživatele ke stažení. Při instalaci však vstupuje do systému nepozorovaně, a proto je tak nebezpečný. Instalací trojského koně získává útočník plný přístup k systému uživatele, což může mít závažné důsledky. Útočník má možnost číst, odesílat, či dokonce manipulovat s nejcennějšími daty a soubory oběti.[33]

---

[31] AYCOCK, J. *Spyware and Adware.* Springer US, 2010, s. 91–92.
[32] THOMAS, F. *Adware: The Only Book You'll Ever Need.* Lulu Press, Inc, 2015, s. 47–49.
[33] OSTERHOUDT, M. *Computer Health Made Easy V.2 - Beware of the "Wares" Adware, Malware and Spyware*. Lulu Press, Inc, 2013, s.40–42.

3.6.4 Keylogger

Keylogger je sofistikovaný software, který má schopnost tajně zaznamenávat každý stisk klávesnice na cílovém počítačovém systému. Jeho hlavním úkolem je sbírat citlivá data, včetně uživatelských jmen a hesel, bankovních účtů, přístupových údajů k sociálním sítím a dalších důležitých informací.

Keylogger se specializuje na tajnou činnost. Bez povšimnutí se usadí na cílovém systému a zůstává skrytý, aniž by oběti věděly, že jsou sledovány. To mu dává schopnost sledovat interakce uživatele s klávesnicí a uchovávat klíčové údaje. Cílem keyloggeru je získat citlivé informace, které mohou být později zneužity. Útočníci mohou využít ukradených údajů k odcizení finančních prostředků, porušení soukromí nebo ke spáchání jiných škodlivých činů.[34]

3.6.5 Ransomware

Ransomware, často nazývaný jako „výkupné-viry“, představuje v dnešní době jednu z největších hrozeb v oblasti IT bezpečnosti. Tato forma malwaru v sobě spojuje slova „výkupné“ (anglicky „ransom“) a „software“. Ransomware je sofistikovaným druhem škodlivého softwaru a dokáže způsobit značné problémy. Ransomware může proniknout do zařízení různými způsoby, například přes infikované e-maily s nebezpečnými odkazy, při návštěvách kompromitovaných webových stránek nebo při instalaci podezřelých aplikací. To, co ransomware výrazně odlišuje od běžného malwaru, je jeho schopnost šifrovat soubory daného uživatele, čímž se stávají nečitelnými, nebo zablokovat celé zařízení.[35]

Prvním typem ransomwaru jsou tzv. šifrovače (kryptory). Tyto škodlivé programy zašifrují soubory tak, že se stanou neotevíratelnými a nepřístupnými. K odemčení poškozených souborů je třeba dešifrovacího klíče, který útočníci slibují poskytnout poté, co obdrží výkupné. Druhým typem jsou blokátory (blockers), jež zcela zablokují zařízení poškozeného a znemožní mu jeho používání. Blokátory mohou být o něco méně katastrofické, protože data zůstávají nepoškozena a oběti mají větší šanci na obnovení svých souborů poté, co je odstraněna blokace.[36]

[34] AYCOCK, J. *Spyware and Adware.* Springer US, 2010, s. 94.
[35] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 221.
[36] DAVID, V. *Co je ransomware a jaké škody může napáchat?* [online]. [cit. 2023-11-03]. Dostupné z WWW: https://insmart.cz/co-je-ransomware/.

Výkupné je hlavní motivací útočníků používajících ransomware. Vyžadují ho jako protihodnotu za opětovné zpřístupnění uzamčených souborů a systémů. Částka požadovaná za obnovení přístupu obvykle závisí na velikosti cílené organizace, obsahu a důležitosti uzamčených souborů pro uživatele. Avšak i když oběť zaplatí výkupné, nikdy není zcela jisté, že svá data získá zpět.

4 Legislativa spojená s kyberkriminalitou

S nárůstem kybernetické kriminality vyvstala naléhavá potřeba vytvořit nový legislativní rámec, který by jasně definoval a trestal tuto formu trestné činnosti. Je nezbytné identifikovat, jaké činy lze označit za kyberkriminalitu a jaké konkrétní tresty by měly být ukládány pachatelům. S neustálým vývojem informačních a komunikačních technologií (ICT) je nezbytné, aby státy jak na vnitrostátní, tak na mezinárodní úrovni přijímaly nové právní předpisy, jež budou lépe ochraňovat tato digitální prostředí a jejich uživatele před trestnými činy. Důležité je také zdůraznit, že kybernetická kriminalita často překračuje hranice jednotlivých států, a proto je spolupráce mezi státy na mezinárodní úrovni klíčová. Existence mezinárodních dohod a úmluv je zásadní pro úspěšný boj s touto formou kriminality.

4.1 Legislativa v ČR

V rámci legislativy České republiky existuje několik předpisů, které se vážou ke kybernetické kriminalitě.

4.1.1 Trestní zákoník

Trestní právo České republiky ustanovením trestního zákoníku reaguje na zvyšující se hrozbu kybernetické kriminality, existující legislativa však často neposkytuje dostatečné nástroje k postižení pachatelů kybernetických trestných činů. I přes tyto nedostatky je trestní zákoník v České republice schopen reflektovat nový druh kriminality a poskytuje ustanovení týkající se kybernetického zločinu. Následující seznam obsahuje několik nejčastějších trestných činů, které mohou být páchány i v kyberprostoru:

- § 180 Neoprávněné nakládání s osobními údaji
- § 191 Šíření pornografie
- § 192 Výroba a jiné nakládání s dětskou pornografií
- § 193 Zneužití dítěte k výrobě pornografie
- § 205 Krádež
- § 206 Zpronevěra
- § 209 Podvod
- § 230 Neoprávněný přístup k počítačovému systému a nosiči informací
- § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
- § 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

- § 270 Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi.[37]

4.1.2 Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů

Tento zákon stanovuje práva a povinnosti subjektů, stejně jako pravomoci a působnost veřejných orgánů v oblasti kybernetické bezpečnosti. Dále se věnuje zajištění bezpečnosti sítí elektronických komunikací a informačních systémů. Je třeba poznamenat, že tento zákon se nevztahuje na informační nebo komunikační systémy operující s utajovanými informacemi. Zákon č. 181/2014 Sb. byl později novelizován zákonem č. 205/2017 Sb., který mění původní znění zákona o kybernetické bezpečnosti spolu s některými dalšími právními úpravami.[38]

4.1.3 NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) hraje klíčovou roli v oblasti ochrany České republiky před kybernetickými hrozbami. V rámci svých aktivit NÚKIB podporuje a spravuje Vládní CERT České republiky (GovCERT.CZ), což je důležitá složka pro monitorování kybernetických hrozeb a reakcí na ně v rámci státní správy. Specializuje se také na prevenci proti kybernetickým hrozbám pro kritickou informační infrastrukturu, čímž přispívá k bezpečnosti klíčových systémů.

Další důležitou oblastí činnosti NÚKIB je koordinace řešení kybernetických bezpečnostních incidentů u subjektů kritické infrastruktury, provozovatelů základních služeb a orgánů veřejné správy. Tímto způsobem úřad aktivně přispívá k ochraně důležitých funkcí státu a ekonomiky. Kromě toho se NÚKIB zaměřuje na osvětovou a vzdělávací činnost a zapojuje veřejnost do vzdělávacích aktivit týkajících se kybernetické bezpečnosti.

Klíčová je také spolupráce s národními i mezinárodními organizacemi, jelikož umožňuje sdílení informací a osvědčených postupů v oblasti kybernetické bezpečnosti. Centrum se rovněž účastní kybernetických cvičení na národní i mezinárodní úrovni, což je důležité pro testování reakce na kybernetické hrozby a zkoušení připravenosti. Angažuje se také v oblasti výzkumu a vývoje souvisejícího s kybernetickou bezpečností,

[37] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. In Sbírka zákonů, Česká republika. 2009, částka 11.
[38] ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In Sbírka zákonů, Česká republika. 2014, částka 75.

čímž přispívá k neustálému vylepšování stávajících metod a technologií v této kritické oblasti.[39]

4.1.4 Vládní CERT

Vládní CERT (Computer Emergency Response Team) představuje klíčový útvar pro ochranu kritické informační infrastruktury v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti. Vzhledem k rostoucímu propojení kritických systémů s internetem je nezbytné, aby stát přijal veškerá nezbytná opatření k jejich bezpečnosti. V případě selhání preventivních opatření je zásadní mít tým jako je CERT, který dokáže rychle a účelně reagovat na útoky na infrastrukturu.[40]

4.2 Mezinárodní úmluvy

Mezinárodní úmluvy hrají klíčovou roli v boji proti kybernetické kriminalitě v rámci Evropské unie. Dvě nejdůležitější dohody jsou Úmluva Rady Evropy o kybernetické kriminalitě a dodatek k této úmluvě. Kromě těchto úmluv hraje Evropská unie významnou roli v ochraně před kyberkriminalitou prostřednictvím vydávání sdělení. Tato sdělení obsahují směrnice a rady usnadňující členským státům zvyšování úrovně kybernetické bezpečnosti a koordinaci mezinárodních opatření.[41]

4.2.1 Úmluva Rady Evropy č.185 o kybernetické kriminalitě a její dodatek

Úmluva Rady Evropy č. 185 o kybernetické kriminalitě, známá také jako Budapešťská úmluva, představuje mezinárodní právní nástroj v boji proti kybernetické kriminalitě. Byla přijata v roce 2001 a má za cíl posílit prevenci, vyšetřování a stíhání trestných činů spáchaných prostřednictvím počítačových sítí a informačních technologií. Tato úmluva stanovuje základní principy a společné standardy, jež mají členské státy dodržovat v boji proti kybernetické kriminalitě. Mezi klíčové aspekty patří definice různých kybernetických trestných činů, spolupráce mezi státy při vyšetřování a trestním stíhání a také zajištění práv obětí.[42]

[39] *Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka* [online]. [cit. 2023-11-05]. Dostupné z WWW: https://www.nukib.cz/cs/kyberneticka-bezpecnost.
[40] *Národní úřad pro kybernetickou a informační bezpečnost: Vládní CERT* [online]. [cit. 2023-11-05]. Dostupné z WWW: https://www.nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/.
[41] KOLOUCH, J. a VOLEVECKÝ, P. *Trestněprávní ochrana před kybernetickou kriminalitou*. Praha,2013, s. 65.
[42] ČESKO. Sdělení č. 104/2013 Sb. m. s., o sjednání Úmluvy o počítačové kriminalitě. In Sbírka zákonů, Česká republika.2013, částka 56.

Dodatek k této úmluvě rozšiřuje její působnost a zavádí další opatření ke zlepšení mezinárodní spolupráce v boji proti kybernetické kriminalitě. Obsahuje například ustanovení o výměně informací a důkazů mezi úřady různých členských států.

Budapešťská úmluva a její dodatek jsou důležitými kroky směrem k celosvětovému úsilí o zlepšení kybernetické bezpečnosti a ochrany před kybernetickou kriminalitou. Tato úmluva byla podepsána jménem České republiky 9. 2. 2005 a pro Českou republiku vstoupila v platnost podle odstavce 4 článku 36 dne 1. 12. 2013.[43]

[43] *Dodatkový protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů* [online]. [cit. 2023-11-05]. Dostupné z WWW: https://rm.coe.int/16804931bf.

