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

BAKALÁŘSKÁ PRÁCE

Kybernetická bezpečnost uživatelů v České republice a jejich znalosti problematiky

Autor práce: Jakub Hubka

Studijní obor: Bezpečnostně právní činnost ve veřejné správě

Forma studia: kombinované

Vedoucí práce: RNDr. Růžena Ferebauerová

Katedra: Katedra právních oborů a bezpečnostních studií

2022

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

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Jakub Hubka
Studijní program: Bezpečnostně právní činnost
Studijní obor: Bezpečnostně právní činnost ve veřejné správě
Forma studia: Kombinovaná
Místo studia: Příbram

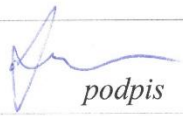
Název bakalářské práce: Kybernetická bezpečnost uživatelů v České republice a jejich znalosti problematiky

Název bakalářské práce v anglickém jazyce: Cyber Security of the Users in the Czech Republic and their Knowledge about the Issue

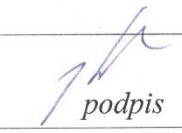
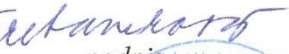
Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, titul): RNDr. Růžena Ferebauerová

Datum zadání bakalářské práce (měsíc, rok): prosinec, 2020

Cíl bakalářské práce: Hlavním cílem bakalářské práce je objasnit pojem kybernetického prostoru a posoudit schopnost uživatelů rozpoznat bezpečnostní hrozby. Vedlejším cílem je na základě šetření navrhnout doporučení pro uživatele všech věkových kategorií pro bezpečný průchod internetem.

Student: Jakub Hubka	6.4.21 *datum*	 *podpis*
Vedoucí práce: RNDr. Růžena Ferebauerová	6.4.21 *datum*	 *podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	25.5.2021 *datum*	 *podpis*
Prorektorka pro studium a vnitřní záležitosti: RNDr. Růžena Ferebauerová	16.5.21 *datum*	 *podpis*
Pověřený rektor: doc. Ing. Jiří Dušek, Ph.D.	31.5.2021 *datum*	 *podpis*

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

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

.....

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

ABSTRAKT

HUBKA, J. *Kybernetická bezpečnost uživatelů v České republice a jejich znalost problematiky: bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, 2021. 68 s. Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová.

Klíčová slova: kybernetický prostor, internet, hrozba, počítač, uživatel, kriminalita

Bakalářská práce představuje historii kybernetického prostoru a jeho základní pojmy spolu s kybernetickou kriminalitou. V teoretické části se především zaměřuje na vybrané hrozby internetu, které mohou ohrozit prakticky každého uživatele počítače. Dále bakalářská práce ve své teoretické části uvádí možné způsoby prevence proti kybernetické kriminalitě. Praktická část se skládá z dotazníkového šetření, kde je popsán výběr respondentů, sběru a analýzy získaných dat. Dále obsahuje rozhovor s experty z NÚKIB.

Hlavním cílem bakalářské práce je objasnit pojem kybernetického prostoru a na základě dotazníkového šetření posoudit schopnost uživatelů rozpoznat bezpečnostní hrozby. Vedlejším cílem je na základě šetření navrhnout doporučení pro uživatele všech věkových kategorií pro bezpečné používání internetu.

ABSTRACT

HUBKA, J. *Kybernetická bezpečnost uživatelů v České republice a jejich znalost problematiky: bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, 2021. 68 s. Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová.

Key words: cyberspace, internet, threat, computer, user, criminality

The bachelor thesis presents the history of cyberspace, its basic terms and cybercrime. The theoretical part of this thesis is mainly focused on selected internet threats which may threaten every computer user and lists possible ways to prevent cybercrime. The practical part consists of a questionnaire survey, which describes the selection of respondents, data collection and analysis. Then it contains interview with an NÚKIB experts.

The main objective of the thesis was to clarify cyberspace concept. On the basis of the questionnaire survey assess the ability of users to identify security threats. The minor objective was to suggest internet safety recommendations for users of all ages based on the survey.

Obsah

Úvod

Málokterý obor prošel tak rychlým vývojem během několika let jako informační technologie. Ať chceme, či nechceme, počítače nás ovlivňují neustále jak pozitivně, tak i negativně. Kybernetický prostor není tvořen pouze elektronikou, jako je například: telefon, notebook, tablet, chytrá televize nebo modem. Je tvořen také koncovými uživateli. Dnes ve 21. století je uživatelem tohoto prostoru téměř každý. Pokud zvedneme hlavu například v tramvaji, všimneme si, že více jak polovina cestujících kouká do mobilního telefonu. Mezi uživatele řadíme kohokoliv, kdo využívá internet, platí kreditní kartou nebo používá internetové bankovnictví. Mnoho činností jako je hraní her, studování na internetu či sledování videí dokáže ohrozit nás i naše okolí. Je velice důležité vědět, jakým způsobem se v tomto prostoru chovat. Může zde být ohroženo naše jmění, psychické i fyzické zdraví. Je zde mnoho případů, kdy útok v kyberprostoru skončil úmrtím člověka. Nejvíce je ohrožen člověk, který nedokáže rozpoznat hrozbu. Ovšem v kybernetickém prostoru nemusí být ohrožen jen člověk, ale i stát. Důležité je umět hrozbu rozpoznat a vědět, jak na ni reagovat. Často je to velice složité, protože útočníci jsou schopni například vytvořit identické stránky banky uživatele, což může sloužit k tomu, že útočníci získají přihlašovací údaje uživatelů. Mnoho našich činností, které provádíme v reálném životě přenášíme do toho virtuálního, avšak přenos těchto činností rozhodně není bezrizikový. Abychom byli schopni fungovat musíme tato rizika znát a vědět, jak je minimalizovat, protože cokoliv nahrajeme do virtuálního světa už nikdy nemáme šanci úplně smazat. Musíme si také pamatovat, že nikdy nevíme, kdo sedí na druhé straně komunikace.

Dalším důvodem nárůstu využití internetu je pandemie Covid-19, kvůli které se internet začal využívat úplně jiným způsobem. Pokud zmíníme například uzavření obchodů, tak prudce stoupl počet online plateb a nákupů. Zde na nás mohou číhat nástrahy, jakými jsou např. falešné obchody, které požadují platbu předem. Změnila se i výuka ve školách. Ta začala probíhat online. Čili i taková situace, jakou je pandemie, dokáže naprosto změnit využití virtuálního prostředí a tím do svého světa vtáhne velké množství uživatelů neboli potenciálních obětí trestných činů.

Bakalářská práce se popisuje historii kybernetického prostoru a počítačů. Řeší základní pojmy spojené s virtuálním prostředím, které by měl znát každý, kdo se chce nějakým způsobem orientovat v tomto prostoru. V práci jsou uvedeny nejběžnější typy

útoků, které ohrožují uživatele internetu. V této části bude popsán postup těchto útoků a jakým způsobem se mohou případně šířit.

Téma kybernetické bezpečnosti jsem si vybral, z důvodu předchozích zkušeností ze střední školy, na které jsem studoval obor informační a komunikační technologie. Téma virtuálního prostředí mi je blízké už od mladého věku. Jako malý jsem se počítačům věnoval několik hodin denně. Celkově mám pocit, že by uživatelé měli mít větší přehled o nástrahách internetu a kyberprostoru, neboť rizika jsou poměrně značná.

1 Cíl a metodika bakalářské práce

Bakalářská práce popisuje historický vývoj kybernetického prostoru. V současné době využití internetu značně vzrostlo, což je pravděpodobně důsledkem COVID-19. IT technologie začaly hromadně využívat i děti mladšího školního věku. Neznalost bezpečného chování v tomto prostředí ohrožuje všechny věkové kategorie, a proto budou řešeny aktuální problémy v tomto prostoru, jako např. kyberšikana, phishing, viry atd. Dále bude pomocí dotazníkového šetření zjištěna aktuální situace chování uživatelů na internetu.

Hlavním cílem bakalářské práce je objasnit pojem kybernetického prostoru a na základě dotazníkového šetření posoudit schopnost uživatelů rozpoznat bezpečnostní hrozby. Vedlejším cílem je na základě šetření navrhnout doporučení pro uživatele všech věkových kategorií pro bezpečný průchod internetem.

V teoretické části bakalářské práce byla využita literární rešerše a její následná komparace a syntéza. V praktické části byly využity následující metody a techniky zkoumání:

- logické metody – analýza a syntéza,
- komparační metoda,
- kvantitativní výzkum pomocí dotazníkového šetření,
- řízený strukturovaný rozhovor s odborníky.

Tyto metody a techniky zkoumání byly následně zpracovány do přehledných tabulek a grafů.

2 Vysvětlení pojmů

Jádro procesoru – procesor nacházející se uvnitř daného procesoru, čím více jader procesor má tím je výkonnější.

Hardware – veškeré fyzické vybavení počítače.

Upgrade – výměna výrobku za novější, lepší verzi.

TCP/IP – sada protokolů pro komunikaci v počítačové síti, je hlavním protokolem celosvětové sítě Internet. Tato sada protokolů určuje pravidla pro komunikaci v síti.

IP Adresa – jednoznačné identifikační číslo rozhraní daného počítače v síti. Dnes se používá Ipv4 a Ipv6.

Taktování – zvýšení pracovní frekvence daného hardwaru. Užívá se nejčastěji pro zvýšení výkonu u procesoru, grafické karty či paměti RAM.

BIOS – je základním programem počítače, který řídí komunikaci s hardwarem na nejnižší úrovni

Paměť ROM – Read Only Memory – paměť pro uložení BIOSU, nezávislá na elektrice (nebude vymazána po odpojení ze sítě).

Dvoufázové ověření – další vrstva zabezpečení vašeho účtu. Může být provedeno zasláním speciálního kódu na telefonní číslo či do autentizační aplikace, například Česká spořitelna využívá pro své dvoufázové ověření aplikaci *„George Klíč“*.

Payload – Data škodlivého softwaru, která odkazují na konkrétní škodlivou či nebezpečnou činnost.

3 Historie kybernetického prostoru

Sputnik

Sputnik byla první, lidstvem vytvořená, umělá družice, která byla vypuštěna do vesmíru. Tato událost stála na počátku vzniku celého kybernetického světa, jenž známe dnes. Družice byla vypuštěna roku 4. října 1957 Sovětským svazem. Sestrojena byla na konci 50. let 20. století raketovým inženýrem Sergejem Koroljovem. Družice měla kulový tvar o průměru 58 cm a hmotnost 83,5 kg. SSSR tímto „vědeckým kouskem" předehnal Spojené státy americké ve vesmírném výzkumu. Vesmírný výzkum souvisí s vojenskými technologiemi, což byla pro USA bezpečnostní hrozba nemalých rozměrů. Americká administrativa si toto nebezpečí velice dobře uvědomovala, a proto ministerstvo obrany založilo roku 1958 společnost ARPA (Advanced Research Project Agency, česky Agentura pro pokročilé výzkumné projekty). V kruzích počítačových technologií začalo vznikat mnoho neformálních skupin programátorů, kteří jsou dnes nazývaní „hackeři". Takovéto skupiny vznikaly především na univerzitách, například MIT Boston či Berkeley Los Angeles.

ARPANET

V roce 1958 americký prezident **Dwight Eisenhower** jmenoval prezidenta Massachusettského výzkumného ústavu **Jamese Killiana** jako svého poradce pro vědu a pověřil ho vytvořením Úřadu pro projekty pokročilého výzkumu *(ARPA)*, aby Spojené státy získaly technologickou převahu nad Sovětským svazem a vybudovaly účinnou obranu proti případnému sovětskému raketovému útoku z vesmíru.[1] V roce 1969 vzniká první čtyřuzlová síť, jejímž hlavním úkolem bylo především prakticky ověřit schopnost přepojování paketů a umožnit dálkovou správu tehdy nejvýkonnějších superpočítačů. Uzly propojovaly následující univerzity – Los Angeles, Santa Barbara, Stanford a Utah. Roku 1971 má síť ARPANET 15 uzlů a následující rok již 37. Tentýž rok vymyslel a implementoval Ray Tomlinson e-mailový program pro tuto síť. Do roku 1973 e-maily tvořily až 75 % síťového provozu. V roce 1972 na konferenci o počítačích a komunikacích ve Washingtonu byla síť ARPANET poprvé předvedena veřejnosti. Obsahovala přibližně 20 routerů a 50 počítačů. Po této konferenci byla firma ARPA přejmenována na DARPA (Defense Advanced Research Project Agency, česky Agentura ministerstva obrany pro pokročilé výzkumné projekty). O rok později se připojují první zahraniční uzly z Velké Británie a Norska. Tato zahraniční síť, jež se připojila

[1]HAUBEN, M. *Historie sítě ARPANET/Internet*. 2003, s. 6. ISBN 999-00-000-7834-9.

k ARPANETU obsahovala 43 hlavních počítačů a 18 navzájem propojených uzlů. Zásadní rok byl 1983, kdy se od ARPANETU oddělila vojenská síť zvaná MILNET a též se přešlo z používaného protokolu NCP na dodnes využívaný TCP/IP. Tímto byl položen základní kámen dnešního internetu.

Vývoj počítačů

3.1.1 Prehistorie počítačů

S historií kybernetického prostoru souvisí vývoj zařízení (dnes počítačů), které tento kybernetický prostor tvoří. I dávná historie ukazuje, že se člověk snažil vytvořit předmět pro zjednodušení či automatizaci práce. Tyto předměty lze považovat za předchůdce dnešních počítačů. Mezi první pomůcky, můžeme počítat zaznamenávání výpočtů pomocí škrábanců na předměty. Jeden takový byl nalezen ve Věstonicích na Moravě v roce 1937, pojmenován byl „vrubovka" a jednalo se o kost s vruby. Oficiálně řadíme mezi první přístroj na počítání „abakus". Vznik abaku je skryt hluboko v historii. Domníváme se, že byl vynalezen přibližně před pěti tisíci lety v Malé Asii, odkud se rozšířil do Číny a Japonska. Následně byl objeven v Řecku a Římě.[2] Abakus byl dřevěný rámeček uvnitř něhož byly drátky, na kterých různé byly mince, popřípadě kamínky. Zjednodušeně řečeno bylo to klasické počítadlo, s jehož pomocí se prováděly matematické operace. V Číně byl znám od 13. století pod jménem *suan pan* a ten je tvořen třinácti sloupci se dvěma korálky nahoře (nebe) a pěti korálky dole (země).

Počátek historie modernějších počítačů je v 15. století v íránské astronomii. Představitelem byl Jamshid ben Masúd, avšak titul prvního vynálezce počítacího stroje se připisuje německému profesorovi Wilhelmu Shickardovi. Ten v roce 1623 sestrojil své počítací hodiny.

Mechanický stroj byl schopný násobit a dělit, přičemž tyto dvě operace prováděl pomocí logaritmů na sčítání a odčítání a k reprezentaci desítkových čísel používal kolečka s deseti zuby.[3]

Jedním z předních vynálezců v oblasti počítačových strojů byl Charles Babbage z Anglie. Jeho hlavním cílem bylo minimalizovat chyby, ke kterým docházelo při ručních

[2]ZELENÝ, J., MANNOVÁ, B. *Historie výpočetní techniky*. Praha: Scientia, 2006, s. 14. Stručné dějiny oborů. ISBN 80-86960-04-8.
[3] ZELENÝ, J., MANNOVÁ, B. *Historie výpočetní techniky*. Praha: Scientia, 2006, s. 18. Stručné dějiny oborů. ISBN 80-86960-04-8.

výpočtech. V roce 1822 začal s konstrukcí diferenčního stroje, který dokončil po 10 letech. S výsledkem nebyl příliš spokojen, a proto o rok později začal sestrojovat stroj nový, který by umožňoval jakékoliv matematické operace a byl nazván analytický stroj. K řízení operací byly použity děrné štítky a jako zdroj energie byla použita pára. Bohužel tento stroj zůstal nedokončený, protože stavba byla přerušena smrtí Charlese Babbage. I když vynález nebyl nikdy dokončen, byla to geniální myšlenka, která inspirovala další vědce. Na toto se navázalo roku 1890, kdy použité analytické stroje používaly pro vložení číselných údajů děrné štítky a automaticky vykonávaly tisíce operací. Děrný štítek sloužil k uchování dat k pozdějšímu použití. Díky těmto štítkům bylo určeno zpracování dat na následujících 100 let.

