Univerzita Hradec Králové

Pedagogická fakulta

Ústav sociálních studií

Darknet jako rizikové prostředí pro děti

Bakalářská práce

Autor:	Kristýna Šrámková
Studijní program:	B 7507 Specializace v pedagogice
Studijní obor:	Sociální patologie a prevence
Vedoucí práce:	doc. PhDr. Václav Bělík, Ph.D.
Oponent práce:	Mgr. Martin Knytl, MCS

Hradec Králové 2021

Univerzita Hradec Králové
Pedagogická fakulta

Zadání bakalářské práce

Autor:	**Kristýna Šrámková**
Studium:	P18P0126
Studijní program:	B7507 Specializace v pedagogice
Studijní obor:	Sociální patologie a prevence
Název bakalářské práce:	**Darknet jako rizikové prostředí pro děti**
Název bakalářské práce AJ:	Darknet as a risk place for children

Cíl, metody, literatura, předpoklady:

Bakalářské práce se zabývá informacemi o Darknetu a převádí je do celistvé formy a vytváří tak práci, jež slouží jako účinný nástroj pro základní orientaci v této problematice. V práci je chronologicky popsán vývoj Darknetu a další zásadní události, jež formovaly současnou podobu této sítě. Rovněž mapuje možnosti, kterými se lze na síť dostat, a to především pomocí nejrůznějších prohlížečů. Součástí práce je i poučení o bezpečném pohybu na této síti a o měně, kterou zde uživatelé platí. Další část se zaobírá jednotlivým vrstvami sítě, tedy nelegálním obsahem, který lze na Darknetu nalézt. Zvláštní pozornost se zaměřuje na dětskou pornografii a vykořisťování dětí. V práci jsou rovněž objasněny protiprávní aspekty související s trestnou činností, jež vzniká v případě použití této sítě. Dále jsou rozebírány možnosti identifikace pachatele pomocí útoku na síť Tor. V empirické části práce mapuje tragické případy útoků na děti pod vlivem sítě Darknet. Použitou metodou zkoumání je experiment a rozhovory s rodiči.

Jan. *CyberCrime*. 1. vydání. Praha: CZ.NIC, z.s.p.o., 2016. 522 stran. CZ.NIC; 14. publikace. ISBN 978-80-88168-15-7.

Jan a kol. *CyberSecurity*. 1. vydání. Praha: CZ.NIC, z.s.p.o., 2019. 556 stran. CZ.NIC; 20. ISBN 978-80-88168-31-7.

GAVORA, Peter. *Úvod do pedagogického výzkumu*. 2., rozš. české vyd. Přeložil Vladimír JÚVA, přeložil Vendula HLAVATÁ. Brno: Paido, 2010. ISBN 978-80-7315.

OZKAYA, Erdal a Rafiqul ISLAM. *Inside the Dark Web*. Boca Raton: CRC Press, 2019. 285 stran. ISBN 978-0367236229.

Garantující pracoviště:	Ústav sociálních studií, Pedagogická fakulta
Vedoucí práce:	doc. PhDr. Václav Bělík, Ph.D.
Oponent:	Mgr. Martin Knytl, MCS
Datum zadání závěrečné práce:	20.2.2020

Prohlášení

Prohlašuji, že předložená práce je mým původním dílem, které jsem vypracoval(a) pod vedením vedoucího bakalářské práce doc. PhDr. Václav Bělík, Ph.D. Veškerou literaturu a další zdroje, z nichž jsem při zpracování čerpal(a), v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Hradci Králové dne 30. 5. 2021 _____

Kristýna Šrámková

Poděkování

Touto cestou bych ráda poděkovala vedoucímu mé bakalářské práce doc. PhDr. Václavu Bělíkovi, Ph.D. za odborné vedení a ochotu, kterou mi v průběhu zpracování bakalářské práce věnoval. Mé poděkování patří též účastníkům dotazníkového šetření a interview. Dále bych chtěla poděkovat Bc. Jakubovi Černému, který mi pomohl bezpečně prozkoumávat odvrácenou stranu sítě Dark web. Na závěr děkuji mé rodině za jejich podporu během celého mého studia.

Anotace

ŠRÁMKOVÁ, Kristýna. *Darknet jako rizikové prostředí pro děti*. Hradec Králové: Pedagogická fakulta Univerzity Hradec Králové, 2021. 84 s. Bakalářská práce.

Bakalářská práce na téma Darknet jako rizikové prostředí pro děti je členěna do šesti kapitol, přičemž prvních pět kapitol zahrnuje poznatky především z odborné literatury a cizojazyčných článků. V teoretické části jsou rozebírány jednotlivé vrstvy internetu spolu s chronologickým vývojem Dark webu a událostmi, jež formulovaly jeho současnou podobu. Dále jsou popsány možnosti bezpečného připojení se k této síti, které současně slouží jako prevence, napomáhající k minimalizaci rizik, jež návštěva Dark webu obnáší. Pozornost je rovněž soustředěna na možnosti ochrany dětí před touto sítí, a to zejména prostřednictvím nejrůznějších nástrojů. Nemalá část práce mapuje sexuálně orientovaný obsah, který je primárně zaměřen na dětskou pornografii. Závěrečná kapitola je věnována vlastnímu výzkumnému šetření. Empirická část práce se dělí na dvě části. První empirická část si klade za cíl zmapovat aktivitu uživatelů na Dark webu prostřednictvím dotazníkového šetření. Druhá empirická část zprostředkovává podrobnější náhled do problematiky prevence v kybernetickém prostoru prostřednictvím strukturovaného rozhovoru, v jehož rámci byly poskytnuty čtyři rozhovory.

Klíčová slova: Dark web, internet, kyberkriminalita, prevence, dětská pornografie

Annotation

ŠRÁMKOVÁ, Kristýna. *Darknet as a risk place for children*. Hradec Králové: Faculty of Education, University of Hradec Králové, 2018. 84 pp. Bachelor Degree Thesis.

This bachelors thesis is divided into six chapters. The aim of this thesis was to describe the generoul principles about the Dark web. The first chapters describe the development of such a dirty and dangerous place as darkweb undoubtedly is. Connecting to the darkweb is very risky. However, this work describes possible connection methods. Personally, I do not recommend anyone to connect. Also there is describe in detail the content that visitior can find, for example child pornography, sale of drugs and weapons.

The experimental part deals with the personal experiences, which were gained from connecting to the darkweb. The final chapter is devoted to the sophisticated research. The constructed questionnaire found out what users do on the Dark web. Also there are interviews from the four strangers, who reveal their view on the cybernetic space.

Keywords.: Dark web, internet, cybercrime, prevention, child pornography

Prohlášení

Prohlašuji, že bakalářská práce je uložena v souladu s rektorským výnosem č. 13/2017 (Řád pro nakládání s bakalářskými, diplomovými, rigorózními, disertačními a habilitačními pracemi na UHK).

Datum:…… Podpis studenta:……

Obsah

Úvod

Bakalářská práce se zabývá nebezpečným kybernetickým prostorem zvaným Dark web. Pro pohodlnější orientaci v problematice jsou v teoretické části zevrubně charakterizovány jednotlivé vrstvy internetu od World Wide Webu po Shadow web. V práci je též chronologicky popsán historický vývoj sítě spolu se zásadními událostmi, jež formulovaly její současnou podobu. Kapitola zabývající se specifikací Dark webu je primárně zaměřena na informace a praktické rady pro pohyb na této síti, jež slouží jako prevence a zároveň napomáhají k minimalizaci rizik. Přestože práce mapuje možnosti, kterými se lze na Dark web dostat, a to především skrze nejrůznější prohlížeče, důrazně nedoporučuji se k této síti připojovat. Jako jeden z možných příkladů pro pohyb na síti je v práci představen nejpopularizovanější internetový prohlížeč TOR. Pro co možná nejbezpečnější pohyb je v teoretické části též objasněn princip fungování služby VPN. Kapitola pojednávající o ochraně dětí před Dark webem mapuje tragické případy a taktéž popisuje způsoby, jimiž rodiče mohou napomoci zajistit bezpečí svých dětí v online prostoru. Pozornost je rovněž soustředěna na sexuálně orientovaný obsah, jenž je primárně zaměřen na dětskou pornografii a vykořisťování dětí. Cílem bakalářské práce je zmapovat kybernetický prostor Dark web jakožto místo, jež představuje možné riziko pro děti a dospívající.

Empirická část práce se dělí na dvě sekce. První část je zaměřena na aktivitu uživatelů Dark webu. Tento úsek práce si stanovuje za cíl zjistit jaké aktivity zde čeští a zahraniční uživatelé provozují a zda je jejich návštěva pouhým jednorázovým aktem, nebo rutinní záležitostí. Lze se domnívat, že pro většinu respondentů byla návštěva Dark webu jednorázovou akcí a návrat do budoucna nebudou zvažovat. Taktéž je pravděpodobné, že nejvyhledávanějším obsahem budou webové stránky zaměřené na prodej drog a zbraní.

V druhé sekci bylo v návaznosti na zpracovanou teoretickou část realizováno vlastní výzkumné šetření, kterého se účastnili absolventka oboru sociální patologie a prevence, příslušníci policie ČR a IT specialista. Za pomoci kvalitativního způsobu zkoumání, respektive polostrukturovaného rozhovoru, je v práci mapován pohled jednotlivých účastníků interviewu na prevenci v kybernetickém prostoru.

Práce vychází především ze zahraničních zdrojů, jelikož se v českém prostředí touto problematikou zaobírá pouze hrstka odborníků.

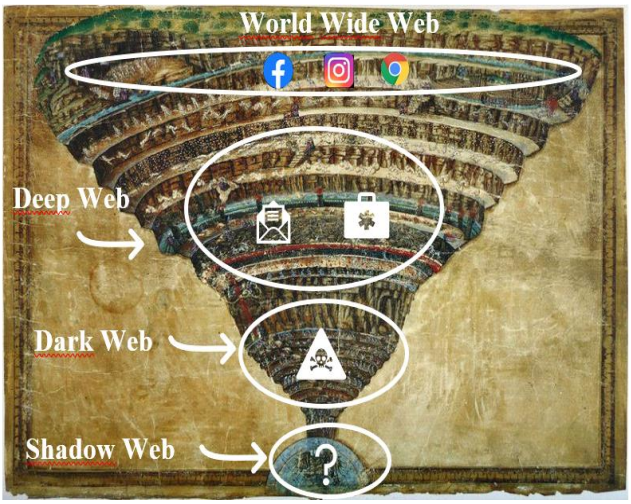
1 Internet a jeho složky, jako rizikové prostředí pro děti

Žijeme v digitální době, a ať už to vnímáme více, či méně, digitální revoluce se týká každého z nás. Naše společnost je založena na vzájemné komunikaci, proto lze internet označit za jeden z největších výdobytků lidstva. Pro moderního člověka má tento vynález nevyčíslitelnou hodnotu. Samotná komunikace nebyla s příchodem internetu nikdy snazší, na tomto místě je dlužno dodat, že ačkoliv je komunikace pohodlnější, aspekty lidského chování se velmi rychle transformují a dochází k útlumu našich sociálních dovedností. Digitální revoluce jistě poskytuje nezměrné možnosti benefitů, přesto je však více než žádoucí porozumět silám, které určují způsoby, jakými nás technologické možnosti skutečně ovlivňují.

Internet lze chápat jako jakousi digitální verzi světa, v němž žijeme. Takovýto svět se může na první pohled zdát jako vcelku bezpečné místo, ale čím hlouběji onen svět objevujeme, tím více znepokojující se nám může jevit. Samotný internet bych přirovnala k Danteho ztvárnění pekla (viz obrázek č. 1), jenž se skládá z několika soustředěných kruhů sestupujících až k samotnému padlému andělu Luciferovi.

Dostat se k pomyslnému Luciferovi není nikterak náročné. Pokud hovoříme o Dark webu, lze velmi snadno propadnout představě, že se jedná o nedostupné a utajované místo v hlubinách kybernetického prostoru.

Dominik Stroukal ve své publikaci výstižně uvádí, že Darknet nelze přirovnávat k jakési utajované zprávě v trezoru na dně oceánu, nýbrž k rádiovým vlnám, existujícím všude kolem nás, aniž bychom o nich věděli. Pokud toužíme zjistit, jaký obsah přenášejí, pak pouze stačí pořídit si vhodný radiopřijímač. (Stroukal, 2020, s. 9)



Obrázek č. 1 - **Vrstvy internetu**

World Wide Web

Jedná se o celosvětovou veřejnou počítačovou síť, jež je kooperací nejrůznějších organizací, které spojily své vlastní počítačové sítě do jedné globální. (Wittmann, Bukovanský, 1998, s. 7)

Tato část sítě bývá známa pod názvem viditelný web, surface web nebo také indexový web, který je snadno dostupný skrze standardní vyhledávače, jako jsou Yahoo, Bing nebo Google. Jedná se o nejméně objemnou část internetu, zabírající pouhá 4 % z celkového kybernetického prostoru. Tento fakt je více než šokující, při představě množství informací, jež se nacházejí v tak malém procentu. Jako příklad bych ráda uvedla internetový prohlížeč Google, který při každém vyhledávání najde přes milión výsledků. Sussman uvádí, že nelegální činnost je zde v porovnání se zbytkem internetu malá. (Sussman, 2018, online; Sabarinath, 2019, online)

Ačkoliv internet pokrývá téměř celý svět, nejedná se o byrokratickou organizaci „sešněrovanou“ striktními předpisy. Popis metod vzájemné komunikace, a to na všech úrovních, u nichž bychom očekávali závazně platné normy (nezbytné pro to, aby se jednotlivé komponenty „domluvily“), jsou celosvětově známé pod názvem RFC (Request For Comments). Termín, jenž je téměř vždy zkracován na pouhá tři písmena, přitom označuje dokumenty o důležitosti srovnatelné s ústavou či zákony. Veškeré RFC dokumenty lze nalézt na běžném internetu. (Berka, 1996, s. 10)

Dlužno dodat, že se v rámci internetu utvořily takzvané darknety neboli temné sítě. Tyto darknety prezentují sítě, ke kterým se lze připojit skrze speciální software, například prohlížeč Tor, ale i jiné. Opakem darknetů jsou clearnety, tedy nikoliv temné sítě, ale jak název napovídá, sítě čisté. (Stroukal, 2020, s. 20)

Deep Web

Deep web tvoří největší část internetu, respektive 90 %, a nachází se těsně pod povrchem celosvětového webu. Pohyb v této části sítě začíná být složitý, jelikož na rozdíl od povrchového webu není indexován pomocí „běžných“ vyhledávačů. Většinu obsahu, jež je skryta před zrakem vyhledávačů, nelze označit za nelegální. A dle nejrůznějších odhadů ve skutečnosti ani nelegální není. Patří sem vyjma nelegálního obsahu také všechny e-maily, soukromé konverzace na Facebooku, neveřejné statusy na sociálních sítích nebo fóra, k nimž je zapotřebí hesla. (Stroukal, 2020, s. 19-20)

Uživatel zde může narazit na věci, jako jsou osobní lékařské údaje, webové stránky s předplatným, legální dokumenty atd. Většina těchto dat bývá šifrována, nelze je tedy vyhledávat, ovšem důvodem není skrývání nelegální činnosti, ale jde zde o chránění důvěrných informací před širší veřejností. Obsah hlubokého webu může být přístupný URL nebo IP adresou a jednotlivé stránky zde mohou vyžadovat heslo či jiný bezpečnostní přístup. (Zambuto, 2018, online; Varma, 2018, online)

Zdroje Deep webu lze rozdělit do následujících kategorií:

a) Dynamický obsah je tvořen dynamicky generovanými stránkami, jež požadovanou informaci vrátí pouze na základě přímého dotazu (vyplnění vyhledávacích polí) a které jsou dostupné prostřednictvím formuláře. Takovýto obsah je takříkajíc „uzamčen“ v databázích (komerční databázová centra, digitální knihovny, online katalogy). Vyjma výše zmíněného zde mají své místo i institucionální zdroje citlivé na ochranu, elektronické časopisy, knihy a sborníky, na které se vztahují autorská práva a jejichž obsah je zpoplatněn. (Kuželíková, Nekuda, Poláček, 2008, s. 28)
a) Neprolinkovaný obsah zahrnuje stránky, na které není odkazováno a jsou nedostupné pro roboty, kteří indexují webový prostor. (Kuželíková, Nekuda, Poláček, 2008, s. 28)
b) U soukromých webů, kde jsou zdroje chráněné heslem, je vyžadována registrace a následné přihlášení. (Kuželíková, Nekuda, Poláček, 2008, s. 28)
c) Obsah s omezeným přístupem zahrnuje i to, co není v běžném textovém formátu (HTML, DOC, PDF apod.). Obsah bývá kódován do multimediálních souborů (obraz nebo video), či je uložen ve specifických formátech. (Kuželíková, Nekuda, Poláček, 2008, s. 28)

Za hlavní rysy Deep webu lze dle Bergmana považovat:

a) Za zcela zásadní rys Bergaman považuje samotný rozsah Deep webu. Bergman uvádí, že 60 nejrozsáhlejších databázových center soustřeďuje přibližně 750 TB informací, toto množství dat pro představu 40x přesahuje velikost běžně dostupného internetu neboli Indexového webu.
b) Deep web je nejrychleji se rozrůstající oblastí nových informací na internetu.
c) Více než polovina obsahu na Deep webu je veřejně přístupná a nezpoplatněná. (Kuželíková, Nekuda, Poláček, 2008, s. 27)

Dark Web

Nyní přecházíme k poslední, a tudíž nejhlouběji se nacházející části sítě, jíž bude věnována většina bakalářské práce. Temný web je součástí Deep webu, na který se přistupuje skrze darknety a tvoří zbývajících 6 % kybernetického prostoru. Setkáváme se zde s obdobnou situací jako u Deep webu, respektive tato síť není taktéž indexována pomocí vyhledávačů. Pro připojení je zcela nezbytné obstarat si speciální prohlížeč nebo jiný nástroj umožňující přístup k vyhledávanému obsahu. Na základě zjištěných informací lze stanovit závěr, že převážně se používá prohlížeč TOR (The Onion Router), který zajistí uživateli Dark webu „bezpečný“ pohyb na síti pomocí šifrování internetového provozu přes nejrůznější vrstvy. Tento kybernetický prostor je znám jako útočiště pro nejrůznější kybernetickou trestnou činnost. (Zambuto, 2018, online)

Mnohdy se lze setkat s nepřesnými definicemi, které tvrdí, že Dark web je ta část Deep webu, ve které se provozují pouze nelegální činnosti. Jedná se o velmi častou definici, která ovšem není zcela správná. Nelegální činnost se odehrává mnohdy i na indexovém webu, kupříkladu když někdo na bazaru prodává věci, které odcizil. A ještě častěji na Deep webu, kde lidé mezi sebou obchodují s nelegálním zbožím skrze sociální sítě či e-mail. Kromě toho se lze na Dark webu setkat i s legální činností. Ostatně svou webovou stránku zde má i CIA. (Stroukal, 2020, s. 21)

V rámci Dark webu lze nalézt nespočet stránek, kde probíhají obchody s legálními komoditami (kryptoměna), ale uživatelé zde narazí zejména na obchodování s nelegálními komoditami (drogy, zbraně, odcizené údaje, pornografický materiál atd.) Kromě uzavírání nelegálních obchodů lze na Dark webu narazit také na poskytování nelegálních služeb, jakými jsou hacking nebo vraždy na objednávku. Co se týče nájemných zabijáků, je otázkou, zda se nejedná o pouhý hoax a snahu vylákat z potencionálních zájemců nemalé obnosy bitcoinů. Přinejmenším u nájemného hackingu se ale s největší pravděpodobností nejedná pouze o fámy. V souvislosti s hackingem se vyskytly domněnky, které předkládají, že krachující finanční ústavy zejména v Rusku využívají hackerské útoky k tomu, aby utajily předchozí úmyslné či nedbalostní delikty. Tuto myšlenku nelze vyloučit, a to také ani u jiných nežli finančních institucí. (Smejkal, 2018, s. 82)

Deep web a Dark web jsou nová *terra incognita*. Navzdory významným krokům, které lidstvo učinilo při mapování fyzického světa, stále na nás čeká nespočet neprobádaných míst, která doposud nebyla plně zdokumentovány. Podobně tomu je

i u kyberprostoru. A přesto, jak se rozšiřuje pomyslný ostrov našeho vědomí, rozšiřuje se i naše nevědomost. Je důležité si uvědomit, že s výkonnými prohlížeči, jakými jsou Google či Bing, máme k dispozici jen malý zlomek na povrchu enormního datového oceánu. Ve skutečnosti na nás čeká stále neprobádaná *terra incognita*. (Smejkal, 2018, s. 83)

Shadow Web

Za nejkontroverznější vrstvu lze označit Shadow web, který se má údajně nacházet ještě o něco hlouběji než již zmiňovaný Dark web. Předpokládá se, že by zde mělo docházet ještě k závažnějším trestným činnostem. V případě, že uživatel vstoupí do kybernetického prostoru Dark webu, nalezne zde spoustu reklam, jež klamou falešnou nabídkou propagující přístup do této části sítě výměnou za bitcoiny. Ovšem tento podvod je již pro většinu uživatelů známý. Tento fakt přispívá k hanobení kryptoměny, která sama o sobě není pro společnost škodlivá. Koncept Shadow webu je horlivě diskutován na nejrůznějších fórech, jako je například Reddit. Spousta světových vědců v oblasti kybernetické bezpečnosti hlásá, že Shadow web není nic jiného než zvěst. Pokud zatím tato část webu není reálná, neznamená to, že by v budoucnu nemohla být. (Cihodariu, 2019, online)

Světlá stránka Dark webu

Jak již bylo zmíněno výše, veškerý obsah a činnosti na Dark webu nejsou nelegální. Prvotním záměrem tvůrců Dark webu nebylo páchat zlo, pouze vytvořili prostor neomezené komunikace bez cenzur a zábran, zkrátka bezpečnou a zcela anonymní digitální síť. Dark web slouží jako komunikační kanál pro občany, v jejichž zemi je potlačována svoboda slova. Anonymitu, jež nabízí Tor, zprostředkovává aktivistům možnost zveřejnit zprávy z totalitních režimů, které je utlačují a každodenně ohrožují jejich životy. Jedním z příkladů pozitivního užitku z Dark webu je takzvané arabské jaro. Lze konstatovat, že bez podpory této sítě by protestanti nedosáhli takové dynamiky a posunu. Pro tyto lidi se Dark web stal takříkajíc záchranným kruhem. Dále je tato síť využívána v zemích, kde je přístup k internetu přísně kriminalizován. K nalezení je zde nespočet užitečných informací a webových stránek. Uživatel na tomto místě narazí na veškeré informace týkající se ochrany soukromí a kryptoměny. Existuje celá škála privátních a šifrovaných e-mailových služeb, instrukce k instalaci anonymního operačního sytému a pokročilé rady pro ochranu soukromí. Obzvláště přínosná je pak možnost dohledání kompletních vydání těžko dostupných publikací a taktéž souborů politických zpráv. Na Intel Exchange se vedou anonymní diskuze na aktuální témata a konspirační teorie (Co Vám Google neřekl, Oblast 51, Rakovina: konspirace a vyléčení atd.). Darknet taktéž slouží disidentům, whistleblowerům či investigativním novinářům jako prostředek pro chráněnou komunikaci. Nechybí zde ani „temná“ verze Facebooku, kde se uživateli skýtá možnost komunikace pod rouškou anonymity. Přestože má uživatel možnost navštívit nespočet legálních a mnohdy i přitažlivých stránek, musí mít neustále na paměti, že se stále nalézá na místě, které se neřídí žádnými předpisy. (PS21, 2015, online; Guccione, 2019, online; Salát, 2017, online)

2 Historie Dark webu

Počátky

Historie skrytého webu se datuje již od počátku samotného internetu. Za zcela klíčový moment lze označit 29. říjen roku 1969. V tento den mladý student kalifornské univerzity v Los Angeles (UCLA) poslal první elektronickou zprávu mezi počítači. Pro tento přenos zvolil systém známý pod názvem ARPANET. Koncept ARPANET je akronym pro název Advanced Research Projects Agency Network. Jednalo se o pojmenování grantové agentury ministerstva obrany USA, která v počátcích ARPANET finančně podporovala. Nutno dodat, že Dark web tak, jak ho známe nyní, nebyl ve svých počátcích součástí ARPANETU. Nicméně netrvalo dlouho a lidé začali tuto technologii využívat pro své záležitosti, jež chtěli uchovat v tajnosti. Za zcela první online aukci uskutečněnou skrze tuto síť je považován prodej konopí počátkem 70. let. Tuto událost mají na svědomí mladí studenti Stanfordu. (Aira group, 2016, online; Butler, 2018, online; Breeding, 2016, online)

80. léta

Internet v období osmdesátých let je typický svou nedosažitelností, neboť pro běžného občana je přístup k němu stálé pouhým snem. Lidé si začali uvědomovat svou bezbrannost, která je vystavovala stále častěji svízelným situacím, jelikož ukládaní citlivých a nezákonných dat se zdálo být prakticky nemožné. Internet byl i nadále otevřeným prostorem, což značně komplikovalo vyhýbání se transparentnosti. Uživatelé se snažili této situaci vyhnout, a tak vyvinuli takzvané „datové ráje“. Místo, jež umožní ukládat citlivé informace tak, aby byly co nejlépe skryté od všetečných očí úřadů. Značné množství datových rájů se nacházelo na Karibských ostrovech, konkrétně v Anguille, a v mnoha hlediscích se jejich princip fungovaní podobal daňovým rájům. Princip rájů spočíval v jejich umístění, neboť spadaly mimo jakoukoli hlavní zemi, tudíž zde platila jiná pravidla, a lidé se tak mohli vyhnout určitým zákonům. (Breeding, 2016, online; Butler, 2018, online)

90. léta

V devadesátých letech se síť World Wide Web dostává významně do popředí digitálního dění. Za tento posun vděčí především webovým technologiím, jakými jsou HTTP a FTP současně s grafickými počítači, které dovedou spravovat webový prohlížeč.