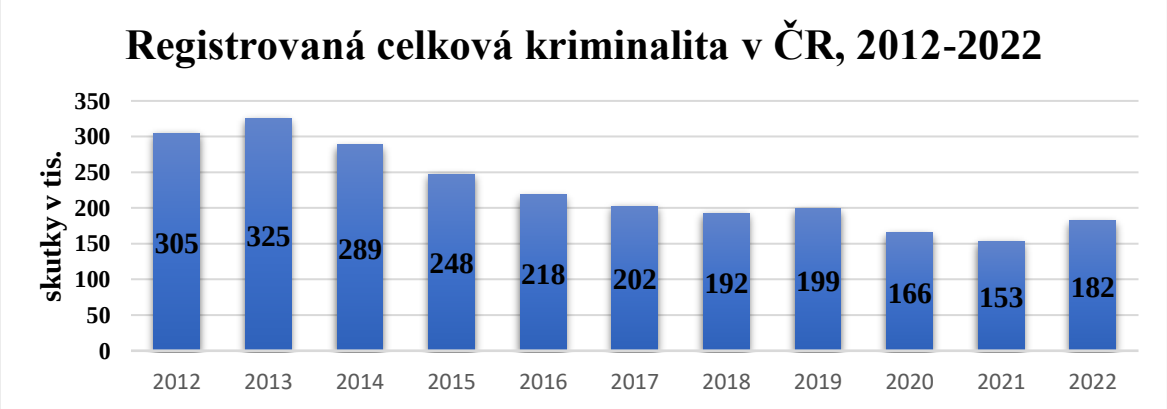
5 Současný stav kybernetické kriminality

S rostoucím využíváním kybernetického prostoru se neustále rozšiřuje okruh jeho uživatelů a s ním i množství nových a sofistikovanějších způsobů kybernetické trestné činnosti. Tento globální fenomén je patrný z mnoha statistik a přehledů nejen na mezinárodní úrovni, ale také v rámci České republiky. Vzhledem k vysoké míře latence kybernetické kriminality se však nabízí otázka, do jaké míry jsou statistická data vypovídající o současném stavu kybernetické trestné činnosti reálná. I když jsou konkrétní čísla pouze špičkou ledovce, dostupná data umožňují alespoň identifikovat vývojový trend kybernetické kriminality, a predikovat tak její budoucí směřování.

5.1 Vnitrostátní úroveň

Z dlouhodobého hlediska lze v České republice pozorovat spíše klesající tendenci kriminality, a to od roku 1994, jak je znázorněno na Obrázku 1. Avšak v roce 2022 tento dlouhodobý trend náhle ustal a orgány činné v trestním řízení se musely vypořádat s výrazným nárůstem registrované trestné činnosti. Policie ČR v tomto roce evidovala 181 991 případů, což představuje nárůst o 28 758 případů (18,8 %) ve srovnání s předchozím rokem. Při zkoumání časových řad je nutné vzít v úvahu výrazná specifická období v letech 2020 až 2022. Roky 2020 a 2021 byly poznamenány pandemií covidu-19 a s ní souvisejícími opatřeními v rámci lockdownu, což významně ovlivnilo míru kriminality směrem k jejímu razantnímu snížení. Naopak ruská agrese proti Ukrajině měla v roce 2022 výrazný dopad na nárůst registrované kriminality. Tato událost negativně ovlivnila různé oblasti vnitřní bezpečnosti, včetně kriminality.

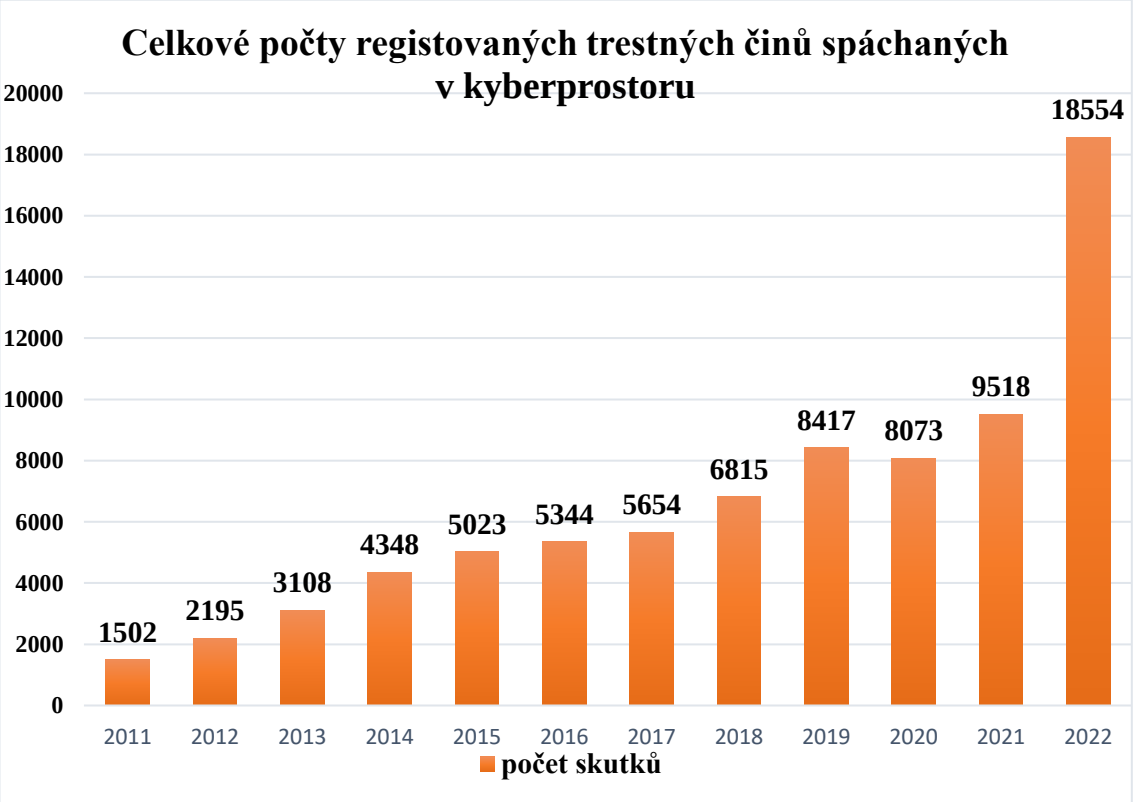
Obrázek 1: Kriminalita v České republice[44]



[44] *Český statistický úřad* [online]. [cit. 2023-12-04].
Dostupné z WWW: https://www.czso.cz/documents/10180/221256712/08000923.pdf/, s. 10.

Na rozdíl od celkové kriminality v České republice je u kybernetické kriminality evidován trvalý vzestup, jak ilustruje Obrázek 2 s údaji získanými od Policie ČR. V roce 2022 došlo k jejímu alarmujícímu nárůstu, neboť bylo zaznamenáno 18 884 trestných činů v kyberprostoru, což představuje téměř dvojnásobek ve srovnání s rokem 2021. Tento vývoj je velice znepokojivý, jelikož právě v letech 2020 a 2021 došlo, v důsledku onemocnění covid-19, k výraznému přesunu aktivit z reálného do virtuálního prostředí. V roce 2022 se život postupně vracel k běžným podmínkám, přesto však došlo téměř ke zdvojnásobení evidovaných trestných činů (94,9 %) spadajících do kyberprostoru. Tento nárůst pravděpodobně souvisí s probíhající válkou na Ukrajině.

Obrázek 2: Nápad trestné činnosti kybernetické kriminality a kriminality páchané na internetu 2011–2022[45]



Policie ČR k uvedenému grafu uvádí následující: *„Stále platí, že nejrozšířenější oblastí trestných činů v rámci ostatní kriminality páchané v kyberprostoru je majetková trestná činnost, nejčastěji různá jednání kvalifikovaná jako podvod (§ 209 trestního zákoníku). Dále byly ve větším množství páchány trestné činy pomocí internetu v oblasti poškozování a zneužití záznamu na nosiči informací (§§ 230, 231 a 232), v oblasti mravnostních trestných činů, v oblasti neoprávněného držení platebního prostředku*

[45] *Český statistický úřad* [online]. [cit. 2023-12-05].
Dostupné z WWW: https://www.czso.cz/documents/10180/221256712/08000923.pdf/, s. 9.

a konečně trestných činů v oblasti porušování autorského práva a porušování práv k autorské známce (§ 155).“[46]

Z dostupných dat lze predikovat, že vzrůstající trend kybernetické kriminality bude trvat i nadále, neboť za rok 2023 počet evidovaných trestných činů spadajících do problematiky kybernetické kriminality převýšil 20 tisíc případů.

5.2 Globální úroveň

Globální prostředí kybernetické bezpečnosti zažívá v posledních letech rapidní nárůst hrozeb. Během pandemie se pachatelé zaměřili na nedostatečně zabezpečené sítě, v době, kdy firmy přecházely na práci z domova. V roce 2020 se počet malwarových útoků zvýšil o ohromujících 358 % ve srovnání s rokem 2019. Od té doby se kybernetické útoky do roku 2021 celosvětově zvýšily o 125 %. Rostoucí objemy kybernetických útoků nadále ohrožují podniky i jednotlivce i v roce 2022. Také ruská invaze na Ukrajinu měla zásadní dopad na kybernetické hrozby. Od začátku konfliktu se počet phishingových útoků na e-mailové adresy evropských a amerických firem zosmínásobil. V prvním čtvrtletí roku 2022 došlo také k narušení bezpečnosti téměř 3,6 milionu ruských uživatelů internetu, což představuje mezičtvrtletní nárůst o 11 %.[47]

S cílem ochránit ukrajinskou kritickou infrastrukturu před ruskými útoky zahájilo Spojené království v roce 2022 tzv. „Ukrajinský kybernetický program“. Spojené království vydalo počáteční balíček ve výši 6,35 milionu liber jako reakci na zvýšenou ruskou kybernetickou aktivitu bezprostředně po invazi na Ukrajinu. Tento program reaguje na incidenty a poskytuje ochranu ukrajinským vládním subjektům před útoky, dále ochranu před distribuovaným odmítnutím služeb (DDoS), aby měli občané stále přístup ke kritickým informacím a byli chráněni před útoky na firewally. Phishing zůstává nejčastější formou trestné činnosti páchané online. V roce 2021 se stalo obětí phishingových útoků údajně 323 972 uživatelů internetu. To znamená, že polovina uživatelů, kteří utrpěli únik dat, se stala obětí phishingového útoku. Během vrcholu pandemie vzrostl počet phishingových incidentů o 220 %.[48]

[46] *Policie ČR: Z dlouhodobého pohledu je kriminalita na historicky nejnižší úrovni, má to ale své důvody. Kybernetická kriminalita má naopak vzestupnou tendenci.* [online]. [cit. 2023-12-05]. Dostupné z WWW: https://securityguide.cz/policie-cr-z-dlouhodobeho-pohledu-je-kriminalita-na-historicky-nejnizsi-urovni-ma-to-ale-sve-duvody-kyberneticka-kriminalita-ma-naopak-vzestupnou-tendenci/.
[47] *The Latest 2023 Cyber Crime Statistics (updated December 2023)* [online]. [cit. 2023-12-05]. Dostupné z WWW: https://aag-it.com/the-latest-cyber-crime-statistics/.
[48] *The Latest 2023 Cyber Crime Statistics (updated December 2023)* [online]. [cit. 2023-12-05]. Dostupné z WWW: https://aag-it.com/the-latest-cyber-crime-statistics/.

Statistiky

V roce 2021 byla odhalena téměř 1 miliarda podvodných e-mailů, setkal se s nimi 1 z 5 uživatelů internetu. Toto množství je možné vysvětlit neustálým výskytem phishingových útoků. V roce 2022 utrpěly podniky v průměru škodu ve výši 4,35 milionu dolarů v důsledku úniků dat. V první polovině roku 2022 bylo celosvětově zaznamenáno přibližně 236,1 milionů ransomwarových útoků. Kybernetické útoky postihly 39 % britských firem v roce 2022. Během první poloviny roku 2022 bylo 53,35 milionu občanů USA postiženo kybernetickou kriminalitou.[49]

[49] *The Latest 2023 Cyber Crime Statistics (updated December 2023)* [online]. [cit. 2023-12-05]. Dostupné z WWW: https://aag-it.com/the-latest-cyber-crime-statistics/.

6 Prevence kybernetické kriminality

Prevence je klíčovým nástrojem v boji s různými hrozbami a nežádoucími jevy v dnešní společnosti. Můžeme ji definovat jako *„souhrn opatření zaměřených na předcházení nežádoucím jevům.“*[50] Využívá se napříč různými oblastmi činností k eliminaci rizik, předcházení nepříznivým událostem a hledání účinných opatření k ochraně před těmito nebezpečími.

Vzhledem k obrovskému technologickému pokroku je dnes již běžné, že téměř každé dítě vlastní mobilní telefon. Prudký vývoj technologií umožnil psát na mobilním telefonu zprávy, provádět videohovory, objednávat jídlo nebo vstupenky na kulturní a sportovní události, a to vše online. Tyto služby jsou pohodlné a příjemné, ale na druhou stranu mohou být i problematické a nebezpečné.[51]

Kvůli pokročilým mobilním zařízením, počítačům a sociálním sítím jsou děti a mladiství vystaveni značnému riziku. Rodiče si mnohdy neuvědomují tyto hrozby, pravděpodobně z důvodu nedostatku času nebo kvůli omezenému přehledu o online aktivitách svých dětí. Je otázkou, zda jde o nedostatek času věnovaného dětem, nebo o větší počítačovou gramotnost dětí ve srovnání s jejich rodiči. Prevence v oblasti kyberkriminality hraje klíčovou roli v minimalizaci tohoto rizika v prostředí internetu. Jedná se o společenský problém ovlivňující každou vrstvu populace od dětí přes dospělé až po seniory. Kyberkriminalita představuje stálou hrozbu, a proto je nezbytné hledat nové metody a postupy pro její účinné řešení. Kriminální prvky jsou v tomto odvětví mimořádně vynalézavé a často jsou o krok před námi.