Dle historie se postupně došlo k specifikaci, co je současný moderní počítač. Moderní počítač musí být binární, což znamená využívání dvojkové soustavy (Binární soustava – číselná soustava, kde se využívá pouze číslic 1 a 0), elektronický, tedy je sestaven z elektronických součástek (elektronky, diody, tranzistory a integrované obvody), a univerzální. Univerzální znamená, že je schopen řešit více než jednu úlohu, tím se odlišuje od všech předchozích zařízení. A v poslední řadě musí splňovat Von Neumannovu architekturu. Architektura představuje čtyři navzájem propojené bloky:

- aritmeticko-logické jednotky,
- řídící jednotky (řadiče),
- operační paměti,
- zařízení pro vstup a výstup.[4]

Úplně první moderní počítač, který vychází z předpokladů nelze s jistotou určit. Řada literárních pramenů se v tomto určení liší, avšak mezi první moderní počítače můžeme zařadit Zuse Z1 až Z4. Vyrobeny byly v Německu stejnojmenným inženýrem Konradem Zusem. Roku 1941 předvedl model Z3, který je označován jako první programovatelný počítač na světě, jenž opravdu fungoval.[5] Naprostým vrcholem ve vývoji této doby se stal MARK I. Navržen byl v USA Howardem Aikenem s vydatnou podporou firmy IBM. I když se zatím nejednalo o plný význam slova „počítač“, MARK

[4] ZELENÝ, J., MANNOVÁ, B. *Historie výpočetní techniky*. Praha: Scientia, 2006, s. 28. Stručné dějiny oborů. ISBN 80-86960-04-8.
[5] Historie výpočetní techniky 1941–1950. *Historie počítačů v Československu 1950–1975* [online]. Copyright © 2005 [cit. 11.11.2021]. Dostupné z: <https://historiepocitacu.cz/1941-1950.html>.

I spoustu rysů naplňoval. Byl řízen programem, avšak neměl vnitřní paměť programů. Dlouhý byl 10,6 metru a vysoký 2,6 metru. Celková váha tohoto stroje dosahovala 5 tun. Ke chlazení se používal led, jehož denní spotřeba dosahovala několik tun. Využíván byl do roku 1959 americkým námořnictvem pro výpočet balistických střel. MARK I a II využívaly ještě elektromagnetických prvků. MARK III a IV již používaly elektronky a tranzistory. Následující počítače řadíme do jednotlivých generací.

3.1.2 První generace počítačů

Časové období této generace řadíme do let 1946–1953. Hardware těchto počítačů tvořily elektronky. Programování bylo řešeno procedurálně, což znamená, že výpočet je řešen posloupností a je přesně daný postup (algoritmus), jakým způsobem zadanou úlohu vyřešit. Uživatelské rozhraní neboli rozhraní, přes které procházely vstupy a výstupy byly řešeny pomocí přepínačů, děrných štítků nebo tiskáren. Velikost těchto počítačů dosahovala několika metrů a většinou zabraly prostor celé místnosti. Produkovaly velké množství tepla, hluku a jejich údržba byla velice náročná. Náročnosti bylo ulehčeno, když roku 1948 firma IBM zavedla výměnné moduly. Při vzniku poruchy nebyla vyhledávána vadná část, ale byl vyměněn celý modul. V této době spolu počítače ještě neuměly nijak komunikovat. Počítače sloužily pro účely vlády, armády či velkých firem. Do první generace řadíme například ENIAC, který byl vyroben roku 1946 v USA nebo Manchester Mark I vyrobený roku 1949 ve Velké Británii.

3.1.3 Druhá generace počítačů

2. generace počítačů je z období 1954–1963. Hranice tohoto období značí pokrok v technologii, která se užívala. Tranzistory doplňovaly nebo zcela nahrazovaly doposud užívané elektronky. Tento upgrade zvýšil rychlost zpracování dat a spolehlivost celého stroje. Díky použití tranzistorů docházelo k postupnému zmenšování počítačů a přechodu na velkovýrobu. Tím byla snížena i samotná cena strojů. Hlavní charakteristikou 2. generace byly řádkové tiskárny, pomocí kterých se zrychlil i celkový výstup dat předávaný uživateli. V roce 1962 firma Teletype vypustila produkt Teletype model 33. Jednalo se o první široce užívaný terminál s psacím strojem a děrnou páskou.[6] Novinkou ve světě počítačů byla začínající komunikace více zařízení mezi sebou, což bylo zajištěno pomocí modemu. Modem byl schopen přenášet binární data přes telefonní linku. S přibývajícím výkonem a spolehlivostí již nestačilo dosud používané programování.

[6] ZELENÝ, J., MANNOVÁ, B. *Historie výpočetní techniky*. Praha: Scientia, 2006, s. 65. Stručné dějiny oborů. ISBN 80-86960-04-8

Výsledkem snahy po větší efektivitě bylo zavedení programovacích jazyků – Fotran, Algola a Cobol.[7] Pokroku se využilo projektem SAGE, který začal roku 1953. SAGE byl využit během války pro sledování vzdušného prostoru.

3.1.4 Třetí generace počítačů

Tato generace se datuje od roku 1964 do roku 1972. Na počátku nové generace je nástup integrovaných obvodů spolu s větším množství tranzistorů, ke kterým se přidávají čipy. Začínají vznikat další programovací jazyky, jež umožňují tvoření nových uživatelských aplikací. Programovací jazyky byly například Basic, Fortran, C či pokročilejší C++. V této době již existuje ARPA, a proto můžeme říct, že už začínaly počítače komunikovat v malé síti neboli síti LAN. Též v této době přicházely na scénu první operační systémy, avšak nejednalo se o systémy, jak je známe dnes. Tyto neměly žádné GUI. Využívalo se tzv. terminálu. V těchto terminálech byly vstupy a výstupy zadávány do textového rozhraní. Paměť počítače byla rozdělena na pevné sekce. Jedna tato část patřila operačnímu systému další sekce poté patřily uloženým programům. Po určitém čase nastal v tomto řešení problém, který spočíval ve velikosti hlavní paměti. Tato paměť byla finančně náročná a malá. V následující době se počítačový inženýři věnovali zmenšení velikosti operačního systému, jenž se nacházel v této hlavní paměti. Později se začaly využívat magnetické disky. Jejich kapacita roku 1973 byla 400 MB za cenu 279 USD/MB. V roce 1980 firma IBM nabízela disky s kapacitou 2,5 GB s cenou 35 USD/MB.[8]

3.1.5 Další generace počítačů

Další generace počítačů se do roku 2000 svým vnějším vzhledem oproti třetí generaci lišily minimálně, avšak prvky uvnitř počítače byly na jiné úrovni. První integrovaný obvod byl vyroben firmou Intel v roce 1971 a nesl název Intel 4004. Tento integrovaný obvod obsahoval na čipu všechny části počítače. Jednou z mnoha významných událostí bylo roku 1980 uvedení na trh osobního počítače ZX Spektrum. Počítač pocházel z Velké Británie a prodával se ve svém osmibitovém provedení až do roku 1990, kdy byl nahrazen lepší šestnáctibitovou verzí. Vývoj počítačů se rozhodně nezastavil a určitě to nemá v dohledné době v plánu. Počítačům stále narůstá výkon a zmenšuje se velikost. Například je dnes běžné mít počítač v hodinkách, který má

[7] ZELENÝ, J., MANNOVÁ, B. *Historie výpočetní techniky*. Praha: Scientia, 2006, s. 75. Stručné dějiny oborů. ISBN 80-86960-04-8.
[8] ZELENÝ, J., MANNOVÁ, B. *Historie výpočetní techniky*. Praha: Scientia, 2006, s. 108. Stručné dějiny oborů. ISBN 80-86960-04-8.

několikanásobně větší výkon než zmíněný ZX Spektrum. Pro porovnání, počítače v roce 2000 obsahovaly procesor s jedním jádrem o maximální frekvenci 1 GHz, dnes je standardní procesor o frekvenci 3,6 GHz s minimálně 4 jádry. Paměťové zařízení neboli disky mají též větší kapacitu a menší rozměry. Kapacita disků od 2000 do 2006 dosahovala maximální hodnoty 8 GB. Dnes v počítačích používáme disky s kapacitou 1 TB (1 TB = 1000 GB). Tyto disky můžeme dále propojovat s dalšími, až do prakticky neomezené velikosti.

4 Pojmy spojené s kybernetickým prostorem

Kybernetická bezpečnost

„Kybernetická bezpečnost v posledním desetiletí získala na významu a stala se tak jednou z hlavních priorit v mnoha národních politikách. Je tomu zejména díky přesahu do jiných bezpečnostních sfér a taktéž díky incidentům, které tento pojem nechvalně proslavily a přiměly i širokou veřejnost přemýšlet o potřebě zabezpečení v kyberprostoru. S tím souvisí potřeba chránit kyberprostor tak, aby v nejvyšší možné míře byla zachována komplexní bezpečnost České republiky a zároveň práva jedinců na informační sebeurčení.“[9]

Vymezení pojmu kybernetická bezpečnost může být poněkud problematické. Někteří si pod tímto pojmem představují určité oddělení v oblasti IT, kde se nacházejí pouze vystudovaní odborníci, jež se starají o naši bezpečnost ve virtuálním světě. Tato myšlenka je však chybná. Pro pochopení kybernetické bezpečnosti je nutné tento svět, ve kterém se „útočné“ a „obranné“ akce odehrávají, poznat. První zmínka o kyberprostoru se objevila roku 1982 v povídce „*Jak vypálit chrom*“. Autor William Gibson uvedl v románu Neuromancer, že kyberprostor je:

„Konsensuální halucinace každý den zakoušená miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky… Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie světla seřazené v neprostoru mysli, shluky a souhvězdí dat. Jako světla města,[10] *…“*

Z aktuální definice vyplývá, že kyberprostorem se myslí digitální prostředí, ve kterém probíhá vznik informací, které se dále zpracovávají a vyměňují. Celé toto prostředí je tvořeno službami, informačními systémy a počítačovými sítěmi. [11] Tento prostor obsahuje složky informačních a komunikačních technologií, které pomocí protokolu TCP/IP tvoří globální počítačovou síť. Prostor je dynamický, neustále se měnící systém. Jeho podoba závisí na mnoha prvcích, například neustále vyvíjející se hardware. Jeho velikost je prakticky neomezená a každou sekundou se zvětšuje. Zákonem udávaná definice kyberprostoru dle Zákona č. 181/2014 Sb., se rozumí: „*kybernetickým prostorem digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené*

[9] Zpráva o stavu kybernetické bezpečnosti ČR – 2017. Národní úřad pro kybernetickou a informační bezpečnost – Zprávy o stavu KB <http://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/>. [online] [cit. 09.11.2021].
[10] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CYBERSECURITY*. Praha: CZ.NIC, z. s. p. o., 2019, s. 35. ISBN 978-80-88168-34-8.
[11] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013, s. 59. ISBN 978-80-7251-397-0.

informačními systémy, a službami a sítěmi elektronických komunikací“[12]. Pokud budeme zkoumat slovní spojení kybernetická bezpečnost, je vhodné si toto sousloví rozdělit. Slovo *kyber* představuje souvislost s členy informačních technologií a kyberprostorem. Bezpečnost můžeme definovat několika způsoby. Například autor Josef Požár ve své knize definuje bezpečnost takto: „*bezpečnost jako vlastnost nějakého objektu nebo subjektu, která určuje stupeň, míru jeho ochrany proti možným škodám a hrozbám*“[13]. Při zajišťování bezpečnosti jsou důležité následující otázky:

- o čí bezpečnost se jedná? (stát, jednotlivec);
- jaké hodnoty jsou chráněny? (data);
- před čím mají být tyto hodnoty chráněny? (kybernetický útok);
- co musíme udělat pro ochranu těchto hodnot?[14]

Význam slovního spojení kybernetická bezpečnost nemá opět pouze jednu definici. Definice, která se mi ale nejvíce zamlouvá je: „*Souhrn právních, organizačních, technických a vzdělávacích prostředků směřující k zajištění ochrany kybernetického prostoru“*[15]

Kyberkriminalita

V dnešní době je internet nejvíce využívaným kybernetickým prostorem na světě. Aktuálně ho využívá 4,1 miliardy lidí, což je více než polovina celé populace. V České republice využívá internet dle Českého statistického úřadu 81,4% populace starší 16 let.[16] Nejvíce uživatelů nalezneme ve věkové kategorii od 16 do 24 let. V této věkové kategorii internet používá 98,6 % lidí. Z těchto statistiky můžeme vyčíst, že kriminalitou v kybernetickém prostoru může být zasažena většina populace. Široký rozmach všech informačních technologií přináší mnoho výhod, ale také spoustu rizik. Počítačová kriminalita neboli též kyberkriminalita je trestná činnost, kde počítač figuruje jako nástroj

[12] 181/2014 Sb. Zákon o kybernetické bezpečnosti. *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Copyright © AION CS, s.r.o. 2010 [cit. 09.11.2021]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2014-181>.
[13] POŽÁR J. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005, s. 37. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-86898-38-5.
[14]KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CYBERSECURITY*. Praha: CZ.NIC, z. s. p. o., 2019, s. 35. ISBN 978-80-88168-34-8.
[15]JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013, s. 57. ISBN 978-80-7251-397-0.
[16] Informační společnost v číslech-2021 [online]. Praha: Český statistický úřad, 2021 [cit. 2021-12-21]. Dostupné z: <https://www.czso.cz/csu/czso/informacni-spolecnost-v-cislech-2021>.

nebo jako předmět útoku. Jednotná definice kyberkriminality neexistuje v teorii ani legislativě, avšak definují ji tři hlavní atributy: (1) uskutečňuje se ve virtuálním prostředí; (2) obsahuje nové deviantní chování, tj. takové chování, které by bez virtuálního prostoru neexistovalo; (3) novinky v trestněprávních reakcích (například digitální forenzní analýza).[17] Existují charakteristiky, které ztěžují trestní stíhání těchto činů. Patří sem přeshraniční charakter internetu. Pachatel může napadnout kohokoliv na světě odkudkoliv na světě. Pronikání do počítačů v síti není nijak omezeno. Neexistují žádné „virtuální" hranice pro kontrolu ilegální činnosti. Dále je to standardizace softwaru, díky které stoupá schopnost zvládat vyšší počet úkolů, nebo přesměrování datového toku. Toto znamená, že pachatel útočí například z Berlína, ale díky přesměrování či skrytí své IP adresy to vypadá na útok z jiného místa. Nejčastějšími pachateli ve virtuálním prostředí jsou hackeři či crackeři. Rozdílů mezi těmito pachateli je více.

Hardware

Pojem hardware vyjadřuje fyzicky hmatatelné součástky počítače. Hardware pochází z anglického významu „technické vybavení". Veškeré tyto prvky obsažené v počítači jsou zapotřebí pro celkové fungování a jsou jeho nezbytnou součástí. Tento hardware můžeme dělit na dvě kategorie.

4.1.1 Vnitřní vybavení počítače

Bez těchto komponentů není počítač schopen vlastního fungování. Žádná z těchto částí není programovatelná (pozn. pokud nepočítáme taktování grafické karty či procesoru). Mezi základní a nezbytné části řadíme: procesor, operační paměť, hard disk či ssd disk, napájecí zdroj a základní desku na níž jsou komponenty zapojeny. Dále zde můžeme zařadit i hardware, který není nutný pro start počítače, ale je též fyzicky hmatatelný a uvnitř počítače. Patří sem: grafická karta, síťová karta, zvuková karta nebo dvd mechanika.

4.1.2 Periferie

Mezi periferie počítače zařazujeme komponenty, bez kterých je počítač sám o sobě schopný fungovat. Tyto části jsou připojovány kabelem, technologií bluetooth či WiFi. Nejčastěji se jedná o myš, klávesnici, webkameru, reproduktory atd.[18]

[17] ZAVRŠNIK, A. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. s. 4. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7552-758-5.
[18] KOLOUCH, J., *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016, s. 59. CZ.NIC. ISBN 978-80-88168-15-7.

Software

Software je nejvíce používaným pojmem, co se týče programů a programovatelné části počítače. Objevují se zde i pojmy programové vybavení a počítačový program. Mezi těmito pojmy je však rozdíl. **Programové vybavení** jsou programy a přidružená dokumentace, pro vnitřní hardware počítače, které umožňují jeho další využití**.** **Počítačový program** můžeme popsat jako přesně daný postup (algoritmus), jakým má být počítačem zpracován. Je tvořen jedním či více soubory. Na počítačový program se vztahují autorská práva stejně jako například na knihu či film.

Software je pojem, který označuje programové vybavení, bez kterého není počítač schopen fungovat. „*Software jsou instrukce, které způsobí, že počítač může být využit. Označuje tedy „logickou“ část počítače, kterou nelze vnímat přímo lidskými smysly, tj. „vidět ji nebo si na ni sáhnout“. V širším slova smyslu to jsou veškeré informace, které jsou v počítači nějakým způsobem uloženy a dále se dělí podle způsobu použití do dvou základních skupin. Jsou to PROGRAMY a DATA.“*[19]

Software poté dělíme na další kategorie:

- **Publice domain –** Volně šiřitelné programy, které je možné dále upravovat podle uživatele, nicméně i tyto programy podléhají autorskému zákonu. Může se jednat například o 7-Zip.