Konec devadesátých let lze z hlediska digitálního odvětví označit za průlomový. Dochází k technologickému posunu, který zprostředkuje sdílení značného množství dat peer-to-peer (P2P), jako příklad lze uvést sdílení multimédií online. Obzvláště MP3 technologie jsou v těchto letech kontroverzním tématem. Uživatelé mohli bez větších obtíží sdílet MP3 a další hudební soubory, a to za pomoci již zmíněného peer-to-peer. Několik klíčových webů, které využívaly tento typ sdílení souborů, zůstalo v prostoru World Wide Webu. Ve známost vzešly především dva webové servery, které se v těchto letech těšily značné popularitě, a to Napster a LimeWire, ovšem jednalo se spíše o výjimky. Bylo zcela nepřípustné odcizovat hudbu a poskytovat ji lidem zdarma, a tak není divu, že o takovéto neindexované služby nebylo na Dark webu nouze. (Butler, 2018, online; Breeding, 2016, online)

Rok 2000

V tomto roce vznikl skutečný Dark web, na jehož vzniku má nemalou zásluhu irský softwarový vývojář Ian Clark, jenž vydal jako součást své vysokoškolské práce nový a pokrokový webový prohlížeč známý jako Freenet. Tato služba je stále aktuální a hojně využívaná. Freenet se od prohlížečů typu Opera odlišuje především tím, že uživateli umožňuje procházet internet v bezpodmínečné anonymitě, a činí ho tak nevysledovatelným. Federální vláda zanedlouho začala prohlížeč Freenet využívat k vyhledávání nezákonného obsahu a jeho následnému zrušení. I přes pokrok Freenetu byla výměna peněz v anonymním prostředí neuvěřitelně složitá, jelikož uživatel musel stále platit hotovostí. Zlom nastal koncem roku 2000, kdy byl svět seznámen s kryptoměnou ve formě takzvaných bitcoinů.

Za zmínku nepochybně stojí i soběstačný datový přístav HavenCo, který se pokoušel uložit citlivé informace na místo, které nebude pod kontrolou vlády. Zprvu se celý nápad jevil jako sen každého uživatele Dark webu, nicméně dnes je operace téměř ukončena.

Nejpodstatnější vývoj Dark webu nastal v roce 2002, a to vydáním prohlížeče TOR (The Onion Router). Bylo by pošetilé domnívat se, že by dnes Dark web bez této technologie mohl existovat. (Butler, 2018, online; Breeding, 2016, online)

Rok 2010

V tomto roce je vývoj Dark webu nezadržitelná lavina, jež se stává každým rokem mohutnější a nepřestává pohlcovat informace i prostor. Rok 2010 prezentuje etapu, v níž se TOR a kryptoměna setkávají, aby společně zformovaly první černé trhy. Inovátorem v oblasti černého trhu se stala věhlasná Silk road, která ovšem již delší dobu není v provozu.

Dark web se začíná dostávat do povědomí i běžným občanům a stává se tématem veřejného zájmu. Již není jen pouhou hrozbou, o které je diskutováno na konferencích orientovaných na kybernetickou bezpečnost. Vzniká enormní množství článků zaměřených na tento kybernetický prostor. Rovněž se objevují odborné články, snažící se objasnit skutečnosti týkající se této problematiky, jako jsou markantní rozdíly mezi obsáhlým Deep webem a nepatrným Dark webem.

Bylo jen otázkou času, než teroristické organizace začnou využívat Dark web pro komunikaci a koordinaci své nezákonné činnosti. Vzhledem ke skutečnosti původního účelu TOR prohlížeče vytvořeného USA si troufám tvrdit, že je celá tato situace při nejmenším ironická. (Butler, 2018, online)

Současnost

Hovoříme-li o současnosti, pak je nutno podotknout, že nynější situace, týkající se Dark webu, se do značné míry uklidnila a dochází k mírnému úpadku. Avšak stále existuje pestrobarevná paleta skrytých služeb a webových stránek mimo prostor běžného webu. Ačkoliv Dark web zaujímá relativně malý prostor (pouhých 6 %), jeho dopad je vzhledem k velikosti samotné sítě značně neúměrný. Schopnosti některých hackerů na síti jsou vskutku mistrovské. Kupříkladu rozhodne-li se skupinka schopných hackerů spolupracovat, dokážou přivést miliardovou společnost k bankrotu. Černé trhy nabízejí nespočet druhů omamných látek, které si může zakoupit kdokoliv, kdo projeví zájem a je ochoten zaplatit mnohdy astronomické částky. V roce 2016 byla také zveřejněna studie (nazvaná „Cryptopolitik a Darknet“) od vědců z King's College London, v níž vyšlo najevo, že stěžejní využití Dark webu spočívá v provozování nezákonné činnosti.

Podařilo se jim vypátrat 5 205 webových stránek TOR, z nichž dokázali identifikovat obsah u 2 723 z nich. Zjistili, že z 57 % (1 547) poskytují nezákonné služby a informace (materiály pro dospělé zahrnující násilí, dětská pornografie, týrání zvířat, odcizené kreditní karty atd.). (Butler, 2018, online; Breeding, 2016, online)

3 Specifika Dark webu

Dříve, než se potencionální uživatel rozhodne vstoupit do kybernetického prostoru Dark webu, by měl brát v potaz možná rizika, jež k této síti neodmyslitelně patří, a s obezřetností volit webové stránky, které navštíví.

Trestní složka

Návštěvník této sítě musí mít neustále na vědomí, že se nachází v prostoru, ve kterém jsou zahrnuty i webové stránky provozované zločinci. Vyjma nelegálního zboží, jež zde takříkajíc praská ve švech, se může uživatel lehce dostat do potíží, a to sice být zneužit nebo okraden. (Symanovich, 2018, online)

Porušení zákona

Ačkoli se jedná o anonymní síť, neznamená to, že je uživatel zcela skryt před zraky úřadů. Za svou činnost může být jedinec stíhán. Kryptoměna, která v digitálním prostředí slouží jako platidlo využívané u veškerých transakcí, může úřady přivést na stopu a pomoci odhalit protiprávně jednajícího uživatele. (Symanovich, 2018, online)

Pochybné odkazy

Není všechno zlato, co se třpytí. To je české přísloví, kterým by se měl řídit každý návštěvník sítě. Pokud uživatel klikne na odkaz, není cesty zpět, může být přesměrován k obsahu, který pravděpodobně vůbec nechtěl vidět. Další nástrahou po rozkliknutí odkazu může být nechtěné stažení souboru, který infikuje počítač tzv. malwarem. Malware může mimo jiné zapříčinit odcizení osobních údajů týkajících se platební karty či jiných finančních dat spotřebitele. (Symanovich, 2018, online)

Instalace prohlížeče TOR

Stěžejní pro pohyb na jakékoli síti je prohlížeč, bez něhož se uživatel neobejde. Jedním z nejpopulárnějších prohlížečů pro pohyb na Dark webu je TOR (The Onion Router). Jedná se o webový prohlížeč typu Firefox, ovšem speciálně upraveného pro anonymní pohyb. Na internetu je možno narazit na širokou škálu prohlížečů, prostřednictvím nichž se lze na síť dostat (I2P, Freenet, OneSwarm atd.). Nicméně již zmiňovaný TOR patří mezi nejhojněji využívané prohlížeče. Na tomto místě je dlužno dodat, že TOR prohlížeč je zcela zdarma a přístupný pro operační systémy Linux, Mac

OS X a Windows. TOR se vyznačuje zvláště užitečnou vlastností, pomocí níž vyčnívá nad všemi ostatními prohlížeči. Jeho navržení umožňuje uživateli předejít činnosti, která by mohla vést k odhalení jeho identity, jedná se kupříkladu o změnu velikosti proporcí okna prohlížeče. Instalace TORU není nikterak obtížná, jelikož Indexový web skýtá celou řadu odkazů pro stažení tohoto prohlížeče. Pokud ovšem potencionální uživatel nechce riskovat možnou infikaci svého počítače malwarem, všeobecně doporučovanou webovou stránkou pro bezpečnou instalaci je *www.torproject.org*. Nejen před instalací TORU, ale především před samotnou návštěvou Dark webu se doporučuje zakrýt objektiv webové kamery kusem tmavé pásky. (Porup, 2019, online; Shim, 2019, online)

Za hlavní nedostatek prohlížeče TOR považuji nemožnost připojit se k mnohým webovým prominentním službám, které TOR blokuje. Dalším nedostatkem, je dle mého názoru četné množství captchas, tzv. Turingovi testy, jež složí k odlišení počítačů od lidí, a kterými je uživatel nucen se proklikat.

Anonymní pohyb na síti

Jak již bylo zmíněno výše, pohyb na Dark webu a TORU je zcela legální, toto tvrzní se však na aktivity mnohých uživatelů nevztahuje. Aby uživatel sítě, pokud možno co nejvíce minimalizoval potencionální nepříjemnosti, jakými jsou zákeřné útoky či vysledování právními orgány, je více než žádoucí aplikovat následující opatření:

a) Po stažení TOR prohlížeče je vhodné kliknout na logo "*S*", které lze nalézt po levé straně vedle adresového řádku prohlížeče, a poté kliknout na položku „*Globálně zakázat používání skriptů*“.

b) Dále je vhodné si zapnout firewall Windows či Mac, který slouží jako tzv. „bezpečnostní brána“, bránící před neoprávněnými průniky do sítě a odesílání dat ze sítě bez vědomí a souhlasu uživatele.

c) Za žádných okolností by se neměl stahovat obsah z webových stránek na síti TOR. Toto opatření se vztahuje i na soubory pdf. či doc. Zejména nebezpečné je pak sdílení torrentů. (TOR a TOR Browser: Pro anonymní brouzdání po internetu, 2017, online)

Služba VPN (Virtuální privátní síť)

Pokud se kdokoliv chystá navštívit zrádný svět Dark webu, je na místě zvážit zaplacení služby VPN. Pokud si uživatel opatří prohlížeč TOR, měl by mít na paměti, že pomocí TORU je skryta pouze jeho identita, nikoliv však poloha. VPN uživateli pomáhá maskovat polohu tím, že nezobrazuje jeho skutečnou IP adresu, nýbrž IP adresu vytvořenou VPN systémem. Jednoduše řečeno VPN vytvoří pomyslný tunel z klientova zařízení na server VPN a posléze na samotný web. Je nezbytné, aby uživatel neustále respektoval možné nástrahy, které na Dark webu hrozí prakticky na každém „rohu" a chránil se vhodnými prostředky. Při výběru VPN lze nalézt desítky poskytovatelů této služby, přičemž ceny se pohybují okolo 5 až 10 dolarů měsíčně. V nabídce jsou také bezplatné verze této služby, ovšem za cenu sníženého množství dat na měsíc, které klient může využít. (Shim, 2019, online; Mazyar, 2019, online)

Z osobních zkušeností mohu doporučit jednoduchou aplikaci TunnelBear, která umožňuje bezplatně čerpat 500 MB měsíčně. Tato aplikace dále nabízí neomezené „tunelování", ovšem pouze pokud je klient ochotný si připlatit 5 dolarů měsíčně.

Vyhledávač Hidden Wiki

Ne nadarmo se říká, že Hidden Wiki je výchozím bodem pro ty, kteří se chytají surfovat na Dark webu. Takzvanou „skrytou" Wiki lze označit za pomyslný katalog s odkazy na nejoblíbenější místa internetového podsvětí, jež jsou přehledně uspořádány do jednotlivých kategorií. Na seznam s některými odkazy lze ovšem narazit i na „clearnetu". Z vlastních zkušeností mohu konstatovat, že většina odkazů je již nefunkční. Uživatel má ovšem možnost navštívit širokou škálu černých trhů obchodujících s drogami, falešnou dokumentací, odcizenými účty PayPal, dětskou pornografií, návody na výrobu bomb, ale i stránky zaměřující se na „praní" bitcoinů. Skrytá Wiki je provozována na doménách onion, ke kterým má přístup pouze TOR či brána TOR. (Mills, 2020, online)

Na Hidden Wiki je možno narazit na takzvané mirrory. Jedná se o odkazy na podvodné weby, které vytvářejí identickou kopii již zajeté a hojně užívané stránky. Stránky se na Hidden Wiki nalézají, jelikož je může kdokoliv upravovat. Tyto weby vznikají za jediným účelem, a to sice podvést a okrást jejich návštěvníka. (Mills, 2020, online)

3.1 Kryptoměna

Jedná se o novodobé platidlo (virtuální měnu) tvořené počítačovým kódem. Digitální měna neboli kryptoměna se stala platebním prostředkem v mnoha zemích a je využívána řadou prodejců zboží a služeb (Dell, Reddit, Time Magazine atd.). V České republice je toto platidlo z hlediska zákona a daní považováno za věc, nikoliv měnu. Existuje celá řada kryptoměn a každá z nich má svou vlastní platební síť, ve které je možné ji využít. Kryptoměny jsou nezávislé, respektive nepodléhají žádným bankám ani vládním orgánům, které by mohly ovlivňovat jejich hodnotu. Reálná hodnota měny je poměrně nestálá a určuje ji nabídka a poptávka jejich uživatelů. Převod kryptoměny je velice rychlý, a to i tehdy, jedná-li se o platbu z jednoho konce světa na druhý. Co se týče nákladů na převod, tak jsou v porovnání s běžným typem transakcí minimální. Jednou z nejoceňovanějších vlastností kryptoměn je anonymita, kterou zajišťují, a tak není divu, že je hojně využívána právě kriminálními živly. Jelikož je kryptoměna využívána k nezákonným účelům a představuje významnou překážku při stíhání organizovaných zločinců, kteří své platební transakce mohou velmi snadno skrývat před finančními ústavy, jež podléhají legislativě, je důležitá, a to především z hlediska trestního řízení. Anonymita jednotlivých měn má své hranice a mnohdy se mezi sebou značně liší. Za zcela nejrozšířenější kryptoměnu lze považovat bitcoin. (Soukup, 2019, online; Langer, 2019, online; Završnik, 2017, s. 100)

V dnešní době lze narazit na více než sto aktivních kryptoměn, s nimiž se obchoduje. První decentralizovanou kryptoměnou na světě je bitcoin. Již zmíněná decentralizovanost je zásadní novinkou ve světě kryptoměn. Jelikož nad touto měnou nemá nikdo ústřední moc, nemůže ji tak nikdo ani „zrušit“. Lze také konstatovat, že je zcela vyloučené, aby někdo udělal chybu, jež by byla osudná pro celý systém, jelikož neexistuje centrální server, který by mohl zkolabovat. Platební systém je v tomto ohledu robustnější. Decentralizovanost dále přináší rovnoprávnost účastníkům. Systém je takto odolný především proto, že roli dohledu na sebe přebírají matematická pravidla. (Završnik, 2017, s. 100)

Vladimír Smejkal ve své publikaci uvádí případ, jenž názorně ilustruje klady a zápory kryptoměn. Vývojář firmy Parity, působící na platformě Ethereum, na které je možné vytvářet elektronické peněženky, jimiž může disponovat pouze a jen skupina uživatelů (tzv. multisignature wallet), se zřejmě náhodou, možná však úmyslně, stal v určitém okamžiku (6.11. 2017) vlastníkem všech multi-sig peněženek, které obsahovaly

kolem sedmi miliard korun. V panice se pokusil peníze vrátit a kód (knihovnu, ze které se stala nedorozuměním peněženka) smazal. Situace se ovšem tímto krokem nevyřešila. Veškeré peněženky, které ovládl, nadále vyžadovaly jeho souhlas k manipulaci s jakýmikoli prostředky na daných účtech. Jelikož však knihovnu smazal a zápis o tomto smazání je již napevno zapsán v tzv. účetní knize (blockchain), kterou všichni sdílí, nemají majitelé těchto peněženek žádný způsob, jak se ke svým prostředkům dostat. Z povahy fungování kryptoměn vyplývá, že transakce, která je jednou provedena a zapsána do oné účetní knihy, je nevratná. Pokud by však uživatel chtěl transakci anulovat, muselo by se na tom dohodnout 51 % všech uživatelů (tzv. uzlů) sítě Ether. (Smejkal, 2018, s. 799)

Virtuální peněženka

Kryptoměna nemá fyzickou podobu, jedná se o měnu, která existuje pouze ve virtuálním prostoru. Pokud chce uživatel provést nebo přijmout transakci, musí si založit takzvanou virtuální peněženku. Jelikož se na trhu vyskytuje celá řada měn, situace se tím uživateli mírně komplikuje. Každá jednotlivá měna má svou vlastní virtuální peněženku. Princip programu spočívá v propojení počítače s počítači ostatních uživatelů využívajících tutéž kryptoměnu. Peněženka vygeneruje jedinečnou adresu, tvořenou z písmen a číslic, jejíž součástí nejsou žádné osobní údaje. Adresa funguje na podobném principu jako bankovní účet, respektive uživatelé na adresu mohou zasílat digitální mince. (Langer, 2019, online)

Vytěžování (mining)

Vytěžování je centrální způsob vydávání měny a také matematické pozadí všech kryptoměn. Jeho hlavním úkolem je produkování nových bitcoinů a potvrzování transakcí v síti, jinými slovy lze vytěžování označit za počítání. Celkově je každých 10 minut vygenerováno 25 bitcoinů. (Završnik, 2017, s. 101)

Vytěžování ovšem není levnou záležitostí. Vytěžení jediné bitcoinové mince stojí 140 tisíc korun. Kurz bitcoinu momentálně tuto sumu převyšuje, ovšem je nutné také započítat nejen nezbytné pravidelné investice do hardwaru, ale také náklady na elektřinu. Investice do bitcoinu je velmi choulostivá, jelikož hodnota této kryptoměny může kdykoliv prudce klesnout (nebo se zvýšit). (Vančura, 2020, online)

3.2 Monero (XMR) vs Bitcoin

Ačkoliv se kryptoměna bitcoin těšila nemalé slávě, v poslední době byl zaznamenám postupný úpadek a přechod na měnu monero. Klesající zájem kriminálních živlů o bitcoiny lze poměrně snadno zpozorovat právě na Dark webu. Shone Anstey, spoluzakladatel a prezident Blockchain Intelligence Group, se zhostil tohoto nelehkého úkolu a vypátral přesný počet transakcí souvisejících s kriminální činností. V rozhovoru pro server CNBC uvedl, že počet transakcí, při nichž je využívána měna bitcoin, klesl v roce 2016 téměř o polovinu z celkového objemu na zhruba 20 %. Této změny na Dark webu si všiml taktéž Úřad pro vnitřní bezpečnost Spojených států. Subjekty páchající trestnou činnost začínají vyhledávat jiné digitální měny, a to především monero a etherum. Příčinu náhlé změny odborníci připisují technologii blockchain, na které je bitcoin postaven. Pokud si uživatel obstará bitcoin z bankomatu a následně jej použije k nákupu nelegálního zboží, bude zřejmé, odkud peníze přišly. U malých částek v bankomatu uživatel nemusí uvádět své jméno, ovšem pokud by policie potřebovala, lze se dle času podívat na kamery v okolí a najít pachatele nebude zas tak složité. Blockchain pracuje na principu veřejného záznamu transakcí, který je dostupný online. Jedná se o jakousi účetní knihu, do níž se může kdokoliv podívat. Z toho vyplývá, že uživatelé se při své činnosti neobejdou bez veřejné adresy složené z čísel a písmen, až poté jsou schopni přijímat platby. Tento způsob databáze má za následek možné odhalení identity. Zpravodajské agentury tak jsou schopny sledovat pohyb finančních prostředků na zvolené adresy, které mohou poskytovat kupříkladu hackeři. Pomocí nich pak potencionálního zločince identifikují, jakmile se snaží vyplatit prostřednictvím více regulovaného subjektu. (Kloučková, 2017, online; Vančura, 2018, online, Stroukal, 2020 s. 25)

Za další výhodu monera lze označit nízké poplatky za každou transakci, ty se snižují se stále se zvyšujícím počtem uživatelů. Jedná se o pravý opak bitcoinu, kde se zvyšují poplatky, čím více plateb je provedeno. (Vančura, 2018, online)

4 Jak chránit děti před Dark webem

Ne nadarmo se říká, že zakázané ovoce chutná nejlépe. Dark web se v poslední době těší nemalému zájmu, a to především médií, ale rovněž i filmového průmyslu. Zvyšující se zájmem o tento tajemný kybernetický prostor lze pozorovat nejen u dospělých, ale zejména pak mezi dětmi. (Bretta, 2020, online)

Mnoho rodičů se začalo mít na pozoru poté, co se v médiích objevila tragická zpráva o sebevraždě britské středoškolačky Leiliani Clarke z The Sun. Dívka měla pravidelně navštěvovat takzvané sebevražedné chatovací místnosti na Dark webu. Matka dívky k celému případu dodává: *„Netuším, jak to našla, ale 16letá dívka by na takovém webu neměla být.“* Naneštěstí je takovýchto příběhů s tragickým koncem více. Dalším případem je 16letý australský chlapec Prestona Bridge, který zemřel po požití drog, zakoupených na jednom z nejznámějších černých trhů Silk Road. (Bretta, 2020, online)

Dark web obecně není pro většinu mladších dětí tak atraktivní. Neexistují zde žádná sociální média a děti zde nenarazí na své přátelé. Přesto však Dark web disponuje pestrou škálou atrakcí, které mohou přitahovat zejména starší děti, jedná se například o falešné ID pro koupi alkoholu, drog či zbraní. Důvodem však může být i pouhá zvědavost, myšlenka tajného světa, kde mohou být anonymní, je velmi lákavá. Děti se rády učí a objevují, je tedy zcela přirozené, že některé z nich mohou mít potřebu prozkoumat toto internetové podsvětí, s čímž je však spojeno obrovské riziko, které si mnohdy neuvědomují. (Bretta, 2020, online)

Existuje pouze jeden způsob, jak vstoupit na Dark web, a to skrze prohlížeče TOR, rodiče tak mohou pro ochranu svých dětí do zařízení nainstalovat aplikaci „*Family Zone*“. Tato aplikace dokáže identifikovat TOR a nespočet dalších aplikací, které kybernetičtí odborníci označili za „*nebezpečné*“. Pokud má rodič podezření, že jeho dítě používá TOR na nechráněném zařízení, měl by se pokusit v dotyčném zařízení vyhledat v nainstalovaných aplikacích výraz „*TOR*“. Dlužno dodat, že prohlížeč TOR není kompatibilní s iPhonem nebo iPadem. Pokud rodič zjistí, že byl výše zmiňovaný prohlížeč dítětem nainstalován, nestačí jej pouze odebrat, je nutné, aby rodič svému dítěti vysvětlil, proč tak učinil, a zajistit tak, aby dítě pochopilo nebezpečí, která Dark web skýtá. Rodič tak převezme odpovědnost a stanoví dítěti hranice, které mu zajistí bezpečí. (Bretta, 2020, online)

Další možností je instalace monitorovacího softwaru „*GoGuardian*“. Tento nástroj rodičům umožní řídit, k čemu budou mít jeho dítě přístup online. Softwarem lze blokovat

weby, filtrovat obsah pomocí klíčových slov a sledovat, co děti hledají. Tím je zajištěno, že nenarazí na věci, které mohou být škodlivé, ba dokonce nebezpečné. (GoGuardian, 2020, online)

Jak ilustruje tragický případ Leilani Clarke, k užití Dark Webu může dítě přivést deprese a úzkost, nikoli kriminální úmysl. Pokud má rodič podezření, že jeho dítě přemýšlí o automutilaci, či dokonce sebevraždě, je nezbytné neodkladně vyhledat odbornou pomoc. (Bretta, 2020, online)

Dle expertky na online bezpečnost Claire Steadové existuje hned několik způsobů, kterými mohou rodiče pomoci dětem zajistit bezpečí v online prostoru.