Prevenci v oblasti kriminality lze obecně definovat jako *„zabránění trestné činnosti ještě předtím, než k ní dojde.“*[52] Primární prevence kriminality je zaměřena na předcházení, odvrácení a snižování příležitostí k samotnému páchání kriminality. Směřuje k obecné populaci a místům, která nejsou kriminalitou zatížena. Usiluje o aktivní podporu společensky akceptovatelného chování. Sekundární prevence kriminality zahrnuje intervenci vůči osobám nebo místům identifikovaným jako náchylnější ke kriminalitě. Adresáti této prevence jsou vymezeni konkrétněji, např. podle teritoria, věku,

[50] MARTANOVÁ, V., B. JANÍKOVÁ, T. DANĚČKOVÁ, et al. *Učební texty ke specializačnímu studiu pro školní metodiky prevence*. Praha: Centrum adiktologie Psychiatrické kliniky 1. lékařské fakulty a VFN, Univerzita Karlova, 2007, s. 10.
[51] PRŮCHA, J., WALTEROVÁ, E., MAREŠ, J. *Pedagogický slovník. 7.* aktualiz. a rozš. vyd. Praha: Portál, 2013, s. 219.
[52] CHALUPOVÁ, K., ŠTEFUNKOVÁ, M., ŠEJVL, J. *Základy prevence kriminality pro pedagogické pracovníky.* Praha: Klinika adiktologie, 1. lékařská fakulta Univerzity Karlovy v Praze a Všeobecná fakultní nemocnice v Praze. Togga, 2012, s. 11.

způsobu ohrožení apod. Terciální prevence je zaměřena na pachatele, oběti a na místa, kde se kriminalita již odehrává. Jejím cílem je zabránit dalšímu páchání kriminality.[53]

6.1 Základní pravidla pro bezpečné užívání internetu

Dnešní digitální svět nabízí nekonečné možnosti pro vzdělávání, zábavu a komunikaci. S tím však souvisí také bezpečnostní rizika, která mohou postihnout zejména mladistvé osoby a děti. Bezpečné používání internetu je klíčové pro ochranu osobních údajů, duševního zdraví a prevenci kybernetických útoků.[54] Následující body jsou vhodnou primární prevencí v oblasti kyberkriminality.

Vzdělání v oblasti online bezpečnosti

- *Diskuze o různých online hrozbách*. Pravidelné rozhovory s mladými lidmi o různých formách online hrozeb, jako jsou kyberšikana, podvody a škodlivý obsah, jim pomáhají lépe porozumět potenciálním rizikům.
- *Podpora kritického myšlení*. Aktivní podpora rozvoje kritického myšlení umožňuje mladým uživatelům rozpoznat potenciálně nebezpečné situace online a vhodně na ně reagovat.

Nastavení bezpečnostních filtrů a omezení přístupu

- *Rodinné filtry a omezení věkových skupin*. Používání rodinných filtrů a omezení podle věkových skupin pomáhá rodičům kontrolovat přístup dětí k obsahu a zajišťuje, že děti nejsou vystaveny nevhodnému materiálu.
- *Diskuze o nevhodných webových stránkách.* Diskuze s dětmi o důvodech, proč jsou určité webové stránky nevhodné, může podporovat jejich schopnost samostatného rozhodování.

Silné heslo

Použití bezpečného hesla je základem preventivní činnosti na sociálních sítích i v celém kybernetickém prostoru. Silné heslo na sociálních sítích a obecně v kybernetickém prostoru může zabránit mnoha útokům, které mohou mít za cíl odcizení účtu uživatele na dané sociální síti.[55]

[53] CHALUPOVÁ, K., ŠTEFUNKOVÁ, M., ŠEJVL, J. *Základy prevence kriminality pro pedagogické pracovníky*. Praha: Klinika adiktologie, 1. lékařská fakulta Univerzity Karlovy v Praze a Všeobecná fakultní nemocnice v Praze. Togga, 2012, s.15–16.
[54] KOLOUCH, J. CyberCrime. Praha, 2016, s. 172.
[55] KOŽÍŠEK, M., PÍSECKÝ,V. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. s. 36–37.

- *Dvoufázové ověření*. Heslo na sociálních sítích může být posilněno takzvaným dvoufázovým ověřením, které lze nastavit téměř na každé sociální síti. V případě přihlašování se na uživatelský profil z jiného zařízení (z jiného počítače či telefonu kamaráda) sociální síť vyžaduje ověření prostřednictvím kódu zaslaného uživateli na e-mail nebo telefon. V běžném pokusu o nabourání se či odcizení uživatelského účtu toto dvoufázové ověření může překazit nespočet pokusů.[56]

Obezřetnost při sdílení informací

Mladí lidé by měli být instruováni, aby pečlivě vybírali informace, které se rozhodnou sdílet online. Je důležité, aby si byli vědomi možných důsledků při sdílení svých osobních údajů a aby se obrátili na dospělé, pokud mají podezření na nevhodné chování nebo obtěžování.[57]

Ochrana před kyberšikanou

Rodiče by měli být schopni rozpoznat projevy kyberšikany a aktivně komunikovat s dětmi o této problematice. Důležité je, aby mladí uživatelé měli prostor sdílet své zkušenosti a okamžitě informovat dospělé o jakýchkoli projevech kyberšikany.[58]

Monitoring online aktivit

Rodiče by měli využívat nástroje pro sledování online aktivit, aby pravidelně kontrolovali, jaké webové stránky navštěvují jejich děti a jak interagují s ostatními uživateli. Nicméně je také důležité respektovat soukromí dětí a udržovat rovnováhu mezi kontrolou a důvěrou.

Sdílení bezpečných online zážitků

Pojem „sociální síť na internetu“ označuje virtuální propojení lidí a místo, kde uživatelé sdílí své informace. Toto sdílení tvoří jádro sociálních sítí. Mezi nejznámější sociální sítě patří Facebook, Twitter, Snapchat, TikTok, Instagram a mnohé další. Tyto

[56] KOHOUT, R.,KARCHŇÁK, R. *Bezpečnost v online prostředí*. Karlovy Vary: Biblio Karlovy Vary, 2016. s.15–21.
[57]KAMIL, K., SZOTKOWSKI, R., KUBALA. L. *Bezpečné chování na internetu pro kluky a pro holky – náměty na výukové aktivity* [online]. [cit. 2023-12-12]. Dostupné z WWW: https://www.e-bezpeci.cz/index.php/ke-stazeni/tiskoviny/159-bezpecne-chovani-na-internetu-pro-kluky-a-pro-holky-2022/file , s. 23.
[58] KAMIL, K., SZOTKOWSKI, R., KUBALA. L. Bezpečné chování na internetu pro kluky a pro holky – náměty na výukové aktivity [online]. [cit. 2023-12-12]. Dostupné z WWW: https://www.e-bezpeci.cz/index.php/ke-stazeni/tiskoviny/159-bezpecne-chovani-na-internetu-pro-kluky-a-pro-holky-2022/file , s. 35.

platformy umožňují uživatelům virtuální realizaci, sdílení osobních příspěvků a fotografií.[59]

Sociální síť Facebook v 2. kvartálu roku 2023 ohlásila 3 miliardy aktivních účtů. V tomto kontextu je důležité chápat, jaké informace sdílíme online, a vyvarovat se některým rizikům.[60] Mezi informace, které bychom na sociálních sítích zveřejňovat neměli, patří:

- intimní a vztahové problémy,
- fotografie z duchovních akcí,
- nelegální chování uživatele,
- záznamy o aktuální poloze,
- osobní údaje, které by mohly být zneužity,
- čas dovolené,
- intimní fotografie potomků.[61]

6.2 Preventivní programy v ČR

Prevence kybernetické kriminality zahrnuje projekty zaměřené na osvětu dětí i rodičů v oblasti hrozeb na internetu a sociálních sítích. Tyto projekty mají za cíl pozitivně ovlivnit chování uživatelů a zvyšovat povědomí o kybernetických rizicích. Hlavním cílem je posílit celkové povědomí a šířit důležitá pravidla chování na sociálních sítích a v kybernetickém prostoru. Dané aktivity jsou zaměřeny na rozvoj vzdělání v oblasti kybernetické bezpečnosti a na vytvoření bezpečného online prostředí. Podporují tak osvojení klíčových dovedností pro bezpečné a odpovědné chování na internetu.

Mezi tyto projekty patří kampaň „Prokoukl to! A ty?“, která byla spuštěna ve spolupráci s Olomouckým krajem a získala finanční podporu z Programu prevence kriminality na místní úrovni pro rok 2023. Kromě toho jsou dlouhodobě v provozu projekty a kampaně jako „Bezpečně v kyberprostoru“, „Kyberbezpečí a děti v síti“, „Internetem bezpečně“ a „Tvoje cesta onlinem“.

[59] ČERNÁ, M., ČERNÝ, M. *Úvod do problematiky sociálních sítí* [online]. [cit. 2023-12-14]. Dostupné z WWW:http://clanky.rvp.cz/clanek/o/g/15075/UVOD-DO-PROBLEMATIKY-SOCIALNICH-SITI.html/.
[60] HUŠKOVÁ, L. *Facebook překročil hranici 3 miliard uživatelů* [online]. [cit. 2023-12-14]. Dostupné z WWW: https://newsfeed.cz/facebook-prekrocil-hranici-3-miliard-uzivatelu/.
[61] SEXTING. *vše, co chcete vědět o sextingu* [online]. [cit. 2023-12-14]. Dostupné z WWW: www.sexting.cz.

Prokoukl to! A ty?

Kampaň s názvem „Prokoukl to! A ty?“ si klade za cíl informovat veřejnost o aktuálních nástrahách a podvodných praktikách, s nimiž se mohou lidé setkat při komunikaci v online prostředí. Ústřední postavou kampaně je kreslená komiksová postava, sympatický pan Prokoukl, který sám čelí různým nástrahám v kyberprostoru, ale zároveň o nich přemýšlí a dokáže včas rozpoznat, že se bude jednat o něco nekalého. Díky svým správným úvahám a ověřování si informací odhalí podvod dříve, než udělá krok špatným směrem.[62]

Tvoje cesta onlinem

V průběhu roku 2019 vznikl inovativní koncept policejní prevence, spojující stávající aktivity s novými iniciativami. Koncept je strukturován do tří sekcí, přičemž klíčovým zaměřením jsou priority policejního prezidenta: drogová kriminalita, bezpečnost v online prostředí a bezpečnost v dopravě. Zvláště se apeluje na veřejnost, aby byla odpovědná za své vlastní bezpečí, což se týká i rodičů, kteří mají zodpovědnost za bezpečí svých dětí. Sekce „Tvoje cesta onlinem“ se věnuje bezpečnosti v digitálním prostředí. Koncept byl vytvořen ve spolupráci s ČSOB a poskytuje metodiky a návody, určené zejména pro rodiče a děti, jak účinně přistupovat k prevenci kriminality v online prostředí. Tento koncept poskytuje komplexní a moderní přístup k policejní prevenci a reaguje na aktuální výzvy digitální doby.[63]

Bezpečně v kyberprostoru

Projekt „Bezpečně v kyberprostoru“ má ambiciózní cíl omezit šíření nebezpečných počítačových jevů v Jihomoravském kraji, zaměřuje se přitom na uživatele osobních počítačů. V rámci této iniciativy probíhá široké spektrum vzdělávacích aktivit, jako jsou semináře, tvorba metodických DVD pro učitele informačních a komunikačních technologií, natáčení video-spotů, soutěže, výstavy, publikace brožur pro rodiče, letáků a interaktivních komiksů. Projekt rovněž spravuje internetové stránky a facebookový profil a momentálně je v procesu vytváření mobilní aplikace. V Jihomoravském kraji je přes 650 základních a středních škol. V rámci projektu jsou proškolováni ředitelé, učitelé informačních a komunikačních technologií, metodici prevence, žáci a rodiče

[62] VYBÍHALOVÁ, J. *Prokoukl to! A ty*? [online]. [cit. 2023-12-14].
Dostupné z WWW: https://www.policie.cz/clanek/prokoukl-to-a-vy.aspx.
[63] HODÁČKOVÁ, V. *Tvoje cesta* [online]. [cit. 2023-12-16].
Dostupné z WWW: https://www.policie.cz/clanek/tvoje-cesta.aspx.

a v neposlední řadě rovněž Policie ČR, úředníci na obecních úřadech i na krajském úřadě, probační úředníci, pracovníci orgánů sociálně právní ochrany dětí i široká veřejnost.[64]

Kyberbezpečí a Děti v síti

Program „Kyberbezpečí“ předává informace o bezpečném chování na internetu, zejména v rámci sociálních sítí, chatu a dalších veřejných komunikačních prostředků. Jeho zaměření spočívá v uvědomění si rizik virtuální komunikace a v poskytnutí nástrojů k obraně před případným virtuálním či reálným nátlakem.