- **Firmware – Určitý** druh sofwaru, který se vztahuje ke konkrétním komponentům počítače. V tomto případě se jedná o název BIOS. Tento BIOS je uložen v paměti ROM a je neměnný a předem definovaný výrobcem.

- **Freeware –** Volně šiřitelné programy prostřednictvím internetu, které neumožňují uživatelské úpravy. Tento software zcela podléhá autorským právům. Jsou to například: Opera, Google Chrome, Ccleaner a další.

- **Shareware –** Tyto programy jsou přístupné ke stažení na internetu. Po předem nastaveném čase od spuštění programu je uživatel vyzván

[19] PORADA, V., KONRÁD, Z. *Metodika vyšetřování softwarového pirátství*. Praha: Policejní akademie České republiky, 1999, s. 43. ISBN 80-7251-024-x.

k zakoupení licence. Jedná se o tzv. Trial verzi. Ve většině případů má ještě tato verze omezené funkce oproti plné.

- **Komerční software –** Program, který není volně šiřitelné a uživatel jej musí zakoupit. Jednat se může například o Adobe Photoshop, Final Cut, Camtasia Studio nebo Pinnacle studio.[20]

Typy kybernetické hrozby

4.1.3 Crackeři vs Hackeři

Hacker je člověk, jehož hlavní zájem je objevování tajemství ve virtuálním světě kam se běžný uživatel nemá šanci dostat. Mezi tyto lidi patří většinou programátoři a převažují zde dobré úmysly. Většinou se hackeři snaží nalézt bezpečnostní chyby v operačních systémech či programech. Získané informace poté předávají vývojářům daných programů pro jejich opravu. Hackeři se stále snaží prohlubovat své znalosti, které poté sdílí s ostatními hackery a nikdy nekonají s úmyslem daná data zničit.

Cracker je prakticky opakem hackera. Jeho úmysly jsou vždy zlomyslné. Proniká do všemožných programů s cílem najít bezpečnostní chybu a využít ji. Buď tato data schválně zničí, aby způsobil škodu, nebo získané informace prodávají konkurenci. Crackery dále dělíme na 2 kategorie. Do první kategorie spadají ti, kteří odhalili bezpečnostní díry a píší programy, jež dále zneužívají těchto problémů. V této kategorii se nacházejí pouze zkušení programátoři. Druhou kategorií nazýváme „script kiddie“ (v překladu skriptující děcka). Ti tyto programy sami nepíší, ale pouze vědí, kde daný program sehnat a jak ho spustit.[21]

Častým nástroj crackerů se nazývá „rekognoskace“. Mnoho lidí si pod tímto slovem představuje špionáž či špehování. Ve své podstatě v komunitě crackerů se jedná o podobný význam. Zde se rekognoskace využívá pro shromáždění informací na cílený objekt. Na základě získaných informací si cracker udělá přesný obrázek o svém cíli. Tyto informace mohou být například: nejlepší čas útoku, cesta útoku nebo provedení útoku.

[20] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016, s. 64. CZ.NIC. ISBN 978-80-88168-15-7.
[21] ANONYMOUS. *Maximální bezpečnost*. 4. vyd. Praha: Softpress, c2004, s. 73. ISBN 80-86497-65-8.

Využívá se zde mnoho programů pro monitoring sítě, odkud vycházejí důležité informace.

Další možností nemusí být zjišťování informací ve virtuálním světě, nýbrž může využít **sociálního inženýrství**. Sociální inženýrství může přiblížit daný příklad. „*Cracker A hodlá zaútočit na softwarovou společnost ABC123 s.r.o. a proto chce zjistit uživatelská jména, hesla a možná dokonce bezpečnostní opatření o firmě ABC123. Začne tím, že zavolá na hlavní číslo společnosti ABC123, vysvětlí sekretářce, že je ve firmě nový, že pracuje mimo sídlo společnosti a že by potřeboval zjistit číslo na technickou podporu, aby si zřídil svůj účet a heslo. Cracker A následně zavolá na technickou podporu, vysvětlí pracovníkovi na telefonu situaci a požádá ho o uživatelské jméno a heslo. Následně se zeptá, jakým způsobem může získat přístup do firmy zvenčí. Pracovník technické podpory mu ochotně sdělí požadované informace, aniž by vyzvídal příčiny vedoucí k tomuto požadavku.*“[22] Další možností útočníka je prohledávání odpadu z dané firmy. V těchto popelnicích může najít IP adresy, stará hesla, popřípadě mapu sítě.

4.1.4 Phishing

Phishing je forma kybernetického útoku, která má za cíl vylákat z oběti citlivé informace prostřednictvím falešného e-mailu. Zde se využívá také již zmíněného sociálního inženýrství. Často tito útočníci také usilují o získání telefonního čísla, čísla občanského průkazu, přístupu do internetového bankovnictví apod. Ve falešném e-mailu může být oběť například vyzvána k zaplacení balíčku, který si neobjednala viz obrázek 1. V tomto případě uživatel klikne na „Zaplat ted“. Následně bude přesměrován na webové stránky útočníka, kde vyplní číslo kreditní karty, ukončení platnosti karty, CVV kód ze zadní strany karty a další údaje. Díky tomuto kroku útočník získá uživatelovy kompletní údaje o jeho kreditní kartě. A v případě že uživatel nemá zřízené dvoufázové ověření, tak může útočník platit

Obrázek 1: Falešný e-mail od ČP

Zdroj: E-mail autora.

[22] ANONYMOUS. *Maximální bezpečnost*. 4. vyd. Praha: Softpress, c2004, s. 75. ISBN 80-86497-65-8.

cokoliv prostřednictvím cizí karty. Jak daný phishingový útok poznat? Pokud se podíváme na uvedený příklad, můžeme zde nalézt mnoho věcí pomocí, kterých odhalíme, že se jedná o podvod. 1. V této zprávě chybí formální oslovení zákazníka. 2. V celém textu chybí diakritika. V případě zprávy od skutečné české pošty by určitě nechyběla. 3. E-mail nás odkazuje na cizí stránku, na které budeme muset pravděpodobně sdělit své osobní údaje. V tomto případě údaje z kreditní karty. Dalšími znaky podvodu může být například vysoká naléhavost. Zaplatit či sdělit své údaje musíte co nejrychleji. Nebo vám může být nabídnuto zboží zdarma, které normálně stojí několik tisíc korun. Phisingový útok může být ještě poslán z podezřelé webové stránky. Česká pošta či banka nikdy nebude odesílat zprávu přes doménu např.: „*www.ahmudgalil.com*“.

4.1.5 Sniffing

Tento druh kybernetické kriminality je odvozen od anglického slova „sniff“. V překladu to znamená čmuchat či čenichat. Sniffing znamená neoprávněné odposlouchávání komunikace na síti. Činnost, jež vypadá nevinně, může být trestně kvalifikovaná. Pro to, aby bylo možné sniffing kvalifikovat jako trestný, musí pachatel jednat nelegálně a bez vědomí či souhlasu uživatele. Sniffing lze užít pro přípravu blížícího se útoku. Útočník „odposlouchává “ zadávaná hesla.[23] Tato hesla může prodávat třetí straně nebo je sám použije pro chystaný útok. Keylogger je program, který je schopný snímat stisky kláves a následně je odesílat útočníkovi. Dopadení tohoto pachatele je prakticky nemožné. V dnešní době se útočníci schovávají za jiné IP adresy, přesměrovávají svůj provoz na jiné datové linky apod. V případě, že bude přeci jen útočník dopaden, je zde řešen pro trestný čin dle § 182 zákona č. 40/2009 Sb. Porušení tajemství dopravovaných zpráv. V případě prokázání viny hrozí útočníkovi až pět let vězení. [24]

4.1.6 Ransomware

Jedná se škodlivý kód, který uživateli „uzamkne“ počítač či určité součásti a pro jeho odemčení požadují výkupné. Ransomware lze lehce identifikovat. Většinou se na monitoru zobrazí zpráva s požadavkem na zaplacení požadované částky. V žádném případě není nutné částku, která se nejčastěji požaduje v kryptoměnách, platit.

[23] FEREBAUEROVÁ, R., PEKÁREK O. *Aplikovaná informatika*. České Budějovice: Vysoká škola evropských a regionálních studií, 2014, s. 119. ISBN 978-80-87472-74-3.
[24] 40/2009 Sb. Trestní zákoník. *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Copyright © AION CS, s.r.o. 2010 [cit. 31.03.2022]. Dostupné z:<https://www.zakonyprolidi.cz/cs/2009-40>

Ransomware může mít několik podob. Je schopen šifrovat celý pevný disk a bránit ve spuštění operačního systému nebo blokuje určité soubory uložené v počítači. Nemusí však napadat jen počítače. Ransomware je schopen cílit i na android zařízení, kterým vytváří či mění PIN kód a tím zamezuje přístup. Nejlepší obranou proti tomuto útoku je záloha dat, v případě nutnosti přeinstalace či pravidelné aktualizace všech programů v počítači včetně operačního systému.[25]

4.1.7 Spam

„*Spam je definován jako nevyžádaná elektronická pošta, která zahrnuje jakékoli komerční e-maily adresovaný příjemci, se kterým odesílatel nemá žádné obchodní nebo osobní vztahy a nebyl s ním udělen příjemcův souhlas.“*[26]

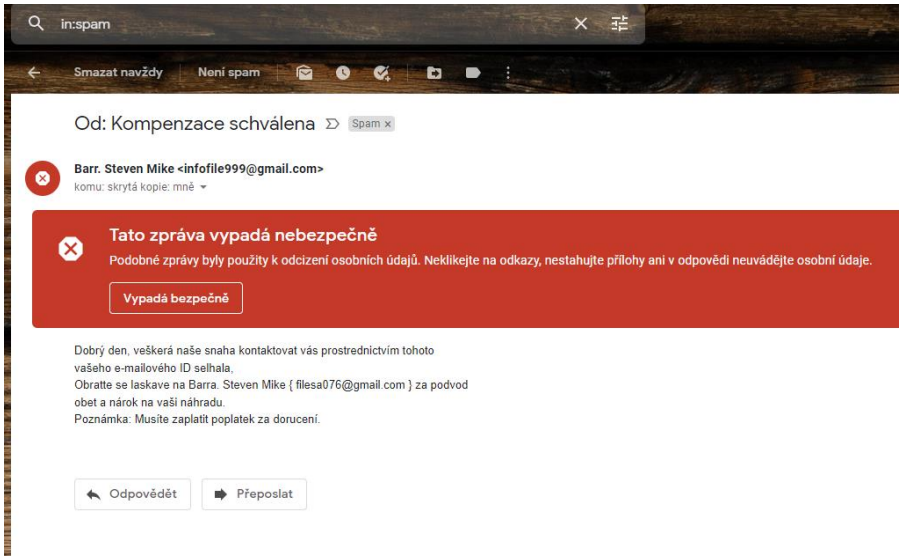
Jedná se tedy o nevyžádané, automatické rozesílání komerčních zpráv v hromadném množství. E-mail, který se řadí mezi spam většinou splňuje následující kritéria:

- **hromadné rozesílání –** e-mail není určen pouze pro jednu osobu, ale je rozesílán velkému množství uživatelů;
- **anonymní –** většinou ty zprávy chodí od neidentifikovatelných uživatelů, který pouze chtějí daného uživatele podvést;
- **je nevyžádaný –** příjemce si dané aktualizace nikde nevyžádal a neočekává je. za spam se e-mail nepovažuje, pokud si zažádáme o tzv. „newsletter“.[27]

Spam, nejen štve uživatele, který ho obdrží, ale zabírá též určitý síťový výkon a paměť e-mailové schránky.[28] Tento e-mail často zahrnuje výhru v loterii, do které se uživatel nepřihlašoval, nebo žádosti o laskavost či jiné finanční nabídky. Spam může být též užit pro phishing (více viz 3.5.2.). V dnešní době dokáží e-mailové servery pomocí svých filtrů spam rozpoznat a tím uživatele chránit, avšak ne vše, co spadne do složky spam musí spamem být.

[25] Co je to ransomware a jak se proti němu bránit? | ESET. *Malware Protection & Internet Security | ESET* [online]. Copyright © 1992 [cit. 05.01.2022]. Dostupné z: <https://www.eset.com/cz/ransomware/>.
[26] KREMLING, J., PARKER, M. Sharp A. *Cyberspace, cybersecurity, and cybercrime*. Los Angeles: London, 2018, s. 146. ISBN 9781506347257.
[27] Druh e-mailové zprávy, kterou firmy zasílají uživatelům, kteří o to projevili zájem.
[28] PANDE, J. *Introduction to Cyber Security*. Haldwani: Uttarakhand Open University, 2017, s. 23. ISBN 978-93-84813-96-3.

Obrázek 2 Příklad spamu.[29]



4.1.8 DoS, DDoS útoky

DoS je zkratkou z anglického spojení Denial of Service, což v překladu znamená „odepření přístupu“. Hlavním cílem tohoto útoku je odepření či snížení výkonu napadeného počítače. Tento útok probíhá zahlcením systému pomocí opakujícího se požadavku. Směrován může být jak na koncové zařízení, tak na provoz mezi serverem a počítačem. Projevem mohou být například nedostupné webové stránky. DoS je vždy řízen pouze z jednoho počítače, a proto je obrana vcelku jednoduchá. Obrana může být provedena odpojením daného útočníka. DDoS je v překladu „distribuované odepření přístupu“. V tomto případě je ofenzíva prováděna z více počítačů najednou. Obrana vůči DDoS je složitější, protože útočníků je více a jsou různě geograficky rozmístěni. [30]Podniknuty byly útoky například vůči společnostem Facebook či Yahoo!. Cílem DoS či DDos není přímo infikovat daný počítač, ale omezit jeho funkčnost či výkon. DDoS též využívají botnety (Internetový robot, která funguje automaticky a autonomně.), pro zjednodušení a zesílení útoku. DoS či DDoS probíhají každý den ve velkém množství a není možno se jich úplně zbavit.[31] Mezi nejzákladnější metody řadíme zahlcení příkazem ping či falšování zdrojové adresy. V případě, že je Dos nebo DDos posouzen jako trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací dle

[29] Zdroj: Vlastní e-mail.
[30] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016, s. 296. CZ.NIC. ISBN 978-80-88168-15-7.
[31] Viz www.digitalattackmap.com/

§ 230 odst. 2 TZ, je možné uložit trest odnětí svobody až na tři roky.Výše trestu však závisí na rozsahu a způsobené škodě.[32]

4.1.9 Viry a červi

Mezi jedny z největších hrozeb pro běžné uživatele jsou viry. Je to škodlivý software, který je možno nazývat též „Malware“. Tento škodlivý program má za cíl konat nechtěnou či škodlivou činnost proti vůli uživatele.[33] Přirovnat ho lze i k viru biologickému. *Chřipka je dobrým příkladem viru, který se může šířit od jedné osoby k druhé. Do jaké míry onemocníte, záleží na typu chřipky a na tom, zda jste očkovaní. Jakmile jste infikováni chřipkou, můžete virus také šířit na všechny osoby, se kterými přijdete do styku.*[34] Účinek daného viru, který je uložen v jeho kódu nazýváme payload. Dle tohoto kódu rozlišujeme nebezpečnost od té malé až po tu nejvyšší. Malware označuje souhrn všech kategorií viru. Jedná se například o trojské koně, červy, adware a popřípadě spyware. Nejčastěji jsou mezi sebou zaměňovány viry a červi. Hlavním rozdílem těchto virů je šíření. V případě viru je šíření závislé na jednání uživatele. Virus se například může infikovat do všech souborů s příponou „rar“. Infikované soubory poté rozesílá nevědomě uživatel. Oproti tomu počítačový červ je schopen se šířit nezávisle na vůli uživatele a tím se stát plně samostatným. Počítač se může nakazit otevřením přílohy v e-mailu. Infikovaný počítač poté sám rozesílá danou hrozbu mezi ostatní počítače. Tzv. payload může, ale také nemusí virus obsahovat. Mezi prakticky neškodné viry můžeme uvést například virus Yankee Doodle. Tento virus napadal soubory s koncovkou „exe“ a „com“. Způsoboval to, že každý den v 17.00 zahrál melodii Yankee Doodle.[35] U kategorie červ existuje případ se jménem „I love you“. Je považován za nejničivější na světě. Tento červ se šířil kybernetickým prostorem pomocí elektronické pošty MS Outlook. Po otevření přílohy se sám rozeslal na všechny účty v adresáři. Tento červ způsoboval zahlcení e-mailových serverů a přemazávání souborů uložených

[32] JANSA, L., OTEVŘEL O., ČERMÁK, J., MALIŠ, P., HOSTAŠ, P., MATĚJKA, M., MATEJKA, J. *Internetové právo*. Brno: Computer Press, 2016, s. 399. ISBN 978-80-251-4664-4.
[33] What is Malware and How to Protect Against It? | Kaspersky. *Kaspersky Cyber Security Solutions for Home & Business | Kaspersky* [online]. Copyright © [cit. 27.01.2022]. Dostupné z: <https://usa.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it>.
[34] MCCARTHY, L., WELDON-SIVIY, D. ed. *Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online*. Praha: CZ.NIC, 2013, s. 42. ISBN 978-80-904248-6-9.
[35] Yankeedoodle - The Virus Encyclopedia. *Main Page - The Virus Encyclopedia* [online]. Dostupné z: <http://virus.wikidot.com/yankeedoodle>.

v napadeném počítači. Podle dosavadních informací tento červ napadl v roce 2000 až 45 milionů počítačů.[36]

Dalším druhem počítačového viru je tzv. „Trojský Kůň“. Funguje na stejném principu jako bájná lest při Trojské válce. Tento vir se napřed tváří jako neškodný program, ke kterému je připojen nebezpečný zdrojový kód. Po nainstalování programu se do uživatelského počítače zanese payload. Nejčastěji bývá trojský kůň součástí bezplatných programů či vizuálního vylepšení počítače v podobě spořiče obrazovky. Na rozdíl od červů se trojský kůň sám nešíří. Uživatelé si ho stahují sami v domnění, že jde o bezpečný software. Využití je často od ztráty výkonu po úplné vymazání dat až po kompletní ovládnutí infikovaného počítače.[37]

4.1.10 Kyberkriminalita spojena se sociálními sítěmi

Za většinou dosud popsaných hrozeb ve virtuálním světě stáli především programátoři, kteří vymýšleli určité programy na ohrožení počítačů. Nebezpečí na internetu mohou vytvářet i běžní uživatelé, a to bez jakýchkoliv složitých nástrojů.