1. **Učit se**

   Jednou z nejdůležitějších věcí, kterou může rodič udělat. je, že bude takříkajíc držet krok s nejnovějšími technologickými trendy a populárními aplikacemi. Pokud se seznámí s populárními aplikacemi, jakými jsou Instagram či Snapchat, bude mít lepší představu o rizicích, kterým se dítě vystavuje, a o tom, jak jim co nejefektivněji předcházet. (Vonow, 2018, online)

2. **Zkontrolovat nastavení ochrany osobních údajů**

   Jedním z nejjednodušších způsobů, jak zajistit, aby dítě bylo v bezpečí, je využití integrované rodičovské kontroly. Hlavní aplikace a služby. jakými jsou Facebook nebo televizní přijímač Sky, mají způsoby, kterými je možno omezit přístup pro děti a mladistvé. (Vonow, 2018, online)

3. **Získat si děti, když jsou off-line**

   Mnohdy je bohužel nutné dětem připomenout, že existuje také celý svět off-line, aby se tak zmírnil dopad potenciální kyberšikany, což Claire Steadová nazývá „*největší obavou ohledně bezpečnosti online*“. (Vonow, 2018, online)

4. **Promluvit si s dětmi**

   Tento bod je zdaleka nejdůležitější. Rodiče by měli být schopni zajistit, aby si jejich děti byly vědomy rizik, kterým čelí v online prostoru. Je také

důležité, aby děti věděly, že je rodič vyslechne i tehdy, když se dostanou do svízelných situací. (Vonow, 2018, online)

4.1 Nebezpečí World Wide Webu

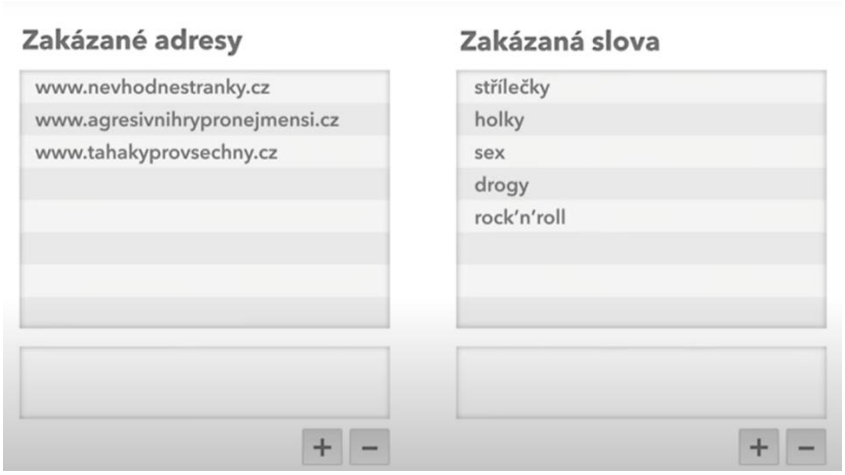
„*Pozdě bycha honit*“ aneb včasná prevence je důležitá a vede k předcházením škod, které mnohdy již nelze zcela napravit. Je více než žádoucí, aby rodiče investovali svou energii a čas do prevence, tedy debatě o rizicích, vytvoření pravidel a nainstalování vhodného softwaru. Skrze včasnou prevenci lze předejít vzniku nepříjemné krizové situace, která může mít za následek nejen uklidňování rozrušeného dítěte či odvirování počítače, ale také návštěvu psychologa, ba dokonce kontaktování policie. (Krčmářová, 2012, s. 59)

Dnešní děti se s internetem setkávají v již poměrně útlém věku, některé dokonce i dříve, než začnou být školou povinné. Proto je vhodné, aby rodiče a učitelé dítě seznámili s riziky, jež k návštěvě internetu zákonitě patří. Přestože lze na internetu nalézt nespočet stránek určených právě pro děti, je velmi pravděpodobné, že se nebudou zajímat pouze o ně. Při surfování po internetu pak můžou narazit na stránky s nežádoucím zaměřením, jakým je agresivně, sexuálně či rasisticky orientovaný obsah. Takováto setkání mohou dítě negativně zasáhnout, skrze tento fakt vznikla na trhu škála rodičovských zámků a filtrů. Tyto aplikace jsou mnohdy již součástí antivirových balíčků a existuje celá řada aplikací pro chytré telefony. (CZ.NIC, 2012-2014, online)

4.2 Rodičovské filtry

V aplikacích rodičovských filtrů rodič může zablokovat nebo naopak povolit konkrétní webové stránky. Může taktéž zakázat přístup na určité typy a skupiny stránek, přičemž tyto aplikace automaticky odfiltruje. Služba také vytváří záznam stránek, které děti navštěvují, jaké informace na internetu vyhledávají a jaká je jejich činnost na sociálních sítích. Vyjma toho rodičovské filtry disponují funkcí vymezující čas, který dítě může denně strávit na internetu, lze také nastavit jiný počet hodin (minut) pro všední dny a víkendy. Některé rodičovské filtry jsou schopny rodičům na e-mailovou adresu zaslat upozornění v případě, že se jeho dítě pokusí navštívit stránku, kterou rodič uvedl na seznam tzv. „*černé listiny*“ (viz obrázek č. 2). Ovšem ani tyto bezpečnostní nástroje nemohou na 100 % zaručit, že se dítě nesetká s nevhodným obsahem. Denně na internetu

přibývá nespočet nových webových stránek, které pod svým nevinným názvem mohou často skrývat zcela jiný obsah, a technologie rodičovských filtrů je tak nevyhodnotí jako škodlivé. Je však možné, že některé děti mohou být v IT technologiích zdatnější než jejich rodiče. V takovémto případě se rodič může obrátit na odborníky, kteří jejich operační sytém nastaví tak, že ho již jejich děti nebudou schopni obejít. (CZ.NIC, 2012-2014, online)



Obrázek č. 2 - **Rodičovský filtr** (CZ.NIC, 2012)

Odborník na e-bezpečí Kamil Kopecký uvádí, že přísná restriktivní opatření bezpečnost dítěte v kyberprostoru nezajistí. Dítě bude dříve či později toužit opatření překonat či obejít, a to například využíváním zařízení mimo dosah rodiče, kupříkladu počítače v knihovně, ve škole či u kamaráda. Je tedy daleko důležitější, aby se rodič zaměřil především na vybudování zdravého vztahu s dítětem, který je postaven na vzájemné důvěře a podpoře. Pokud bude mít dítě k rodiči důvěru, nebude se bát svěřovat i v krizových situacích. (Kopecký, 2015, online)

Jakmile rodič zjistí cokoliv nevhodného nebo se mu dítě svěří se zhlédnutím závadného obsahu, navázáním kontaktu s vulgárním člověkem či jinou rizikovou situací, neměl by za žádných okolností jednat zbrkle, nebo dokonce pohoršeně. Naopak by se měl snažit situaci pochopit a v klidu si o ní s dítětem promluvit. Dítě nesmí ztratit v rodiči důvěru, je důležité, aby se příště nebálo opět s problémem svěřit. (Burdová, Traxler, 2014, s. 11)

„Dobrá, odpovědná výchova je výchovou proaktivní. Proaktivní přístup k životu znamená, že se snažíme mít vliv na to, aby se staly ty „správné věci“. Dá se říci, že proaktivní výchova je tou nejlepší prevencí, jak se nedostat do situace, kdy už je každá

rada drahá. Pokud většinu toho, co chtějí děti dělat, dělat mohou, byť s určitým omezením, celkem bez problémů přijímají i to, že jsou věci, které (zatím) nesmějí dělat vůbec. Naopak tam, kde se mnoho věcí nesmí, děti bojují za každou maličkost.“ (Krčmářová, 2012, s. 59)

4.3 Výzkum v oblasti chování dětí na internetu

Společnost O2 společně s Centrem prevence rizikové virtuální komunikace (PRVoK) Pedagogické fakulty Univerzity Palackého v Olomouci uskutečnila v roce 2019 jeden z nejrozsáhlejších výzkumů v oblasti chování dětí na internetu. Výzkumu se zúčastnilo 27 177 dětí ve věku 7 až 17 let. Cílem výzkumu bylo především zmapovat, aktivitu českých dětí na internetu. Součástí výzkumu bylo také zmapování aktuálně nejvýznamnějších rizik, což je zcela klíčové pro správné nastavení edukace a prevence. (Kopecký, Szotkowski, Pajurková, 2019, online)

Děti jsou v online světě značně aktivní, využívají řady aplikací a sociálních sítí. Sociálně sítě aktivně používá více než polovina (51,75 %) dětí ve věku od 7 do 12 let, přestože pravidla jejich používání povolují tyto služby až od 13 let. Z výzkumu je patrné, že se dětští uživatelé na internetu baví především vyhledáváním nejrozličnějších videí na YouTube, následuje Facebook a Instagram. (Kopecký, Szotkowski, Pajurková, 2019, online)

Výzkum se dále zaměřil na rizikové chování dětí na internetu, přičemž je patrné, že více než polovina respondentů přiznává zkušenost s kybernetickou agresí skrze Facebooku, 43 % pak konkrétně přes Facebook Messenger. Děti zažily kyberagresi také prostřednictvím Instagramu, SMS nebo MMS. Dominantní je dle předpokladu klasická verbální agrese, jejíž obětí se stalo 27 % českých dětí. Nově si děti stěžují také na tzv. sharenting. Přes 1 900 (7,8 %) dětí potvrdilo, že rodiče nahráli na internet jejich fotku nebo video, aniž by s tím děti souhlasily. (Kopecký, Szotkowski, Pajurková, 2019, online)

Mezi významné rizikové chování na internetu spadá i seznamování. Více než čtvrtina dětí potvrdila, že „*na síti*“ dostala nabídku osobního setkání od člověka, kterého neznaly. Znepokojující je však fakt, že 70 % dětí na schůzku skutečně dorazilo. Výsledky výzkumu v této oblasti lze i přes vysoké procento hodnotit jako mírně optimistické, jelikož došlo od posledního měření v roce 2014 k poklesu u všech sledovaných forem kybernetické agrese, a to o celých 5 %. (Kopecký, Szotkowski, Pajurková, 2019, online)

„*Přestože výsledky našeho rozsáhlého výzkumu jsou alarmující, jsem ráda, že jednoznačně potvrzují, že prevence a edukace jsou správnou cestou a fungují,*“ uvádí Marie Mališková, CSR manažerka společnosti O2. „*Děti jsou zranitelné, a přestože se v online světě pohybují často více a sebejistěji než my dospělí, potřebují od nás pomoc a podporu. I proto se prostřednictvím projektu O2 Chytrá škola obracíme především na pedagogy a rodiče a na portálu O2Chytráškola.cz jim přinášíme jednoduché rady, výukové materiály a aktuální informace z online světa,*“ dodává. (Kopecký, Szotkowski, Pajurková, 2019, online)

5 Dark web jako rizikové prostředí s ohledem na sociálně patologické jevy

Temná tržiště na Dark webu jsou jako sedmihlavá saň, usekni jednu hlavu a narostou další dvě. Jedno je ale jisté, konkurence mezi jednotlivými tržišti sílí, což má za následek nepřetržitý zánik a vznik nových tržišť. V jedné chvíli je největší velmocí tržiště Dream Market a následující den toto tržiště zanikne a nahradí ho v čele žebříčku podstatně menší Wall Monopol, který ovšem následně opět zaniká. Jeden čas byl největším online tržištěm Sheep Marketplace, před ním Silk Road. Jindy se zase nejlépe vedlo AlphaBay a následně Hanse. To vše se událo během pouhých devíti let. V rámci temných tržišť vznikají monopolní struktury, které ale také rychle zanikají. Základním nepsaným pravidlem provozovatele temných tržišť je sledování konkurence a schopnost přizpůsobit se technologickým změnám, zejména pak těm, které se týkají zabezpečení. Podnikání na Dark webu tak představuje neustálý boj o přežití. (Stroukal, 2020, s. 138-139)

Temných tržišť již vzniklo mnoho. Nelze však jistě nalézt všechna tržiště. Dominiku Stroukalovi se podařilo napočítat celkem 147 historicky existujících tržišť. K o něco nižšímu číslu došlo před dvěma lety i European Monitoring Centre for Drugs and Drug Addiction. Dle této organizace drtivá většina tržišť nepřežije první rok. Toto tvrzení svědčí o silně konkurenčním prostředí. Nicméně trh vykazoval v každé době jednoho velkého dominantního hráče. Po Silk Road získal dominanci Sheep Marketplace, následně Agora, poté AlphaBay, pak Dream Market, poté Wall Street Market a v době po vydání této bakalářské práce zajisté někdo jiný. (Stroukal, 2020, s. 143)

5.1 Drogy a návykové látky na Dark webu

Dream Market

Dream Market je jedním z nejstarších a nejdůvěryhodnějších trhů, na který lze na Dark webu narazit. Trh funguje od roku 2013, kdy se ještě jednalo o nepatrné tržiště ve stínů gigantů, jako byl Silkroute, Hansamarket, Alphabay a další. Nyní jsou však všechna tři zmíněná tržiště zrušena donucovacími orgány a Dream Market se stal oblíbeným prostorem pro prodej drog všeho druhu. Před samotným nákupem zboží je nutné podstoupit jednoduchý registrační proces, ve kterém není zapotřebí uvádět osobní

údaje či email. K registraci si uživatel vystačí se smyšleným jménem a heslem, poté už může nakupovat dle libosti. Na trhu lze nalézt více než 124 400 produktů, přičemž z 50 % se jedná o drogy. Na Dream Marketu lze nalézt pouze čtyři kategorie, což je považováno za značnou výhodu, jelikož většina podobných trhů jich obsahuje mnohonásobně více, což klientelu dokáže zmást. Zmíněnými čtyřmi kategoriemi jsou drogy, digitální zboží, služby a ostatní. Drogy jsou rozděleny do několika kategorií (viz tabulka č. 1). (The Dark web links, 2018, online)

Tabulka č. 1: **Dream Market–kategorie drog**

Barbituráty	Extáze	Recepty
Benzodiazepiny	Konopí	Psychedelika
Disociační drogy	Opioidy	Steroidy
Stimulanty	RCs	Prášky na hubnutí

Zdroj: autor

V kategorii digitální zboží lze nalézt nejrůznější elektronické knihy, pirátské softwary a hackované údaje o účtech pro Netflix. V neposlední řadě lze na trhu nalézt již zmiňovanou kategorii vše ostatní, která svým obsahem nespadá ani do jedné z výše uvedených kategorií. Tato kategorie mimo jiné skýtá nejrůznější padělky, šperky a laboratorní potřeby. V současné době lze na Dream Marketu platit pouze kryptoměnou bitcoin nebo monero. (The Dark web links, 2018, online)

5.2 Dark web v době koronavirové

„*Kvůli koronaviru došly drogy, narkomani mohou umírat,“* tak zněl titulek zprávy publikované na serveru iDnes 31. 3. 2020. Později byl titulek změněn na méně pejorativní, avšak hlavní informace zněla stejně, a to sice, že drogy došly.

Dle nového výzkumu od Vánoc roku 2019 do 27. dubna 2020 vzrostla nabídka drog na Dark webu o enormních 495 %. Zdaleka největší nárůst nabídky byl zaznamenán u kokainu, kde zájem vzrostl o 1 000 %, dále se zvýšila nabídka marihuany konkrétně o 555 % a extáze o celých 224 %. Pouliční prodejci hledali možnosti, jak uzavřít obchod. Jelikož pandemie vyprázdnila ulice, byli mnozí prodejci nuceni se přesunout do digitálního podzemí na Dark Web. Nutno dodat, že drogový obchod je závislý na

obrovském objemu mezinárodní přepravy, v němž se dokáže skrýt a rozmělnit. Poté co byly hranice kvůli koronavirové krizi uzavřeny a byl povolen pouze zlomek původní dopravy, drogy se neměly kam skrýt. V důsledku tohoto opatření byli někteří prodejci nuceni na Dark webu postupně zavírat své krámy. Někteří prodejci se svou tíživou situaci snažili vyřešit zlevněním zboží, které mohlo zákazníkům pomoci v nouzovém stavu, jednalo se například o slevy na víza do zemí, které se dokázaly s pandemií vypořádat lépe. Nedostatkovým zbožím se staly vykradené kreditní karty, jelikož ty jsou nejčastěji získávány od turistů. Jako virus se nicméně na Dark webu začaly šířit i nejrůznější podvodné nabídky, slibující účinné vakcíny proti Covidu-19. *„Vakcína na nový koronavirus (Covid-19) je dostupná, umím nabídnout pět druhů vakcín (možná budu mít za pár dní i víc). Prodávat ji je velké riziko, takže jsem udělal tuhle webovou stránku. Na jednu adresu umím poslat jednu vakcínu, takže pokud potřebujete víc, jen zopakujte všechny kroky znovu s jinou adresou. Cena je nízká pouze teď. 120 dolarů za kus.“* Jednalo se o zjevný podvod, o tom není pochyb. Tento podvod samozřejmě nebyl jediný, objevily se taktéž nabídky za tisíce dolarů, zde již nešlo o vakcínu, nýbrž o samotný lék pro již nakažené jedince. V okamžiku, kdy pandemie vypukla a lidé se tak postupně začali potýkat s nedostatkem ochranných pomůcek, se na Dark webu začalo obchodovat nejen s respirátory, ale také s mnohem kurióznějším zbožím. Jeden z obchodníků na webové stránce Own Shop nabídl za 1 000 dolarů svou vlastní krev a sliny. Tento prodejce již údajně koronavirus prodělal a nyní se tak v jeho tělních tekutinách nacházejí protilátky. Zcela nepochybně se objevili prodávající, již měli levné sady testů na koronavirus, a to dokonce i v době, kdy je nikde nebyly schopny opatřit ani vlády. (Stroukal, 2020, s. 202-204; Cuthbertson, 2020, online)

5.3 Sexuálně a násilně orientovaný obsah

Osm terabajtů představuje enormní množství dat. Pro představu, o jak obrovské množství se jedná, lze uvést příklad s publikací o velikosti 207 stran, která by se do tohoto množství vešla přesně deset miliónkrát. Pokud bychom toto datové množství převedli na videozáznam, vyšly by nám dva měsíce nepřetržitého záznamu. Přesně takovéto množství dat dětského porna zachytili britští policisté na Dark webu v březnu roku 2018. V ložnici třiadvacetiletého Korejce bylo nalezeno 250 tisíc videozáznamů, jejichž obsahem byla dětská pornografii. Bohužel i toto je Dark web. (Stroukal, 2020, s. 92)

Nejčastěji se o dětské pornografii na Dark webu lidé dozvídají skrze zprávy, ovšem až poté, co dojde k zatýkání. Nakládání s dětskou pornografií představuje nemalou část Dark webu, na kterou by i většina jeho příznivců nejraději zapomněla. Přitom se jedná o jednu z jeho největších částí. (Stroukal, 2020, s. 93)

O jak velké množství dětské pornografie se jedná? Jednou větou by se dalo říci, že na Dark webu lze narazit na bizarní množství dětského porno materiálu. Britský vědec Gareth Owen se rozhodl zrealizovat studii, jejímž cílem bylo zmapovat dětskou pornografii na Dark webu. *„Než jsme udělali tuhle studii, měl jsem pocit, že Dark web je dobrá věc,“* uvedl v roce 2014 pro časopis Wired. Svůj názor však velmi rychle přehodnotil poté, co zjistil, že **více než 80 %** návštěv na Dark webu je směřováno na stránky s dětskou pornografií. Dle Owena temná tržiště zaujímají pouhých 5 % návštěvnosti a protirežimní nástroje představují zlomek procenta. (Stroukal, 2020, s. 102-103)

Welcome to Video

Jedná se o server, jehož provozovatel byl Jong Woo Son. Obsah tohoto serveru byl striktně zaměřen na dětskou pornografii. Tato stránka na sebe skrze Dark web vydělávala prostřednictvím plateb v bitcoinech. Uživatelé těchto stránek museli tedy před zhlédnutím zaplatit, a to v kreditech. Tyto kredity bylo možno získat dvěma způsoby. První možností, jak si tyto kredity obstarat, byla jejich koupě za bitcoiny. Druhou možností bylo nahrání videa s dětskou pornografií. Na tomto principu funguje i mnoho stránek na surface webu. Jedná se o účinný způsob, jak motivovat uživatele videa nejen k pasivnímu stahování, ale také k podílení se na jejich distribuci a tvorbě. Sone skončil za mřížemi spolu s dalšími 337 uživatel, které se podařilo dopadnout. Mezi nimi se dle vyjádření úřadů nacházel i občan České republiky. (Stroukal, 2020, s. 92)

Lolita City

Již samotný název této webové stránky predikuje její obsah, orientující se na dětskou pornografii. Toto místo je elektronickým rájem pro všechny pedofily. V roce 2011 zde bylo k získání 100 GB pornografického materiálu. V nabídce webu lze nalézt pornografická videa, softcore i hardcore fotografie. Věkové kategorie dětí se pohybují od novorozenců po 17leté dívky a chlapce. Přístup k tomuto webu je možný pouze přes síť TOR. Na webu lze nalézt i takzvané Lolita City's forums. Stejně jako na mnoha dalších pedofilních fórech i zde jsou horlivé debaty ohledně utlačování pedofilů, kteří se považují za diskriminovanou menšinu. (Edddy, 2011, online; O'neill, 2013, online)

Childs Play

Jedná se o doposud nejrozsáhlejší webovou stránku s dětskou pornografií na Dark webu. Toto tvrzní má původ v počtu registrovaných profilů. Stránka byla v provozu celkem jedenáct měsíců a jejím provozovatelem byla australská policejní jednotka Taskos Argos. Policie zveřejňovala fotografie, na nichž byly děti zneužívány. Vytvořila program, který stahoval obsah hned z několika fór týkajících se zneužívání dětí. Cílem akce bylo zajistit uživatelská jména a data uživatelů navštěvujících jimi vytvořenou stránku. Policie při zjišťování dat využívala takzvané tepelné mapy, pomocí nichž byli schopni určit, kdy přesně uživatel sleduje či zveřejňuje nelegální materiál. Dalším krokem byla lokalizace časového pásma a samotného uživatele. Akce byla úspěšná, ovšem popudila značné množství lidí. Ivar Stokkereit, právní poradce Dětského fondu OSN (UNICEF) v Norsku konstatoval, že se jedná o *„jasné porušení Úmluvy OSN o právech dítěte, i když záměrem policie je dlouhodobě zabránit novým trestným činům "*. (VG, 2018, online)

Policie byla osočena, že použila materiál s dětskou pornografií jako návnadu k chytání pedofilů. K celému případu se dá snad jen dodat, že účel světí prostředky. (Times, 2019, online; VG, 2018, online)

Na obranu policistů je nutno podotknout, že jednotka Argos, která web provozovala, měla za sebou 20 let zkušeností s vyšetřováním zneužívání dětí. Během několika let se jim podařilo zničit celou řadu organizovaných skupin, a zachránit tak desítky, ne-li stovky dětí. V jednom takovém případě postupovali podobně. Na půl roku se policisté stali správci fóra s názvem The Love Zone na Dark Webu, a když se rozhodli přejít do útoku, zachránili během jediné akce 85 zneužívaných dětí. Také se jim podařilo zatknout Brita jménem Richard Huckle, jenž je dodnes považován za jednoho

z nejobávanějších pedofilů všech dob. Při zatčení byl nalezen podrobný seznam 191 znásilnění, nechyběl ani nejdetailnější rozbor toho, jakým způsobem hrůzné akty vykonával. Násilník dlouhé roky útočil na děti v Malajsii, dle všeho jich mohly být až stovky. Policie ho dokázala usvědčit ovšem pouze z 22 činů, ke kterým měla důkazový video materiál. O dalších souborech se ví, policie se k nim však bohužel nedokázala dostat. Nutno podotknout, že zneužívání dvaceti dvou dětí k odsouzení bohatě stačilo. Huckle za tyto ohavné činy dostal dvaadvacet doživotí, jeho trest však netrval dlouho. Spoluvězni vzali brzy takříkajíc spravedlnost do vlastních rukou a Huckle byl nalezen v říjnu 2019 ve své cele uškrcen a ubodán k smrti. Dalo by se říci, že Richard Huckle byl skutečně výjimečnou zrůdou. Choval se tak arogantně, že nebyl populární ani mezi sobě podobnými. Došel dokonce tak daleko, že vydal šedesátistránkovou knihu s názvem „Pedofilové a chudoba: Průvodce milovníka dětí“. Knihu však naštěstí nikdy nestihl na internet nahrát. (Stroukal, 2020, s. 96-97)

Pink Meth

Jedná se o jednu z nejnavštěvovanějších webových stránek na Dark webu. Obsah webu tvoří pornografické fotografie či videa nezletilých dívek, ty byly na stránku vloženy bez jejich vědomí, obvykle po rozchodu s přítelem. Webová stránka byla vytvořena jedincem známým pod pseudonymem Olaudah Equiano. Na Pink Meth se bylo možné dostat skrz prohlížeč TOR. V současnosti již není možnost stránku navštěvovat ani nalézt, jelikož byla zrušena policií na základě obžaloby studentky, jejíž fotografie na tento web unikly. (Gilbert, 2014, online)