Program primární prevence „Děti v síti“ je koncipován pro rodiče, učitele a širší veřejnost. Jeho hlavním úkolem je předávat rodičům informace o konkrétních rizicích, jimž jsou děti vystaveny při užívání internetu a při online komunikaci. Tímto způsobem pomáhá vytvářet bezpečnější prostředí pro digitální aktivitu dětí.[65]

Internetem bezpečně

Cílem projektu „Internetem bezpečně“ je, prostřednictvím různorodých vzdělávacích aktivit, zvýšit povědomí uživatelů o rizicích v internetovém prostředí. Projekt aktivně reaguje na nové hrozby v oblasti online bezpečnosti a tyto informace sdílí na svých webových stránkách, facebookovém profilu a prostřednictvím vzdělávacích akcí. Snahou projektu je předcházet potenciálním následkům těchto hrozeb a zároveň snižovat množství protiprávního jednání, které se odehrává v kyberprostoru.[66]

[64] PREVENCE KRIMINALITY. *Bezpečně v kyberprostoru* [online]. [cit. 2023-12-16]. Dostupné z WWW: https://prevencekriminality.cz/bezpecne-v-kyberprostoru/.
[65] PREVENCE KRIMINALITY. *Programy primární prevence „Kyberbezpečí“ a „Děti v síti“* [online]. [cit. 2023-12-16]. Dostupné z WWW: https://prevencekriminality.cz/programy-primarni-prevence-kyberbezpeci-a-deti-v-siti/.
[66] PREVENCE KRIMINALITY. *Internetem bezpečně* [online]. [cit. 2023-12-16]. Dostupné z WWW: https://prevencekriminality.cz/internetem-bezpecne/.

7 Praktická část

Praktická část bakalářské práce je zaměřena na studenty Střední školy polytechnické v Českých Budějovicích a má za cíl prozkoumat jejich zkušenosti a povědomí o kybernetických útocích. Konkrétně se snaží identifikovat, s jakými typy kybernetických útoků se studenti setkávají nejčastěji a jak jsou schopni těmto hrozbám čelit. Na základě zjištěných dat budou navržena konkrétní opatření pro podporu bezpečnějšího chování mladistvých na internetu.

Ke sběru dat byl využit dotazníkový průzkum distribuovaný prostřednictvím internetových stránek přes Google formuláře. Dotazník obsahoval celkem 20 otázek, přičemž u každé otázky bylo možné vybírat z pěti předpřipravených odpovědí. Respondenti měli také možnost poskytnout vlastní odpověď, pokud žádná z předložených možností přesně neodpovídala jejich názoru nebo zkušenostem. Tento přístup umožnil získat detailnější a personalizovanější pohled na problematiku kybernetické bezpečnosti mezi vybranými studenty.

Všichni účastníci byli před vyplněním dotazníku informováni, že jejich odpovědi jsou zcela anonymní a budou využity výhradně pro účely této studie. Kvantitativní výzkumná metoda dotazníkového šetření proběhla v období od 1. ledna 2024 do 1. února 2024, přičemž se podařilo získat 123 řádně vyplněných dotazníků. Shromážděná data budou analyzována pomocí statistické analýzy, což zahrnuje vytváření grafů pro vizualizaci výsledků a interpretaci dat.

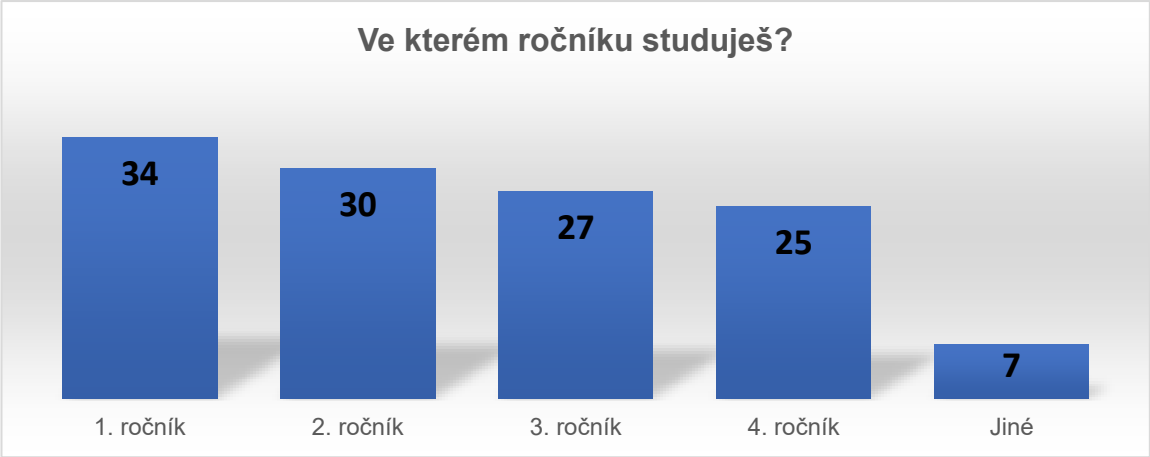
7.1 Stanovené hypotézy

H1: Studenti na Střední polytechnické škole v Českých Budějovicích mají vysokou úroveň znalosti o kybernetických útocích a jsou obeznámeni se všemi riziky spojenými s kyberprostorem.

H2: Škola se snaží o rizicích, která jsou spojená s užíváním internetu, své studenty co nejvíce informovat.

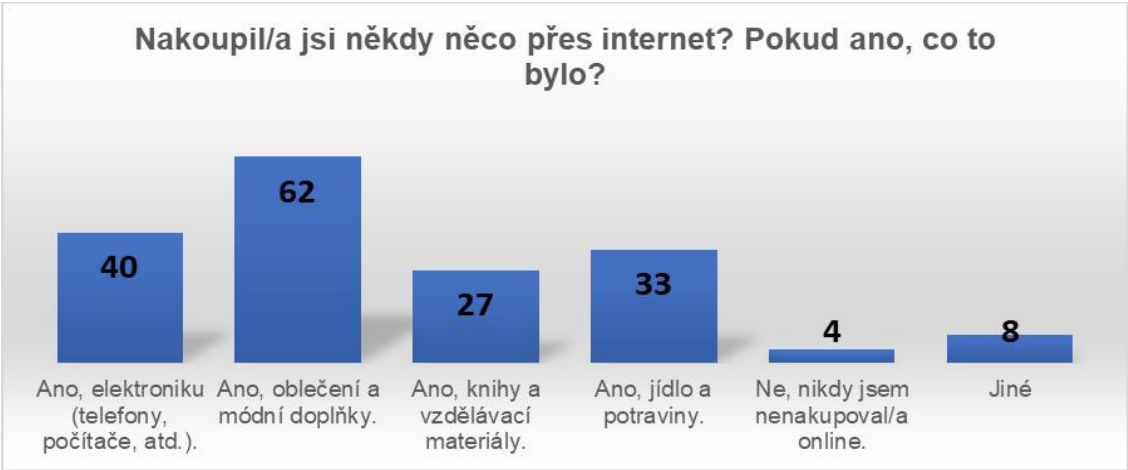
7.2 Vyhodnocení dotazníku

Graf č. 1: Ve kterém ročníku studuješ?[67]



Nejvíce respondentů studuje v 1. ročníku (34), následuje 2. ročník (30), 3. ročník (27) a 4. ročník (25). Dalších 7 respondentů patří do kategorie „jiné“, neboť se jedná o studenty nadstavbových studií, kteří již mají výuční list, ale chtějí si dodělat středoškolské vzdělání zakončené maturitní zkouškou. Jedná se o samostatnou třídu studentů.

Graf č. 2: Nakoupil/a jsi někdy něco přes internet? Pokud ano, co to bylo?[68]



U otázky č. 2 mohli studenti vybrat více odpovědí než jednu, a tudíž zde bylo celkem 170 odpovědí. Nejvíce lidí nakoupilo přes internet oblečení a módní doplňky (62), elektroniku (40), jídlo a potraviny (33), knihy a vzdělávací materiály (27). Pouze 4 respondenti uvedli, že nikdy nenakupovali online. Kategorie „jiné“ zahrnuje

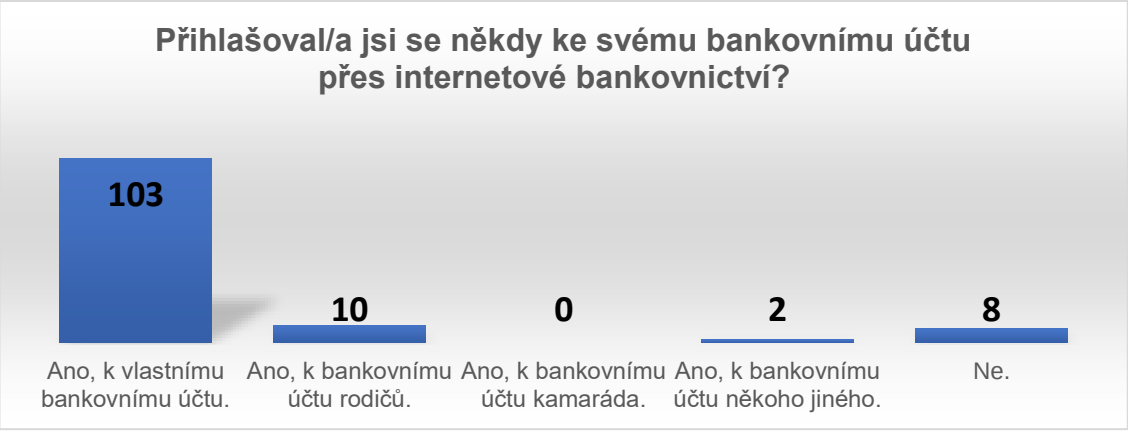
[67] Vlastní zpracování
[68] Vlastní zpracování

8 odpovědí, jedná se například o nákup jízdenek, ubytování či předplatné (Netflix, Spotify).

Graf č. 3: Platil/a jsi někdy platební kartou na internetu? Kde?[69]

U otázky č. 3 mohli studenti vybrat více odpovědí než jednu, a tudíž zde bylo celkem 159 odpovědí. Většina respondentů platila kartou při nákupu na e-shopech (64), za služby (52) či při rezervaci ubytování nebo cestování (30). 7 z nich však nikdy neplatilo online a 6 odpovědí spadalo do kategorie „jiné“, jednalo se mimo jiné o nákup vylepšení do online her, nákup tabákových výrobků a e-booky.