Mohou nás ohrožovat už i pouhým internetový prohlížečem. Mezi kyberkriminalitu, která je spojena se sociálními sítěmi můžeme řadit například:

- kyberšikana,
- kybergrooming,
- sexting.

Kyberšikana

Šikana v realitě záleží na úsilí útočníka ublížit, zesměšnit či urazit oběť jak fyzicky, tak psychicky. Tato šikana se dá převést i do virtuálního světa. Kyberšikana kvůli používání informačních technologií umožňuje opakované útoky na oběť, i když se oběť vzdálí. Tato šikana může být propojena s šikanou v realitě. Například útočník může svou oběť vyfotit v „trapné poloze“, kterou dále upraví a následně šíří po internetu nebo svou

[36] Zákeřný virus I love you napadl před 20 lety desítky milionů počítačů – Novinky.cz. *Novinky.cz – nejčtenější zprávy na českém internetu* [online]. Copyright © 2003 [cit. 28.01.2022]. Dostupné z: <https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/zakerny-virus-i-love-you-napadl-pred-20-lety-desitky-milionu-pocitacu-40322758>.
[37] DONÁT, J., TOMÍŠEK, J. *Právo v síti: průvodce právem na internetu*. V Praze: C.H. Beck, 2016, s. 215. ISBN 978-80-7400-610-4.

oběť fyzicky napadne a daný videozáznam umístí na Facebook. Kyberšikana je jedním z hlavních problémů dnešní mládeže. Mnozí útočníci si ani kolikrát neuvědomují závažnost svého jednání. Hodně často si myslí, že jde o pouhý žert, avšak druhá strana to tak vnímat nemusí. Klasická šikana je většinou prováděna pomocí několika dílčích útoků, které mohou sílit, avšak jednou skončí a nemusí se o nich mnoho lidí dozvědět. Oběť tak nemusí být dlouho traumatizována. V případě kyberšikany to neplatí. I jeden příspěvek může být neustále sdílen a nelze ho definitivně vymazat. Kdykoliv se může opět objevit a oběť ohrozit vícekrát i po ukončení šikany. Mezi jeden z prvních a nejtragičtějších případů kyberšikany se odehrál v Polsku. *„Pět spolužáků podrobilo Annu před celou třídou sexuální šikaně (strhali z ní šaty a předstírali, že ji znásilňují). Celou scénu nahráli na mobil a vyhrožovali dívce, že nahrávku zveřejní na internetu. To také později udělali, video umístili na stránku YouTube. Pro Annu to měla být pomsta za to, že s jedním z chlapců nechtěla chodit".*[38] Anna nakonec spáchala sebevraždu. Z tohoto důvodu je dnes kyberšikana dle mého názoru nebezpečnější než šikana klasická.

Kybergrooming

Jedná se o psychologickou manipulaci s obětí prostřednictvím internetu, například přes sociální síť Facebook či WhatsApp. Útočník se snaží v oběti vyvolat falešnou důvěru, a tím osobu přemluvit k osobní schůzce. Výsledkem této schůzky je sexuální či jiné fyzické napadení. Obětmi může být kdokoliv. Nejčastěji jsou oběťmi dívky ve věku 11–17 let. Tyto dívky často trpí nedostatkem sebedůvěry či pocitem osamění. Kybergrooming začíná vyvoláním důvěry a izolováním oběti od okolí. Pokračuje různým podplácením (nabízení peněz, dárky) a vyvoláním emoční závislosti oběti na útočníkovi. Na základě provedených kroků oběť přemluví k osobní schůzce, kde může být proveden útok[39]. Zde jeden příklad kybergroomingu: „*Muž z Karlovarska prostřednictvím sociální sítě Facebook vyhledával mladé dívky ve věku 10 – 14 let, se kterými si následně psal a vyžadoval zaslání intimních fotografií. Někdy za zaslání intimní fotografie nabízel peníze nebo drahý mobilní telefon. Takto oslovil velké množství mladých dívek a celou konverzaci vedl v takovém duchu, aby se s dívkami mohl následně setkat. Matka jedné z dívek však na konverzaci své dcery s tímto mužem přišla a kontaktovala Policii ČR. I přes to, že Policie ČR pachatele zjistila a obvinila, ve svém jednání dále pokračoval a s jednou z dívek se dokonce setkal. Soudem byl proto vzat do vazby a hrozí mu až 5 let*

[38] *Projekt E-bezpečí - E-Bezpečí* [online]. Copyright © [cit. 28.01.2022]. Dostupné z: <https://www.e-bezpeci.cz/index.php/ke-stazeni/tiskoviny/4-prehledovy-list-kybersikana-1-a-2/file>.
[39] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016, s. 313. CZ.NIC. ISBN 978-80-88168-15-7.

trestu odnětí svobody.[40]“ Pokud si na internetu píšeme s někým cizím, tak si nemůžeme být nikdy jistí tím, kdo ve skutečnosti je na druhé straně komunikace. Kdokoliv se může vydávat za kohokoliv[41].

Sexting

Název sexting vznikl spojením dvou slov: sex a texting. Jedna z prvních užívaných definic vnímá sexting jako: „*akt rozesílání nahých fotografií mezi mobilními telefony či dalšími elektronickými médii, např. internetem*.“[42] Jde tedy o rozesílání textových zpráv, videa či fotek se sexuálním obsahem. Tento obsah vytvářejí samotné oběti sextingu. Může se to stát například při vztahu, kdy si osoby navzájem posílají dané zprávy či soubory. Sexting sám o sobě není trestný, trestné je až zneužití takového obsahu. Často k tomu dochází např. při rozchodu útočníka s obětí. Pachatel materiál užívá pro nátlak na oběť. Nejčastěji oběti vyhrožuje, že materiál zveřejní, pokud mu nebude zaslán další nebo ho využívá pro splnění jeho daných podmínek. Velkým problémem sextingu v online prostředí je ztráta kontroly nad šířeným materiálem. Fotky se mohou po internetu šířit několik let. Může to způsobit ztrátu zaměstnání nebo pachatel dopustí přestupků či trestných činů (šíření dětské pornografie, ohrožování výchovy dítěte, sexuální nátlak apod.). Známý případ sextingu se odehrál na Floridě v USA. Nezletilému Phillipu Alpertovi poslala jeho 16. letá přítelkyně své nahé fotografie. Když se rozešli, Phillip fotografie rozeslal více něž 70 lidem. Důsledkem jeho jednání bylo odsouzení na 5 let za šíření dětské pornografie a do svých 43 let bude Phillip umístěn do registru sexuálních útočníků[43]. Z případů z České republice můžeme uvést vznik tzv. „*Roztahovaček*“. Jedná se o facebookové stránky, na které byly umisťovány citlivé fotografie dívek. Největší stránka s názvem „Roztahovačky“ měla v době zrušení přes 6 000 fanoušků. V případě zveřejnění fotek bez souhlasu dané osoby, se dotčená osoba může domáhat ochrany svých práv v rámci občanskoprávního řízení.[44]

---

[40] Kybergrooming - INTERNETEM BEZPEČNĚ. *INTERNETEM BEZPEČNĚ - Užívejme internet bezpečnějším způsobem* [online]. Copyright © 2018 INTERNETEM BEZPEČNĚ. Všechna práva vyhrazena. [cit. 03.02.2022]. Dostupné z: <https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybergrooming/>.

[41] VANĚK, J., NOVÁK, J., KALIKA D. *Jak na Internet bezpečně*. Ilustroval Aneta BISKUPOVÁ. Praha: CZ.NIC, z.s.p.o., 2018, s. 89. CZ.NIC. ISBN 978-80-88168-29-4.

[42] KOPECKÝ, K. *Rizika internetové komunikace v teorii a praxi*. Olomouc: Univerzita Palackého v Olomouci, 2013, s. 25. ISBN 978-80-244-3571-8.

[43] Sexting.cz - vse, co chcete vedet o sextingu. *Sexting.cz - vse, co chcete vedet o sextingu* [online]. Dostupné z: <http://www.sexting.cz>.

[44] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016, s. 316. CZ.NIC. ISBN 978-80-88168-15-7

Kybernetická bezpečnost v ČR

Dne 13. srpna 2014 podepsal prezident republiky Miloš Zeman zákon: č. 181/2014 o kybernetické bezpečnosti, který je účinný od 1. ledna 2015. Tento zákon je postaven na 2 zásadách. Zásada první je minimalizace zásahu do soukromý uživatelů a druhá zásada je individuální odpovědnost za bezpečnost vlastních informačních systémů. Dále se tento zákon opírá o 3 základní pilíře:[45]

- standardizaci (bezpečnostní opatření),
- hlášení kybernetických problémů,
- reakce na problémy.

Pro zajímavost: V roce 2020 bylo v České republice vedeno nejvíce kybernetických útoků proti zdravotnickému sektoru. Prudký nárůst vůči tomuto sektoru lze přičítat také probíhající pandemii COVID-19. Celkový nárůst útoků na zdravotnické sektory ke konci roku 2020 byl 45%, zatímco v ostatních odvětvích „pouze“ 22%.[46]

4.1.11 Národní úřad pro kybernetickou a informační bezpečnost

Hlavním správním orgánem, v oblasti kybernetické bezpečnosti v ČR je Národní úřad pro kybernetickou a informační bezpečnost (dále NÚKIB). Vznikl 1. srpna 2017 na základě zákona č. 205/2017 Sb. Stará se o ochranu utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany (Kryptografie neboli šifrování je nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí).[47] Další jeho starostí je řešení problematiky regulované služby Galileo.[48] NÚKIB má aktuálně 3 pracoviště. Jedno se nachází v Praze a dvě další v Brně. Hlavní sídlo se nachází na adrese: Mučednická 1125/31, Brno. Aktuálním ředitelem je Ing. Karel Řehka, který se pravidelně účastní jednání Bezpečnostní rady státu

[45] ČAPEK, J., HUB, M., ROUDNÝ, R., KOPÁČKOVÁ, H., FUKA, J., IBL, M. *Vybrané aspekty kybernetické bezpečnosti*. Pardubice: Univerzita Pardubice, 2015, s. 25. ISBN 978-80-7395-953-1.

[46] Rok 2020 přinesl kromě pandemie koronaviru i více kybernetických útoků na nemocnice | mobilenet.cz. *mobilenet.cz – Mobilní telefony, notebooky a technologie budoucnosti* [online]. Copyright © 2021 24net s.r.o. Všechna práva vyhrazena. [cit. 09.11.2021]. Dostupné z: <https://mobilenet.cz/clanky/rok-2020-prinesl-krome-pandemie-koronaviru-i-vice-kybernetickych-utoku-na-nemocnice-43079>.

[47] Kryptografie neboli šifrování je nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí.

[48] Galileo-autonomní globální družicový polohový systém (GNSS), financovaný evropskou unií.

a je též členem Výboru pro kybernetickou bezpečnost. Jmenovaný je vládou, která jediná ho může odvolat.

Další úkoly NÚKIB[49]:

- příprava a koordinace kybernetických cvičení v ČR a zahraničí;
- příprava zákonů a podzákonných norem v oblasti kybernetické bezpečnosti;
- vytyčení národní strategie v boji pro útokům;
- podpora vzdělání v kybernetice.

Od roku 2015 v České republice působí dva bezpečnostní týmy – vládní a národní. Národní CSIRT.CZ spravuje národní doménu CZ a dále má za úkol řešit bezpečnostní události v sítí na území celé České republiky. Druhý bezpečnostní tým vládní CERT spadá pod Národní centrum kybernetické bezpečnosti. Tento orgán se specializuje v první řadě na ochranu kritické infrastruktury a významných informačních systémů[50].

4.1.12 Preventivní projekty v ČR

V Evropě patří Česká republika v oblasti prevence mezi jedny z nejlepších států. Vzniká u nás celá řada projektů. Obsaženy jsou zde všechny věkové kategorie od základní školy až po seniory. Česká republika se snaží pomocí projektů minimalizovat nebezpečí na internetu. Uveďme si několik z těchto nejvýznamnějších projektů.

Seznam se bezpečně

Program „Seznam se bezpečně“ vytvořila firma Seznam.cz. Jedná se projekt, který souvisí se sociální sítí „Lide.cz“. Zde mohli uživatelé této sociální sítě pozorovat jevy, které je ohrožují používáním sociální sítě. Na začátku své existence sloužil pro odhalování závadného obsahu (dětská pornografie, podvodné aktivity). Odhalený obsah předaly bezpečnostní týmy policii ČR. Významným milníkem tohoto projektu je natočení stejnojmenného filmu, který byl rozeslán všem uživatelům. Následně byl natočen druhý díl věnovaný dětské prostituci, sociálnímu inženýrství a seznamování, třetí a zatím

[49] Národní úřad pro kybernetickou a informační bezpečnost - O úřadu. *Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka* [online]. Dostupné z: <https://www.nukib.cz/cs/o-nukib/o-uradu/>.
[50] KRÁL, M. *Bezpečný internet: chraňte sebe i svůj počítač*. Praha: Grada Publishing, 2015, s. 134. Průvodce (Grada). ISBN 978-80-247-5453-6.

poslední epizoda uvádí případ skautských vedoucích, kteří prostřednictvím internetu zneužili 39 dětí. Tento díl je určen především pro rodiče.[51] Webová stránka tohoto projektu byla zrušena, avšak je film zhlédnout na internetové adrese: https://www.stream.cz/seznam-se-bezpecne.

E-Bezpečí

Velice dobře propracovaný projekt, který je veden Univerzitou Palackého v Olomouci. Primárně směřuje na děti, protože jsou hrozbám internetu vystaveny nejvíce a jsou nejzranitelnější. Mezi témata patří: kyberšikana, spam, hoax, problémy v síti Facebook, phishing aj. Další cílovou skupinou jsou rodiče, pedagogové a další osoby, které s dětmi pracují. V současné době je projekt národním projektem, který též podává pomocnou ruku všem, kteří se stali obětí některé z online hrozeb.[52] E-Bezpečí nabízí velké množství besed či kurzů pro zájemce všech věkových kategorií. V rámci těchto workshopů se účastníci snaží poznávat rizika a naučit se správně reagovat v případě setkání s nimi. Jedním z úspěchu E-Bezpečí je 1. místo v Evropské ceně prevence kriminality. Webová stránka projektu je na adrese: https://www.e-bezpeci.cz/index.php.

Bezpečný internet

Projekt vznikl za účelem rizika, která hrozí na internetu a na konkrétních případech ukazují, jak se jim bránit. Necílí na žádné konkrétní skupiny, ale obecně na všechny uživatele internetu. Bezpečný internet je zcela zdarma a na své webové stránce (http://www.bezpecnyinternet.cz) dává možnost přečíst si rady, návody a zkušenosti internetových služeb. Po otevření stránky si uživatel může zvolit, v jaké cílové skupině se nachází (začínající uživatel, pokročilý, rodič, dítě či škola).