Destrukce Daisy

Destrukce Daisy je nechvalně známé video, které se na Dark webu stalo legendou. Jednalo se o tak surové a kruté záběry, že se v Austrálii začalo znovu uvažovat o trestu smrti. Tvůrcem onoho videa je Peter Gerard Scully, který pod záminkou jídla lákal chudé děti k sobě domů, kde je poté následně znásilňoval, držel na vodítku a nechával kopat vlastní hroby. Scully také pod pseudonymem Peter Ridell či Peter Russell vybudoval na Dark webu jednu z vůbec nejmorbidnějších sítí s placenými videonahrávkami obsahujícími dětskou pornografií. Jedno z mnoha videí si od něj koupil i jeho kolega a australský spoluobčan Matthew David Graham, známý pod přezdívkou Lux. Graham sám provozoval celou řadu serverů s násilím, jednalo se například o webovou stránku Hurt 2 The Core, kam se chodil uspokojovat i sám Scully. Video, které si od něj Graham

koupil, neslo již zmiňovaný název „*Destrukce Daisy*“. V tomto videu jsou zachyceny natolik zvrácené záběry, že lidé na internetu byli jednomyslně přesvědčeni, že se musí jednat o podvrh. Poté co se o tomto videu dozvěděly úřady, vyvinuly veškeré úsilí k tomu, aby už žádné podobné video nebylo nikdy natočeno. Na konci února 2015 se Scullyho podařilo dopadnout. Po dopadení, policisté zjistili, co se stalo se třemi dívkami, které byly ve videu surově zneužívány. Dvanáctiletá Liza brutální útok přežila, ovšem nese si doživotní následky. Jedenáctiletá Cindy již takové „štěstí“ neměla, po natočení videa byla Scullym mučena, zneužita a následně byla donucena si vykopat svůj vlastní hrob. Poté co byla dívka s hrobem hotova, byla uškrcena, což je také zaznamenáno na Scullyho kameře. Daisy, třetí a také nejmladší oběť, po které je celé video pojmenováno, bylo pouhých osmnáct měsíců. Scully se na svobodu již nikdy nedostane, a jak je dobře známo, spoluvězni nemají pro ubližování dětem příliš velké pochopení. (Stroukal, 2020, s. 93-94)

Snappening

Snapchat je na první pohled zábavná aplikace, která přinesla, a to především mladší generaci, novinku ve sdílení fotografií a videí. Přestože již aplikace neposkytuje výrazná vylepšení, o nová rizika s ní spojena není nouze. Princip této aplikace spočívá v jednoduchém zasílání fotografií či videí, které je možno zobrazit pouze po omezený čas. Lze si u svých příspěvků kupříkladu nastavit, že příjemce je bude schopen vidět po dobu pěti vteřin, než „nadobro“ zmizí. Provozovatelé aplikace garantují, že zaslaný materiál po uplynutí stanovené doby zmizí a nikam se neuloží. V této souvislosti však provozovatelé opomíjejí zmínit fakt, jaké reálné riziko uživateli hrozí, a to sice, že si jeho zaslané fotografie příjemce zvěční pomocí funkce screenshot. Aplikace toto jednání dokáže odhalit a následně uživatele upozornit. Ovšem v konečném důsledku se tím nic nemění. Navíc kopii příspěvku lze vytvořit i jiným způsobem. (Kubala, 2019, s. 38-41)

V této digitální době již existuje aplikace prakticky na cokoliv. Tudíž netrvalo dlouho a začal se mezi uživateli Snapchatu šířit program SnapSave, který si stačilo jednoduše nainstalovat, a veškeré zobrazené fotografie a videa se automaticky uložily do telefonu, aniž by o tom odesílatel věděl. Mělo to ale jeden zcela zásadní zádrhel. Aby aplikace mohla fungovat, získala oprávnění pro stahování fotografií ze Snapchatu a jejich následné ukládání do telefonu. Každé video a fotografii, kterou uživatel poslal adresátovi, také přišlo na server podvodné aplikace. Kdesi na vzdáleném serveru se

postupně začaly kumulovat gigabajty fotografií a videí. Přes aplikaci si samozřejmě lidé posílali lechtivé snímky. Ovšem jak již bylo zmíněno výše, Snapchat využívají především děti. Poté stačilo jediné, a to sice aby se někdo naboural na servery aplikace SnapSave a data ukradl. Na začátku října roku 2014 skutečně došlo k nabourání se do toho serveru a 13 gigabajtů fotografií a videí se objevilo na internetu. Stovky tisíc fotografií a videí s dětským pornem si tak našly svou cestu i na torrenty. Na scéně se dokonce objevil i uživatel, který vytvořil index, aby zájemci o dětskou pornografii mohli tak enormním množstvím materiálu procházet snadněji. Této aféře se začalo přezdívat Snappening. (Stroukal, 2020, s. 98-99)

Peddo Support Comunity

Jedná se patrně o jednu z největších komunit pro pedofily, na kterou lze na Dark webu narazit. Toto fórum obsahuje více než tisíce příspěvků s pedofilní tématikou. Uživatelé si zde vyměňují zážitky, rady a zkušenosti, jak dosáhnout svých cílů. Fórum rozděluje uživatele do dvou kategorií. „Konzervativní" pedofilové jsou uživatelé, jejichž zájem o děti přetrvává čistě ve sféře fantazírování. Zbytek fóra se nachází mimo jakékoliv myslitelné meze a stojí tedy na „nekonzervativní" straně. (Stroukal, 2020, s. 99-100)

Autoři příspěvků u svého profilu vyplňují věkovou a genderovou preferenci. Uživatel s přezdívkou Midamoto uvádí, že preferuje 3+ dívky. Další uživatel OneLove má preferenci dívek ve věku 7 až 12 let. Zajímavostí je, že na tomto fóru se nenachází žádný fotografický či videomateriál s dětskou pornografií, ba naopak je zde vyloženě zakázán. Fórum se tak snaží tvářit, že vlastně nedělá nic špatného. Pedofilové si zde vytvořili komunitu, ve které si mezi sebou radí, jak se vnitřně vypořádat s pocity, jež cítí. Největší pozornosti se však těší diskuzní příspěvky zaměřené na rady, jak se tajně uspokojovat. Uživatel s přezdívkou Pedrobear44 zde například otevřel horlivou debatu na téma, jak úžasné místo pro pedofily je aquapark. Fórum bylo již několikrát uzavřeno, ale stále se obnovuje ze zálohy na jiných místech. (Stroukal, 2020, s. 100)

Anonymous (Anon)

Anonymous je celosvětově známé a obávané anonymní hnutí. Jedná se o amorfní a na sobě nezávislé nehierarchické hnutí hackitivistů (hacker-aktivisty), kteří se čas od času spojí za účelem využití svých digitálních schopností, aby vyslali veřejnosti nějaký signál. Jedním z takovýchto signálů se stala operace Darknet, během které se

hacktivistům podařilo publikovat IP adresy uživatelů stránek s dětskou pornografií. (Besser, 2015, online; Stroukal, 2020, s. 102)

„Operace Darknet nikdy neměla za cíl sundat Tor či darknety. Jediným cílem operace Darknet bylo odhalit, že služby jako Tor byly zničeny jedním procentem těch, kteří je užívají pro dětskou pornografii,“ napsali Anonymous. Skupina taktéž výstižně dodává, že: *„Dětská pornografie NENÍ SVOBODOU SLOVA.“* (Stroukal, 2020, s. 102)

Celá akce byla dle slov samotných tvůrců jednoduchá. V říjnu roku 2011 vydali rozšíření pro internetový prohlížeč Firefox, který řada lidí využívá pro připojení skrze Tor na Dark web. Při použití inkriminovaných stránek tlačítko odeslalo uživatelovu IP adresu Anonymous a přístup zablokovalo. Celý zákrok trval 24 hodin a tvůrcům se podařilo zveřejnit 190 IP adres. Dále se hackerům podařilo na nějakou dobu vyřadit z provozu 40 obsáhlých webů, které dětskou pornografii zveřejňovaly. Zda informace někdy k něčemu využily bezpečnostní složky, není známo, ale Anonymous poukázali, že sami uživatelé internetu na Dark Webu se chtějí bránit. Dark web není pouze černobílé místo, vedle padouchů lze narazit i na hrdiny. (Stroukal, 2020, s. 103-104)

Europol

Europol roku 2013 ve své tiskové zprávě uvádí vskutku znepokojivé svědectví. „*Převážná většina materiálu se zneužívanými dětmi je nadále distribuována zadarmo na otevřeném internetu, avšak využívání skrytých služeb, jako je Tor, činí pro bezpečnostní složky čím dál obtížnější identifikaci útočníků a sítí stojících za výrobou a distribucí materiálu se sexuálním zneužíváním dětí.“* tvrdí. (Stroukal, 2020, s. 104)

Europol dále upozorňuje na nový trend, a to sice online sledování zneužívání dětí v reálném čase. Europol informuje explicitně o cenách, jedno video vychází v přepočtu na 10 dolarů a čtvrtletní předplatné pak vyjde zájemce na 50 dolarů. Nejdražší je natočení zcela nového videa, cena se pohybuje okolo 1 200 dolarů za nahrávku. Vzhledem k tomu, že kvalitní video studio má ve svém kapesním telefonu již téměř každý, se Europol obává, že trh s těmito „domácími“ videi na objednávku poroste. Ekonomicky to dává smysl, jelikož narozdíl od nájemných vrahů se zákazníci pravidelně vrací. Problém ve streamování dětského porna ale nepramení pouze a jen z jeho komplikovaného vysledování. Pokud si sledující nevytváří kopii, tak se nejedná o sdílení materiálu. Nicméně právo na to pamatuje a trestá i to, ovšem jak Europol konstatuje, takovéto případy jsou velmi ojedinělé. (Stroukal, 2020, s. 105)

Stroukal ve své publikaci uvádí webové stránky Europolu, (**europol.europa.eu/stopchildabuse**) na kterých jsou zveřejněny kousky fotografií z videí, které se doposud nepodařilo identifikovat. Často je k vidění oblečení s logem nebo pohled na budovu. Dle mého názoru by bylo více než žádoucí veřejnost obeznámit s touto webovou stránkou a zvýšit tak nejen pravděpodobnost identifikace pachatele, ale také možnosti záchrany zneužívaného dítě.

Red Room

Red Room je webovou stránkou, kde lze narazit na skutečné zlo. Uživatelé se po zaplacení vstupního poplatku, mohou připojit k živému vysílání znásilnění, vraždy nebo interaktivního mučení. V interaktivním mučení má klient možnost si zvolit, po zaplacení určitého obnosu, jakými způsoby bude oběť trpět. Jedná se o zvrácenou verzi aukce, kde mučitel udělá vše, co zákazník požaduje, který je ochotný nabídnout vysoké množství peněz v podobě kryptoměny. Na Dark webu lze nalézt nespočet stránek, vydávajících se za Red Roomy, ovšem obvykle se jedná o podvodné stránky, jež se snaží z potencionálních uživatelů vymámit bitcoiny. Na běžném indexovém webu lze nalézt internetová fóra vedoucí diskuze na téma, jak proniknout do Red Roomu. Existence těchto webů není na síti Tor možná, jelikož se jedná o velmi pomalou síť, na které nelze streamovat živé video. (Harper, 2019, online)

6 Aktivita uživatelů Dark webu

Následující kapitola pojednává o výzkumných šetřeních, jež byly realizovány v rámci bakalářské práce a byly sestaveny tak, aby korespondovaly s tématem celé práce. Výzkumnými metodami jsou dotazníkové šetření a interview.

6.1 Dotazníkové šetření

Pro svou bakalářskou práci jsme si zvolila jednu z metod standardizovaného vědeckého výzkumu, tedy dotazníkové šetření.

Gavora definuje dotazník jako způsob kladení otázek, jejichž cílem je získávání písemných odpovědí. (Gavora, s. 121, 2010)

Pro tuto metodu jsem se rozhodla, jelikož uživatelé Dark webu tvoří velmi specifickou skupinu respondentů. Realizaci online rozhovoru s uživateli této sítě považuji za příliš riskantní, neboť by uskutečnění samotného interview vyžadovalo návštěvu speciálních diskuzních fór na Dark webu.

Jelikož se jedná o citlivé téma, byla jsem nucena zvolit méně osobní otázky, na základě zkušeností s prvním pokusem o dotazníkové šetření. Při prvním pokusu o dotazníkové šetření jsem zvolila otázky, které zasahovaly do hloubky problematiky, a odezva byla velmi malá. V novém dotazníku se tedy zaměřuji na povrchovější zmapování aktivity respondentů, abych získala co největší možné množství dat. V kapitole jsou dále představeny užité metody, stanovené hypotézy. Dotazník, který byl koncipován k této bakalářské práci, obsahuje 17 otevřených i uzavřených otázek.

Výzkumný vzorek

Výzkumný vzorek dotazníkového šetření tvořili návštěvníci sítě zvané Dark web. Soustavně bylo oslovováno různými cestami několik diskuzních fór, jež se svým obsahem primárně zaměřují na Dark web. Dotazník byl umístěn na sociální síť Facebook, a to zejména na několik studijních a veřejných skupin. Na tomto místě je dlužno dodat, že potenciálně bylo na sociálních sítí osloveno téměř 14 000 respondentů. Jelikož se jedná o velmi specifickou skupinu osob, podařilo se mi vyprofilovat 54 respondentů, jenž mají s Dark webem zkušenost. Většinu dotazovaných tvořili respondenti mužského pohlaví (31), zbytek tvořily ženy (23). Dotazovaní byli rozličných stupňů vzdělání, nejvíce byli zastoupeni respondenti s vysokoškolským vzděláním (28), dále pak následovalo vzdělání středoškolské (17), vyučen s maturitou (6), vyučen (2) a dotazníkového ošetření se

zúčastnila pouze jedna osoba se základním vzděláním. Výzkumného šetření se zúčastnili respondenti různých věkových kategorií, převážná většina dotazovaných (27) byla ve věku 19 až 25 let.

Cíle a hypotézy

Hlavním cílem výzkumného šetření bylo zmapovat aktivitu uživatelů Dark webu. Tento cíl byl původně rozšířen o zjištění rozdílu mezi zahraničním a českými uživateli. Bohužel se mi vzhledem k specifickému vzorku respondentů nepodařilo získat dostatečné množství dotazovaných ze zahraniční. Dále jsem si stanovila dílčí cíle, a to zejména zjistit, zda se uživatelé před vstupem dostatečně obeznámili s riziky této sítě, dále co respondenty vedlo k návštěvě, co konkrétně dotazovaní vyhledávají a zda návštěva splnila jejich očekávání. V bakalářské práci je stanoveno pět základních hypotéz.

Hypotézy byly stanoveny následovně:

H1: Z pohledu zkoumané skupiny budou více zastoupeni muži než ženy. (Hypotézou se zabývají otázky č. 1, 2, 3 a 4.)

H2: Více než polovina respondentů se před samotným vstupem na Dark web dostatečně obeznámí s riziky. (Hypotézou se zabývají otázky č. 5 a 6.)

H3: Nadpoloviční většina respondentů uvede reálné obavy, že při návštěvě Dark webu došlo k odhalení jejich identity. (Hypotézou se zabývají otázky č. 15 a 16.)

H4: Více než polovina dotazovaných, mající zkušenost s Dark webem, jej již znovu nebude navštěvovat. (Hypotézou se zabývají otázky č. 7, 8, 9, 10, 11, 12, 13 a 14.)

H5: Více jak polovina respondentů uvede, že návštěva Dark webu splnila jejich očekávání. (Hypotézou se zabývá otázka č. 17)

Celý můj koncept je shrnut do následující tabulky.

Tabulka č. 2: **Koncept dotazníku**

Cíl výzkumného šetření	**Dílčí cíle**	**Příslušné otázky**
Zmapovat aktivity uživatelů Dark webu	Identifikační otázky	1. Připojili jste se někdy k webu známému pod názvem Dark web?
		2. Jste muž, nebo žena?
		3. Jaké je Vaše nejvyšší dosažené vzdělání?
		4. Do jaké věkové kategorie byste se zařadili?
	Zjistit seznámení se s riziky	5. Seznámili jste se s možnými riziky před vstupem na tento web?
		6. Jak jste se o existenci Darkwebu dozvěděli?
	Zjistit důvod návštěvy	7. Zaujal Vás Darkweb a navštěvujete jej pravidelně?
		8. Co Vás vedlo k připojení se k tomuto webu?
	Zjistit obsah, jenž uživatelé vyhledávají	9. Na jaký obsah jste na Dark webu narazili?
		10.Jaký obsah nejčastěji vyhledáváte?
		11. Objednávali jste si z webu nějaký produkt či službu?

Cíl výzkumného šetření	Dílčí cíle	Příslušné otázky
		12. Co jste si na Dark webu objednali?
Zmapovat aktivity uživatelů Dark webu	Zjistit obsah, jejž uživatelé vyhledávají	13. Dorazila Vám objednávka, či byla služba vykonána?
		14. Nabízeli jste někdy své služby či produkty na Darkwebu?
	Zjistit, zda návštěva splnila očekávání respondenta	15. Máte obavy, že při návštěvě Dark webu někdo odhalil Vaši identitu?
		16. Vyhrožoval Vám někdo po návštěvě Dark webu?
		17. Splnila návštěva tohoto webu Vaše očekávání?

Zdroj: autor

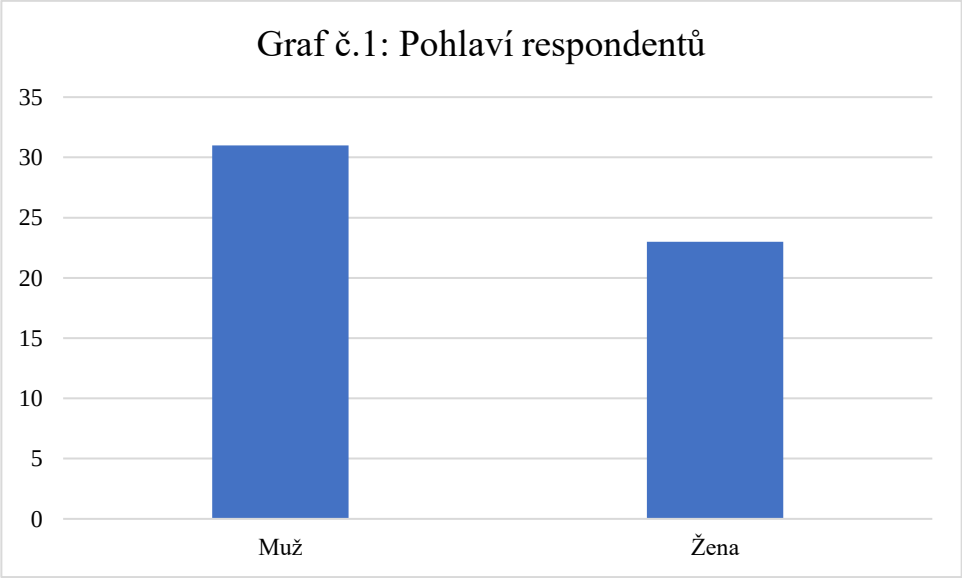
6.2 Výsledky dotazníkového šetření

Dotazník vyplnilo celkem 54 respondentů, kteří alespoň jednou navštívili Dark web, přičemž se jednalo o 31 mužů a 23 žen. Jak jednotliví respondenti na otázky odpovídali, jsem rozpracovala do grafů, jež obsahují otázky a odpovědi, ze kterých respondenti následně vybírali, popřípadě odpovědi, které poté svévolně doplnili. Zda se hypotézy potvrdily, či vyvrátily, je obsaženo v kapitole závěr.

Otázka č. 1: Připojili jste se někdy k webu známému pod názvem Dark web?

Dotazníkové šetření začíná otázkou, zda respondent někdy navštívil web zvaný Dark web, pokud je odpověď záporná, tak pro něj dotazníkové šetření končí. Na otázku odpovědělo kladně 54 respondentů. Jak již bylo zmíněno výše, potenciálně bylo na sociálních sítí osloveno téměř 14 000 respondentů. Dotazník byl umístěn na diskuzní fóra a také na několik studijních a veřejných skupin. Ze studijních skupin se jedná o soukromou skupinu „UPCE, koleje“. Z veřejných skupin byl dotazník vložen například do skupiny s názvem „Dark web mysteries“.

Otázka č. 2: Uveďte, jakého jste pohlaví.

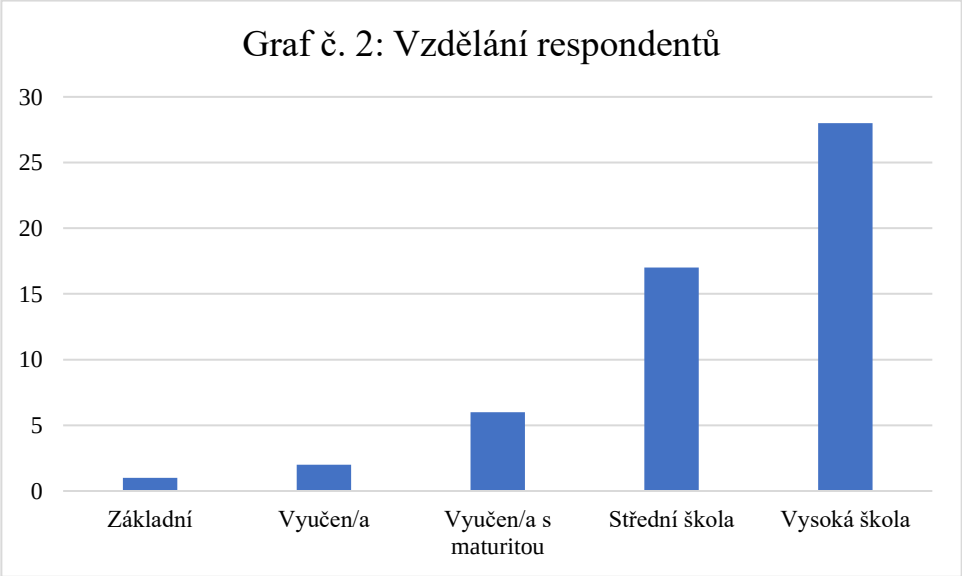


Větší část dotazovaných byla mužského pohlaví (31), zbytek tvořily ženy (23). Jelikož se jedná o kybernetický prostor, jenž je známý svou stinnou stránkou, lze předpokládat, že bude převaha mužských respondentů. Dle mého názoru muži častěji vyhledávají adrenalin nežli ženy. O účincích adrenalinu lze nalézt nespočet studií, mnohdy je však mylně uváděno, že adrenalin vyvolává stres, avšak tento hormon má zcela

opačný účinek. V prvé řadě nastoupí stres a až poté tělo začne produkovat zvýšené množství adrenalinu.

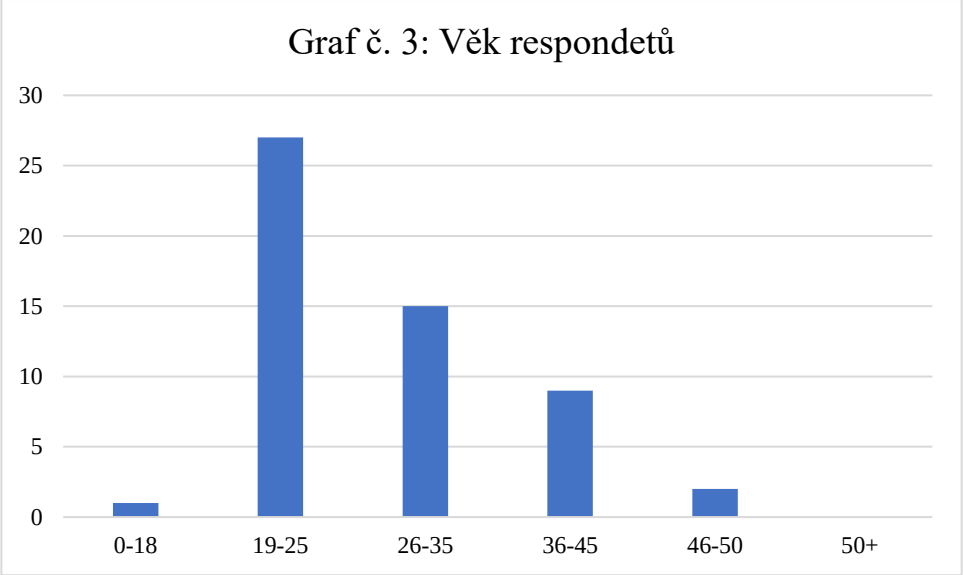
Psycholožka Marie Vágnerová dodává, že: *„Muži mají tendenci k rizikovému chování, potřebují dosahovat sebepotvrzení riskantní aktivitou, ať už jde o fyzické nebezpečí či profesní aktivity. Cesta k mužnosti bývá spojena s nutností podstupovat různé zkoušky a dokazovat si svou sílu a odolnost.“* (Jesenská, 2019, online)

Otázka č. 3: Vaše nejvyšší dosažené vzdělání?