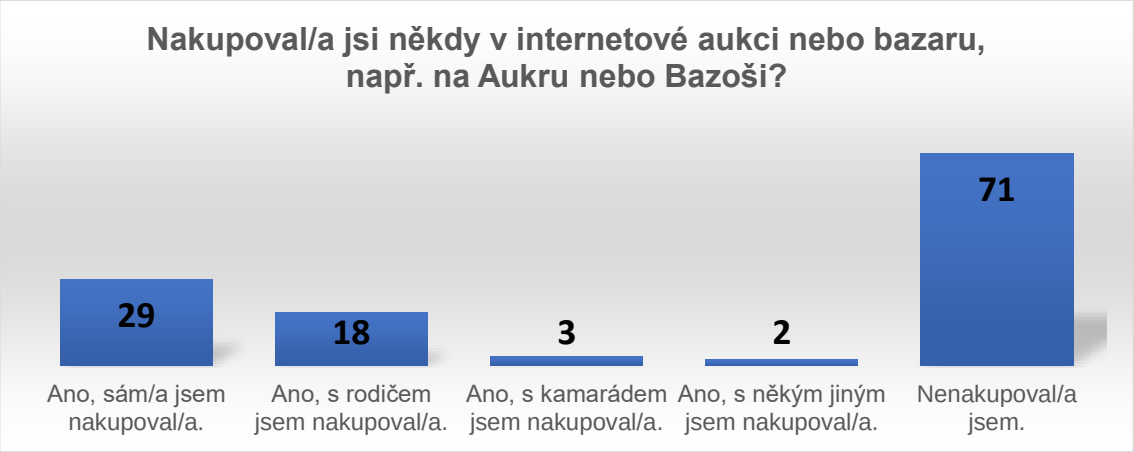
Graf č. 4: Přihlašoval/a ses někdy ke svému bankovnímu účtu přes internetové bankovnictví?[70]



Většina respondentů (103) se přihlašuje k vlastnímu bankovnímu účtu online, 10 se přihlašuje k účtu rodičů a velmi malý počet (2) k účtu někoho jiného. Nikdo neuváděl přihlášení k účtu kamaráda a 8 respondentů uvedlo, že se nikdy nepřihlásili ke svému bankovnímu účtu online.

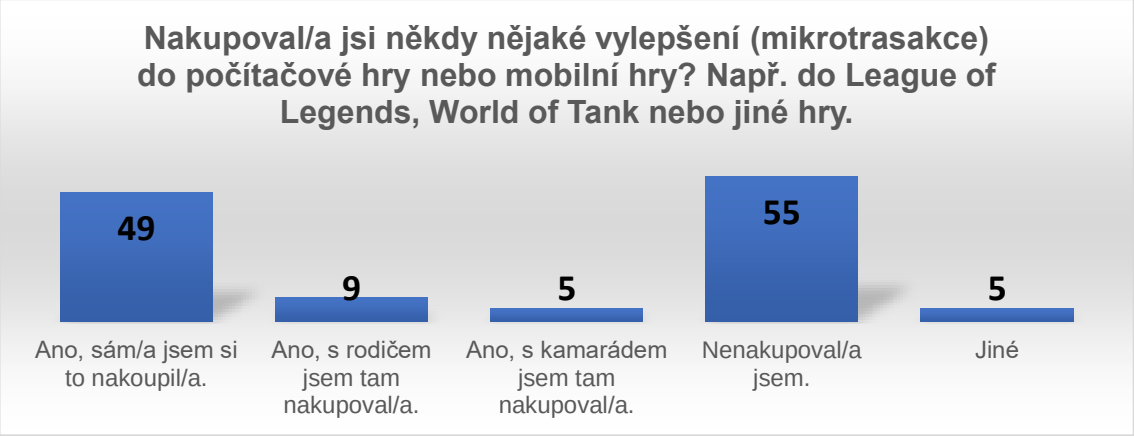
[69] Vlastní zpracování
[70] Vlastní zpracování

Graf č. 5: Nakupoval/a jsi někdy v internetové aukci nebo bazaru, např. na Aukru nebo Bazoši?[71]



Většina respondentů nikdy nenakupovala v internetových aukcích nebo bazarech (71), zatímco někteří nakupovali samostatně (29), s rodičem (18), s kamarádem (3), případně s někým jiným (2). Tito studenti uvedli konkrétně babičku a tetu.

Graf č. 6: Nakupoval/a jsi někdy nějaká vylepšení (mikrotransakce) do počítačové hry nebo mobilní hry? Např. do League of Legends, World of Tank nebo jiné hry.[72]



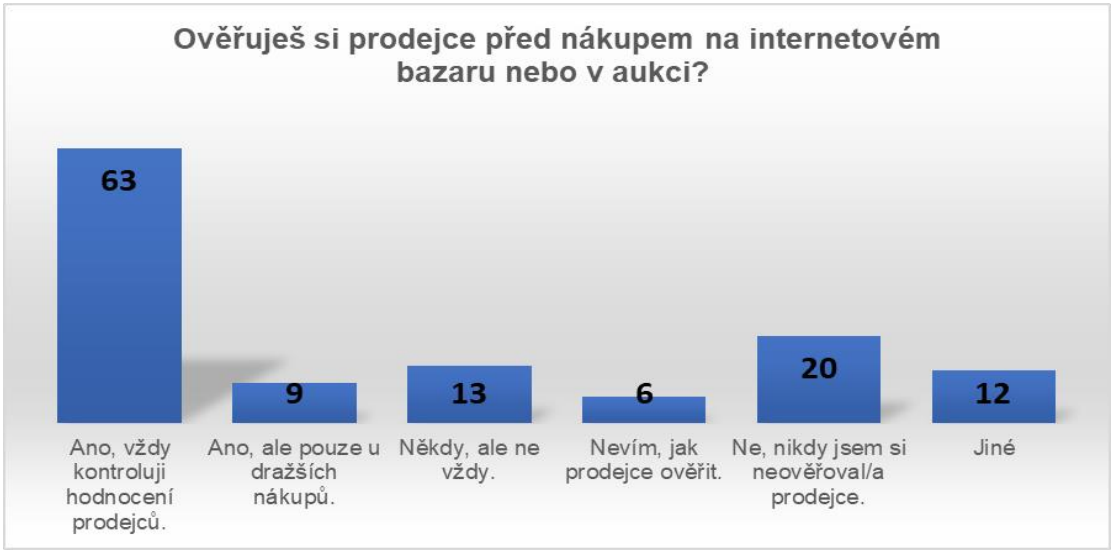
Nejvíce respondentů nekupovalo žádné vylepšení do počítačových her (55), případně jej převážně nakupovali samostatně (49). Menší počet respondentů nakupoval s rodičem (9) nebo s kamarádem (5). Další odpovědi spadají do kategorie „jiné“ (5), kde respondenti uvedli, co přesně si koupili do hry, například vizuální doplňky nebo vylepšení do konkrétní hry.

[71] Vlastní zpracování
[72] Vlastní zpracování

Graf č. 7: Ověřuješ si internetový obchod (e-shop) před nákupem zboží, abys nebyl/a podveden/a?[73]

Nejvíce respondentů vždy kontroluje recenze a hodnocení (53), někteří ověřují pouze neznámé e-shopy (45). Ostatní respondenti (18) to dělají jen někdy, malý počet (4) nikdy e-shop neověřovalo a velmi málo respondentů (3) neví, jak e-shop ověřit.

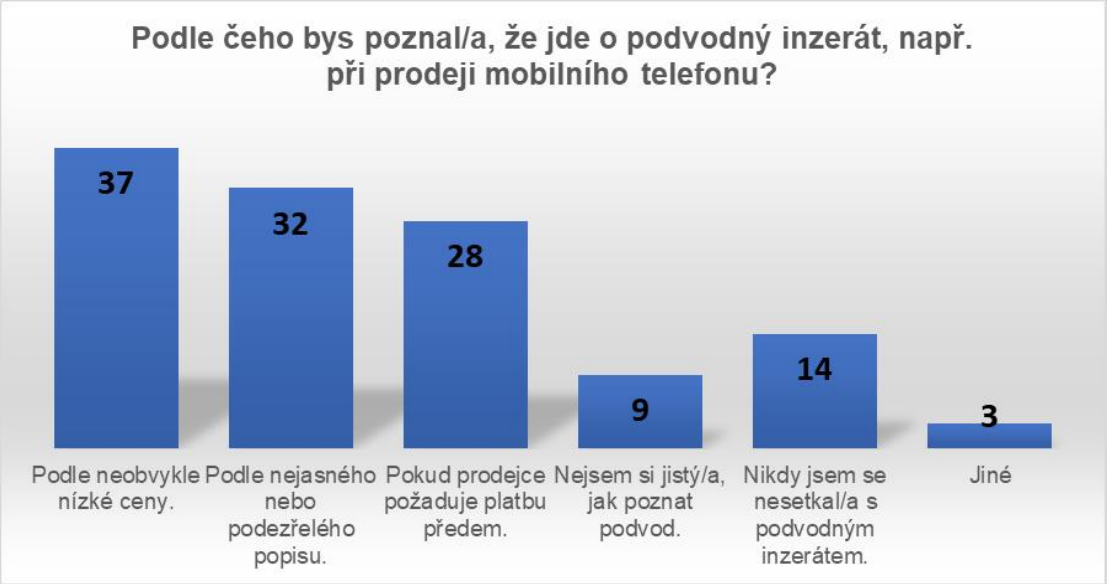
Graf č. 8: Ověřuješ si prodejce před nákupem na internetovém bazaru nebo v aukci?[74]



Většina respondentů (63) vždy kontroluje hodnocení prodejců, velký počet studentů (20) však ověření neprovádí nikdy. Někteří (13) ověřují prodejce jen občas, jiní (9) ho prověřují pouze u dražších nákupů. Malá skupina studentů (6) neví, jak prodejce ověřit. Ostatní odpovědi (12) byly zařazeny do kategorie „jiné“, kde respondenti popsali, co přesně dělají pro ověření, například si daného prodejce zkouší vyhledat ve veřejně dostupných zdrojích nebo ho kontrolují přes sociální síť Facebook.

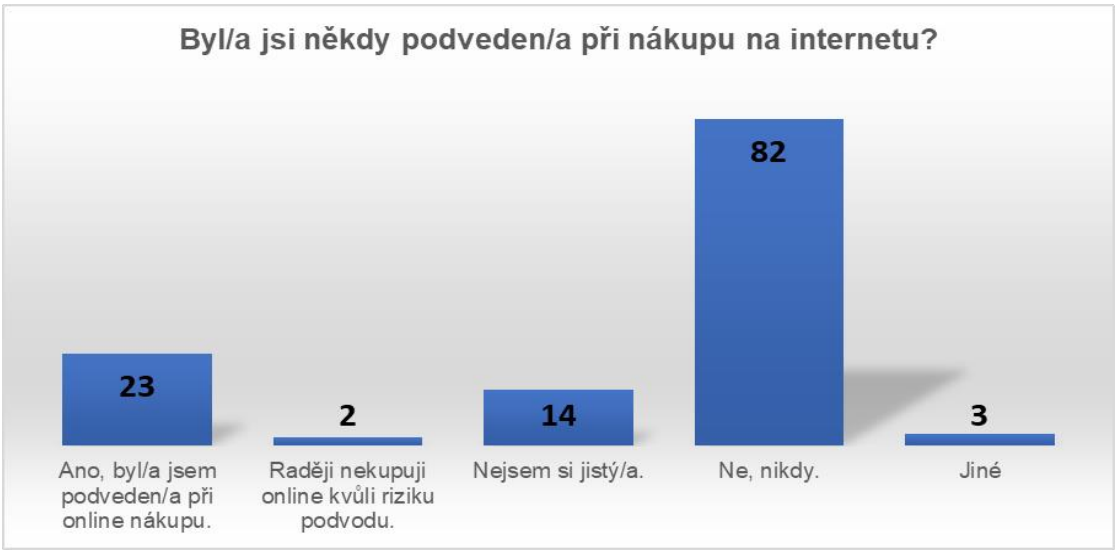
[73] Vlastní zpracování
[74] Vlastní zpracování

Graf č. 9: Podle čeho bys poznal/a, že jde o podvodný inzerát, např. při prodeji mobilního telefonu?[75]



Nejvíce respondentů (37) by podvod poznalo podle neobvykle nízké ceny, další (32) by byli podezřívaví vůči nejasnému nebo podezřelému popisu. Početná skupina respondentů (28) by považovala inzerát za podvodný, pokud by prodejce požadoval platbu předem. 14 studentů uvedlo, že nikdy nenarazili na podvodný inzerát. Někteří respondenti (9) si nejsou jisti, jak podvod poznat. Ostatní odpovědi (3) byly zařazeny do kategorie „jiné“, kde bylo například uvedeno, že podvod byl rozpoznán přes podezřelou internetovou doménu webové stránky.

Graf č. 10: Byl/a jsi někdy podveden/a při nákupu na internetu?[76]



[75] Vlastní zpracování
[76] Vlastní zpracování

Největší skupina respondentů (82) uvedla, že nikdy nebyla podvedena při nákupu na internetu. Značná část studentů (23) však někdy podvedena byla. Někteří (14) si nejsou jisti a menší počet (2) se vyhýbá online nákupům kvůli riziku podvodu. Ostatní odpovědi (3) spadají do kategorie „jiné“, kde respondenti například uváděli, že se obětí podvodu stali jejich rodiče.