Linky pomoci

V případě, že jste se stali obětí nějaké hrozby, máte možnost zavolat na určitá sdružení, které vám pomohou. První je **Linka bezpečí**. Oddělení linky bezpečí slouží dětem a mladým lidem při jejich těžkých životních situacích. Pokud se dostanete do problému a potřebujete Linku bezpečí kontaktovat můžete tak učinit prostřednictvím telefonního čísla 116111, které je dostupné 24 hodin denně nebo e-mailové adresy

[51] KOŽÍŠEK, M., PÍSECKÝ, V. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016, s. 144. ISBN 978-80-247-5595-3.
[52] Informace o projektu - E-Bezpečí. *Projekt E-bezpečí - E-Bezpečí* [online]. Dostupné z: <https://www.e-bezpeci.cz/index.php/o-projektu/oprojektu>.

pomoc@linkabezpeci.cz. Hovor je zdarma jak z mobilního telefonu, tak z pevné linky. Člověk se zde může svěřit, že se stal například obětí jakékoliv formy šikany. Nejčastěji jsou volajícími ti, kteří se nemohou nikomu svěřit nebo se za svůj problém stydí. Druhou důležitou linkou je **Bílý kruh bezpečí.** Bílý kruh poskytuje obětem kriminality psychologické a sociální poradenství a praktické rady. Její bezplatná NonStop linka je 116006.

5 Praktická část

Praktická část bakalářské práce se bude skládat z dotazníkového šetření a rozhovorů s experty NÚKIB. Dotazníkové šetření se bude zabývat uživateli internetu a jejich povědomím o hrozbách, jež se na internetu nacházejí.

Výběr respondentů

Praktická část bakalářské práce byla realizována v době pandemie Covid-19, a proto byli respondenti osloveni pouze online formou. Dotazník byl vytvořen pomocí internetového portálu vyplnto.cz. Díky tomuto webu je možné vytvořit strukturu dotazníku, popřípadě odfiltrovat nepotřebná data. Po nastavení dotazníku byl vygenerován internetový odkaz, který byl následně sdílen na sociálních sítích jako je Facebook či Instagram. Prostřednictvím Facebooku byl dotazník šířen pomocí skupin typu: „Dotazníky k vyplnění " nebo „Dotazníky v bakalářským pracím", kde funguje pravidlo: „Vyplníš, Vyplním." Pro získání většího počtu respondentů byl souběžně dotazník odeslán na základní a střední školu. Na těchto školách dotazník vyplňovali jak žáci, tak také učitelé.

Sběr dat

Sběr dat probíhal od 17.02.2022 – 02.03.2022. Dotazník se nachází na internetové adrese: https://www.vyplnto.cz/realizovane-pruzkumy/75742/. Na dotazník odpovědělo 386 respondentů. Po ukončení sběru dat jsem prošel otázku po otázce a z šetření vyřadil 17 respondentů, jejichž odpovědi nedávaly příliš smysl. Celková návratnost dotazníku byla 84,4%. Dotazník byl sestaven z 18–23 otázek. Nacházely se zde otázky jak uzavřené, tak otevřené a průměrný čas zodpovězení otázek byl 5 minut. Vygenerovaný odkaz byl sdílen na sociální síti Facebook a Instagram. Rozeslán byl také do následujících škol:

- Gymnázium a SOŠ Plasy,
- Masarykova základní škola Horní Bříza,
- VOŠ a SPŠE Plzeň.

Dotazníkové šetření

Po otevření internetového odkazu se uživateli zobrazí úvodní informace. Pod těmito informacemi se nachází tlačítko „Vyplnit dotazník". Po kliknutí na toto tlačítko se respondentovi otevře dotazník s kladenými otázkami. Celkový počet otázek je 18–23.

Otázka první se dotazuje na pohlaví respondenta. Zde se respondenti rozdělí na muže a ženy.

Druhá otázka se týkala věku. Zde mohl uživatel zvolit mezi 5 nabízenými odpověďmi. Po konzultaci s vedoucí bakalářské práce byl zvoleno rozmezí takto: 6–15 let, 16–20 let, 21–40 let, 41–60, 61 a více let.

V otázce třetí uživatel zvolil své nejvyšší dosažené vzdělání. V případě, že odpovídali žáci základních školy, tak ti zvolili vzdělání základní. Pokud odpovídal žák střední školy, tak zvolil středoškolské. Podle svého oboru též volil, jestli středoškolské s maturitou či výučním listem. Ostatní uživatelé, kteří již nestudují volili podle svého nejvyššího dosaženého vzdělaní.

V následující otázce respondent hodnotil svého znalosti používání počítače. Na výběr měl z těchto 4 možností: běžný uživatel, pokročilý, specialista či začátečník.

Pátá otázka zněla: „Jaké pojmy znáte?“ Byly zde uvedeny 3 pojmy: kybernetická bezpečnost, kybernetická hrozba, kybernetická kriminalita. V případě, že uživatel neznal ani jeden pojem zvolil odpověď: „Neznám žádný“. V této otázce musel respondent zvolit minimálně jednu odpověď, avšak maximálně tři. V případě, že zvolil odpověď číslo 4 tedy, že nezná žádný pojem, nemohl zvolit již žádnou další možnost.

Šestá otázka se ptá, jak moc uživatel souhlasí s tím, že by každý, kdo používá počítač, měl znát nástrahy virtuálního prostředí. Forma odpovědi byla uzavřená.

Sedmá otázka byla pouze pro uživatele, kteří zvolili, že nesouhlasí s tvrzením v otázce šesté. Forma odpovědi byla otevřená a uživatel se mohl vyjádřit z jakého důvodu nesouhlasí.

Osmá otázka zněla: „Jaké hrozby virtuálního prostředí (Internetu) znáte? Zvolit můžete více odpovědí.“ Forma odpovědi byla uzavřená a respondent musel zvolit alespoň jednu možnost.

V deváté otázce byl uživatel tázán zdali měl někdy osobní zkušenost s kybernetická kriminalitou. Na výběr bylo ze tří možností. „Ano“, „Ne“, „Nevím“. Pokud byla zvolena odpověď „Ano“, tak uživatel pokračoval otázkou číslo 10. Pokud odpověď byla „Ne“ či „Nevím“, pokračoval respondent otázkou číslo 11.

Otázka číslo deset byla pouze pro uživatele, kteří se setkali s kybernetickou kriminalitou. Forma odpovědi byla otevřená a uživatel zde uvedl s jakou kybernetickou kriminalitou se setkal.

Jedenáctá otázka zněla: „Poslal/a jste nebo zveřejnil/a někdy svou intimní fotografii?“ Na výběr bylo pouze ze dvou možností a to: „Ano“ či „Ne“.

Ve dvanácté otázce šlo o to, jestli uživatel využívá sociální sítě. Opět forma odpovědi byla uzavřená. Na výběr bylo pouze ze dvou možností a to: „Ano“ či „Ne“. V případě, že uživatel zvolil „Ano“, byl v otázce číslo třináct tázán, jaké sociální sítě využívá. Jestli respondent sociální sítě nevyužívá, pokračoval až otázkou číslo čtrnáct.

Třináctá otázka zněla: „Jaké sociální sítě používáte? Vybrat můžete více odpovědí.“ Tato otázka byla pouze pro uživatele, kteří sociální sítě využívají. Forma odpovědi byla uzavřená a na výběr bylo deset možností, ze kterých musel respondent zvolit alespoň jednu.

Čtrnáctá otázka zněla: „Používáte ochranu proti kybernetickým hrozbám?“. Forma odpovědi byla uzavřená a na výběr byly 2 možnosti. Možnosti byli: „Ano“ či „Ne“. Pokud uživatel zvolil možnost „Ano“ pokračoval otázkou číslo 15, jestliže zvolil „Ne“, pokračoval až otázkou číslo 16.

Patnáctá otázka byla pouze pro uživatele, kteří odpověděli, že využívají ochranu svého počítače. Jednalo se o doplňující otázku k otázce 14, kde uživatel mohl zvolit z nabízených možností, popřípadě napsat svými slovy, jak si chrání svůj počítač.

V šestnácté otázce byla fotografie internetové hrozby, která může komukoliv dorazit do e-mailu. Uživatel měl odpovědět, jak zareaguje, pokud mu do zpráv dorazí. Forma odpovědi byla polouzavřená. Respondent mohl vybrat jednu z dvou nabízených možností, nebo odpovědět vlastními slovy co udělá.

Sedmnáctá otázka byla prakticky stejná jako otázka šestnáct. Jen se zde lišila podoba hrozby.

Otázka osmnáct zněla: „Jaký druh internetové kriminality je podle vás nejvíce nebezpečný?“ Forma odpovědi byla polouzavřená. Uživatel mohl zvolit z nabízených

možností nebo zvolit odpověď „Jiné“, která ho navedla na otázku devatenáct. Jestliže respondent zvolil aspoň jednu z uvedených hrozeb, pokračoval otázkou číslo dvacet.

Devatenáctá otázka byla pouze pro uživatele, kteří v předchozí otázce zvolili odpověď „Jiné“. Forma odpovědi byla otevřená, a uživatel zde musel napsat jaká hrozba je podle něj nejnebezpečnější.

Ve dvacáté otázce měl respondent zhodnotit, jestli je schopen hrozbu na internetu rozeznat. Forma odpovědi byla uzavřená.

Dvacátá první otázka zněla: „Měl by se stát více věnovat prevenci v oblasti kybernetické kriminality?“ Forma odpovědi byla uzavřená a uživatel zde měl vybrat, jestli souhlasí či nikoliv.

Ve dvacáté druhé otázce byl uživatel tázán, jestli se někdy nějakým způsobem vzdělával v oblasti chování na internetu či kybernetických hrozeb. Forma odpovědi byla uzavřená. Respondent se mohl rozhodnout mezi: „Ano“ či „Ne“.

Dvacátá třetí otázka se uživatele ptá, jestli by měl zájem získávat informace o nových hrozbách na internetu a možných způsobech ochrany vůči nim. Forma odpovědi byla uzavřená.

Analýza získaných dat

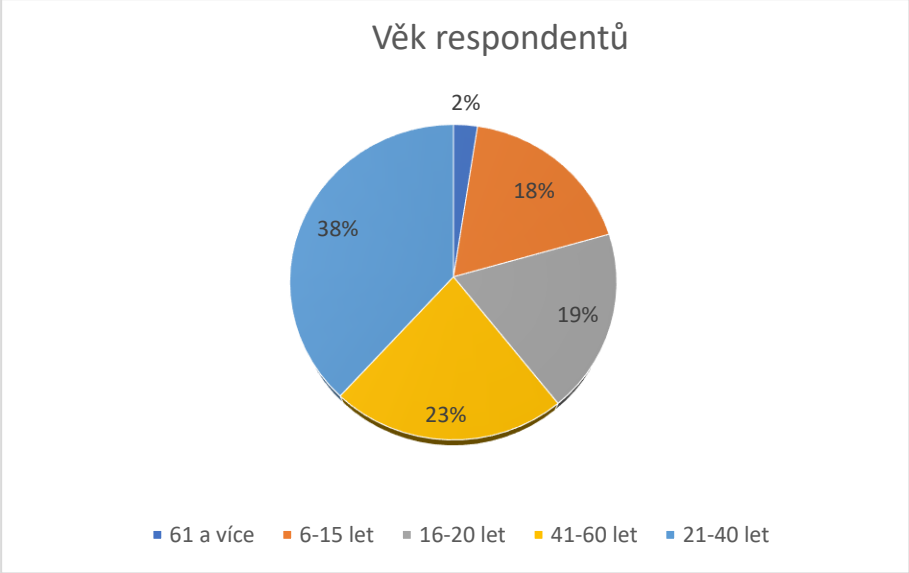
Z první otázky vyplývá, že na dotazník z celkového počtu 369 respondentů odpovídaly především ženy viz Graf číslo 1. Významný vliv na vyplnění dotazníku měla i ochota daných respondentů, kterou projevily především ženy. Vzhledem k tomu, že dotazník byl poskytnut pouze v online formě a sdílen na sociálních sítích či poslán do škol, nebylo možné ovlivnit, jaké pohlaví bude odpovídat více, popřípadě se snažit o vyrovnané rozložení.

Graf 1: Poměr můžu a žen, kteří se zúčastnili šetření[53]

[53] Zdroj: vlastní zpracování.

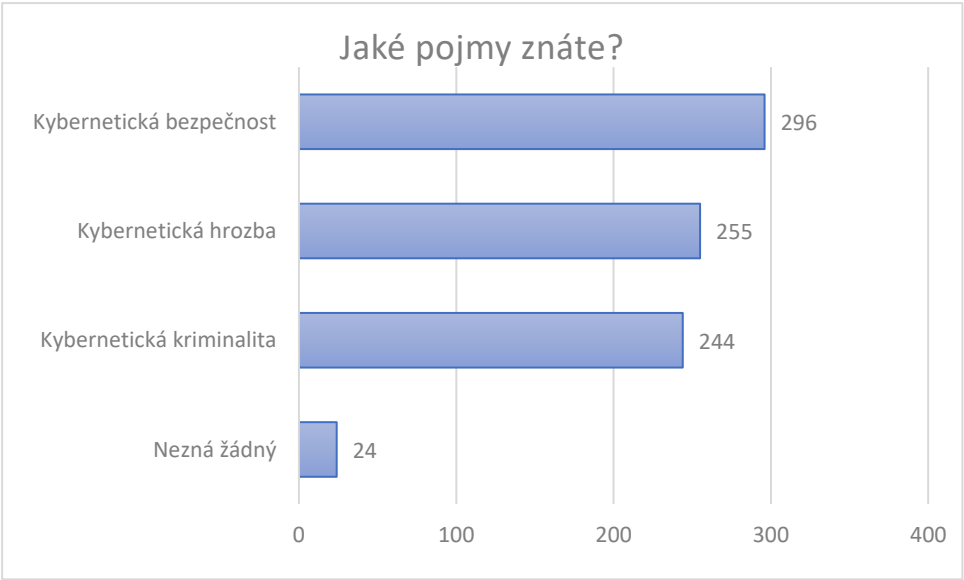
V otázce druhé můžeme na názorném grafu vyčíst, že nejvíce odpovídali uživatelé ve věku 21–40 let, a naopak nejméně lidí ve věku 61 a více let. Toto může být způsobeno tím, že nejvíce času na počítači tráví právě uživatelé ve věku 21–40 let, a proto od nich je nejvíce odpovědí.

Graf 2 Věk respondentů[54]



Pokud bychom řešili první 3 základní pojmy, kterými byly: kybernetická bezpečnost, kybernetická hrozba a kybernetická kriminalita, tak nejvíce známým je pojem kybernetické bezpečnosti. Ze všech tázaných ho zná 80 % respondentů.

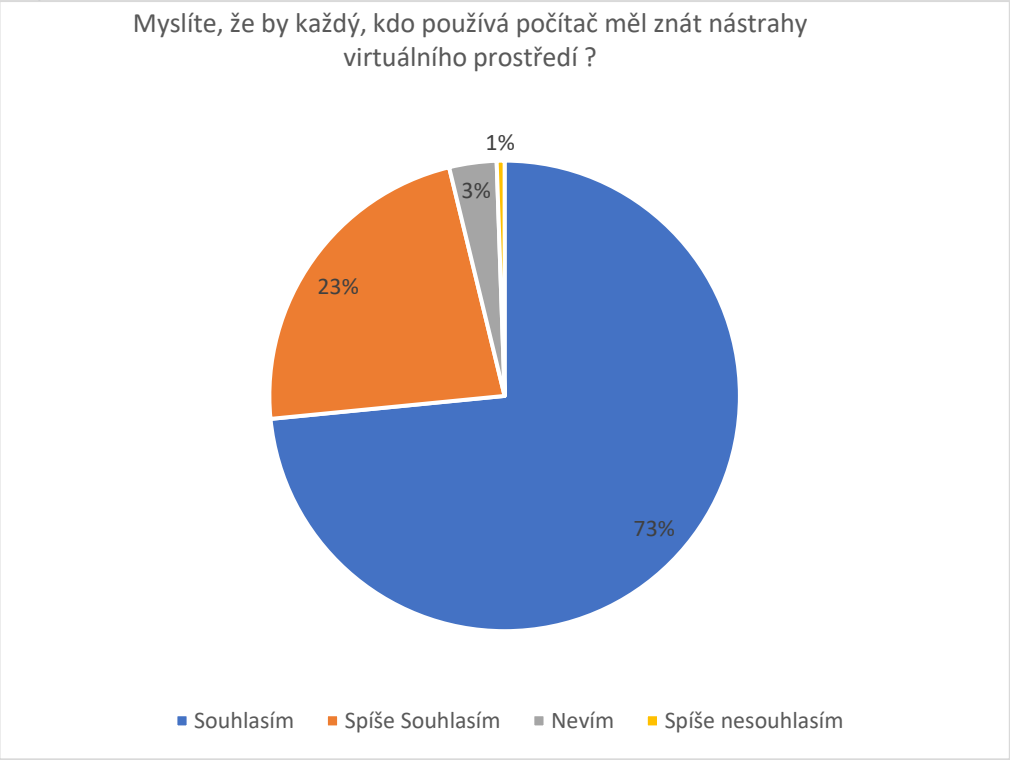
Graf 3 Počet respondentů, jenž znají daný pojem[55]



[54] Zdroj: Vlastní zpracování.
[55] Zdroj: Vlastní zpracování.