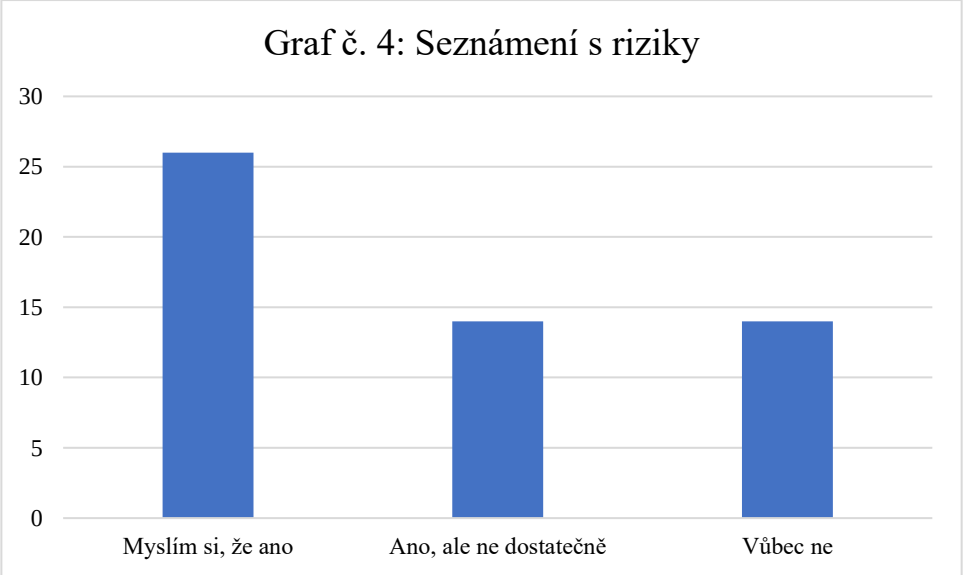
Dotazovaní respondenti byli různého stupně vzdělání, přičemž je možné konstatovat, že nejčastěji se jednalo o vysokoškolské vzdělání (28), dále pak středoškolské (17), vyučen s maturitou (6), vyučen (2) a pouze jedna osoba měla základní vzděláním. Předpokládám, že převahu vysokoškolského vzdělání u respondentů lze přikládat faktu, že dotazník byl mimo jiné vložen na studijní skupinu „UPCE, koleje“.

Otázka č. 4: Do jaké věkové kategorie byste se zařadili?



Výzkumného šetření se zúčastnily osoby rozličných věkových kategorií. Z odpovědí vyplývá, že polovinu dotazovaných (27) tvořili lidé ve věku 19 až 25 let. Opět se domnívám, že věk respondentů byl ovlivněn platformou, na kterou byl dotazník vkládán. Druhá nejčetnější skupina (15) byla tvořena respondenty ve věku 26 až 35 let. Třetí pozici (9) obsadili respondenti ve věku 36 až 45 let. Dva respondenti byli ve věku 46 až 50 let. A pouze jeden respondent byl ve věku do 18 let.

Otázka č. 5: Seznámili jste se s možnými riziky před vstupem na tento web?



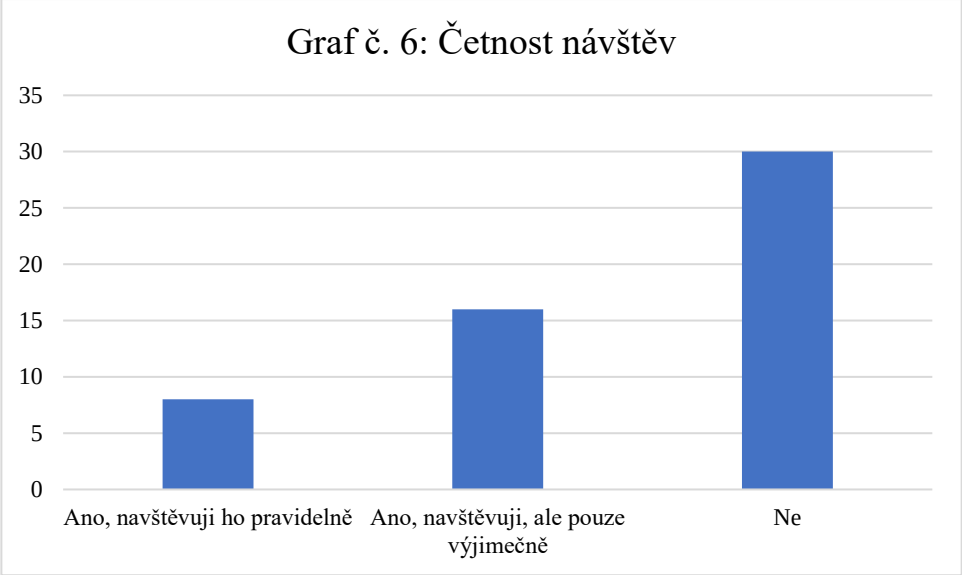
Téměř polovina respondentů (26) se před vstupem na Dark web dostatečně obeznámila s riziky, která na síti hrozí. Seznámení se s riziky před samotným vstupem na

tuto síť má nezastupitelnou roli v ochraně uživatele před možným zneužitím. Je důležité, aby měl uživatel neustále na paměti, že jakmile rozklikne odkaz, není cesty zpět. Přestože se jedná o anonymní prostor, uživatel není zcela skryt před zraky úřadů a za jakoukoliv nelegální činnost může být stíhán. Částečné a žádné seznámení s riziky bylo početně vyrovnané (14). Částečné seznámení s riziky je v tomto případě naprosto nedostačující. Obávám se, že uživatelé, kteří se dostatečně neobeznámí s riziky, riskují přinejmenším infikování svého zařízení Malwarem, jenž může mimo jiné zapříčinit odcizení osobních údajů týkajících se platební karty či jiných finančních dat spotřebitele.

Otázka č. 6: Jak jste se o existenci Dark webu dozvěděli?

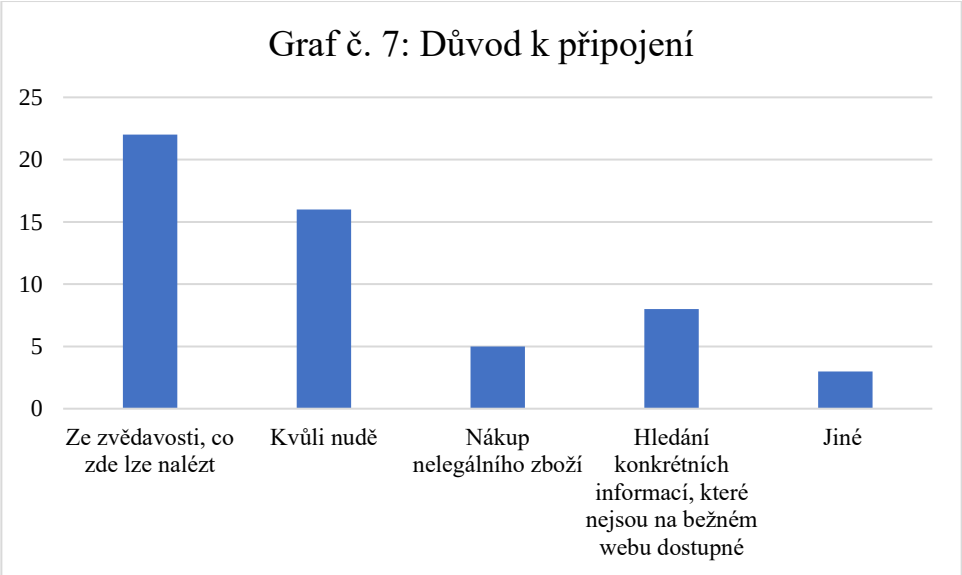
Drtivá většina respondentů (34) se o existenci Dark webu dozvěděla prostřednictvím internetu. Touto odpovědí jsem nebyla nikterak zaskočena, jelikož lze na indexovém webu, který je snadno dostupný skrze standardní vyhledávače, narazit na nespočet stránek, blogů a diskusních fór zaměřujících se na tuto temnou síť. Na tomto místě je dlužno dodat, že potencionální uživatel si na indexovém webu může poměrně snadno dohledat informace, jak se před vstupem na samotnou síť chránit a snížit tak riziko zneužití na minimum. Dále se nejčastěji respondenti o Dark webu dozvídají prostřednictvím svých přátelé (9). Zbývající odpovědi zahrnovaly rodinu (1), práci (2), televizi (5) či školu (3).

Otázka č. 7: Zaujal Vás Dark web a navštěvujete jej pravidelně?



Z odpovědí na otázku zabývající se opětovnou návštěvou Dark webu jsem byla překvapená, předpokládala jsem, že zájem o opětovnou návštěvu této sítě bude minimální. Z výše uvedených odpovědí vyplývá, že 30 respondentů účastnících se dotazníkového šetření již Dark web znovu nenavštěvuje. Zbylá část respondentů (24) Dark web navštěvuje pravidelně či výjimečně.

Otázka č. 8: Co Vás vedlo k připojení se k tomuto webu?



Nejčastějším důvodem k připojení (22) byla zvědavost. Přestože se uživatel rozhodne Dark web navštívit čistě ze zvědavosti, obávám se, že neskončí pouze na stránkách, jež se svým obsahem zaměřují na prodej omamných látek. Možná jsem naivní,

ale předpokládám, že pokud se jedinec rozhodne Dark web navštívit čistě ze zvědavosti a potřeby objevovat něco nového, před vstupem se dostatečně seznámí s riziky, jelikož se bude chtít dozvědět co nejvíce informací. Dle mého názoru mají uživatelé Dark webu velmi snadný přístup k lehkým i tvrdým drogám či zbraním. Ovšem pro čistě zvědavé návštěvníky může být zklamáním, že mnoho indexů Dark webu, které se netýkají prodeje drog či zbraní, nefungují. Různá "creepy" videa, utajené materiály nebo rekrutování do možných kultů jsou zde k nalezení jen zřídka. Většina webů obsahujících tato témata je složitě dohledatelná a vyžaduje různé způsoby prokázání, a to v těch lepších případech. V těch horších je pro přístup na web požadováno splnění nejrůznějších úkolů.

Jako druhý nejčastější důvod návštěvy respondenti uváděli nudu (16). Pokud je hlavní příčinou návštěvy Dark webu nuda, je dle mého názoru více pravděpodobné, že se uživatel před vstupem na síť s riziky dostatečně neseznámí, neboť se o prevenci nebude zajímat. Jako třetí nejčastější důvod návštěvy (8) uživatelé uváděli hledání informací, které nejsou na indexovém webu dostupné. Pouhých 5 uživatelů navštívilo Dark web za účelem nákupu nelegálního zboží. V dotazníkovém šetření 3 respondenti uvedli, že Dark web navštívili z důvodu:

a) zaplnění volného času v nemocnici po operaci.
b) kvůli „kšeftům“.
c) viděl jsem to v TV a chtěl jsem najít konkrétní věc.

Otázka č. 9: Na jaký obsah jste na Dark webu narazili?

Z odpovědí respondentů je patrné, že se na Dark webu nejčastěji potýkali s podobným obsahem, jednalo se především o pornografický materiál (dětský, zvířecí, hardcore porno), prodej drog a zbraní. Vzhledem k tomu, že jsem pro potřeby této bakalářské práce Dark web sama navštívila, jsem očekávala, že právě se výše zmiňovaným obsahem se respondenti budou nejčastěji setkávat. Přestože se jednalo pouze o letmé nahlédnutí pod roušku této stinné stránky internetu, troufám si tvrdit, že jsem si o webu vytvořila obrázek. Ovšem několik respondentů (8) uvedlo, že na Dark webu narazili na obsah s odlišnou tématikou, jednalo se především o:

a) Vražda na zakázku
b) Konspirační webové stránky a politicky orientované stránky
c) Fórum pro pedofily
d) Obchod s bílým masem

e) Praní špinavých peněz, celkově obchodování s bitcoiny a nelegálními komodity
f) Návody na výrobu bomby a drog
g) Místnosti typu Red room
h) Videa se zvráceným obsahem (násilí, týrání, znásilnění)

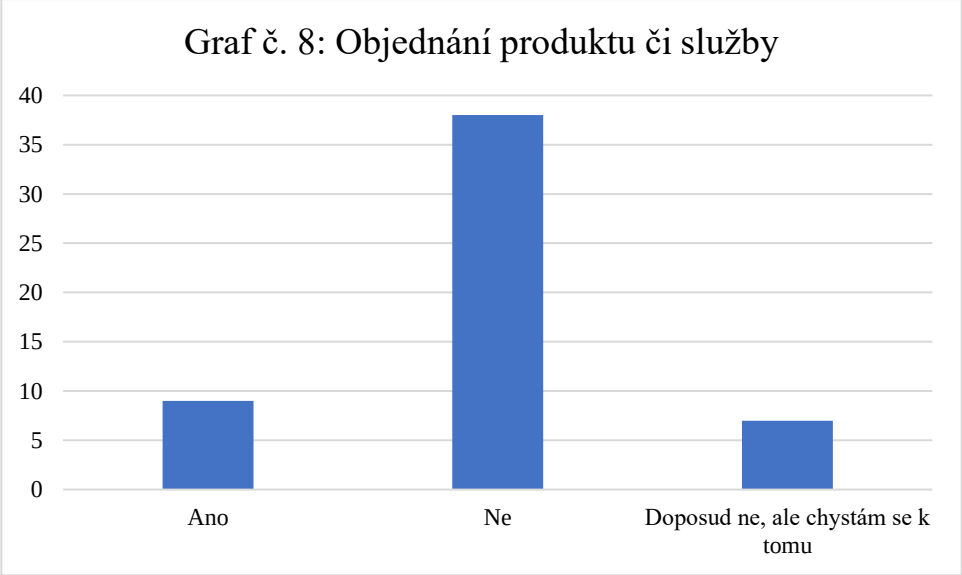
Otázka č. 10: Jaký obsah nejčastěji vyhledáváte?

Dle mého předpokladu uživatelé nejčastěji vyhledávali obsah, jenž se primárně zaměřuje na prodej nelegálního zboží. Na výběr má uživatel z mnoha stránek nabízejících například zfalšování dokladů. Jedním z nich je UK Passports. Zde má uživatel možnost obstarat si falešný pas nebo bankovní účet společně s platební kartou. Falešné doklady působí velmi realisticky a dle prodejců je takřka nemožné rozeznat falsum od skutečného dokladu. Cena je poměrně vysoká, za pas zájemce zaplatí v přepočtu 1000 GBP (29 778 CZK) a cena bankovního účtu činí 700GBP (20 845 CZK). Dále uživatelé často vyhledávali nejrůznější stránky zaměřující se na prodej zbraní. Na Dark webu si uživatel může bez vynaložení většího úsilí obstarat například ruční zbraň Glock 19 za cenu 500 GBP (14 889 CZK). Není žádným tajemstvím, že častým důvodem návštěvy Dark webu je koupě drog, a respondenti dotazníkového šetření nebyli výjimkou. Uváděli, že právě prodej omamných látek je zaujal. Je nutno dodat, že Dark web nabízí pestrou škálu webů, kde lze nalézt snad každou drogu, na kterou zájemce pomyslí. Ovšem řada respondentů (11) odpověděla zcela odlišně:

a) Věci týkající se vlády a politiky.
b) Stránky s torrenty.
c) Zajímalo mě, jestli tady najdu informace o sobě, a našla jsem je.
d) Vyhledávala jsem prášky na hubnutí, které nejsou k prodeji v obchodech.
e) Od všeho kousek, zajímalo mě, kolik stojí objednání vraždy a jak si ji mohu objednat.
f) Navštěvuji darkweb Facebook.
g) Obvykle se snažím najít obsah, který je něčím zvláštní (paranormální).
h) Cheaty na Fifu.
i) Hledal jsem informace o hackování Facebooku účtu.
j) Nepoužívám ho pro vyhledávání něčeho konkrétního, spíše pro bezpečné sdílení souborů.

k) Nejčastěji bych to nenazvala, ale hledala jsem třeba informace o padělání dokladů a zajímalo mě, jestli si tady můžu koupit dítě, protože jsem o tom slyšela.

Otázka č. 11: Objednávali jste si z webu nějaký produkt či službu?



V následující otázce jsem zjišťovala, zda si uživatelé v minulosti na Dark webu objednali nějaký produkt či službu. Z odpovědí je patrné, že 38 dotazovaných služby Dark webu nevyužilo. Nutno dodat, že 9 respondentů, již služby Dark webu v minulosti skutečně využili, nebo se k tomu v budoucnu chystají (7). Vzhledem k anonymitě, která k Dark webu neodmyslitelně patří, mne odpověď respondentů nepřekvapila, ba naopak jsem čekala, že kladně odpoví více respondentů.

Otázka č. 12: Co jste si na Dark webu objednali?

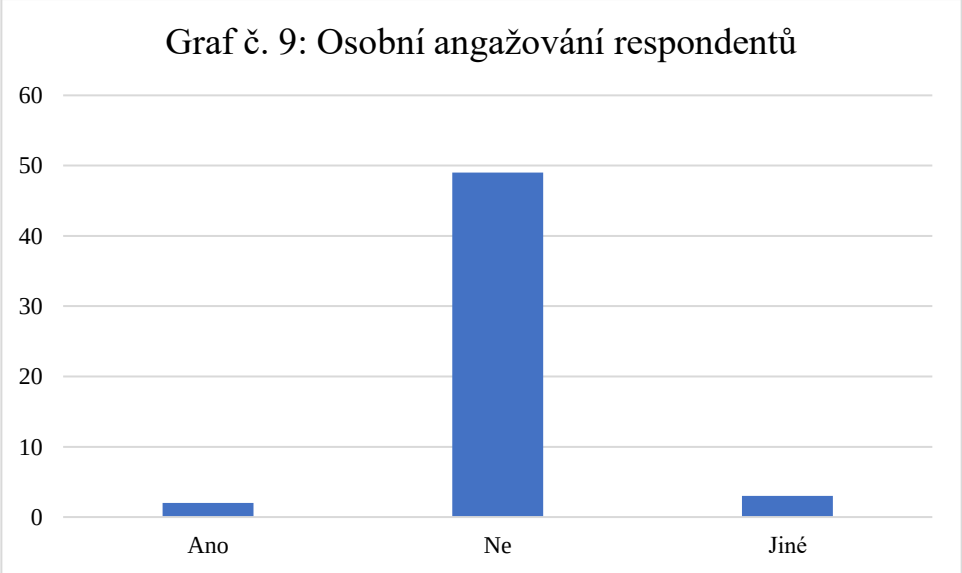
Na otázku č. 11 odpovědělo kladně 9 respondentů. Jak jsem předpokládala, uživatelé si na Dark webu nejčastěji objednávali zejména omamné látky. Velmi mne zaujala odpověď respondenta, který se zmínil, že si z Dark webu objednal tzv. „Darknet box“. Jedná se o novodobý trend, který je populární zejména na internetové platformě YouTube. Tvůrci videí si na Dark webu mnohdy i za několik tisíc dolarů objednají tzv. „mystery box“, jedná se o obyčejnou krabici, plnou nejrůznějších neznámých předmětů. Shlédla jsem několik videí, ve kterých lidé otevírají výše zmíněné boxy. V tomto „mystery boxu“ lze narazit na nejednu podivnost a to například: woodoo panenka, USB flash disk s nejrůznějšími videi, použité dětské oblečení, biologický materiál, zbraně atd. Další odpovědi respondentů byly následující:

a) Amfetamínovú pastu, mdma, ket (isomer S)
b) Prášky podporující hubnutí
c) Darknet box
d) Pravý tabák z Kolumbie
e) 2x pornografický materiál
f) Byliny
g) Drogy
h) Koks

Otázka č. 13: Dorazila Vám objednávka či byla služba vykonána?

Z výše zmiňovaných devíti dotazovaných sedm respondentů objednaný produkt skutečně obdrželo. Zbylí dva respondenti se svého produktu zatím nedočkali. Odpovědi respondentů na tuto otázku mne překvapily, jelikož jsem se domnívala, že produkt skutečně obdrží jen zlomek respondentů.

Otázka č. 14: Nabízeli jste někdy své služby či produkty na Dark webu?

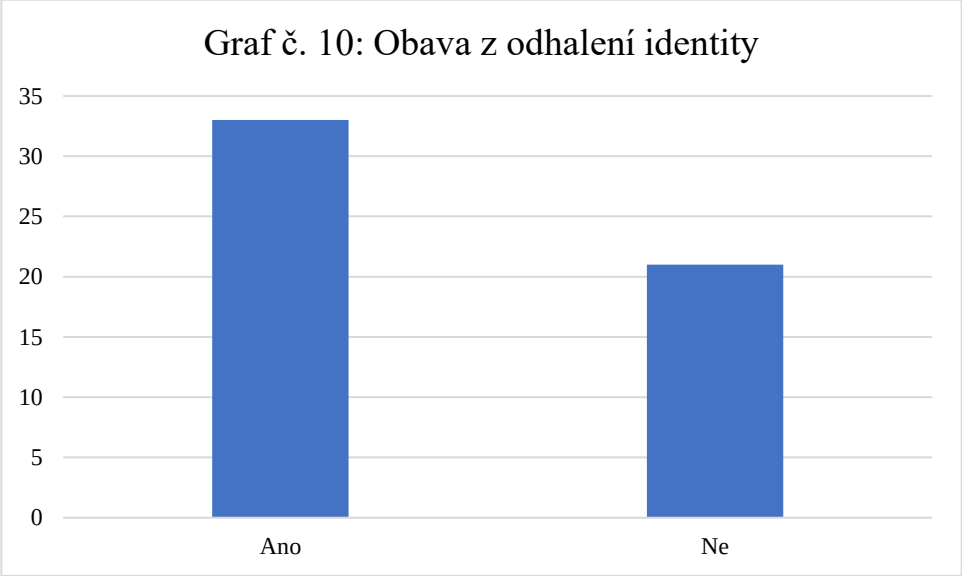


Jiné:

a) Nevím jak.
b) Sdílel soubory.
c) Jak mohu nabízet?

Na výše zmíněnou otázku odpovědělo 49 respondentů záporně, pouze 3 dotazovaní se osobně angažovali a nabízeli své služby či zboží. Jeden z respondentů, který nabízel své služby, dodal, že se jednalo o sdílení souborů. Pro sdílení souborů na Dark webu slouží například nástroj s názvem „OnionShare“, jenž zprostředkovává bezpečné a anonymní sdílení souborů v síti Tor.

Otázka č. 15: Máte obavy, že při návštěvě Dark webu někdo odhalil Vaši identitu?



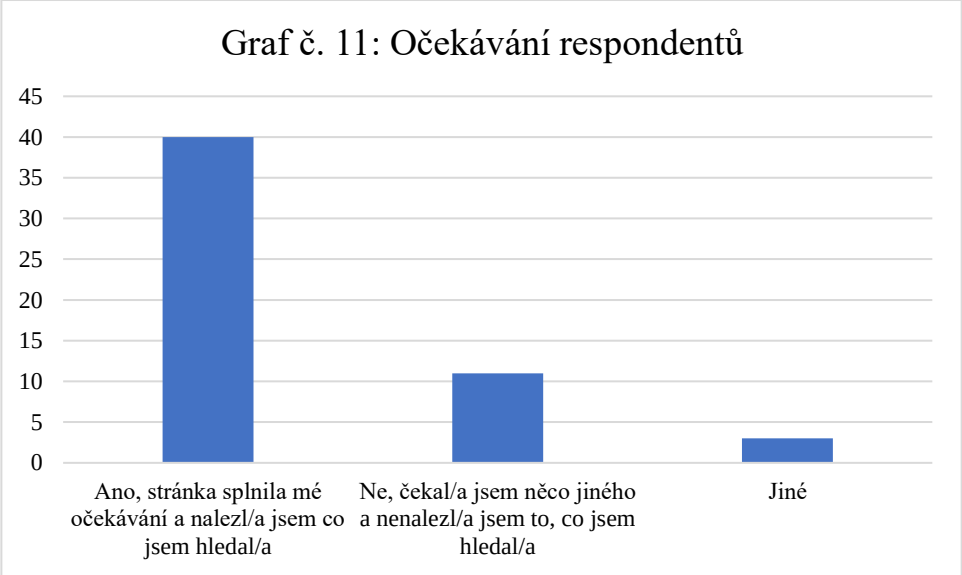
Z odpovědí je patrné, že více jak polovina respondentů (33) má reálné obavy, že při návštěvě sítě mohlo dojít k odhalení jejich identity. Zbytek dotazovaných (21) takovéto obavy nepociťuje. Pokud se uživatel sítě rozhodne Dark web navštívit, je zde reálná možnost, že dojde k odhalení jeho identity. Je proto důležité, aby uživatel učinil potřebná ochranná opatření, která jsou zcela nezbytná pro pohyb na této síti. Je důležité, aby si uživatel vyhledal software, jenž slouží ke skrytí IP adresy, obecně známý jako VPN. Dle mého názoru je vhodný software s názvem TunnelBear, který je velice bezpečný, ovšem není určený pro větší přenosy dat. Je však nutné mít na paměti, že první je potřeba spustit službu VPN a až poté TOR.