Graf č. 11: Přišel Ti někdy nevyžádaný e-mail (spam) od neznámého odesílatele?[77]

Většina respondentů (41) uvedla, že nevyžádaný e-mail (spam) dostává velmi zřídka. Další početná skupina studentů (32) odpověděla, že spam dostávají často, a podobný počet studentů (31) uvedl, že spamové e-maily dostává občas. Menší počet studentů (15) nikdy žádný nevyžádaný e-mail neobdržel. Velmi malá skupina (2) nevěděla, co je to spam, a další (2) odpovědi byly zařazeny do kategorie „jiné“, kde bylo například uvedeno, že se studenti kvůli spamu stali obětí podvodu.

[77] Vlastní zpracování

Graf č. 12: Dostal/a jsi někdy odkaz do mobilu nebo e-mailu, aby ses přihlásil/a někam, např. do banky, na Facebook?[78]

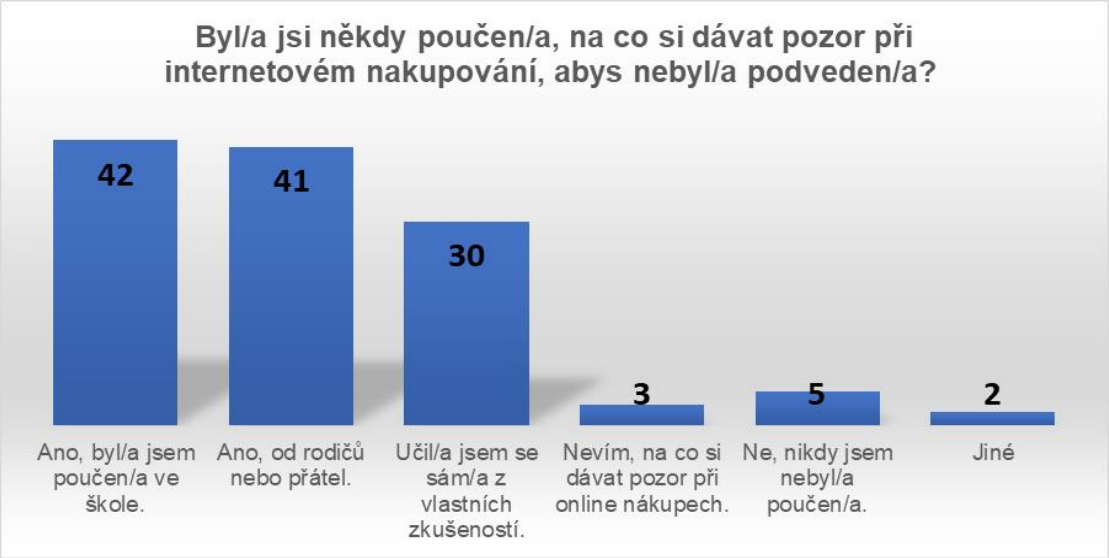
Většina respondentů (65) dostala podvodný odkaz, ale nikdy na něj neklikla. Značná část respondentů (24) nikdy podvodný odkaz nedostala, podobný počet studentů (23) uvedl, že si nejsou jisti. Několik respondentů (9) na podvodný odkaz kliknulo a malý počet (2) neví, jak podvodný odkaz rozeznat.

Graf č. 13: Byl/a jsi někdy vystaven/a pokusu o phishing, např. přes falešný odkaz v SMS nebo messengeru?[79]

[78] Vlastní zpracování:
[79] Vlastní zpracování

Většina respondentů (62) uvedla, že byla vystavena pokusu o phishing, ale poznala to a na odkaz neklikla. Další početná skupina (25) uvedla, že nikdy nebyla vystavena takovému pokusu. Někteří (19) si nejsou jistí, co to phishing je, a malý počet (9) uvedl, že byl obětí phishingového útoku. Podobný počet respondentů (8) neví, jak se phishing projevuje.

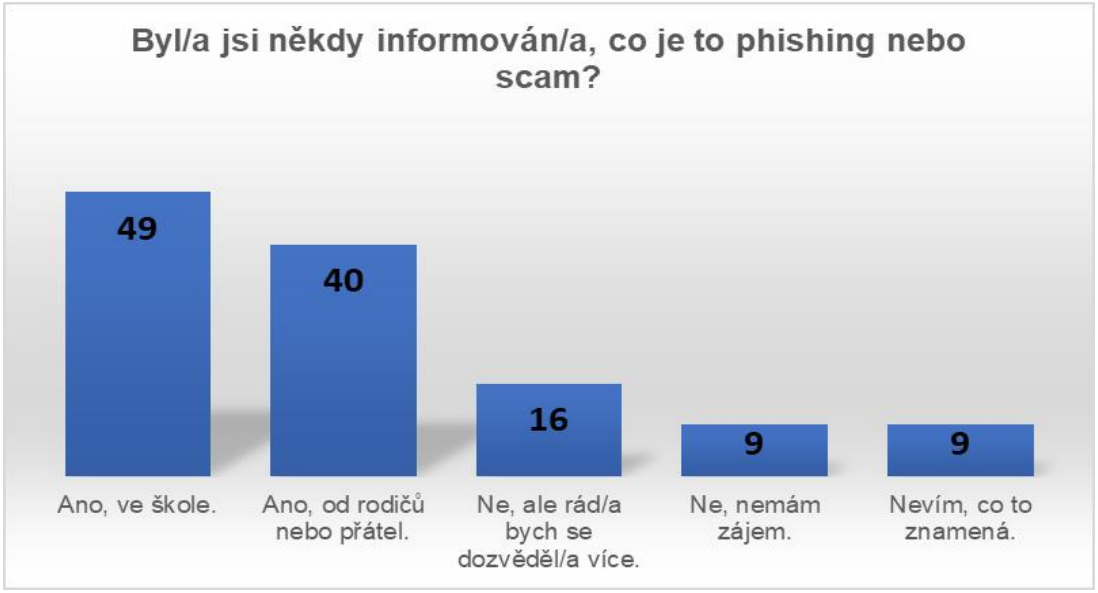
Graf č. 14: Byl/a jsi někdy poučen/a, na co si dávat pozor při internetovém nakupování, abys nebyl/a podveden/a?[80]



Nejvíce respondentů (42) uvedlo, že byli poučeni ve škole. Podobný počet (41) byl informován od rodičů nebo přátel. Další skupina (30) se učila sama z vlastních zkušeností. Malý počet (5) nikdy nebyl poučen, a ještě menší počet (3) neví, na co si dávat při online nákupech pozor. Další odpovědi (2) spadají do kategorie „jiné“, kde například studenti uvedli, že byli s tématem obeznámeni díky YouTube videu.

[80] Vlastní zpracování

Graf č. 15: Byl/a jsi někdy informován/a, co je to phishing nebo scam?[81]



Většina respondentů (49) odpověděla, že byla informována ve škole. Podobný počet (40) byl poučen od rodičů nebo přátel. Další (16) nebyli informováni, ale rádi by se dozvěděli více. Menší počet (9) nemá o toto téma zájem a stejný počet (9) neví, co tyto termíny znamenají.

Graf č. 16: Byl/a jsi poučen/a, jak reagovat na nevyžádaný e-mail nebo na nedovolené vniknutí do tvého účtu na sociální síti?[82]

[81] Vlastní zpracování
[82] Vlastní zpracování

Většina respondentů (60) byla poučena a ví, jak reagovat na nevyžádané e-maily či nedovolená vniknutí na jejich účet. Menší skupina (30) nebyla poučena, ale dokáže se rozhodnout intuitivně. Někteří (15) v této situaci nikdy nebyli, menší počet (14) nebyl poučen a není si jistý, jak v takové situaci reagovat. Velmi malý počet (4) nemá e-mail nebo sociální sítě.

Graf č. 17: Znáš nějakou internetovou stránku, kde si můžeš zjistit hodnocení a recenze e-shopů?[83]

Většina respondentů (50) zná a používá tyto typy webových stránek. Další skupina (33) o takových stránkách ví, ale nepoužívá je. Někteří respondenti (16) nevědí, že něco takového existuje, podobný počet (15) stránky nezná, ale má zájem se dozvědět více. Malý počet (9) o takové informace nemá zájem.

[83] Vlastní zpracování

Graf č. 18: Setkal/a ses někdy s virem (malwarem), který Ti zablokoval zařízení a požadoval zaplacení?[84]

Značná skupina respondentů (40) s malwarem nepřišla do kontaktu, ale ví, jak se bránit. Stejný počet (40) však o malwaru nikdy neslyšel. Další početná skupina (30) nemá s malwarem zkušenost a neví, jak se před ním chránit. Malý počet respondentů (8) se stal obětí malwaru. Ostatní odpovědi (5) spadají do kategorie „jiné“, kde například studenti uvedli, jak se takový malware choval v PC, a jeden ze studentů odpověděl, že zaplatil požadovanou finanční hotovost za odblokování zařízení.

Graf č. 19: Odkud získáváš informace o kybernetických útocích a bezpečnosti na internetu? [85]

[84] Vlastní zpracování
[85] Vlastní zpracování

Nejvíce respondentů (44) získává informace o kybernetických útocích ze sociálních médií, jako jsou Twitter a Facebook. Další skupina (33) čte články a zprávy na internetu. Jiní (19) se o tomto tématu dozvídají prostřednictvím přednášek a kurzů ve škole, menší počet (10) využívá vzdělávací portály a online kurzy. Diskuze s přáteli nebo odborníky v oboru jsou zdrojem pro 15 respondentů a další odpovědi (2) byly zařazeny do kategorie „jiné“, kde byla jako zdroj informací uvedena například videa na YouTube.

Graf č. 20: Žádal tě někdy někdo přes sociální síť o zaslání drobné platby nebo přeposlání kódu z mobilu?[86]

Většina respondentů (50) byla požádána, aby poslala platbu či kód, ale ignorovala to nebo odmítla. Další početná skupina (48) takto nikdy kontaktována nebyla. Malý počet (11) uvedl, že platbu nebo kód poslal. Někteří (10) si nejsou jisti nebo si nemohou vzpomenout, zda se s něčím takovým setkali, a malý počet (4) preferuje na tuto otázku neodpovídat.

7.3 Diskuze

Hodnocení dat naznačuje, že studenti Střední polytechnické školy v Českých Budějovicích mají určitou úroveň povědomí o kybernetických hrozbách a bezpečnostních opatřeních v kyberprostoru. Výsledky odhalují, že většina studentů byla vystavena různým formám kybernetické bezpečnostní edukace, ať už formálně, či neformálně.

[86] Vlastní zpracování: Graf č. 20

H1: Znalosti o kybernetických útocích a rizicích

Při hodnocení první hypotézy (H1), která předpokládá, že studenti mají vysokou úroveň znalosti o kybernetických útocích, je třeba vzít v úvahu velké množství odpovědí naznačujících, že studenti byli informováni o kybernetických útocích buď ve škole (49), nebo rodinou a přáteli (40). 60 respondentů bylo poučeno, jak reagovat na nevyžádané komunikační pokusy. Toto svědčí o základním povědomí studentů o kybernetických hrozbách. Nicméně existuje i několik studentů, kteří nebyli s těmito informacemi dosud seznámeni, tudíž úroveň znalostí není zcela dostatečná.

H2: Informovanost studentů školou

Druhá hypotéza (H2) se týká úsilí školy informovat studenty o rizicích spojených s používáním internetu. Na základě dat je patrné, že škola hraje klíčovou roli v edukaci, neboť 33 respondentů uvedlo, že získali informace o kybernetických útocích ve školním prostředí. Tato čísla, společně s počtem studentů, kteří byli informováni o phishingu ve škole (49), ukazují, že školy se snaží téma bezpečnosti na internetu zařazovat do svých vzdělávacích programů. Přestože je tato snaha zřejmá, zdá se, že škola by mohla zintenzivnit své úsilí o větší osvětu vzhledem k počtu studentů, kteří zůstávají neinformováni nebo si nejsou jistí svými znalostmi.

Na základě analýzy poskytnutých dat lze konstatovat, že hypotéza H1 není potvrzena. I když studenti vykazují určitou úroveň znalostí, nejsou si všichni plně vědomi rizik spojených s kyberprostorem. Hypotéza H2 je potvrzena, protože data ukazují, že škola podniká kroky k informování studentů o kybernetických hrozbách.