Dále bylo v dotazníku řešeno, jestli si uživatelé myslí, že je potřeba znát nástrahy virtuálního prostředí. Díky této otázce můžeme konstatovat, že 96% respondentů souhlasí či spíše souhlasí, a tím pádem se zajímají o tyto nástrahy. Nejvíce s tímto výrokem souhlasí vysokoškolští uživatelé. Objevil se zde i jeden respondent se základním vzděláním ve věkové kategorii 6–15 let, který nesouhlasil a myslel si, že není potřeba nástrahy znát.

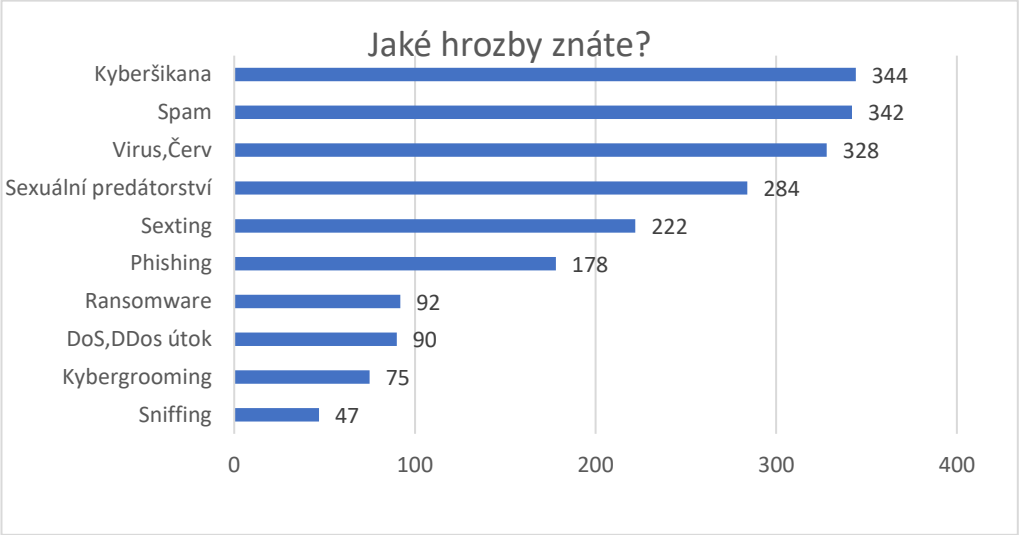
Graf 4 Názor uživatelů na otázku číslo 6. [56]



Abychom mohli říct, že uživatel je schopen poznat bezpečnostní hrozbu, museli jsme se zeptat, jestli a popřípadě jaké hrozby zná. K tomuto nám sloužila otázka číslo 8. V této otázce bylo vybráno 10 nejčastějších hrozeb na internetu. Nejvíce uživatelé znají kyberšikanu, spam či virus. Všechny tyto hrozby zná minimálně 90 % respondentů. 75 % dotázaných zná též sexuální predátorství. Způsobeno to může být filmem „V síti“, který vyšel v roce 2020 a tímto problémem se zabývá. Naopak nejmenší povědomí mají uživatelé o sniffingu. Zde tento problém zná pouze 12 % dotázaných.

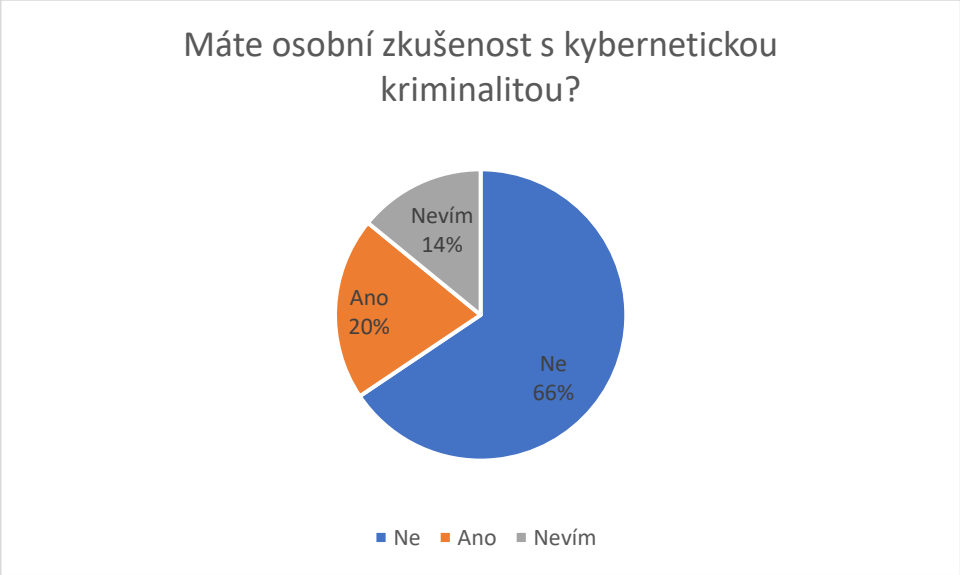
[56] Zdroj: vlastní zpracování.

Graf 5 Jak jsou známé hrozby[57]



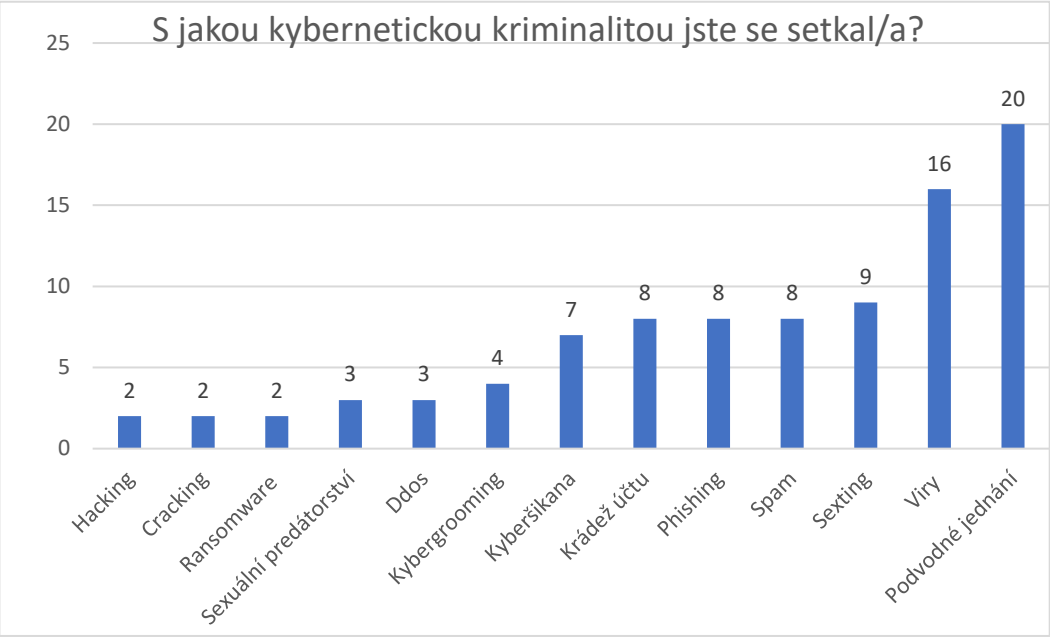
Z odpovědí na devátou otázku jsem zjistil, kteří uživatelé se již stali obětí kybernetické kriminality a následně i jaké. V grafu vidíme, že obětí kybernetické kriminality se stalo 20 % dotázaných. Více se zde stávali oběťmi respondenti s maturitním vzděláním. Bylo zde 21 obětí s maturitním vzděláním oproti 17 obětem se základním vzděláním.

Graf 6 Jaké procento uživatelů se setkalo s kybernetickou kriminalitou[58]



[57] Zdroj: vlastní zpracování.
[58] Zdroj: vlastní zpracování.

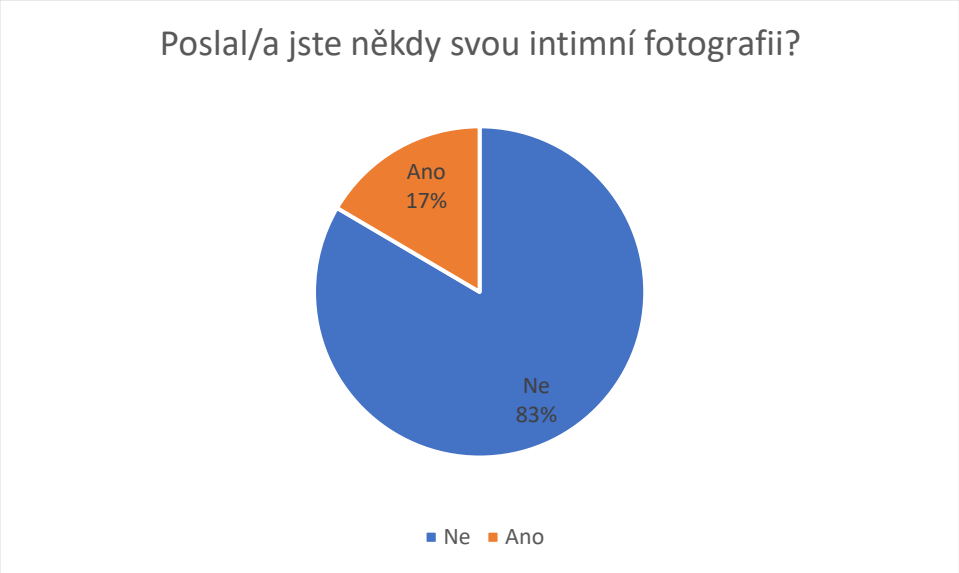
Graf 7 Zkušenosti uživatelů s kybernetickou kriminalitou[59]



V grafu 7 vidíme, že nejčastěji se respondenti stávali oběťmi podvodného jednání a virů. Díky tomuto výsledku se můžeme domnívat, že nejčastější hrozbou je tedy podvodné jednání. Předpokládám, že lidé kteří se obětí dané hrozby již stali, jsou schopni ji poznat a reagovat na ni díky své předchozí zkušenosti.

V jedenácté otázce byl respondent dotázán, jestli někdy poslal či zveřejnil svou intimní fotografii. Tato otázka byla z důvodu hrozby tzv. sextingu. Sexting není nebezpečný v době páchání, ale může danou osobu dohnat v budoucnosti.

Graf 8 Jaké % uživatelů poslalo své intimní fotografie?



[59] Zdroj: vlastní zpracování.

Dle získaných odpovědí nejvíce fotografie tohoto typu zasílají ženy ve věku 21–40 let s maturitním vzděláním. V této kategorii poslalo fotografie 29 žen, avšak co je alarmující je kladný počet odpovědí u žen ve věku mezi 6–15 lety.

Obrázek 3 Odpovědi u otázky číslo 11[60]

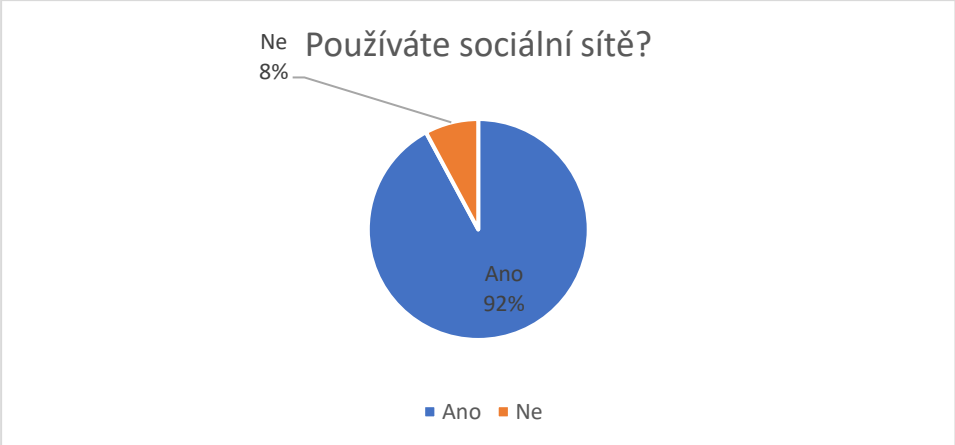
Poslal/a jste nebo zveřejnil/a někdy svou intimní fotografii?

Odpovědi / Segmenty	Všichni respondenti	Muž					Žena			
		6–15	16–20	21–40	41 – 60	61 a více	6–15	16–20	21–40	41 – 60
Ano	61 16.5%	0 0%	4 13.8%	11 21.2%	1 5.3%	0 0%	4 10.8%	10 25%	29 32.6%	2 3.1%
Ne	308 83.5%	30 100%	25 86.2%	41 78.8%	18 94.7%	4 100%	33 89.2%	30 75%	60 67.4%	62 96.9%

V této věkové kategorii své intimní fotografie zaslaly 4 dívky. Problémem je nejspíše to, že si dívky neuvědomují a nerozpoznávají v tomto hrozbu, která je může v budoucnosti dohnat. Navíc ve věku do 18 let se jedná o šíření dětské pornografie. Tyto dívky nejsou ohroženy jen sextingem, nýbrž se mohou stát obětí kyberšikany.

Obětí kyberšikany, sextingu či kybergrooming bývají nejvíce uživatelé sociálních sítí. Graf 9 odhaluje, že uživatelem sociálních sítí je dnes skoro každý.

Graf 9: Jaké % uživatelů využívá sociální sítě.[61]

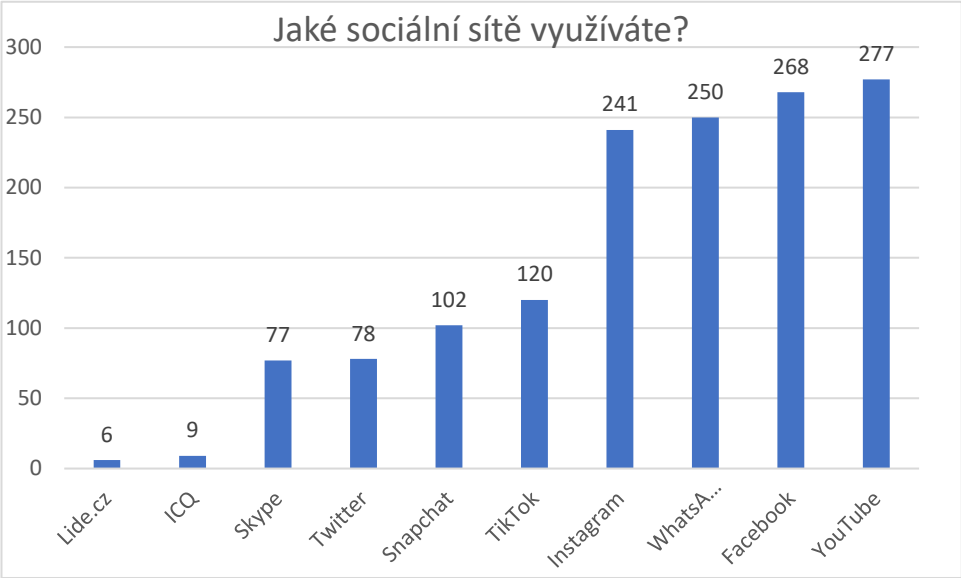


Nejvíce sociální sítě využívají uživatelé ve věku 21–40 let, nejméně naopak ve věku 61 a více let. Ten výsledek může být způsoben rozdílnými generacemi uživatelů. Aktuálně

[60] Zdroj: vlastní zpracování.
[61] Zdroj: vlastní zpracování.

je nejvyužívanější sociální sítí YouTube a Facebook. Tyto 2 sociální platformy využívá 80 % dotázaných.