Otázka č. 16: Vyhrožoval Vám někdo po návštěvě Dark webu?

Všichni respondenti (54) odpověděli na tuto otázku záporně a žádné vyhrožování po návštěvě Dark webu neproběhlo. Odpověď na tuto otázku mne mile překvapila, avšak nutno dodat, že přestože nedošlo k žádnému vyhrožování, je důležité, aby uživatelé, kteří

se rozhodnou Dark web i nadále využívat, byli stále ostražití a dodržovali pravidla bezpečného pohybu na této síti.

Otázka č. 17: Splnila návštěva tohoto webu Vaše očekávání?



Většina respondentů (40) uvádí, že návštěva sítě splnila jejich očekávání a nalezli zde to, co hledali. Zbylých 11 dotazovaných odpovědělo záporně. Jak jsem již zmínila, čistě pro zvědavé návštěvníky může být návštěva Dark webu zklamáním, jelikož je mnoho indexů Dark webu, které se netýkají prodeje drog či zbraní, nefunkčních. Zbylí 3 respondenti odpověděli vlastními slovy (viz níže).

Jiné:

a) Návštěva byla ze zvědavosti. Už bych ho nikdy nenavštívila, nedá se ani říct, že něco splnilo mé očekávání.
b) Tak 50 na 50.
c) Nic jsem neočekávala.

Souhrn zkoumání a ověření hypotéz

Hlavním cílem výzkumného šetření bylo zmapovat aktivitu uživatelů Dark webu. Lze konstatovat, že cíl byl naplněn. Výzkumný soubor tvořili respondenti rozličného vzdělání a věku. Tito respondenti byli vybíráni náhodně skrze nejrůznější sociální sítě. Ve výzkumném šetření bylo dále stanoveno několik dílčích cílů. Prvním dílčím cílem bylo zjistit obeznámení uživatelů s riziky před vstupem na síť. Z šetření je patrné, že více

jak polovina respondentů (26) si myslí, že se s nimi dostatečně obeznámila. Částečné a žádné seznámení s riziky bylo početně vyrovnané. Jelikož se většina respondentů (34) o existenci Dark webu dozvěděla prostřednictvím internetu, očekávala bych, že počet respondentů, již se s riziky obeznámili důkladněji, bude vyšší, jelikož v souvislosti s Dark webem je na internetu nespočet varování. Druhým dílčím cílem bylo zjistit důvod návštěvy sítě Dark web. Nejvíce respondentů (22) uvedlo jako důvod návštěvy zvědavost, což jsem také předpokládala, velmi mne však překvapilo, že celých 16 respondentů síť navštívilo z nudy. Mým očekáváním bylo, že tato odpověď bude nejméně zastoupená, jelikož se jedná o prostředí, jež skýtá různá nebezpečí, ba naopak tato odpověď byla na druhém místě. Třetím dílčím cílem bylo zjisti, jaký obsah uživatelé nejčastěji vyhledávají. Nejčastěji vyhledávaným obsahem byly stránky zabývající se prodejem nelegálního zboží, jako jsou drogy, zbraně a falešné doklady. Čtvrtým dílčím úkolem bylo zjistit, zda návštěva Dark webu splnila očekávání respondentů. Drtivá většina respondentů (40) odpověděla, že Dark web splnil jejich očekávání a nalezli zde to, co hledali.

Byla stanovena hypotéza č. 1: *Z pohledu zkoumané skupiny budou více zastoupeni muži než ženy.* Hypotéza byla potvrzena.

Lze konstatovat, že dotazníkového ošetření se skutečně zúčastnili převážně respondenti mužského pohlaví (31). Jak jsem již zmínila výše, tak muži inklinují k rizikovému chování a v životě potřebují dosahovat sebepotvrzení jakoukoliv riskantní aktivitou. Z výsledků dotazníkového šetření dále vyplývá, že nejvyšší zastoupení v šetření měli respondenti s vysokoškolským vzděláním (28). Přihlédneme-li k povaze platforem, na které byl dotazník vkládán, jedná se o předvídatelné zjištění.

Byla stanovena hypotéza č. 2: *Více než polovina respondentů se před samotným vstupem na Dark web dostatečně obeznámí s riziky.* Hypotéza byla vyvrácena.

S riziky se dostatečně obeznámilo 26 respondentů, avšak očekávala jsem, že toto číslo bude značně vyšší, jelikož se jedná o záludné místo, které budí patřičný respekt. Pokud je záměrem uživatele „pouhé“ vyhledávání pirátských kopií filmů, či hudby je vystaven potencionálnímu riziku. Ovšem pokud uživatel bezmyšlenkovitě proklikává jednotlivé odkazy, aniž by dbal větší pozornosti, riziko se značně zvyšuje. Jak uvádí aktivní uživatel Dark webu: *„Zlatou radou je jednoduše neklikat na nic, co vypadá podezřele. Nezkušený uživatel může skončit minimálně s keyloggerem (hackovací nástroj, pozn. tazatele) v PC a do hodiny s prázdným bankovním účtem. V jiném případě se zase můžete prokliknout na stránku s něčím hodně nepříjemným, co vás asi dokáže změnit.*

Vždy říkám, že na síti se nikdy nevyplácí nikomu 100 % věřit a na Dark webu toto platí přesně 100x tolik. Řiďte se tím a hned je riziko poloviční.“ (Kňazovický, 2019, s. 43)

Byla stanovena hypotéza č. 3: ***Nadpoloviční většina respondentů uvede reálné obavy, že při návštěvě Dark webu došlo k odhalení jejich identity.*** **Hypotéza byla potvrzena.**

Z šetření vyplývá, že 33 respondentů má reálné obavy, z možného odhalení jejich identity. Přestože mnozí provozovatelé se snaží zajistit co možná nejvyšší anonymitu, identitu na Dark webu mohou odhalit některé JavaScripty. Odhalenému uživateli pak může hrozit policejní vyšetřování, stalking, kyberstalking, zneužití identity či odcizení peněz atd. Proto je velmi důležité, aby uživatel dodržoval pravidla bezpečného pohybu na této síti viz kapitola č. 3, výrazně pak sníží riziko odhalení své identity.

Byla stanovena hypotéza č. 4: ***Více než polovina dotazovaných mající zkušenost s Dark webem, jej již znovu nebude navštěvovat.*** **Hypotéza byla potvrzena.**

Dle mého předpokladu více jak polovina (30) respondentů již Dark web nenavštěvuje. Domnívám se, že důvodem je především zklamání respondentů vyplývající z přehnaného očekávaní, co vše lze na Dark webu nalézt. Pokud se pro návštěvu Dark webu uživatel rozhodne pouze z čisté zvědavosti, nemá potřebné znalosti proto, aby se dostal dál než na Hidden wiki.

Byla stanovena hypotéza č. 5: ***Více jak 50 % respondentů uvede, že návštěva Dark webu splnila jejich očekávání.*** **Hypotéza byla potvrzena.**

Více jak polovina respondentů (40) uvedla, že návštěva Dark webu splnila jejich očekávání. Jak jsem předpokládala, dotazníkové šetření tuto hypotézu skutečně potvrdilo. Domnívám se, že za úspěšným potvrzením hypotézy stojí především fakt, že cílem návštěvy většiny respondentů byl obsah, jenž je primárně zaměřen na omamné látky. Takovýto obsah je na Dark webu velmi snadno dostupný, a tudíž není důvod, aby byl respondent zklamán.

6.3 Pohled respondentů na prevenci v kybernetickém prostoru

V praktické části bakalářské práce jsem provedla kvantitativní dotazníkové šetření viz výše, které přineslo povrchnější rozbor aktivit uživatelů Dark webu. Pro hlubší a podrobnější náhled do problematiky prevence v kybernetickém prostoru, které je věnována nemalá část práce, jsem dále zpracovala kvalitativní šetření prostřednictvím strukturovaného rozhovoru, v jehož rámci mi byly poskytnuty čtyři rozhovory.

Dle Gavory lze rozhovor definovat jako *„výzkumnou metodu, která umožňuje zachytit nejen fakta, ale i hlouběji proniknout do motivů a postojů respondentů.“*

Cíl výzkumného šetření

Hlavním cílem šetření je zmapovat pohled účastníků rozhovoru na prevenci v kybernetickém prostoru. Pro získání dat byl využit kvalitativní způsob zkoumání, realizovaný již zmíněnou formou rozhovoru se sociální patolžkou, policisty a IT odborníkem.

Prezentovaný cíl bakalářské práce byl přetvořen do hlavní výzkumné otázky (HVO):

- HVO I. *Jakým způsobem dotazovaní nahlížejí na oblast kybernetického prostoru ve vztahu k dětem a mladistvým?*

Hlavní výzkumná otázka se pak člení do tří dílčích výzkumných otázek (DVO), jež jsou dále rozpracovány do jednotlivých tazatelských otázek (TO):

- DVO I. *Jakým způsobem dotazovaní vnímají rodinu, jakožto jeden ze stěžejních prvků v oblasti prevence?*
    - TO 1. Mnozí rodiče se domnívají, že pokud svému dítěti zakážou používat sociální sítě, tak jej tím nejlépe ochrání. Co si o tom myslíte?
    - TO 2. Jak by měl dle Vašeho názoru postupovat rodič, který se dozví, že jeho dítě navštěvuje nevhodné stránky?
    - TO 3. Máte nějakou preventivní radu pro rodiče, která by mohla napomoci zajistit bezpečnost jejich nezletilých dětí na internetu?
    - TO 4. Řada rodičů přidává fotografie svých dětí na sociální sítě bez jejich svolení tzv. sharenting. Jaký je Váš názor na tuto problematiku?
- DVO II. *Jaké jsou zkušenosti a názory respondentů na možné nástrahy kybernetického prostoru pro nezletilé?*

- TO 5.Jaké jsou z Vašeho odborného pohledu největší hrozby v kybernetickém prostoru pro dítě?
- TO 6. Která věková skupina je dle Vašeho názoru v anonymním prostoru internetu nejzranitelnější? A proč?
- TO 7. Jaký je Váš názor na sociální sítě Facebook, Instagram, Twitter? Dovolil byste Vašemu dítěti, aby je využívalo? Popřípadě od jakého věku?
- TO 8. Pokud byste měl vyjmenovat tři základní pravidla bezpečného pohybu na sítí, která by měla být předána dětem, jaká by to byla?
- TO 9. Jaký máte názor na tzv. rodičovské filtry? Opatřil/a byste si tento typ aplikace v zájmu bezpečí Vašeho dítěte?

➢ DVO III. *Jakým způsobem dotazovaní vnímají školu jakožto jeden ze stěžejních prvků v oblasti prevence?*

- TO 10. Domníváte se, že základní prevenci rizikového chování v online prostředí by dětem měla zprostředkovávat rodina, nebo je to podle Vás úkol školy?
- TO 11. Internet, mobily a sociální sítě jsou zpravidla nedílnou součástí života dětí a dospívajících. Jste onoho názoru, že by se na školách měl zavést předmět, který by žáky učil bezpečnému pohybu na síti? A proč?
- TO 12. Jaký je Váš názor na současnou podobu vzdělávání dětí v oblasti IT (výuka zaměřena na orientace v programech Word, Excel a Powerpoint)?

Tabulka č. 3: **Transformace výzkumného cíle do výzkumných otázek**

Hlavní výzkumná otázka (HVO)	**Dílčí výzkumné otázky (DVO)**	**Indikátory**	**Tazatelské otázky (TO)**
Jakým způsobem dotazovaní nahlížejí na oblast kybernetického prostoru ve vztahu k dětem a mladistvým?	DVO I. Jakým způsobem dotazovaní vnímají rodinu, jakožto jeden ze stěžejních prvků v oblasti prevence?	Povolení užívání sociálních sítí nezletilým	TO 1. Mnozí rodiče se domnívají, že pokud svému dítěti zakážou používat sociální sítě, tak jej tím nejlépe ochrání. Co si o tom myslíte?
		Vhodná reakce rodičů na již stávající problém	TO 2. Jak by měl dle Vašeho názoru postupovat rodič, který se dozví, že jeho dítě navštěvuje nevhodné stránky?
		Vlastní preventivní rada pro rodiče	TO 3. Máte nějakou preventivní radu pro rodiče, která by mohla napomoci zajistit bezpečnost jejich nezletilých dětí na internetu?
		Prevence v rámci nevhodného chování rodičů na síti	TO 4. Řada rodičů přidává fotografie svých dětí na sociální sítě bez jejich svolení tzv. sharenting. Jaký je Váš názor na tuto problematiku?
	DVO II. Jaké jsou zkušenosti a názory respondentů na možné nástrahy kybernetického prostoru pro nezletilé?	Identifikace hrozeb	TO 5. Jaké jsou z Vašeho pohledu největší hrozby v kybernetickém prostoru pro dítě?

Hlavní výzkumná otázka (HVO)	Dílčí výzkumné otázky (DVO)	Indikátory	Tazatelské otázky (TO)
		Riziková skupina	TO 6. Která věková skupina je dle Vašeho názoru v anonymním prostoru internetu nejzranitelnější? A proč?
		Sociální sítě	TO 7. Jaký je Váš názor na sociální sítě Facebook, Instagram, Twitter? Dovolil byste Vašemu dítěti, aby je využívalo? Popřípadě od jakého věku?
		Pravidla bezpečného pohybu na síti	TO 8. Pokud byste měl/a vyjmenovat tři základní pravidla bezpečného pohybu na sítí, která by měla být předána dětem, jaká by to byla?
		Efektivita a přínos rodičovských filtrů	TO 9. Jaký máte názor na tzv. rodičovské filtry? Opatřil/a byste si tento typ aplikace v zájmu bezpečí Vašeho dítěte?

Hlavní výzkumná otázka	Dílčí výzkumné otázky (DVO)	Indikátory	Tazatelské otázky (TO)
	DVO III. Jakým způsobem dotazovaní vnímají školu, jakožto jeden ze stěžejních prvků v oblasti prevence?	Hlavní činitel prevence	TO 10. Domníváte se, že základní prevenci rizikového chování v online prostředí by dětem měla zprostředkovávat rodina, nebo je to podle Vás úkol školy?
		Prostor pro zlepšení	TO 11. Internet, mobily a sociální sítě jsou zpravidla nedílnou součástí života dětí a dospívajících. Jste onoho názoru, že by se na školách měl zavést předmět, který by žáky učil bezpečnému pohybu na síti? A proč?
		Efektivita současné výuky informačních technologií	TO 12. Jaký je Váš názor na současnou podobu vzdělávání dětí v oblasti IT (výuka zaměřena na orientace v programech Word, Excel a Powerpoint)?

Zdroj: autor

Výzkumný vzorek

Selekce účastníků výzkumného šetření byla určena na základě nepravděpodobnostní metody výběru, konkrétně metodou účelového výběru. Dle Miovského se jedná o jednu z nejrozšířenějších metod výběru, s jakou se lze při aplikaci kvalitativního přístupu setkat. Miovský dále uvádí, že účelovost spočívá ve stanovení kritéria, na jehož základě cíleně vyhledáváme pouze ty jedince, kteří danému kritérium odpovídají a zároveň jsou ochotni se výzkumu zúčastnit. (Miovský, 2006, s. 135)

Výzkumný vzorek je tvořen celkem čtyřmi respondenty, jedná se o tři muže a jednu ženu. Pro zachování anonymity budou zúčastnění jedinci dále označování jako respondenti. Pro pohodlnější orientaci v interpretaci dat jsem se rozhodla každému z nich přiřadit číslo. Dále pro přehlednost přikládám tabulku, jež obsahuje tvrdá data.

Tabulka č. 4: **Souhrn respondentů**

Označení respondenta	**Pohlaví**	**Nejvyšší dosažené vzdělání**	**Profese**
R1	žena	Vysokoškolské bakalářské (Sociální patologie a prevence)	Studentka magisterského studia (Sociální pedagogika)
R2	muž	Vysokoškolské magisterské	IT konzultant
R3	muž	Středoškolské maturita	Příslušník PČR (obvodní oddělení)
R4	muž	Středoškolské maturita	Příslušník PČR (pořádková jednotka, instruktor)

Zdroj: autor

6.4 Interpretace zjištěných dat

Následující část práce je zaměřena na rozbor jednotlivých odpovědí získaných na základě vlastního výzkumného šetření. Pro pohodlnější orientaci v textu je tento úsek rozdělen do tří sekcí, dle jednotlivých dílčích výzkumných otázek (viz tabulka č. 3), které jsou pak dále děleny do příslušných tazatelských otázek.

6.5 DVO I.

DVO I. Jakým způsobem dotazovaní vnímají rodinu jakožto jeden ze stěžejních prvků v oblasti prevence?

Ke zpracování první dílčí výzkumné otázky jsem si zvolila tazatelské otázky číslo 1 až 4. V první řadě jsem se zaměřila na rodiče, jakožto stěžejní prvek v rámci prevence kybernetického ohrožení dětí na internetu. Zjišťovala jsem názory respondentů na mnohdy nekompromisní zákazy rodičů, kterými se snaží „ochránit“ své dítě před negativními vlivy sociálních sítí. Dále jsem se zaměřila na preventivní rady a vhodné postupy, které by respondenti doporučili rodičům, jejichž dítě je na síti aktivní. V neposlední řadě jsem zjišťovala názor respondentů na takzvaný sharenting.

TO 1. Mnozí rodiče se domnívají, že pokud svému dítěti zakážou používat sociální sítě, tak jej tím nejlépe ochrání. Co si o tom myslíte?

Všichni respondenti jsou toho názoru, že zakázat dítěti využívat sociální sítě není vhodné a je více než pravděpodobné, že zákaz povede k umocňování zájmu dítěte. Respondentka **R1** se domnívá, že tímto způsobem výchovy se daleko více prohlubuje propast mezi rodičem, dítětem a jejich vzájemnou důvěrou. Pokud rodiče dítěti zakážou využívání sociálních sítí, je více než pravděpodobné, že se dítě bude snažit tento zákaz nějakým způsobem obejít. Dále dodává, že by se rodiče měli zajímat o samotná rizika, která na platformách dítěti hrozí, a stanovit si pravidla, která se budou v souvislosti s internetem dodržovat. Respondent **R2** uvádí, že v této době je takřka nemožné dítěti zabránit v užívání sociálních sítí. A kdyby se jim to přeci jen povedlo, nejedná se o pomyslné vítězství. Pouze by vychovali mladého člověka, jenž bude zneužitelný na sociálních sítích i ve své plnoletosti (například finančními šmejdy). Respondent **R3** dodává: *„Myslím si, že zakázané ovoce chutná nejlépe a takový to zákaz by jen odsunul dítě či mladistvého od svých vrstevníků, kteří se na sociálních sítí běžně pohybují.“* Respondent **R4** je toho názoru, že zákazy v tomto případě nic nevyřeší, jelikož si dítě

k používání sociálních sítí cestu jednou zákonitě najít musí. Respondent se obává, že by takovéto dítě bylo z kolektivu ostatními vyčleněno.

TO 2. Jak by měl dle Vašeho názoru postupovat rodič, který se dozví, že jeho dítě navštěvuje nevhodné stránky?

Všichni respondenti se jednoznačně shodují, že zcela zásadní úlohu by v tomto případě měla sehrát komunikace. Respondentka **R1** uvádí, že je důležité, aby rodič s dítětem o těchto věcech mluvil a také zjistil důvod, jak a proč se na tyto stránky dítě dostalo. Dále je vhodné dítě upozornit, že stránky, jež navštívilo, pro něj nejsou vhodné. Respondentka shledává jako jednu z možností využití rodičovské kontroly, jež slouží k zamezení návštěvy nevhodné stránky dítětem. Respondentka dále upozorňuje na věk dítěte, který v tomto případě má významnou roli. Je patrné, že jinak bude rodič jednat s osmiletým chlapcem, který se na tyto stránky dostane, a jinak se čtrnáctiletým. Obdobně odpovídá respondent **R2**: *„Nezbývá než si s dítětem o tom otevřeně promluvit.“* Respondent **R3** dodává, že vyjma samotné rozmluvy s dítětem je v případě velmi vzpurného dítěte vhodné zvážit instalaci programu do PC zabezpečujícího jeho ochranu. Respondent **R4** se také vyjádřil k nezastupitelné roli komunikace rodiče s dítětem, která je dle jeho názoru zcela zásadní pro objasnění této problematiky.

TO3. Máte nějakou preventivní radu pro rodiče, která by mohla napomoci zajistit bezpečnost jejich nezletilých dětí na internetu?

Respondentka **R1** vnímá jako stěžejní opatření rodičovské kontroly, kde je možnost si zvolit stránky, které budou blokovány. Tímto způsobem se dá předejít návštěvě nechtěné stránky. Skrze toto zabezpečení lze také regulovat čas strávený na počítači či mobilu, který rodič dítěti určí. Další radou je dle respondentky neméně důležité budování důvěry mezi dítětem a rodičem. Je žádoucí, aby se rodiče alespoň minimálně orientovali na sociálních sítích a byli schopni tak s dětmi konzultovat možné rizikové jevy, které je mohou na internetu potkat. Je nezbytné, aby i témata sociálních sítí a kyberprostoru byla doma probírána. Respondent **R2** je dále toho názoru, že základem je „kamarádský“ vztah s dítětem. Pokud dítě narazí na internetu na něco nebezpečného, samo to rodičům poví. Vedle toho respondent dodává, že *„pokud se rodiče v online prostředí příliš nevyznají a nevědí, jaké informace svým dětem předat, měli by se sami rodiče v rámci svých možností dovzdělat.“* Respondent **R3** má obdobný názor jako respondentka R1, a to sice že důležitá je včasná informovanost dítěte o škodlivosti některých webů. Dále používání monitoringu-ochranných programů, kde je znemožněno se nezletilému na takovýto portál

dostat. Komunikaci, naslouchání a porozumění zmínil také respondent **R4** jakožto stěžejní prvky v prevenci, jež by mohly napomoci zajistit bezpečnost nezletilých dětí na internetu.

TO 4. Řada rodičů přidává fotografie svých dětí na sociální sítě bez jejich svolení (tzv. sharenting). Jaký je Váš názor na tuto problematiku?

Respondentka **R1** s tímto trendem nesouhlasí a uvádí: *„Když se podíváte na Instagram, tak je plný malých dětí, které jsou pár dní/měsíců staré, a dokonce se zde objevují i fotky přímo z porodního sálu. Většina profilů je veřejných, může se na tyto fotografie podívat kdokoliv. Tyto obrázky patří do rodinných alb, a ne na sociální sítě. Nikdy nevíte, kdo se na Váš profil podívá a jaké úmysly s přidanými fotografiemi má. Na internet patří umělecké fotky dětí. Absolutně nevhodné je přidávat záznamy z dovolených, kde jsou děti polonahé u moře či u bazénu. Navíc je dle statistik prokázáno, že Česká republika a servery, jako například rajce.idnes, patří mezi nejnavštěvovanější mezi pedofily, kteří používají fotografie pro své vlastní účely.“* Respondent **R2** považuje takovéto jednání za IT negramotnost a nemělo by k tomu docházet. Zatímco respondent **R3** vnímá jako zásadní problém především možné budoucí zesměšnění dítěte: “*Někteří rodiče nezletilých dětí mají sociální sítě jako prostředek, jak se se pochlubit či ukázat ostatním, kde byli, co dělají, co jedli a pili atd…neuvědomují si přitom, že vkládání fotografií svého dítěte, jak kupříkladu Anička poprvé kaká na nočníku, může být pro Aničku za 8-10 let, až někdo fotografii bude sdílet mezi vrstevníky, veliký problém“* Dále respondent **R4** s tímto novodobým fenoménem nesouhlasí a dodává: *„Nikdy jsem žádné fotografie svých dětí na sociální sítě neumístil. Hlavním důvodem je bezpečnost mé rodiny v souvislosti s mým zaměstnáním. Pracuji jako policista a několikrát mi bylo vyhrožováno fyzickou likvidací. Domnívám se, že tímto způsobem chráním svou rodinu.“*

Shrnutí dílčí výzkumné otázky I.