Je důležité zdůraznit, že kybernetická bezpečnost není jen otázkou informací, ale také praktických dovedností a zvyků. Vzdělávací programy by měly studenty nejen informovat, ale také trénovat v bezpečných online praktikách, jako je zavádění silných hesel, používání dvoufázové autentizace a pravidelná aktualizace softwaru. Důraz by měl být kladen také na kritické myšlení a schopnost rozpoznat podezřelé chování online, například nevyžádané e-maily nebo zprávy, podvodné webové stránky a neoprávněné pokusy o přístup k účtům.

Významným faktem je, že poměrně velký počet studentů (50) uvádí, že si ověřuje informace o e-shopech před provedením nákupu, což naznačuje proaktivní přístup k online bezpečnosti. Nicméně existuje ještě mnoho studentů, kteří nejsou obeznámeni s riziky nebo nevědí, jak se chránit před potenciálními kybernetickými útoky.

Je třeba podotknout, že vzhledem k dynamické povaze kybernetických hrozeb je nutné, aby školní programy byly pružné a aktualizované a aby reflektovaly neustálé změny v kyberprostoru. To zahrnuje nejen tradiční vzdělávací metody, ale také zapojení studentů do simulací, workshopů a interaktivních diskuzí, které je mohou lépe připravit na reálné situace, s nimiž se mohou setkat online.

Závěr

V bakalářské práci byly podrobně zkoumány zkušenosti studentů Střední školy polytechnické v Českých Budějovicích s kybernetickými útoky s cílem identifikovat nejčastější formy těchto útoků a navrhnout opatření pro bezpečnější chování mladistvých na internetu. Vedlejším cílem bylo analyzovat současný stav a trendy vývoje kybernetických útoků, se zvláštním důrazem na důvody jejich meziročního nárůstu v České republice o 20 %.

Hlavní cíl práce, tedy zjistit zkušenosti studentů s kybernetickými útoky a identifikovat nejčastější formy těchto útoků, byl dosažen prostřednictvím kvalitativního výzkumu. Analýza odpovědí respondentů odhalila, že mnoho mladistvých se již setkalo s různými typy kybernetických útoků, avšak jejich schopnost útoky rozpoznat a adekvátně na ně reagovat je omezená. Nejčastější formy útoků, které byly identifikovány, zahrnovaly phishing a malware, což odpovídá globálním trendům.

Dále bylo v rámci vedlejšího cíle analyzováno, proč meziročně v České republice přibývá 20 % kybernetických útoků. Z této analýzy vyplývá, že za tímto nárůstem stojí nejen technologický vývoj a sofistikovanější metody útočníků, ale také zvýšená aktivita uživatelů na internetu a jejich nedostatečná kybernetická gramotnost. Zvláště v době, kdy digitální prostředí hraje v životech mladistvých stále větší roli, je alarmující, že mnozí z nich nejsou schopni rozpoznat základní hrozby, kterým mohou na internetu čelit.

Na základě těchto zjištění bylo formulováno několik klíčových doporučení. Především je nutné zintenzivnit vzdělávací programy zaměřené na kybernetickou bezpečnost ve školách. Ty by měly být navrženy tak, aby oslovily mladé lidi atraktivním způsobem a zároveň jim poskytly praktické návody, jak se chránit před nejběžnějšími formami kybernetických útoků. Je důležité, aby tyto programy nejen informovaly o potenciálních hrozbách, ale aby také podporovaly vývoj kritického myšlení a sebereflexe u mladistvých, což jsou klíčové dovednosti pro fungování v digitálním světě.

Dále je zásadní posílit spolupráci mezi vzdělávacími institucemi, vládními orgány, neziskovými organizacemi a soukromým sektorem v oblasti kybernetické bezpečnosti. Tato spolupráce by měla vést k vytvoření komplexních strategií, které by adresovaly jak prevenci, tak reakci na kybernetické útoky, a to s důrazem na ochranu mladistvých.

V neposlední řadě je nezbytné zlepšit legislativní rámec ochrany dat a soukromí na internetu s cílem posílit ochranu proti kybernetickým útokům. Tento krok by měl být doprovázen osvětovými kampaněmi, které by informovaly veřejnost o jejích právech a o tom, jak se lidé mohou chránit v digitálním prostředí.

Závěrem lze říci, že bakalářská práce přispěla k hlubšímu porozumění problematice kybernetické bezpečnosti mladistvých a nabídla konkrétní návrhy, jak zlepšit jejich bezpečnost na internetu. Je zřejmé, že v digitálním věku, v němž žijeme, je nezbytné, aby mladí lidé byli vybaveni potřebnými znalostmi a dovednostmi k ochraně svého digitálního já. Pouze tak lze zajistit, že budou schopni čelit výzvám, které s sebou nese stále se vyvíjející kyberprostor.

Seznam použitých zdrojů

Literární zdroje

1. AYCOCK, J. *Spyware and Adware. Springer*. Springer: 2011th edition, 2010, s. 160. ISBN 978-0387777405
2. GŘIVNA, T, POLČÁK R. *Kyberkriminalita a právo.* Praha: Auditorium, 2008, s. 220. ISBN 978-80-903786-7-4.
3. CHALUPOVÁ K., ŠTEFUNKOVÁ M. a ŠEJVL J. *Základy prevence kriminality pro pedagogické pracovníky*. Praha: Klinika adiktologie, 1. lékařská fakulta Univerzity Karlovy v Praze a Všeobecná fakultní nemocnice v Praze ve vydavatelství Togga,2012, s. 105. ISBN 978-80-87258-96-5.
4. JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. s. 284. ISBN 978-80-247-1561-2.
5. KOHOUT, R. a KARCHŇÁK, R. *Bezpečnost v online prostředí*. Karlovy Vary: Biblio Karlovy Vary, 2016. s. 67. ISBN 978-80260-9543-9.
6. KOLOUCH, J a VOLEVECKÝ, P. *Trestněprávní ochrana před kybernetickou kriminalitou*. Praha: Policejní akademie České republiky v Praze, 2013. s. 117. ISBN 978- 80-7251-402-1.
7. KOLOUCH, J. a BAŠTA, P. *CyberSecurity*. Edice CZ.NIC, 20. publikace. Praha: CZ.NIC, z.s.p.o., 2019. s. 556. ISBN 978-80-88168-31-7.
8. KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC., s. 522. ISBN 978-80-88168-15-7.
9. KOŽÍŠEK, M. a PÍSECKÝ, V. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. s, 176. ISBN 978-80-247-5595-3.
10. LAPÁČEK, J. *Poznáváme Internet: rychle hotovo!*. Brno: Computer Press, 2007, str. 212.ISBN 978- 80-251-1781-1.
11. OSTERHOUDT, M. *Computer Health Made Easy V.2 - Beware of the "Wares" Adware, Malware and Spyware*. Lulu Press, Inc, 2013. s. 262. ISBN 978-1300054627.
12. PRŮCHA, J., WALTEROVÁ, E., MAREŠ, J. *Pedagogický slovník, 4. vydání*. Praha: Portál, 2021.s. 328. ISBN 80-7178-772-8.
13. SAK, P. *Úvod do teorie bezpečnosti*. Praha: Nakladatelství PETRKLÍČ s.r.o., 2018. 272 s. ISBN 978-80-7229-652-1.

14. SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. s. 640. ISBN 978-80-7380-501-2.
15. SMEJKAL, V., SOKOL, T., VLČEK, M. *Počítačové právo*. Praha: C.H. Beck Beckova edice právo a hospodářství., 1995. s. 264. ISBN 80-7179-009-5.
16. THOMAS, F. *Adware: The Only Book You'll Ever Need.* Lulu Press, Inc, 2015. s. 49. ISBN 978-1329160330.

Elektronické zdroje

1. AVAST. *Phishing* [online]. [cit. 15.10.2023]. Dostupné z WWW: https://www.avast.com/cs-cz/c-phishing
2. ČERNÁ, M., ČERNÝ, M. *Úvod do problematiky sociálních sítí* [online]. [cit. 2023-12-14]. Dostupné z WWW:http://clanky.rvp.cz/clanek/o/g/15075/UVOD-DO-PROBLEMATIKY-SOCIALNICH-SITI.html
3. *Český statistický úřad* [online]. [cit. 2023-12-04]. Dostupné z WWW:https://www.czso.cz/documents/10180/221256712/08000923.pdf
4. *Český statistický úřad* [online]. [cit. 2023-12-05]. Dostupné z WWW: https://www.czso.cz/documents/10180/221256712/08000923.pdf
5. DAVID, V. *Co je ransomware a jaké škody může napáchat?* [online]. [cit. 2023-11-03]. Dostupné z WWW: https://insmart.cz/co-je-ransomware/
6. *Dodatkový protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů* [online]. [cit. 2023-11-05]. Dostupné z WWW: https://rm.coe.int/16804931bf
7. DVOŘÁK, M. *Phishing, pharming a jejich právní postih*. Trestněprávní revue, číslo 34. 2018, s. 84, [online]. [cit. 2023-10-11]. Dostupné z WWW: http://www.beck-online.cz
8. ESET. *Co je vishing?* [online]. [cit. 2023-12-14]. Dostupné z WWW: https://www.eset.com/cz/vishing/
9. HODÁČKOVÁ, V. *Tvoje cesta* [online]. [cit. 2023-12-16]. Dostupné z WWW: https://www.policie.cz/clanek/tvoje-cesta.aspx
10. HRDINA, R. *Podvody na internetových bazarech* [online]. [cit. 2023-10-12]. Dostupné z WWW: https://www.policie.cz/clanek/podvody-na-internetovych-bazarech.aspx

11. HUŠKOVÁ, L. *Facebook překročil hranici 3 miliard uživatelů* [online]. [cit. 2023-12-14]. Dostupné z WWW: https://newsfeed.cz/facebook-prekrocil-hranici-3-miliard-uzivatelu
12. JIRÁSEK, P., NOVÁK, L., POŽÁR J. *Výkladový slovník kybernetické bezpečnosti* [online]. 2. aktualiz. vyd. Praha: AFCEA, s. 59. Dostupný z WWW: https://afcea.cz/cesky-slovnik-pojmu-kyberneticke-bezpecnosti/
13. KAMIL, K., SZOTKOWSKI, R., KUBALA. L. *Bezpečné chování na internetu pro kluky a pro holky – náměty na výukové aktivity* [online]. Univerzita Palackého v Olomouci, [cit. 2023-12-12]. Dostupné z WWW: https://www.e-bezpeci.cz/index.php/ke-stazeni/tiskoviny/159-bezpecne-chovani-na-internetu-pro-kluky-a-pro-holky-2022/file
14. KAMIL, M. *Smishing* [online]. [cit. 2023-10-15]. Dostupné z WWW: https://www.policie.cz/clanek/uzemni-utvary-sprava-severoceskeho-kraje-zpravodajstvi-smishing.aspx
15. KOFROVÁ, P. *Vishing* [online]. [cit. 2023-10-15]. Dostupné z WWW:https://www.policie.cz/clanek/vishing.aspx
16. KORMOŠOVÁ, I. *Podvody na internetu* [online]. [cit. 2023-10-11]. Dostupné z WWW: https://www.policie.cz/clanek/podvody-na-e-shopech.aspx
17. MARTANOVÁ, V., B. JANÍKOVÁ, T. DANĚČKOVÁ, et al. *Učební texty ke specializačnímu studiu pro školní metodiky prevence*. Praha: Centrum adiktologie Psychiatrické kliniky 1. lékařské fakulty a VFN, Univerzita Karlova, 2007. s. 159. ISBN 978-80-254-0525-3.
18. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2023-11-05]. Dostupné z WWW: https://www.nukib.cz/cs/o-nukib
19. *Národní úřad pro kybernetickou a informační bezpečnost*: Vládní CERT [online]. [cit. 2023-11-05]. Dostupné z WWW: https://www.nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/
20. NGSS. *Zločiny v době moderních technologií: Jak řeší české právo kybernetickou kriminalitu a jak se proti ní bránit?* [online]. [cit.2023-10-08]. Dostupné z WWW: https://www.ngss.cz/clanek/zlociny-v-dobe-modernich-technologii-jak-resi-ceske-pravo-kybernetickou-kriminalitu-a-jak-se-proti-ni-branit-2023-05-16
21. *Odbor obecné kriminality* [online]. [cit. 2023-09-24]. Dostupné z WWW: https://www.policie.cz/clanek/uskpv-ook-odborobecnekriminality.aspx