Graf 10 Využití sociálních sítí mezi uživateli[62]



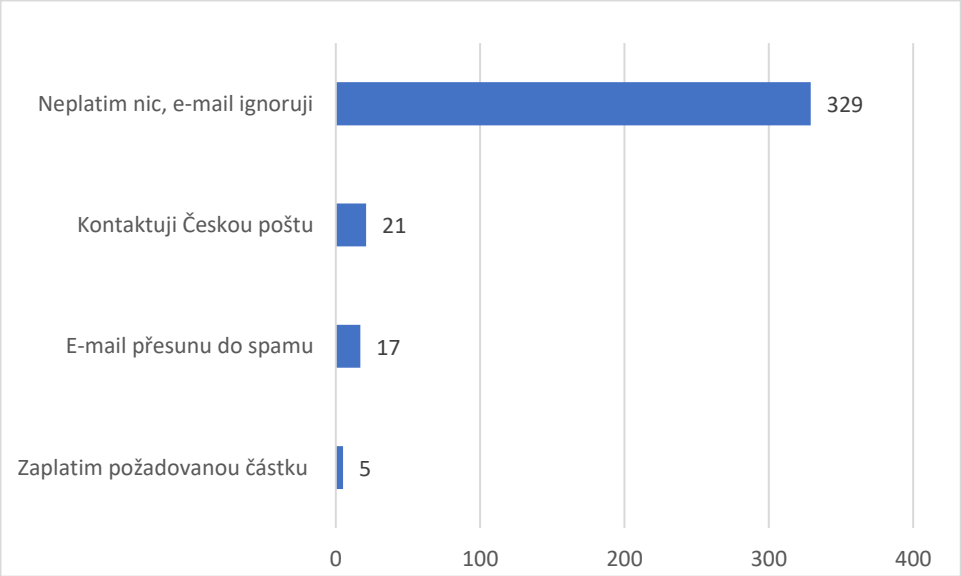
Právě na sociálních sítích na uživatele může číhat nejvíce hrozeb. Jak bylo zmíněno u grafu číslo 7. Pokud se respondent stal obětí kybernetické kriminality, bylo to nejčastěji obětí podvodného jednání. Z tohoto důvodu byly položeny otázky 16 a 17. Byly zde uvedeny příklady podvodného jednání a respondent musel odpovědět, jak zareaguje a jestli hrozbu pozná. V případě 16. otázky odpovědělo 5 uživatelů nesprávně. 4 z těchto uživatelů byli ve věku 6–15 let čili na základní škole. Způsobeno to může být nedostatečnou informovaností dětí. Na následujícím graf vidíme, že 99 % respondentů je schopno hrozbu poznat.

[62] Zdroj: vlastní zpracování

Graf 11 Reakce na první hrozbu[63]

Respondent měl možnost případně doplnit možnosti reakce. Následující graf znázorňuje, jak se respondenti vyjádřili.

Graf 12 Shrnutí reakcí na hrozbu[64]

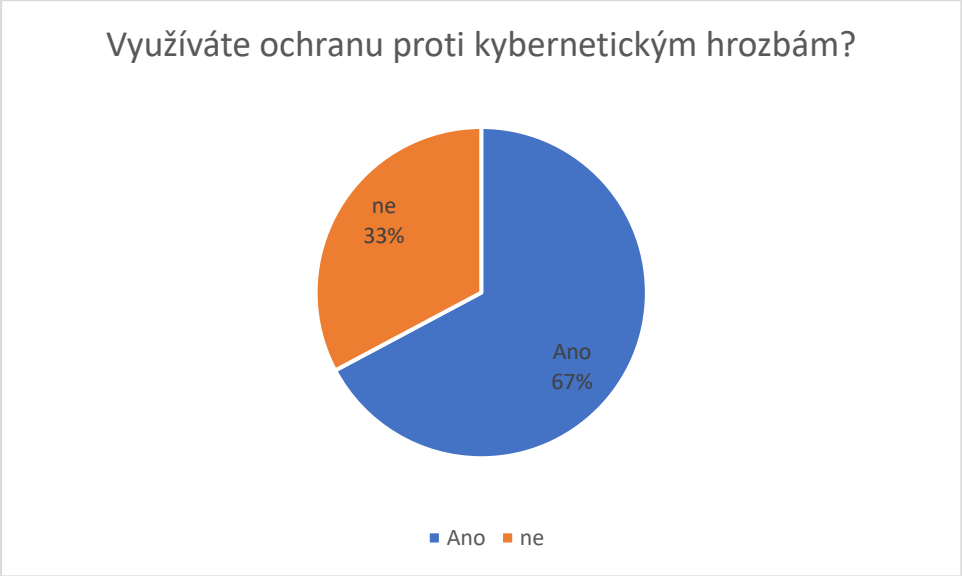


V případě 2. hrozby odpověděli všichni respondenti, kromě dvou, správně. Hrozbu rozeznali a žádný kód by neposílali zpět.

[63] Zdroj: vlastní zpracování.
[64] Zdroj: vlastní zpracování.

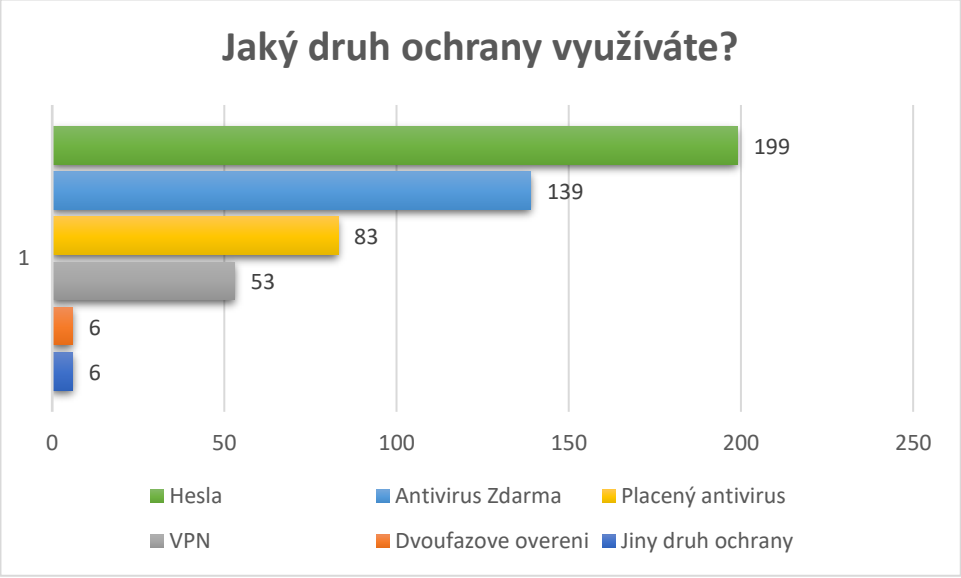
Pro správné rozeznání a odolání hrozbě je důležitá ochrana našeho zařízení. Z tohoto důvodu byl respondent tázán, jestli určitý typ ochrany využívá. V grafu 13 vidíme, že ochranu využívá 67 % tázaných. Zbylých 33 % je daleko více ohroženo, protože bez ochrany nejsou schopni rozeznat například virus.

Graf 13 Jaké % uživatelů využívá ochranu počítače[65]



Respondenti, kteří využívají určitý typ ochrany byli ještě tázáni, jaký druh používají. V grafu 14 jsou znázorněny nejčastější odpovědi.

Graf 14: Druhy použité ochrany[66]

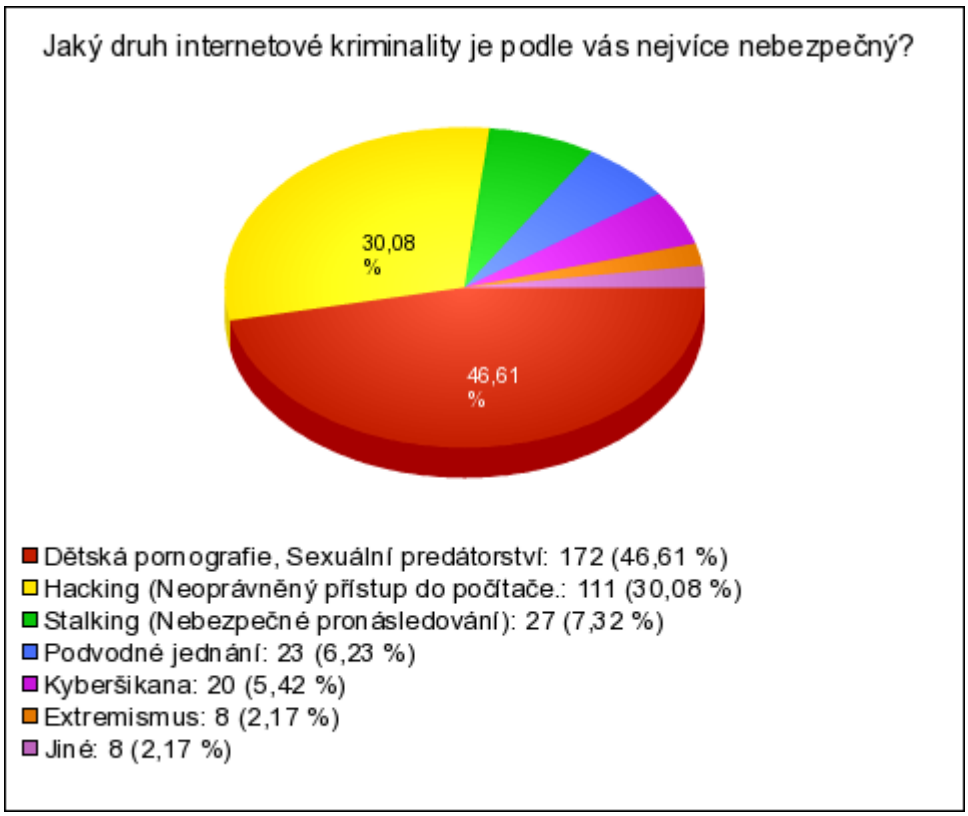


[65] Zdroj: vlastní zpracování.
[66] Zdroj: vlastní zpracování.

Zabezpečení svého zařízení je velice důležité a není dobré ho podceňovat. Čím více ochran využíváme, tím jsme odolnější vůči hrozbám. Kombinace druhů ochran jen násobíme svoji odolnost, a proto by v každém zařízení neměl chybět antivirus a každý by měl využívat dvoufázového ověření.

Důležité je také uvědomit si, která hrozba je nejvíce nebezpečná. Čím nebezpečnější hrozba pro uživatele je, tím si na ni dává větší pozor. V 11. otázce byl respondent tázán, jestli poslal někdy svou intimní fotografii. Zjistili jsme, že ji poslali i dívky, které nebyly starší 15 let. Jednalo se zde tedy o dětskou pornografii. Za nejvíce nebezpečnou hrozbou na internetu respondenti zvolili právě dětskou pornografii.

Graf 15 Nejnebezpečnější druh internetové kriminality podle uživatelů[67]



Respondent byl tázán, jestli si myslí, že zvládne rozpoznat hrozbu. Nejvíce jistí si zde byli respondenti ve věkové kategorii 16–20 let, a naopak nejméně uživatelé ve věku 41 a výše. V této věkové kategorii si není jisto 59 % respondentů. Což z respondentů v tomto věku dělá podle mého dotazníku nejrizikovější skupinu (viz obrázek 4.). V součtu si ale uživatelé převážně myslí, že hrozbu odhalit dokážou (viz graf 16.).

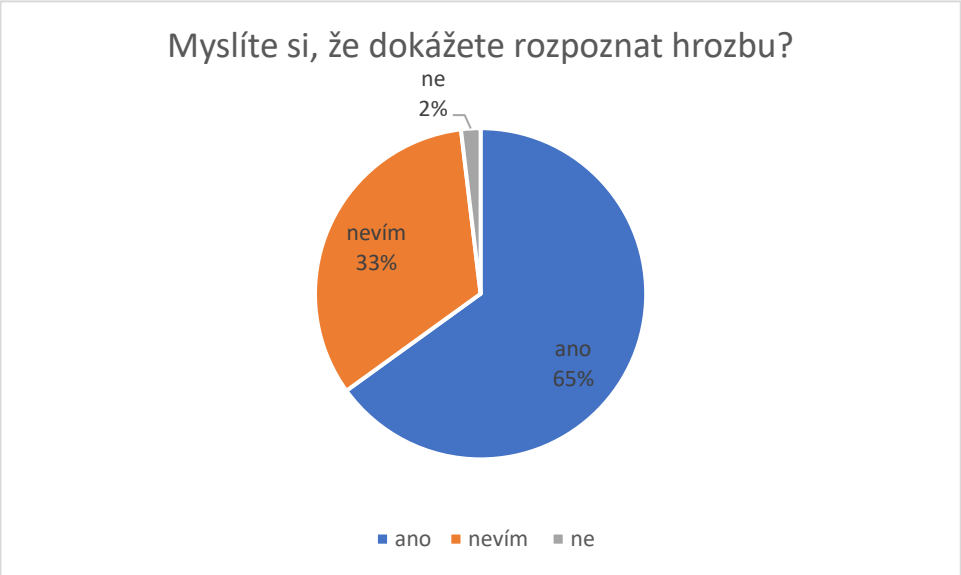
[67] Hubka, J. – *Kybernetická bezpečnost (výsledky průzkumu)*, 2022. Dostupné online na <https://75742.vyplnto.cz>.

Obrázek 4 Výsledky otázky číslo 20[68]

Myslíte si, že zvládnete rozpoznat hrozbu na internetu?

Odpovědi / Segmenty	Všichni respondenti	6–15	16–20	21–40	41 – 60	61 a více
ano	240 65%	47 70.1%	55 79.7%	101 71.6%	34 41%	3 33.3%
ne	7 1.9%	2 3%	0 0%	3 2.1%	1 1.2%	1 11.1%
nevím	122 33.1%	18 26.9%	14 20.3%	37 26.2%	48 57.8%	5 55.6%

Graf 16 Výsledky otázky číslo 21[69]



Vliv na rozpoznání hrozby má určitě již dřívější seznámení prostřednictvím kurzu či nějakého školení. Toto tvrzení nám podporuje další otázka, ve které se na kurz či školení ptám. Zde nám z 240 respondentů, kteří dokážou hrozbu rozeznat, odpovědělo 185, že již nějakým kurzem prošlo. Zároveň z těchto 240 respondentů si 219 myslí, že by se stát měl prevenci věnovat více než se věnuje doposud a 152 z nich by mělo zájem dostávat pravidelné informace o nových hrozbách a možných způsobech ochrany.

[68] Zdroj: vlastní zpracování
[69] Zdroj: vlastní zpracování

Rozhovory

V rámci bakalářské práce jsem položil několik otázek specialistům z NÚKIB. Někteří si přáli zůstat v anonymitě, a proto zde nebudou uvedeny jejich jména. Vzhledem k aktuální situaci bylo vytvořeno několik otázek, které byly zaslány e-mailem. Na tyto otázky jsem se expertů zeptal, protože mě zajímal pohled jejich očima. Jejich odpovědi jsem porovnal s výsledky dotazníkového šetření a následně odvodil závěr.

5.1.1 První rozhovor

1. **Zde poprosím pár vět o vás. (Jméno, postavení ve firmě a na co se především zaměřujete, jak dlouho pracujete v NUKIB atd.)**
   „Oddělení vzdělávání, více než 1 rok."
2. **Jaké jsou aktuálně největší hrozby virtuálního prostoru a proč?**
   „Nevzdělaní a nepoučení uživatelé."
3. **Myslíte si, že obyvatelé ČR znají NUKIB?**
   „Omezeně."
4. **Je běžný uživatel počítače, bez větších znalostí internetu, schopen rozeznat dané hrozby?**
   „Ano po základním poučení."
5. **Používáte sociální sítě, popřípadě jaké?**
   „Ano. FCB, INST, LINKEDIN."
6. **Co je největším problémem těchto sociálních sítí?**
   „Selektivní předkládání informací."
7. **Stal jste se vy sám, nebo někdo z vašeho okolí někdy obětí kybernetické kriminality, popřípadě jaké?**
   „Ne, nejsem si vědom."
8. **Myslíte si, že jsou uživatelé ochotni učit se a poznávat hrozby které jim hrozí a následně umět na ně reagovat?**
   „Ano."
9. **Pokud se chci učit odolávat hrozbám internetu, kde tak mohu učinit?**
   „Na osveta.nukib.cz (kurz Dávej kyber!). U neziskových a soukromých organizací zabývající se osvětou v KB."
10. **Co by měl běžný uživatel znát, než vstoupí do virtuálního prostoru?**
    „Základní zásady pro bezpečné užívání. Hesla, přílohy, připojování wi-fi, phishing atd."