Z uvedených odpovědí vyplývá, že respondenti vnímají rodinu jako stěžejního činitele v oblasti prevence. Všichni dotazovaní se shodli, že zakázat dítěti využívat sociální sítě bude mít za důsledek umocnění touhy zákaz porušit. Z výzkumu je patrné, že zcela zásadní úlohu v prevenci má dle respondentů komunikace mezi rodičem a jeho dítětem. Pokud se rodič dozví, že jeho dítě navštěvuje nevhodné stránky, je důležité, aby si s dítětem o této problematice otevřeně promluvil. V rámci DVO I. byly dále mapovány preventivní rady pro rodiče, jež by napomohly zajistit bezpečnost nezletilých dětí na internetu. Z odpovědí respondentů je zřejmé, že je více než žádoucí pracovat na důvěře

mezi dítětem a rodičem. Polovina respondentů uvedla za účinný nástroj prevence tzv. rodičovskou kontrolu, jež sleduje aktivitu dětí na síti. Respondenti se shodli, že pokud rodič přidává fotografie svých dětí na sociální sítě, a to bez předchozího svolení, jedná se o IT negramotnost a nemělo by k tomu docházet. Je důležité, aby si rodič uvědomil, že internet je zcela veřejné místo a fotografie jejich dítěte může kdokoliv zneužít. Na tomto místě je dlužno dodat: *„Co internet schvátí, již nenavrátí.“*

6.6 DVO II.

DVO II. Jaké jsou zkušenosti a názory respondentů na možné nástrahy kybernetického prostoru pro nezletilé?

K objasnění druhé dílčí výzkumné otázky jsem použila tazatelské otázky číslo 5 až 9, ve kterých byly mapovány především hrozby, na které mohou děti při své návštěvě sítě narazit. Dále jsou otázky koncipovány tak, aby přinesly osobní náhled respondentů na sociální sítě, pravidla bezpečného pohybu, ale také efektivitu a přínos rodičovských filtrů, o kterých mají respondenti, jak je z DVO I. zřejmé, nemalý rozhled.

TO. 5 Jaké jsou z Vašeho odborného pohledu největší hrozby v kybernetickém prostoru pro dítě?

Všichni respondenti za největší hrozbu shledávají kontaktování dítěte falešným profilem za účelem jeho zneužití. Respondentka **R1** doplňuje, že se může jednat o žádost o intimní materiály či dokonce pozvání na osobní schůzku. Respondent **R2** za další výraznou hrozbu považuje prohlížení pornografického materiálu a možný vznik závislosti na kybernetickém prostoru, který by neměl být brán na lehkou váhu. Dítě, které je takto závislé, dle respondenta přichází o mnoho drahocenného času, který by mohlo věnovat něčemu prospěšnému pro svůj vývoj. Respondent **R3** dále zdůrazňuje, že zneužití důvěry dítěte může vést k následnému vydírání např. žádostí o posílání nahých fotografií či dokonce k osobnímu setkání. Svůj názor na nástrahy kybernetického prostoru uvedl také respondent **R4**, jenž za zásadní problém považuje vytržení dítěte z reality. Domnívá se, že děti vnímají virtuální svět jako jakousi obdobu světa reálného, a jsou tak velmi lehce zmanipulovatelné.

TO 6. Která věková skupina je dle Vašeho názoru v anonymním prostoru internetu nejzranitelnější? A proč?

V této otázce se respondenti shodovali zejména v názoru, že čím je dítě mladší, tím, je také zranitelnější a ovlivnitelnější. Respondentka **R1** považuje za nejzranitelnější věkovou skupinu dětí ve věku 8 až 13 let. Dále dodává, že*: „Přestože jsou některé sociální sítě umožněny dětem starším, je zřejmé, že i takováto věková kategorie zde působí. Je to kvůli tomu, že v tomto věku jsou děti velmi lehko manipulovatelné. Nemají tolik představu o reálném, ani o virtuálním světě a neuvědomují si možná rizika, které jsou s užíváním internetu spojena.“* Respondent **R2** by konkrétní věkovou skupinu neurčoval, ale je toho názoru, že čím mladší, a tudíž méně zkušené dítě je, tím více je v online prostoru zranitelné. Respondent **R3** je toho názoru, že nejvíce jsou děti zranitelné ve věku 10 až 15 let, kdy jsou značně důvěřivé a čekají na tu pravou lásku a pocit zamilovanosti, který jim přes písmenka navodí zkušený dospělý člověk. A poté je ke zneužití již jen pouhý pomyslný krůček. Respondent **R4** je stejného názoru jako respondent R3. Za nejzranitelnější věkovou skupinu lze považovat děti ve věku 10 až 15 let. Tato skupina je dle respondenta nejzranitelnější, jelikož je velmi jednoduché takto staré dítě obelstít a zmanipulovat. Respondent je také toho názoru, že dítě spadající do výše zmíněné věkové kategorie, není schopno dostatečně správně vyhodnotit všechny nástrahy kybernetického světa.

TO 7. Jaký je Váš názor na sociální sítě Facebook, Instagram, Twitter? Dovolil byste Vašemu dítěti, aby je využívalo? Popřípadě od jakého věku?

Respondentka **R1** uvádí jakožto uživatelka všech výše zmiňovaných platforem, že do jisté míry lze tyto sociální sítě shledávat za velmi užitečné. Respondentka je toho názoru, že skrze sociální sítě se člověk může nejen inspirovat, ale především poměrně brzy získávat nové informace, mnohdy i dříve než z televize. Dále uvádí, že Facebook a Twitter je v dnešní době spíše na ústupu. Tyto platformy hodnotí jako „sociální sítě pro staré“, tedy takové, které využívají rodiče, a i někteří prarodiče. Většina dětí využívá sociální sítě, jako je Instagram či TikTok. Tyto dvě zmíněné sítě respondentka považuje za více rizikové. Dále dodává: *„Já sama bych dítěti užívání sítí dovolila, a to zhruba od 13 let věku, ale vím, že dnes už se s nimi seznamují i děti mladší. Jak jsem zmiňovala v předchozích otázkách, i v této stojí za zmínku nastavení důvěry mezi rodičem a dítětem. Svolila bych sociální síť, ale chtěla bych mít přehled, jak se tam moje dítě prezentuje. Tím pádem by i věková hranice dítěte, kterou bych tolerovala, mohla být snížena.“*

Dotazovaný respondent **R2** je přesvědčen, že je velmi obtížné utvářet si názor na konkrétní sociální sítě, jelikož vznikají stále nové a také obsah na stávajících se mění. Respondent by si jako otec s dítětem promluvil o tom, jakou konkrétní aktivitu plánuje na dané sociální síti provozovat a buď by jej v dané aktivitě podpořil, nebo by se ji dítěti snažil vymluvit. Obecně by se pokoušel vést dítě k tvůrčí aktivitě namísto pasivní konzumace obsahu sociálních sítí nebo slepého následování trendů. Respondent **R3** by svému dítěti sociální sítě dovolil, jak respondent výstižně dodává, ať se nám to líbí, či ne, sociální sítě jsou nedílnou součástí života mladých lidí. Pokud je dítě dostatečně poučeno a seznámeno s riziky a má důvěru ve své rodiče, nebojí se kupříkladu říci, že bylo osloveno neznámým člověkem, tak nevidí důvod se obávat. Na otázku, od jakého věku by respondent svému dítěti dovolil využívat výše zmíněné platformy, odpověděl: *„Těžko říci, rodič musí sám rozhodnout o vyspělosti například 12leté slečny. Jedna si hraje s barbínami, druhá již má za sebou zkušenost s marihuanou.“* Respondent **R4** uvádí, že osobně nic nenamítá proti používání sociálních sítí, on sám je uživatelem platformy Facebook. Respondent dále zdůrazňuje: *„Jak jsem již zmínil, jsem velmi opatrný s tím, co na sociální sítě vložím. Zřejmě jsem paranoidní, ale na sociálních sítí nemám uvedeno ani své celé jméno a nemám zde vloženou žádnou fotografii, podle které by se má osoba dala identifikovat. Moji přátelé vědí, kdo jsem, mám je v přátelích a oni respektují to, že nemám zájem vkládat jakékoliv fotografie mé osoby, fotografie mé rodiny a žádné další osobní údaje na sociální sítě.“*

TO 8. Pokud byste měl/a vyjmenovat tři základní pravidla bezpečného pohybu na sítí, která by měla být předána dětem, jaká by to byla?

Respondentka **R1** uvádí jako první pravidlo nezveřejňování osobních údajů. Ať už se jedná o to, kde dítě bydlí, kam chodí do školy nebo jakou profesi vykonávají jeho rodiče. Dalším pravidlem by dle respondentky mělo být zabezpečení svých profilů do soukromého režimu a omezení přístupu neznámým lidem ke svému soukromí. K tomu se váže i fakt, aby děti neodpovídaly na zprávy lidem, které neznají ze svého blízkého okolí, popřípadě školy. A jako poslední, avšak neméně důležité pravidlo respondentka shledává nezveřejňování intimních, svůdných a jiných fotek, které by mohly dítě poškodit. Navíc by se při takovémto způsobu chování mohlo jednat o trestný čin. Respondent **R2** zdůrazňuje základní pravidlo včasného prodiskutování toho, co dítě hodlá zveřejnit na internetu ze svého soukromí. Dále by dítě mělo používat pouze ty stránky a online služby, o kterých si předem promluví s rodiči či učiteli, nebo o kterých od nich

slyšely. A v neposlední řadě by nemělo dítě důvěřovat neznámým lidem. Respondent **R3** dodává: *„Nepřijímej žádosti o přátelství s neznámými lidmi i dětmi. Nekomunikuj s cizím člověkem, informuj rodiče o tom, že jsi byl/a kontaktována. Neposílej nikomu žádné fotografie bez předchozího souhlasu jednoho z rodičů.“* Respondent **R4** apeluje především na ochranu soukromí, s níž jde v ruku v ruce nezveřejňování osobních údajů. Dále důrazně doporučuje nedůvěřovat neznámým lidem a vyhnout se posílání fotografií se sexuálním obsahem.

TO 9. Jaký máte názor na tzv. rodičovské filtry? Opatřil/a byste si tento typ aplikace v zájmu bezpečí Vašeho dítěte?

Respondentka **R1** tuto možnost zabezpečení již zmínila výše. Tento způsob ochrany nepovažuje za nevhodný, ba naopak. Respondentka vnímá rodičovskou kontrolu jako nástroj, který může dobře regulovat čas, jejž dítě stráví na telefonu/počítači, a navíc může zamezit tomu, aby dítě navštěvovalo některé nevhodné stránky, například pornografii. Respondentka R1 dále dodává: „*Už teď vím, že bych ráda sama své děti co nejvíce edukovala v oblasti online bezpečnosti a chtěla bych předejít tomu, abych tuto kontrolu musela zavádět. I já jako malá jsem bez ní vyrůstala. Plně si ale uvědomuji, že doba se mění a vliv sociálních sítí má rostoucí tendenci. V současné době se možná orientuji v tom, jak to na sítích chodí, ale kdo ví, co bude za pár let…Každopádně pokud by nebylo zbytí, nebála bych se možnost rodičovské kontroly využít.“* Respondent **R2** je opačného přesvědčení, domnívá se, že rodičovské filtry nejsou ideálním řešením, a je toho názoru, že jejich používání může nabourávat důvěru ve vztahu rodiče a dítěte, především pokud jsou rodičovské filtry použity k sledování aktivity dětí. Nicméně respondent dodává, že: „*Nežijeme v ideálním světě, myslím si, že vhledem k množství nebezpečí na internetu má jejich použití opodstatnění. Zároveň je třeba si i uvědomit, že rodičovské filtry nikdy neodizolují dítě od škodlivého obsahu na sítí na 100 %. Já osobně bych rodičovské filtry použil k blokování škodlivého obsahu, ale nesledoval bych aktivitu dítěte v síti.“* Respondent **R3** doplňuje, že rodičovské filtry považuje za velmi užitečnou aplikaci, a sám ji u svých dětí využívá. Dotazovaný respondent **R4** považuje rodičovské filtry za ideální řešení a v budoucnu hodlá tuto aplikaci pro kontrolu svých dětí na síti využívat.

Shrnutí dílčí výzkumné otázky II.

Z výše uvedeného vyplývá, že respondenti považují, za největší hrozbu, s níž se dítě může na síti potýkat, zejména kontaktování falešným profilem za účelem jeho zneužití. Za další výrazné hrozby respondenti považují prohlížení pornografického materiálu, vytržení z reality či vznik závislosti na samotném kybernetickém prostoru. V otázce zabývající se zranitelností dítěte s ohledem na věk se respondenti shodovali v názoru, že čím nižší je věk dítěte, tím vyšší je jeho zranitelnost. Mladší děti zpravidla nejsou schopny dostatečně správně vyhodnotit všechny nástrahy internetu. Z výzkumu dále vyplývá, že názory respondentů na sociální sítě jsou převážně pozitivní a při vhodném používání mohou být velmi užitečné. Je však na místě, aby dítě bylo dostatečně obeznámeno s riziky, která jsou s užíváním sociálních síti spjata. Za základní pravidla bezpečného pohybu na síti dotazovaní označili především nezveřejňování osobních údajů, dále pak nedůvěřování cizím lidem a nezveřejňování intimních fotografií. Součástí DVO II. bylo zmapovat názory respondentů na tzv. rodičovské filtry. Pohledy respondentů na tuto rodičovskou aplikaci, byly značně smíšené. Většina dotazovaných (R1, R3, R4) považuje rodičovské filtry za velmi užitečné aplikace, jež jsou vhodné nejen pro regulování času, který dítě na elektronickém zařízení stráví, ale navíc mohou zamezit tomu, aby dítě navštěvovalo některé nevhodné stránky. Respondent R2 je toho názoru, že se nejedná o ideální řešení, jelikož jejich používání může nabourávat důvěru ve vztahu rodiče a dítěte, především pokud jsou rodičovské filtry použity k sledování aktivity dětí.

6.7 DVO III.

DVO III. Jakým způsobem dotazovaní vnímají školu jakožto jeden ze stěžejních prvků v oblasti prevence?

K zjištění poslední vytyčené dílčí výzkumné otázky jsem si stanovila tři tazatelské otázky. Skrze tazatelské otázky číslo 10 až 12 jsem se pokusila zmapovat pohled respondentů na roli školství v edukaci a preventivní přípravě dítěte, jež aktivně prozkoumává kybernetický prostor. Zaměřila jsem se zejména na způsob výuky dětí v oblasti kybernetických rizik.

TO 10. Domníváte se, že základní prevenci rizikového chování v online prostředí by dětem měla zprostředkovávat rodina, nebo je to podle Vás úkol školy?

Respondenti R1, R2 a R4 jsou toho názoru, že je velmi důležitý podíl obou dvou složek. Respondentka **R1** uvádí, že spousta rodičů přistupuje k současnému školství jako k instituci, která se má podílet na osvětě dětí. Tak to ale dle jejího názoru není. Respondentka uvádí rodinu jakožto prvního činitele, jenž dítě formuje a dává mu potřebné základy. Respondentka výstižně dodává, že rodiče jsou mnohdy sami bezradní a na internetu se neorientují, jsou šťastní, když se vůbec seznámí s Facebookem. To ovšem ale jejich bariéru mezi dětmi neprolomí. Respondentka dále říká: *„Chápu, že role rodiče je v tomto ohledu velmi náročná. Nejsem ale zastáncem toho, že by problémy dětí na internetu měla do svých rukou brát ze sta procent škola. Ano, považuji za velmi důležité, aby i školní prostředí edukovalo žáky o rizicích internetu a vhodném chování na něm. Je ale na místě, aby se na vzdělávání dětí v tomto ohledu podíleli i rodiče.“*

Obdobného názoru je i respondent **R2**, který si taktéž myslí, že na prevenci rizikového chování by se měla podílet jak rodina, tak škola. Dle respondenta je důležité si uvědomit, že škola může dítěti přinést informace, které rodiče nemají, a naopak rodiče si mohou snadněji vytvořit přátelský vztah s dítětem, což jim může dopomoci se svěřením se dítětem v případě jeho ohrožení v online prostředí. Respondent však vyzdvihuje edukaci v rodině, která má významný vliv na rozvoj a informovanost dítěte, jelikož v době nástupu do školy je již na první prevenci o kybernetických rizicích pozdě. Respondent **R3** výrazně vyzdvihuje roli školy v edukaci dítěte. Domnívá se, že v dnešní době by mělo být více prevence na základních školách a dodává, že: „*Z vlastní zkušenosti vím a myslím si, že školství v tomto směru hodně pokulhává. Povinností rodiče je poučit dítě o nebezpečí, mělo by mít vryto některá pravidla pohybu na sociální sítí, stejně jako má vryto, že na červenou se prostě nepřechází.“* Respondent **R4** se domnívá, že informace o prevenci rizikového chování v online prostředí by dětem měla předat jak škola, tak rodina.

TO 11. Internet, mobily a sociální sítě jsou zpravidla nedílnou součástí života dětí a dospívajících. Jste onoho názoru, že by se na školách měl zavést předmět, který by žáky učil bezpečnému pohybu na síti? A proč?

Respondentka **R1** si jako jediná z dotazovaných není zcela jista, zda by měl být zaveden onen „speciální“ předmětu. Ze své vlastní zkušenosti udává, že děti nemají zájem o rozebírání jednotlivých definice a pojmů, které vlastně dobře znají z praktického hlediska. Dle jejího názoru je dostačující, aby škola zprostředkovala kvalitní besedu, která by měla za náplň informovat děti o možných rizicích, jež jsou s internetem spojeny. Dále

uvádí, že je neméně důležité, aby byl vybrán vhodný řečník. Respondentka doplňuje: *„Vím, že pokud přednášku dělá někdo, kdo je výrazně starší a je na něm znát, že s problematikou není tolik seznámen, děti pak neberou projev s takovou vážností a není pro ně tolik zajímavý.“* Respondent **R2** je opačného názoru, vnímá zavedení předmětu jako správný krok a dodává*: „Rozhodně by se měl zavést. Online prostředí je, jak říkáte, nedílnou součástí našich životů. Stejně tak jako děti učíme, jak se bezpečně pohybovat v provozu na ulici, je třeba jim vysvětlit, jak se pohybovat v online prostoru.“* Respondent **R3** souhlasí se zavedením onoho předmětu a uvádí, že prevence není nikdy dost a pro základní školy to platí dvojnásob. Dotazovaný respondent **R4** považuje zavedení onoho předmětu za nutnost a dodává*: „Internet a kybernetický prostor jsou nedílnou součástí většiny lidí a našich životů. Ve svém zaměstnání se čím dál častěji setkávám se šikanou, podvody, manipulací s lidmi prostřednictvím internetu.“*

TO 12. Jaký je Váš názor na současnou podobu vzdělávání dětí v oblasti IT (výuka zaměřena na orientace v programech Word, Excel a Powerpoint)?

Respondentka **R1** uvádí, že je velmi vděčná, že se na školách tyto dovednosti vyučují, jelikož své poznatky sama zužitkovala při studiu na vysoké škole, a to především při formátování prací či vytváření prezentací v Powerpointu. Dále dodává: *„Nevím, v jakém „duchu“ se nese současná výuka na školách, ale dle mého názoru je velmi důležité, aby bylo vzdělávání dětí v této oblasti realizováno.“* Respondent **R2** je toho názoru, že by se výuka měla více zaměřit na základy programování než na obsluhu konkrétních programů. Respondent by také propojil výuku IT s výukou matematiky. Je přesvědčen, že pokud děti pochopí základy tvorby programů, otevírá jim to mnohem zajímavější možnosti než znalost konkrétních programů. Respondent **R3** zdůrazňuje, že je více než žádoucí, aby mládež tyto programy ovládala. Avšak příhodně dodává, že: *„Než se začne s výukou těchto programů, měly by již děti mít za sebou výuku o bezpečném pohybu v kybernetickém světě. Je to jak v běžném světě, nejprve je autoškola a pak se řídí automobil. Nyní je informovanost o rizicích tak mizivá, že děti „řídí“ bez autoškoly, a to posléze má bohužel někdy katastrofální dopad.“* Dotazovaný respondent **R4** není schopen v současné době na tuto otázku odpovědět, jelikož jeho dítě, které je již školou povinné, prozatím neabsolvovalo předmět zaměřený na IT oblast. Respondent však dodává: *„V současné pandemické krizi jsem mile překvapen, jak děti zvládají on-line distanční výuku a s tím spojenou práci na počítači a internetu.“*

Shrnutí dílčí výzkumné otázky III.

V rámci DVO III. byla zjišťována role školy, jakožto jednoho ze stěžejních prvků v oblasti prevence. Téměř všichni respondenti se shodují, že v prevenci je velmi důležité, aby se angažovala jak rodina, tak škola. Respondent R3 výrazně vyzdvihuje roli školy. Domnívá se, že v dnešní době by mělo být více prevence na základních školách a z vlastních zkušeností uvádí, že školství v tomto směru značně zaostává. Zavedení speciálního předmětu do škol, který by žáky učil bezpečnému pohybu na síti, vnímá většina respondentů jako správný krok. Respondentka R1 si jako jediná z dotazovaných není zcela jista, zda by měl být zaveden onen „speciální" předmět. Domnívá se, že by zcela postačilo zprostředkovat kvalitní besedu, která by děti dostatečně obeznámila s riziky na síti. Názory respondentů na současnou podobu vzdělávání dětí v oblasti IT byly různorodé. Z odpovědí bylo patrné, že názory dotazovaných byly do jisté míry ovlivněny jejich povoláním a dosavadními životními zkušenostmi.

Závěr výzkumného šetření

Cílem výzkumného šetření bylo zmapovat, jakým způsobem dotazovaní nahlížejí na oblast kybernetického prostoru ve vztahu k dětem a mladistvým. Z odpovědí výzkumného šetření vyplývá, že respondenti jsou toho názoru, že rodina má stěžejní význam v edukaci dítěte. Je důležité, aby rodič prevenci v oblasti kyberprostoru nepodceňoval a s dítětem včas o možných rizicích otevřeně hovořil. Dotazovaní dále vnímají zakazování sociálních sítí jako nevhodný prostředek výchovy. Jak zmiňují respondenti, takovýto zákaz činí z kybernetického prostoru o to více atraktivní místo, ke kterému se dítě bude snažit najít cestu za každou cenu. Z odpovědí respondentů je dále patrné, že rodič by měl dítěti nastavit hranice a pravidla, která jsou ve výchově velmi důležitá. Hranice jsou v tomto případě nezbytné a formují bezpečné prostředí pro zdravý vývoj dítěte. Z vlastního výzkumného šetření dále vyplývá, že za základní pravidla bezpečného pohybu na síti respondenti považují zejména nedůvěřování cizím lidem, neposílání intimních fotografií a nezveřejňování citlivých informací. Zcela zásadní je, aby si rodič s dítětem vybudoval pouto vzájemné důvěry. Důvěru lze nastolit pouze, vyskytne-li se ve vztahu rovnováha, která zúčastněným stranám poskytuje prostor pro sebevyjádření a zpětnou vazbu. S důvěrou jde takřkajíc ruku v ruce schopnost empatie a porozumění, které jsou pro vytvoření důvěry klíčové. Pokud však chce mít rodič klid v duši, může si obstarat aplikaci rodičovský filtr. Na tuto aplikaci nahlíží většina

respondentů jako na vhodné řešení, které napomáhá rodičům se správou možností používání internetu pro své dítě. Rodičovská kontrola má také mnoho podob a může zahrnovat funkce, kterými jsou filtrování webových stránek a obsahu, kontrola doby strávené u obrazovky atd. Respondenti se dále shodují, že škola by se v budoucnu měla intenzivněji zabývat vzděláváním dětí v oblasti kybernetických rizik, a to formou besed či vytvoření zcela nového předmětu.

Závěr

Existence Dark webu je pro mnohé stále velkou neznámou. Nejeden uživatel běžného internetu nemá ani zdání, že právě vstoupil do prostoru, který je pouhým ostrůvkem v oceánu kybernetického prostoru. Dark web a internet koexistují v jednom společném prostoru, avšak jsou odděleny pomyslnou barierou, kterou lze znepokojivě snadno překonat. Uživatelé této sítě si mnohdy neuvědomují rizika, která návštěva tohoto webu obnáší. A řídit se pravidlem, co se stane na Dark webu, zůstane na Dark webu, je pošetilost, které může uživatel později hořce litovat. Přestože se jedná o anonymní prostor, lze se bez patřičné ochrany a vyhýbání se určitým typům webových stránek dostat do nemalých problémů. Pokud jde o bezpečnost v reálném světě, jsme mnohdy přehnaně paranoidní a své soukromí si střežíme za vysokými ploty. Ovšem pokud se ocitáme ve virtuálním světě, nezdráháme se o sobě a svých blízkých zveřejňovat citlivé informace, ba dokonce i polohu, kde se právě nacházíme nebo kam se chystáme.

Teoretická část se zabývá informacemi o Dark webu, jež jsou převedeny do celistvé formy. Nahlíží na Dark web z hlediska historického, obsahového, ale také bezpečnostního. Dark web nabízí široké spektrum webových stránek, které má uživatel možnost navštívit. Jelikož rozsah práce neumožňuje obsah sítě rozebrat dopodrobna, což by si jistě zasloužil, je práce zaměřena zejména na sexuálně a drogově orientovaný obsah. Cíl v teoretické části, zmapovat kybernetický prostor Dark web jakožto místo, jež představuje možné riziko pro děti a dospívající, byl dle mého názoru splněn.