22. Policie ČR. *Z dlouhodobého pohledu je kriminalita na historicky nejnižší úrovni, má to ale své důvody kybernetická kriminalita má naopak vzestupnou tendenci* [online]. [cit. 2023-12-05]. Dostupné z WWW: https://securityguide.cz/policie-cr-z-dlouhodobeho-pohledu-je-kriminalita-na-historicky-nejnizsi-urovni-ma-to-ale-sve-duvody-kyberneticka-kriminalita-ma-naopak-vzestupnou-tendenci/
23. PREVENCE KRIMINALITY. *Bezpečně v kyberprostoru* [online]. [cit. 2023-12-16]. Dostupné z WWW: https://prevencekriminality.cz/bezpecne-v-kyberprostoru/
24. PREVENCE KRIMINALITY. *Internetem bezpečně* [online]. [cit. 2023-12-16]. Dostupné z WWW: https://prevencekriminality.cz/internetem-bezpecne/
25. PREVENCE KRIMINALITY. *Programy primární prevence „Kyberbezpečí" a „Děti v síti"* [online]. [cit. 2023-12-16]. Dostupné z WWW: https://prevencekriminality.cz/programy-primarni-prevence-kyberbezpeci-a-deti-v-siti/
26. SEXTING. *Vše, co chcete vědět o sextingu* [online]. [cit. 2023-12-14]. Dostupné z WWW: www.sexting.cz
27. *The Latest 2023 Cyber Crime Statistics (updated December 2023)* [online]. [cit. 2023-12-05]. Dostupné z WWW: https://aag-it.com/the-latest-cyber-crime-statistics
28. VOŘÍŠEK, L. *Phishing v praxi, aneb jak jsem nachytal české studenty* [online]. [cit. 2023-10-15]. Dostupné z WWW: https://cdr.cz/clanek/phishing-jak-jsem-nachytal-ceske-studenty-nova-maturita
29. VYBÍHALOVÁ, J. *Prokoukl to! A ty?* [online]. [cit. 2023-12-14]. Dostupné z WWW: https://www.policie.cz/clanek/prokoukl-to-a-vy.aspx
30. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022* [online]. [cit. 2023-10-15]. Dostupné z WWW:https://nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2022.pdf

Legislativní dokumenty

1. ČESKO. Sdělení č. 104/2013 Sb. m. s., o sjednání Úmluvy o počítačové kriminalitě. In *Sbírka zákonů, Česká republika*.2013, částka 56, s. 10785.
2. ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In *Sbírka zákonů, Česká republika*. 2014, částka 75.

3. ČESKO. Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. In *Sbírka zákonů, Česká republika.* 2009, částka 11, s. 354.

Seznam zkratek

1. **IT** – Informační technologie
2. **IP** – Internet Protocol
3. **ISP** – Internet Service Provider
4. **DoS** – Denial of Service
5. **DDoS** – Distributed Denial of Service
6. **Phishing** – Podvodné techniky zaměřené na získání citlivých informací
7. **Malware** – Škodlivý software
8. **Vishing** – Phishing prováděný prostřednictvím telefonních hovorů
9. **Smishing** – Phishing prováděný prostřednictvím SMS zpráv
10. **Pharming** – Podvodná praxe přesměrování uživatelů na falešné webové stránky
11. **DNS Server** – Domain Name System Server
12. **Spyware** – Špehovací software
13. **Adware** – Reklamní software
14. **Keylogger** – Software nebo hardware zaznamenávající stisky kláves
15. **Ransomware** – Typ malwaru, který šifruje soubory oběti a vyžaduje výkupné
16. **ICT** – Informační a komunikační technologie
17. **NCKB** – Národní centrum kybernetické bezpečnosti (specifické pro danou zemi, může se lišit)
18. **CERT** – Computer Emergency Response Team

Seznam obrázků

Seznam tabulek a grafů

Seznam příloh

Přílohy

Příloha – dotazník

Vážení žáci,

v České republice každým rokem narůstá počet podvodů realizovaných prostřednictvím informačních a komunikačních technologií, zejména na internetu. Vzhledem k této rostoucí hrozbě jsem se rozhodl provést dotazníkové šetření zaměřené na zjištění, jak jsou studenti střední školy informováni a připraveni na tato rizika. Vaše odpovědi zůstanou zcela anonymní a jsou klíčové pro lepší porozumění této problematice. Proto Vás prosím o úplné a pravdivé vyplnění tohoto dotazníku. Děkuji za vaši spolupráci.

1. Ve kterém ročníku studuješ? (Zakřížkuj jednu odpověď)

a) 1.ročník
b) 2. ročník
c) 3. ročník
d) 4. ročník
e) Jiné:

2. Nakoupil/a jsi někdy něco přes internet? Pokud ano, co to bylo? (Zakřížkuj jednu odpověď)

a) Ano, elektroniku (telefony, počítače, atd.).
b) Ano, oblečení a módní doplňky.
c) Ano, knihy a vzdělávací materiály.
d) Ano, jídlo a potraviny.
e) Ne, nikdy jsem nenakupoval/a online.
f) Jiné:

3. Platil/a jsi někdy platební kartou na internetu? Kde? (Zakřížkuj jednu odpověď)

a) Ano, při nákupu na e-shopech.
b) Ano, při platbě za služby (streaming, aplikace).
c) Ano, při rezervaci ubytování nebo cestování.
d) Ne, nikdy jsem neplatil/a online.
e) Jiné:

4. Přihlašoval/a ses někdy ke svému bankovnímu účtu přes internetové bankovnictví? (Zakřížkuj jednu odpověď)

a) Ano, k vlastnímu bankovnímu účtu.
b) Ano, k bankovnímu účtu rodičů.
c) Ano, k bankovnímu účtu kamaráda.
d) Ano, k bankovnímu účtu někoho jiného.
e) Ne.
f) Jiné:

5. Nakupoval/a jsi někdy v internetové aukci nebo bazaru, např. na Aukru nebo Bazoši? (Zakřížkuj jednu odpověď)

a) Ano, sám/a jsem nakupoval/a.
b) Ano, s rodičem jsem nakupoval/a.
c) Ano, s kamarádem jsem nakupoval/a.
d) Ano, s někým jiným jsem nakupoval/a.
e) Nenakupoval/a jsem.
f) Jiné:

6. Nakupoval/a jsi někdy nějaké vylepšení (mikrotrasakce) do počítačové hry nebo mobilní hry? Např. do League of Legends, World of Tank nebo jiné hry. (Zakřížkuj jednu odpověď)

a) Ano, sám/a jsem si to nakoupil/a.
b) Ano, s rodičem jsem tam nakupoval/a.
c) Ano, s kamarádem jsem tam nakupoval/a.
d) Nenakupoval/a jsem.
e) Jiné:

7. Ověřuješ si internetový obchod (e-shop) před nákupem zboží, abys nebyl/a podveden/a? (Zakřížkuj jednu odpověď)

a) Ano, vždy kontroluji recenze a hodnocení.
b) Ano, ale pouze u neznámých e-shopů.
c) Někdy, ale ne vždy.
d) Nevím, jak e-shop ověřit.
e) Ne, nikdy jsem si neověřoval/a e-shop.
f) Jiné:

8. Ověřuješ si prodejce před nákupem na internetovém bazaru nebo v aukci? (Zakřížkuj jednu odpověď)

a) Ano, vždy kontroluji hodnocení prodejců.
b) Ano, ale pouze u dražších nákupů.
c) Někdy, ale ne vždy.
d) Nevím, jak prodejce ověřit.
e) Ne, nikdy jsem si neověřoval/a prodejce.
f) Jiné:

9. Podle čeho bys poznal/a, že jde o podvodný inzerát, např. při prodeji mobilního telefonu? (Zakřížkuj jednu odpověď)

a) Podle neobvykle nízké ceny.
b) Podle nejasného nebo podezřelého popisu.
c) Pokud prodejce požaduje platbu předem.
d) Nejsem si jistý/a, jak poznat podvod.
e) Nikdy jsem se nesetkal/a s podvodným inzerátem.
f) Jiné:

10. Byl/a jsi někdy podveden/a při nákupu na internetu? (Zakřížkuj jednu odpověď)

a) Ano, byl/a jsem podveden/a při online nákupu.
b) Raději nekupuji online kvůli riziku podvodu.
c) Nejsem si jistý/a.
d) Ne, nikdy.
e) Jiné:

11. Přišel Ti někdy nevyžádaný e-mail (spam) od neznámého odesílatele? (Zakřížkuj jednu odpověď)

a) Ano, často dostávám spam.
b) Občas.
c) Velmi zřídka.
d) Nevím, co je to spam.
e) Nikdy.
f) Jiné:

12. Dostal/a jsi někdy odkaz do mobilu nebo e-mailu, aby ses přihlásil/a někam, např. do banky, na Facebook? (Zakřížkuj jednu odpověď)

a) Ano, dostal/a jsem podvodný odkaz a kliknul/a na něj.
b) Ano, ale nikdy na ně neklikám.
c) Nejsem si jistý/a.
d) Nevím, jak rozpoznat podvodný odkaz.
e) Ne, nikdy jsem nedostal/a podvodný odkaz.
f) Jiné:

13. Byl/a jsi někdy vystaven/a pokusu o phishing, např. přes falešný odkaz v SMS nebo messengeru? (Zakřížkuj jednu odpověď)

a) Ano, byl/a jsem obětí phishingového útoku.
b) Ano, ale poznal/a jsem to a nekliknul/a.
c) Nejsem si jistý/a, co je to phishing.
d) Nevím, jak se phishing projevuje.
e) Nikdy.
f) Jiné:

14. Byl/a jsi někdy poučen/a, na co si dávat pozor při internetovém nakupování, abys nebyl/a podveden/a? (Zakřížkuj jednu odpověď)

a) Ano, byl/a jsem poučen/a ve škole.
b) Ano, od rodičů nebo přátel.
c) Učil/a jsem se sám/a z vlastních zkušeností.
d) Nevím, na co si dávat pozor při online nákupech.
e) Ne, nikdy jsem nebyl/a poučen/a.
f) Jiné:

15. Byl/a jsi někdy informován/a, co je to phishing nebo scam? (Zakřížkuj jednu odpověď)

a) Ano, ve škole.
b) Ano, od rodičů nebo přátel.
c) Ne, ale rád/a bych se dozvěděl/a více.
d) Ne, nemám zájem.
e) Nevím, co to znamená.
f) Jiné:

16. Byl/a jsi poučen/a, jak reagovat na nevyžádaný e-mail nebo na nedovolené vniknutí do tvého účtu na sociální síti? (Zakřížkuj jednu odpověď)

a) Ano, byl/a jsem poučen/a a vím, jak reagovat.
b) Ne, ale dokážu se rozhodnout intuitivně.
c) Ne, a nejsem si jistý/a, jak reagovat.
d) Nikdy jsem nebyl/a v této situaci.
e) Nemám e-mail nebo sociální sítě.
f) Jiné:

17. Znáš nějakou internetovou stránku, kde si můžeš zjistit hodnocení a recenze e-shopů? (Zakřížkuj jednu odpověď)

a) Ano, znám a používám.
b) Ano, ale nepoužívám je.
c) Ne, ale měl/a bych zájem se dozvědět více.
d) Nevím, že něco takového existuje.
e) Ne, nemám zájem.
f) Jiné:

18. Setkal/a ses někdy s virem (malwarem), který Ti zablokoval zařízení a požadoval zaplacení? (Zakřížkuj jednu odpověď)

a) Ano, stal/a jsem se obětí malwaru.
b) Ne, ale vím, jak se chránit.
c) Ne, a nevím, jak se chránit.
d) Nikdy jsem o malwaru neslyšel/a.
e) Jiné:

19. Odkud získáváš informace o kybernetických útocích a bezpečnosti na internetu? (Zakřížkuj jednu odpověď)

a) Články a zprávy na internetu.
b) Sociální média, jako jsou Twitter, Facebook.
c) Vzdělávací portály a online kurzy.
d) Přednášky a kurzy na škole.
e) Diskuze s přáteli nebo odborníky v oboru.
f) Jiné:

20. Žádal tě někdy někdo přes sociální síť o zaslání drobné platby nebo přeposlání kódu z mobilu? (Zakřížkuj jednu odpověď)

a) Ano, žádal/a a poslal/a jsem platbu nebo kód.

b) Ano, žádal/a, ale já jsem to ignoroval/a nebo odmítl/a.

c) Ne, nikdy mě nikdo takovým způsobem nekontaktoval.

d) Nejsem si jistý/a, nemohu si vzpomenout.

e) Preferuji neodpovídat na tuto otázku.