Pro výzkumná šetření, jež byla realizována v rámci bakalářské práce, byly zvoleny metody dotazníkové šetření a strukturovaný rozhovor. Pro dotazníkové šetření byl stanoven cíl zmapovat aktivitu uživatelů Dark webu. Prvotním záměrem bylo porovnat aktivity zahraničních a českých uživatelů, ovšem realizace nebyla možná. Dotazníky určené pro zahraniční respondenty byly vkládány na webové stránky a fóra s tématikou Dark web. Ze zahraničních uživatelů vyplnila dotazník pouze hrstka respondentů a ve většině případů, měli dotazovaní podezření, že jsem příslušník policie. Dotazník určený pro české respondenty byl taktéž vkládán na webové stránky a fóra s tématikou Dark webu, ale i studentské skupiny. Sběr dat zaměřený na české uživatele byl dle mého názoru úspěšný, jelikož dotazník vyplnilo 54 respondentů. Toto číslo lze považovat za vysoké, přihlédneme-li ke skutečnosti, že dotazníkové šetření bylo určeno pouze pro jedince mající zkušenost s Dark webem. Cíl v praktické části byl dle mého názoru částečně splněn, jelikož se podařilo získat informace o aktivitě na Dark webu pouze od českých

uživatelů. Má domněnka týkající se vyhledávaného obsahu se potvrdila. Uživatelé skutečně nejčastěji vyhledávají webové stránky zaměřené na prodej drog a zbraní. Má druhá domněnka byla taktéž potvrzena. Předpokládala jsem, že pro více než polovinu respondentů bude návštěva jednorázovou aktivitou. Po dotazníkovém šetření vyšlo najevo, že 30 uživatelů už nehodlá návštěvu znovu opakovat a 24 respondentů využívá síť i nadále.

Pro hlubší náhled do problematiky byla druhá část empirické práce věnována kvalitativnímu šetření prostřednictvím strukturovaného rozhovoru. Pro interview byl stanoven hlavní cíl, zmapovat pohled účastníků rozhovoru na prevenci v kybernetickém prostoru se zaměřením na děti a mladistvé. Respondenti měli přehled o dané problematice a ve svých odpovědích se zpravidla shodovali, popřípadě doplňovali. Respondenti jsou především toho názoru, že rodina má zásadní roli v edukaci dítěte a je více než žádoucí, aby prevence v této oblasti nebyla podceňována a začala již před samotným nástupem dítěte do školy. V rozhovoru se respondenti opakovaně shodovali, že základem všeho jsou důvěra a stanovení hranic. A důvěru lze vybudovat pouze, vyskytne-li se ve vztahu mezi dítětem a rodičem rovnováha, která vytváří prostor pro sebevyjádření. Na důvěře je nutné neustále pracovat a aktivně o ni pečovat. Stanovení hranic a pravidel je nezbytné pro vytvoření bezpečného, avšak stále podnětného prostředí. Za základní pravidla bezpečného pohybu po síti respondenti označili zejména nedůvěřování cizím lidem, neposílání intimních fotografií a nezveřejňování citlivých informací. Na jednotlivé odpovědi mělo mnohdy vliv povolání respondentů, a tak bylo velmi zajímavé vyslechnout si, jak na problematiku nahlíží IT specialista, absolventka sociální patologie a prevence a jak příslušníci policie ČR.

Seznam použitých zdrojů

AIRA GROUP. Co je ARPANET. *Správa sítě: slovník pojmů* [online]. ©2016 [cit. 2019-11-09]. Dostupné z: https://www.sprava-site.eu/arpanet/.

BERKA, Milan. *WWW - multimediální informační prostředí Internetu*. Brno: Unis, 1996, 159 s. ISBN 80-238-0134-1.

BESSER, Vilém. Kdo jsou vlastně vlivní hackeři Anonymous, kteří děsí svět. *Forum 24* [online]. 22. listopad 2015 [cit. 2020-11-29]. Dostupné z: https://www.forum24.cz/kdo-jsou-vlastne-vlivni-hackeri-anonymous-kteri-desi-svet/.

BREEDING, Jordan. The Origin And History Of The Dark Web. *Ranker* [online]. 24 June 2016 [cit. 2019-11-09]. Available from: https://www.ranker.com/list/history-of-the-dark-web/jordan-breeding.

BRETTA, Zone. What parents need to know about the Dark Web. *Family Zone* [online]. [cit. 2020-12-12]. Dostupné z: https://www.familyzone.com/anz/families/blog/what-parents-need-to-know-about-the-dark-web.

BUKOVANSKÝ, Stanislav a Michael WITTMANN. *Co je to vlastně Internet?*. Ostrava: Blesk, 1998, 158 s. ISBN 80-86060-21-7.

BURDOVÁ, Eva a Jan TRAXLER. *Bezpečně na internetu*. Praha: Středočeský kraj ve spolupráci se Vzdělávacím institutem Středočeského kraje (VISK), 2014, 43 s. ISBN 978-80-904864-9-2.

BUTLER, Sydney. Dark Web History: Where Did It Come From? *TechNadu* [online]. 23 December 2018 [cit. 2019-11-09]. Available from: https://www.technadu.com/dark-web-history/52017/.

CIHODARIU, Miriam. Deep Web vs. Dark Web: What is Each and How Do They Work. *Heimdal Security* [online]. 19 April 2019 [cit. 2019-11-02]. Available from: https://heimdalsecurity.com/blog/deep-web-vs-dark-web-what-is-each/.

CUTHBERTSON, Anthony. CORONAVIRUS TRACKED: DARK WEB DRUG SUPPLY SURGES NEARLY 500% DURING COVID-19 PANDEMIC. *Independent* [online]. 1 June 2020 [cit. 2020-11-30]. Dostupné z: https://www.independent.co.uk/life-style/gadgets-and-tech/news/dark-web-drugs-coronavirus-covid-19-a9534236.html.

CZ.NIC. Jak na internet: Ochrana dětí na Internetu. *CZ.NIC* [online]. 2012 - 2014 [cit. 2020-12-26]. Dostupné z: https://www.jaknainternet.cz/page/1201/ochrana-deti-na-internetu/.

Deepnet: is the "dark web" good or evil? *PS21* [online]. 1 April 2015 [cit. 2019-11-05]. Available from: https://projects21.org/2015/04/01/deepnet-is-the-dark-web-good-or-evil/.

Dream Market Review – Best Darknet Marketplace. *The Dark Web Links* [online]. 12 October 2018 [cit. 2019-12-30]. Available from: https://www.thedarkweblinks.com/dream-market/.

EDDY, Max. Anonymous Takes Down Massive Child Pornography Server, Leaks Usernames. *The Mary Sue* [online]. 23 October 2011 [cit. 2020-01-23]. Available from: https://www.themarysue.com/anonymous-child-porn-takedown/.

GAVORA, Peter. *Úvod do pedagogického výzkumu*. 2., rozš. české vyd. Přeložil Vladimír JŮVA, přeložil Vendula HLAVATÁ. Brno: Paido, 2010, 261 s. ISBN 978-80-7315-185-0.

GILBERT, David. Pink Meth Revenge Porn Darknet Website Shut Down by FBI in Operation Onymous. *International Business Times* [online]. 10 November 2014 [cit. 2019-12-30]. Available from: https://www.ibtimes.co.uk/pink-meth-revenge-porn-darknet-website-shut-down-by-fbi-operation-onymous-1474013.

GOGUARDIAN. What You Need to Know About the Deep Web & the Dark Web. *GoGuardian* [online]. [cit. 2020-12-12]. Dostupné z: https://www.goguardian.com/glossary/protect-kids-deep-web/.

GUCCIONE, Darren. What is the dark web? How to access it and what you'll find. *CSO* [online]. 4 July 2019 [cit. 2019-11-05]. Available from: https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html.

HARPER, Ivy. Dark Web Red Rooms: Urban Legend or Worst Content on the Deep Web? *The Dark Web journal* [online]. 24 October 2019 [cit. 2020-01-24]. Available from: https://darkwebjournal.com/dark-web-red-rooms/.

JESENSKÁ, Elena. Potřebuje muž k životu nebezpečí? *Maminka.cz* [online]. 12. prosinec 2019 [cit. 2021-04-03]. Dostupné z: https://www.maminka.cz/clanek/tatinkove/potrebuje-muz-k-zivotu-nebezpeci.

KLOUČKOVÁ, Lucie. Dark web, bitcoin a přesun jinam. *Roklen24* [online]. 2. září 2017 [cit. 2019-12-29]. Dostupné z: https://roklen24.cz/a/iLE2M/dark-web-bitcoin-a-presun-jinam.

KŇAZOVICKÝ, Michal. *Rizika užívání neindexovaných částí Internetu*. Brno, 2019. Bakalářská práce. Vysoká škola regionálního rozvoje a Bankovní institut – AMBIS. Katedra bezpečnosti a práva. Vedoucí práce Magdaléna NÁPLAVOVÁ.

KOPECKÝ, Kamil, René SZOTKOWSKI a Jitka PAJURKOVÁ. Téměř tři čtvrtiny dětí oslovených na internetu se vydají na schůzku s cizím člověkem, ukázal výzkum. *E-bezpečí* [online]. 11. červen 2019 [cit. 2020-12-26]. Dostupné z: https://www.e-bezpeci.cz/index.php/veda-a-vyzkum/ceske-deti-v-kybersvete-2019.

KOPECKÝ, Kamil. Méně než polovina rodičů pravidelně kontroluje, co dělají jejich děti na internetu. *E-bezpečí* [online]. 8. prosinec 2015 [cit. 2020-12-26]. Dostupné z: https://www.e-bezpeci.cz/index.php/rodice-ucitele-zaci/1099-parental-control.

KRČMÁŘOVÁ, Barbora. *Děti a online rizika: sborník studií*. Praha: Sdružení Linka bezpečí, 2012, 178 s. ISBN 978-80-904920-2-8.

KUBALA, Lukáš. Snapchat už nepřináší revoluční novinky, pouze rizika. *E-Bezpečí*, roč. 4, č. 1, s. 38-41. Olomouc: Univerzita Palackého, 2019. ISSN 2571-1679.

KUŽELÍKOVÁ, Lucie, Jaroslav NEKUDA a Jiří POLÁČEK. *Sociálně-ekonomické informace a práce s nimi*. Brno: MUNI, 2008, 88 s. ISBN 978-80-210-4577-4.

LANGER, Jan. KRYPTOMĚNY – využití, budoucnost, investiční virtuální měny, diskuze. *INVESTPLUS* [online]. [cit. 2019-12-29]. Dostupné z: https://investplus.cz/investice/kryptomeny/.

MAZYAR, Hilah. VPN 101 – VPN příručka pro nováčky od vpnMentor. *VpnMentor* [online]. 31. říjen 2019 [cit. 2019-12-29]. Dostupné z: https://cs.vpnmentor.com/blog/vpn-101-vpn-prirucka-pro-novacky-od-vpnmentor/.

MILLS, Matt. The best search engines deep web and dark web: https://itigic.com/cs/best-search-engines-deep-web-dark-web/. *Itigic* [online]. 13 leden 2020 [cit. 2020-12-01]. Dostupné z: https://itigic.com/cs/best-search-engines-deep-web-dark-web/.

MIOVSKÝ, Michal. Kvalitativní přístup a metody v psychologickém výzkumu. 1. vyd. Praha: Grada, 2006. 332 s. ISBN 80-247-1362-4.

O'NEILL, Patrick. Back in booming Lolita City: the online child pornography community is thriving. *Wayback Machine* [online]. 6 June 2013 [cit. 2020-01-23]. Available from: https://web.archive.org/web/20130610072640/http://weirderweb.com/2013/06/06/back-in-booming-lolita-city-the-online-child-pornography-community-is-thriving.

PORUP, J. M. What is the Tor Browser? How it works and how it can help you protect your identity online. *CSO* [online]. 15 October 2019 [cit. 2019-12-29]. Available from: https://www.csoonline.com/article/3287653/what-is-the-tor-browser-how-it-works-and-how-it-can-help-you-protect-your-identity-online.html.

SABARINATH. Darknet Vs Dark Web Vs Deep Web Vs Surface Web: Different Parts Of The World Wide Web. *TechLog360* [online]. 10 June 2019 [cit. 2019-11-02]. Available from: https://techlog360.com/darknet-vs-dark-web-vs-deep-web-vs-surface-web/.

SALÁT, Michal. Pohled do hlubin darknetu. *Avasta blog* [online]. 12. květen 2017 [cit. 2019-11-05]. Dostupné z: https://blog.avast.com/cs/pohled-do-hlubin-darknetu.

SHIM, Timothy. Jak získat přístup k tmavému webu: Prohlížení webů Dark Web, TOR Browser a Onion. *Web Hosting tajné odhalení (WHSR)* [online]. 5 December 2019 [cit. 2019-12-29]. Dostupné z: https://www.webhostingsecretrevealed.net/cs/blog/web-tools/tourist-guide-to-dark-web-accessing-the-dark-web-tor-browser-and-onion-websites/.

SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, 934 s. ISBN 978-80-7380-720-7.

SOUKUP, Tomáš. Kryptoměny - Jak fungují a jak na nich vydělat? Seznam a kurzy kryptoměn. *FINEX.cz* [online]. ©2014-2019 [cit. 2019-12-29]. Dostupné z: https://finex.cz/rubrika/kryptomeny/.

STROUKAL, Dominik. *Dark Web: sex, drogy a bitcoiny*. Praha: Grada, 2020, 207 s. ISBN 978-80-271-2934-8.

SUSSMAN, Bruce. Dark Web vs. Deep Web: What Is the Difference? *SECUREWORLD* [online]. 28 August 2018 [cit. 2019-11-02]. Available from: https://www.secureworldexpo.com/industry-news/dark-web-vs-deep-web.

SYMANOVICH, Steve. How to safely access the deep and dark webs. *Norton: by Symantec* [online]. 16 April 2018 [cit. 2019-11-13]. Available from: https://us.norton.com/internetsecurity-how-to-how-can-i-access-the-deep-web.html.

TIMES, Vision. When Police Run Child Porn Websites. *Vision Times* [online]. 18 October 2018 [cit. 2019-12-30]. Available from: http://www.visiontimes.com/2018/10/18/when-police-run-child-porn-websites.html.

TOR a TOR Browser: Pro anonymní brouzdání po internetu. *Anonymniinternet.cz* [online]. 18. červenec 2017 [cit. 2019-12-30]. Dostupné z: http://anonymniinternet.cz/tag/tor-browser/#.

VANČURA, Tadeáš. Kolik stojí vytěžení jednoho Bitcoinu? Náklady na mining. *Trade Arena.cz* [online]. 30. září 2020 [cit. 2020-11-22]. Dostupné z: https://www.tradearena.cz/rubriky/bitcoin/kolik-stoji-vytezeni-jednoho-bitcoinu-naklady-na-mining_375.html.

VANČURA, Tadeáš. Monero (XMR) vysvětlení - jak a kde koupit. *Trade Arena.cz* [online]. 15. leden 2018 [cit. 2019-12-29]. Dostupné z: https://www.tradearena.cz/rubriky/kryptomeny/monero-xmr-vysvetleni-jak-a-kde-koupit_387.html.

VARMA, Chandra. CISO Guide: Surface Web, Deep Web and Dark Web - Are they different? *Ciso platform* [online]. 19 April 2018 [cit. 2019-11-02]. Available from: https://www.cisoplatform.com/profiles/blogs/surface-web-deep-web-and-dark-web-are-they-different.

VG. Breaking the darknet: Why the police share abuse pics to save children. *NODA* [online]. 15 January 2018 [cit. 2019-12-30]. Available from: http://nodabase.net/cases/breaking-the-darknet-why-the-police-share-abuse-pics-to-save-children/.

VONOW, Brittany. 'SHE WAS OUR SUNSHINE' Schoolgirl, 16, killed herself after visiting suicide chatroom on the dark web following mock GCSE disappointment. *The Sun* [online]. 20 Jul 2018 [cit. 2020-12-12]. Dostupné z: https://www.thesun.co.uk/news/6825420/leilani-clarke-suicide-chatroom-dark-web-gcse-results/.

ZAMBUTO, Chris. Is Your Information Safe From The Dark Web? *Cmit Solutions: Your Technology Team* [online]. 17 March 2018 [cit. 2019-11-02]. Available

from: https://cmitsolutions.com/boston-cambridge/is-your-info-safe-from-the-dark-web/.

ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017, 135 s. Právní monografie. ISBN 978-80-7552-758-5.

Seznam použitých obrázků a tabulek

Přílohy

Příloha 1: **Dotazník výzkumného šetření**

Dobrý den,

jsem studentkou oboru Sociální patologie a prevence na Pedagogické fakultě Univerzity Hradec Králové a touto cestou bych Vás chtěla požádat o vyplnění následujícího dotazníku, jehož výsledky budou součástí praktické části mé bakalářské práce s názvem Darknet jako rizikové prostředí pro děti. Dotazníkové šetření je zcela anonymní. Cílem je zmapovat Vaše chování a aktivitu ve virtuálním prostředí Dark webu.

Předem děkuji za Váš čas.

Kristýna Šrámková

Otázka č. 1: Připojili jste se někdy k webu známém pod názvem Dark web?

a) Ano
b) Ne

Otázka č. 2: Uveďte, jakého jste pohlaví.

a) Žena
b) Muž

Otázka č. 3: Vaše nejvyšší dosažené vzdělání?

a) Základní
b) Vyučen/a
c) Vyučen/a s maturitou
d) Střední škola
e) Vysoká škola

Otázka č. 4: Do jaké věkové kategorie byste se zařadili?

a) 0-18
b) 19-25
c) 26-35
d) 36-45
e) 50+

Otázka č. 5: Seznámili jste se s možnými riziky před vstupem na tento web?

a) Myslím si, že ano
b) Ano, ale ne dostatečně
c) Vůbec ne

Otázka č. 6: Jak jste se o existenci Dark webu dozvěděli?

a) Od přátel
b) Od rodiny
c) Prostřednictvím internetu
d) Prostřednictvím školy
e) Prostřednictvím práce
f) Prostřednictvím televize
g) Jiné

Otázka č. 7: Zaujal Vás Dark web a navštěvujete jej pravidelně?

a) Ano, navštěvuji ho pravidelně
b) Ano, navštěvují, ale pouze výjimečně
c) Ne

Otázka č. 8: Co Vás vedlo k připojení se k tomuto webu?

a) Ze zvědavosti, co zde lze nalézt
b) Kvůli nudě
c) Nákup nelegálního zboží
d) Hledání konkrétních informací, které nejsou na běžném webu dostupné
e) Jiné

Otázka č. 9: Na jaký obsah jste na Dark webu narazili?

…….

Otázka č. 10: Jaký obsah nejčastěji vyhledáváte?

…….

Otázka č. 11: Objednávali jste si z webu nějaký produkt či službu?

a) Ano
b) Ne
c) Doposud ne, ale chystám se k tomu

Otázka č. 12: Co jste si na Dark webu objednali?

…….

Otázka č. 13: Dorazila Vám objednávka, či byla služba vykonána?

a) Ano
b) Ne

Otázka č. 14: Nabízeli jste někdy své služby či produkty na Dark webu?

a) Ano
b) Ne
c) Jiné

Otázka č. 15: Máte obavy, že při návštěvě Dark webu někdo odhalil Vaši identitu?

a) Ano
b) Ne

Otázka č. 16: Vyhrožoval Vám někdo po návštěvě Dark webu?

a) Ano
b) Ne

Otázka č. 17: Splnila návštěva tohoto webu Vaše očekávání?

a) Ano, návštěva splnila mé očekávání a nalezl/a jsem co jsem hledal/a
b) Ne, čekal/a jsem něco jiného a nenalezl/a jsem to, co jsem hledal/a
c) Jiné

Příloha 2: **Interview (Pohled respondentů na prevenci v kybernetickém prostoru**

1. **Mnozí rodiče se domnívají, že pokud svému dítěti zakáží používat sociální sítě, tak jej tím nejlépe ochrání. Co si o tom myslíte?**

Myslím si, že to není správné řešení, protože zákazy v tomto případě nic nevyřeší. Děti si cestu k používání sociálních sítí stejně najdou. A také si myslím, že z kolektivu budou vyčleněny.

2. **Jak by měl dle Vašeho názoru postupovat rodič, který se dozví, že jeho dítě navštěvuje nevhodné stránky?**

Správným postupem v tomto případě je dle mého názoru, komunikace s dítětem a vysvětlení všech nástrah při navštěvování nevhodných stránek. Komunikaci s dítětem vidím jako naprosto zásadní, pro objasnění této problematiky.

3. **Máte nějakou preventivní radu pro rodiče, která by mohla napomoci zajistit bezpečnost jejich nezletilých dětí na internetu?**

Dle mého názoru je komunikace a opakované vysvětlování velmi důležité. Dále zájem o jejich problémy, naslouchání a porozumění.

4. **Řada rodičů přidává fotografie svých dětí na sociální sítě bez jejich svolení tzv. sharenting. Jaký je Váš názor na tuto problematiku?**

S tímto naprosto nesouhlasím. Nikdy jsem žádné fotografie svých dětí na sociální sítě neumístil. Hlavním důvodem v mém případě je bezpečnost mojí rodiny v souvislosti s mým zaměstnáním. Pracuji jako policista a několikrát mi bylo vyhrožováno fyzickou likvidací. Domnívám se, že tímto způsobem chráním svou rodinu.

5. **Z Vašeho odborného pohledu, jaké jsou největší hrozby v kybernetickém prostoru pro dítě?**

Z mého pohledu je velký problém, že děti jsou vytržené od reality. Domnívají se, že virtuální život je podobný nebo stejný, jako ten reálný.

6. **Která věková skupina je dle Vašeho názoru v anonymním prostoru internetu nejzranitelnější? A proč?**

Domnívám se, že je to věková skupina od 10 do 15 let. V tomto věku je velmi jednoduché děti obelstít a manipulovat s nimi. Myslím si, že člověk v tomto věku v dnešní době, není schopen správně vyhodnotit všechny nástrahy kybernetického světa.

7. **Jaký je Váš názor na sociální sítě Facebook, Instagram, Twitter? Dovolil byste Vašemu dítěti, aby je využívalo? Popřípadě od jakého věku?**

Nejsem proti používání sociálních sítí. Sám Facebook používám. Jak jsem již zmínil, jsem velmi opatrný s tím, co na sociální sítě vložím. Zřejmě jsem paranoidní, ale na sociálních sítích nemám uvedeno ani své celé jméno a nemám zde vloženou žádnou fotografii, podle které by se má osoba dala identifikovat. Moji kamarádi vědí, kdo jsem, mám je v přátelích a oni respektují to, že nemám zájem vkládat jakékoli fotografie mé osoby, fotografie mojí rodiny a žádné další osobní údaje na sociální sítě. Svému dítěti bych dovolil používat sociální sítě od 12 let. Po dobu dalších několik let, chci alespoň částečně kontrolovat, co a jaké fotografie moje dítě na sociální sítě vkládá.

8. **Pokud byste měl vyjmenovat tři základní pravidla bezpečného pohybu na sítí, která by měla být předána dětem, jaká by to byla?**

Nedůvěřovat lidem, které osobně nezná. Neposílat nikomu žádné fotografie se sexuálním obsahem. Nesdělovat nikomu žádné svoje osobní údaje.

9. **Jaký máte názor na tzv. rodičovské filtry? Opatřil/a byste si tento typ aplikace v zájmu bezpečí Vašeho dítěte?**

Ano, určitě si v době, kdy moje děti budou více využívat internet, opatřím si rodičovské filtry a budu kontrolovat, co moje děti na internetu dělají.

10. **Domníváte se, že základní prevenci rizikového chování v online prostředí by dětem měla zprostředkovávat rodina, nebo je to podle Vás úkol školy?**

Domnívám se, že to je úkolem, jak rodičů, tak i školy.

11. **Internet, mobily a sociální sítě jsou zpravidla nedílnou součástí života dětí a dospívajících. Jste onoho názoru, že by se na školách měl zavést předmět, který by žáky učil bezpečnému pohybu na síti? A proč?**

Ano, určitě jsem pro zavedení takového předmětu. Internet a kybernetický prostor je nedílnou součástí většiny lidí a našich životů. Vzdělávání v této oblasti a posilování bezpečnosti je dle mého názoru naprostá nutnost. Ve svém zaměstnání se čím dál častěji setkávám s šikanou, podvody, manipulace s lidmi, prostřednictvím internetu.

12. **Jaký je Váš názor na současnou podobu vzdělávání dětí v oblasti IT (výuka zaměřena na orientace v programech Word, Excel a Powerpoint)?**

V současné době nedokáži na tuto otázku odpovědět. Mám malé děti, z nichž jedno je školou povinné, ale ještě nemá žádný předmět týkající se oblasti IT. V současné pandemické krizi jsem mile překvapen, jak děti zvládají on-line distanční výuku a s tím spojenou práci na počítači a internetu.