11. **Pokud se uživatelé stanou obětí této hrozby (souvisí s otázkou číslo 10), na koho nebo kam se mají obrátit?**

    „V případě podezření ze spáchání trestného činu na PČR. V ostatních případech na oborníky KB v jejich organizaci apod.“

12. **Jak se mohu nejlépe chránit před hrozbami?**

    „Dodržováním základních zásad bezpečného pohybu na internetu, které jsou vyučovány například na osveta.nukib.cz (kurz Dávej Kyber!).“

5.1.2 Druhý rozhovor

1. **Zde poprosím pár vět o vás. (Např: jméno, postavení ve firmě a na co se především zaměřujete, jak dlouho pracujete v NUKIB atd.)**

    „Pracuji na oddělení vzdělávání jako referent bezpečnosti státu. Na NÚKIB pracuji od roku 2014, tj. již více než 7 let. Za tu dobu jsem prošel více pracovních pozic, ale po celou dobu se věnuji vzdělávání uživatelů z řad státní správy a veřejnosti v kybernetické bezpečnosti.“

2. **Proč jste se rozhodl pracovat v tomto oboru?**

    „Protože mě baví tato neustále se rozšiřující oblast a uvědomuji si, že odborníky, běžné uživatele i veřejnost je potřeba v tomto směru neustále vzdělávat, abychom alespoň částečně dokázali předcházet případným problémům a incidentům. Aktuálnost daného tématu je tím větší čím více se využívání ICT stává součástí každodenního soukromého i pracovního života.“

3. **Jaké jsou aktuálně největší hrozby virtuálního prostoru a proč?**

    „Na tuto otázku nemám potřebné statistické údaje. V tomto případě je lepší obrátit se na Vládní CERT. Každopádně je potřeba zvážit to, že i sebedokonalejší a sebebezpečnější technologie selže, pokud ji špatně použije uživatel. Z mého úhlu pohledu je nepoučený uživatel velice významnou hrozbou.“

4. **Myslíte si, že obyvatelé ČR znají NUKIB?**

    „Z mého úhlu pohledu se povědomí o NÚKIB za posledních několik let rozšířilo. V odborné komunitě je NÚKIB velmi dobře znám jak u nás, tak i ve světě, a to i díky tomu, že se pravidelně účastníme různých kybernetických cvičení, kde pravidelně zaujímáme jako Česká republika přední příčky.“

5. **Je běžný uživatel počítače, bez větších znalostí internetu, schopen rozeznat dané hrozby?**

„Uživatelé jsou za mě jistě schopni některé hrozby rozeznat a odolat jim. Mnohdy stačí řídit se základními zdravými návyky, kterými se řídíme i v reálném světě – například to, že zamykáme byt, když odcházíme pryč, přecházíme na zelenou nebo zavoláme pomoc, když vidíme někoho v ohrožení. Ovšem vzhledem k tomu, že se kybernetické hrozby neustále vyvíjejí, tak je z mého úhlu pohledu nutné uživatele neustále vzdělávat, aby hrozby rozpoznali a dokázali jim předcházet a případně i spolupracovat na jejich řešení."

6. **Používáte sociální sítě, popřípadě jaké?**

   „Facebook, Spotify, WhatsApp, LinkedIn."

7. **Co je největším problémem těchto sociálních sítí?**

   „Špatné dodržování zdravých návyků pro bezpečnou komunikaci a stále více se rozšiřující podvodné jednání například na prodejních skupinách nebo bazárku. S tím se setkávám poslední dobou stále více."

8. **Stal jste se vy sám, nebo někdo z vašeho okolí někdy obětí kybernetické kriminality, popřípadě jaké?**

   „Přímou zkušenost nemám. Pouze na mě několikrát na prodejní skupině zkusili vymámit peníze za zboží, které jako by prodávali, ale přitom ho neměli. Dávali ho samozřejmě za „velmi dobrou cenu". Jednou na mě zkusili i podvod s tím, že když jsem prodávala kolo, tak pro něj chtěl pán poslat zásilkovou službu. To už jsem zbystřil, protože byl ze stejného města jako já. Poslal mi podvodný odkaz na zaplacení, kde jsem měl přidat poplatek za odeslání zboží, který by mi pak následně vrátil ve formě navýšení částky, kterou mi chtěl zaplatit za kolo. Když jsem jej konfrontoval, již se neozval."

9. **Myslíte si, že jsou uživatelé ochotni učit se a poznávat hrozby které jim hrozí a následně umět na ně reagovat?**

   „Pokud jim ukážeme, jak se to dělá, tak ano. Jak jsem psal výš, mnohdy stačí osvojit si a dodržovat zdravé návyky z reálného světa a dá se předejít spoustě problémům."

10. **Pokud se chci učit odolávat hrozbám internetu, kde tak mohu učinit?**

    „Osvojením zdravých návyků a jejich dodržování stejně jako v reálném světě. Dále pak stačí si jednou za čas projít nějaký online kurz jako je třeba ten od nás."

11. **Co by měl běžný uživatel znát, než vstoupí do virtuálního prostoru?**

    „Zdravé návyky chování z reálného světa a své přihlašovací údaje."

12. **Jaká hrozba je na internetu nejčastější?**

„Na tuto otázku nemám potřebná data. Opět lepší odkázat na Vládní CERT, ale i zde platí to o nepoučeném uživateli.“

13. **Pokud se uživatelé stanou obětí této hrozby (souvisí s otázkou číslo 10), na koho nebo kam se mají obrátit?**

    „Zde záleží, zda se tak stanou ve svém pracovním nebo soukromém čase. Pokud v pracovním, tak je nejlepší obrátit se na někoho, kdo u nich řeší problémy s ICT a hrozby. Pokud se to dotýká jejich soukromého života, tak je za mě nejlepší se obrátit na PČR případně na další instituce, které jsou k tomu určené. Je ale nutné zde brát v potaz také věk uživatelů a případnou újmu, která z incidentu, tedy hrozby, kterou již někdo využil, vznikla.“

14. **Jak se mohu nejlépe chránit před hrozbami?**

    „Dodržováním bezpečnostních pravidel a vzděláváním.“

15. **Co byste doporučil uživatelům, aby se nestali oběťmi hrozeb?**

    „Poslouchejte svoji vnitřní intuici. Dodržujte základní bezpečnostní doporučení a zdravé návyky chování jako z reálného světa.“

Závěr

Bakalářská práce je rozdělena na teoretickou a praktickou část. V teoretické části bakalářské práce je představena historie a vývoj počítačů, a základní pojmy, které s počítači souvisí. Následně po objasnění vývoje jsou představeny hrozby, které ohrožují každého uživatele koncových zařízení. V mé bakalářské práci jsou uvedeny základní hrozby internetu, které by měl znát každý. Po uvedení základní hrozeb jsou uvedeny preventivní programy, ve kterých se může uživatel vzdělávat. Vzdělávání není radno podceňovat, protože pokud uživatel neví, jak hrozba vypadá, není schopen ji poznat a adekvátně na ni reagovat.

Praktická část bakalářské práce byla kombinací dotazníkového šetření a rozhovoru. Pokud šlo o dotazníkové šetření, bylo v něm 23 otázek, na které odpovědělo 400 respondentů, kteří byli odfiltrováni na konečných 369 smysluplných odpovědí. V dotazníkovém šetření byla otázka „Poslal/a jste někdy intimní fotografii?“. Předpokládal jsem, že nejvíce kladných odpovědí bude u žen nad 18 let. Tato myšlenka byla potvrzena, ale nejvíce mě překvapilo číslo u dívek do 15 let. Zde byly 4 kladné odpovědi. Ačkoliv si myslím, že pedagogové ze základních škol či rodiče stále dětem opakují, že takovéto fotografie nemají pořizovat a už vůbec ne posílat, dívky to stále dělají. Právě dívky do 15 let jsou nejvíce ohroženy hrozbou sexuálního predátorství. Tuto hrozbu nejlépe vystihuje dokument „V síti“. Myslím že, tento dokument by měl být pouštěn všem dětem na základních školách, než vstoupí do prostředí sociálních sítí, protože právě problém dětské pornografie je to, co může dívky pronásledovat do konce života nebo jejich život může skončit tragicky.

Dále bylo úkolem praktické části zjistit, jestli jsou uživatelé schopni poznat hrozbu virtuálního prostředí. V dotazníkovém šetření znali uživatelé poměrně dobře různé hrozby. Nejvíce známými hrozbami byla kyberšikana, virus, spam, sexuální predátorství a sexting. Tyto pojmy zná minimálně 75 % dotázaných a jsou schopni je poznat. Méně známými hrozbami byl phishing, ransomware, Dos útok, kybergrooming a sniffing. Přitom phishing a ransomware jsou schopny připravit uživatele o poměrně velké množství peněz. Poté měli respondenti za úkol poznat podle fotografie, zda se jedná o hrozbu a jak by na ni zareagovali. Až na pár výjimek uživatelé hrozbu rozpoznali správně a též správně reagovali. Lidé, kteří již prošli nějakým školení či se nějak vzdělávali před hrozbami znali celkově více hrozeb a uměli lépe reagovat na dva příklady vzorové hrozby. Jak uvádějí ve svých odpovědích experti z NÚKIB: Největší hrozbou virtuálního prostředí je sám pro sebe nepoučený uživatel. Praktickou částí bylo tedy

zjištěno, že uživatelé jsou schopni poznat hrozby. Pokud chtějí ale být ve virtuálním prostředí v úplném bezpečí, je potřeba se stále vzdělávat a poučovat o nových hrozbách. Podle dotazníku má zájem o pravidelné informace o nových hrozbách 65 % respondentů. Dle mého názoru by zájem měl být větší.

Na základě rozhovorů s experty z NÚKIB bych uživatelům doporučil, aby dodržovali základní bezpečnostní doporučení a zdravé návyky z reálného světa, protože dnes se náš reálný život z velké části odehrává v tom virtuálním. Dále je důležitá vysoká obezřetnost vůči všemu, co se na internetu objeví. Každá zpráva může být hrozbou. Pro svojí osobní bezpečnost je důležité používat silná hesla, které kombinujeme nejlépe s dvoufázovým ověřením a antivirusem. Uživatel by se také měl v této problematice vzdělávat. Každým dnem hrozby vypadají jinak a jsou více přesvědčující. Sami experti říkají, že největším problémem jsou uživatelé sami pro sebe, pokud nejsou obeznámeni s tím, co jim hrozí. Možností vzdělávání je mnoho. Uživatelům bych doporučil internetové videokurzy, které je možnost najít zde: https://www.e-bezpeci.cz/videokurzy/. Další možností vzdělání v této problematice jsou určitě tyto internetové stránky: osveta.nukib.cz nebo http://www.bezpecnyinternet.cz. Rozhodně doporučuji nepodcenit vzdělávání, protože pokud nevíme co a jak nás může ohrozit, tak můžeme velice snadno naletět podvodníkům.

Vím, že je dnes velice těžká orientace ve virtuálním prostředí. Myslím si ale, že se této problematice řada odborníků pečlivě věnuje a snaží se uživatele dostatečně poučit. Následně je to už pouze na uživatelích, zdali si budou dávat pozor a uposlechnou doporučení, která jim byla předána.

Seznam použitých zdrojů

Literární zdroje

1. ANONYMOUS. *Maximální bezpečnost*. 4. vyd. Praha: Softpress, c2004, s. 440. ISBN 80-86497-65-8.
2. ČAPEK, J., HUB, M., ROUDNÝ, R., KOPÁČKOVÁ, H., FUKA, J., IBL, M. *Vybrané aspekty kybernetické bezpečnosti*. Pardubice: Univerzita Pardubice, 2015, s. 85. ISBN 978-80-7395-953-1.
3. DONÁT, J., TOMÍŠEK, J. *Právo v síti: průvodce právem na internetu*. V Praze: C.H. Beck, 2016, s. 338. ISBN 978-80-7400-610-4.
4. FEREBAUEROVÁ, R., PEKÁREK, O. *Aplikovaná informatika*. České Budějovice: Vysoká škola evropských a regionálních studií, 2014, s.151. ISBN 978-80-87472-74-3.
5. HAUBEN, M. *Historie sítě ARPANET/Internet*. 2003, s. 33. ISBN 999-00-000-7834-9.
6. JANSA, L., OTEVŘEL, P., ČERMÁK, J., Petr MALIŠ, P, HOSTAŠ, P., Michal MATĚJKA, M., MATEJKA, J. *Internetové právo*. Brno: Computer Press, 2016, s. 432. ISBN 978-80-251-4664-4.
7. JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013, s. 200. ISBN 978-80-7251-397-0.
8. KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016, s. 522. CZ.NIC. ISBN 978-80-88168-15-7.
9. KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CYBERSECURITY*. Praha: CZ.NIC, z. s. p. o., 2019, s. 562. ISBN 978-80-88168-34-8.
10. KOPECKÝ, Kamil. *Rizika internetové komunikace v teorii a praxi*. Olomouc: Univerzita Palackého v Olomouci, 2013, s. 188. ISBN 978-80-244-3571-8.
11. KRÁL, Mojmír. *Bezpečný internet: chraňte sebe i svůj počítač*. Praha: Grada Publishing, 2015, s. 183. Průvodce (Grada). ISBN 978-80-247-5453-6.
12. KREMLING, J., PARKER, M. Sharp A. *Cyberspace, cybersecurity, and cybercrime*. Los Angeles: London, 2018, s. 497. ISBN 9781506347257.
13. MCCARTHY, L., WELDON-SIVIY, D., ed. *Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online*. Praha: CZ.NIC, 2013, s. 318. ISBN 978-80-904248-6-9.

14. PANDE, J. *Introduction to Cyber Security*. Haldwani: Uttarakhand Open University, 2017, s. 151. ISBN 978-93-84813-96-3.
15. PORADA, V., KONRÁD, Z. *Metodika vyšetřování softwarového pirátství*. Praha: Policejní akademie České republiky, 1999, s. 54. ISBN 80-7251-024-x.
16. POŽÁR, J. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005, s. 311. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-86898-38-5.
17. VANĚK, J., NOVÁK, J., KALIKA, D. *Jak na Internet bezpečně*. Ilustroval Aneta BISKUPOVÁ. Praha: CZ.NIC, z.s.p.o., 2018, s. 106. CZ.NIC. ISBN 978-80-88168-29-4.
18. ZAVRŠNIK, A. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017, s. 135. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7552-758-5.
19. ZELENÝ, J., MANNOVÁ B. *Historie výpočetní techniky*. Praha: Scientia, 2006, s. 183. Stručné dějiny oborů. ISBN 80-86960-04-8.

Elektronické zdroje

1. Rok 2020 přinesl kromě pandemie koronaviru i více kybernetických útoků na nemocnice | mobilenet.cz. *mobilenet.cz – Mobilní telefony, notebooky a technologie budoucnosti* [online]. Copyright © 2021 24net s.r.o. Všechna práva vyhrazena. [cit. 09.11.2021]. Dostupné z: <https://mobilenet.cz/clanky/rok-2020-prinesl-krome-pandemie-koronaviru-i-vice-kybernetickych-utoku-na-nemocnice-43079>.
2. Národní úřad pro kybernetickou a informační bezpečnost - O úřadu. *Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka* [online]. Dostupné z: <https://www.nukib.cz/cs/o-nukib/o-uradu/>.
3. Zpráva o stavu kybernetické bezpečnosti ČR – 2017. Národní úřad pro kybernetickou a informační bezpečnost – Zprávy o stavu KB <httpy://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/>. [online] [cit. 09.11.2021]
4. Informační společnost v číslech-2021 [online]. Praha: Český statistický úřad, 2021 [cit. 2021-12-21]. Dostupné z: <https://www.czso.cz/csu/czso/informacni-spolecnost-v-cislech-2021>.

5. Historie výpočetní techniky 1941–1950. *Historie počítačů v Československu 1950–1975* [online]. Copyright © 2005 [cit. 11.11.2021]. Dostupné z: <https://historiepocitacu.cz/1941-1950.html>.
6. Co je to ransomware a jak se proti němu bránit? | ESET. *Malware Protection & Internet Security | ESET* [online]. Copyright © 1992 [cit. 05.01.2022]. Dostupné z: <https://www.eset.com/cz/ransomware/>.
7. What is Malware and How to Protect Against It? | Kaspersky. *Kaspersky Cyber Security Solutions for Home & Business | Kaspersky* [online]. Copyright © [cit. 27.01.2022]. Dostupné z: <https://usa.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it>.
8. Zákeřný virus I love you napadl před 20 lety desítky milionů počítačů - Novinky.cz. *Novinky.cz – nejčtenější zprávy na českém internetu* [online]. Copyright © 2003 [cit. 28.01.2022]. Dostupné z: <https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/zakerny-virus-i-love-you-napadl-pred-20-lety-desitky-milionu-pocitacu-40322758>.
9. Kybergrooming - INTERNETEM BEZPEČNĚ. *INTERNETEM BEZPEČNĚ - Užívejme internet bezpečnějším způsobem* [online]. Copyright © 2018 INTERNETEM BEZPEČNĚ. Všechna práva vyhrazena. [cit. 03.02.2022]. Dostupné z: <https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybergrooming/>
10. Sexting.cz - vse, co chcete vedet o sextingu. *Sexting.cz - vse, co chcete vedet o sextingu* [online]. Dostupné z: <http://www.sexting.cz>
11. Informace o projektu - E-Bezpečí. *Projekt E-bezpečí - E-Bezpečí* [online]. Dostupné z: <https://www.e-bezpeci.cz/index.php/o-projektu/oprojektu>.

Legislativní dokumenty

1. ČESKO (ČESKOSLOVENSKO). Zákon č. 550 České národní rady ze dne 6. prosince 1991 o všeobecném zdravotním pojištění. In *Sbírka zákonů České a Slovenské federativní republiky*. 1991, částka 104, s. 2722-2727. Dostupné z WWW: <http://aplikace.mvcr.cz/archiv2008/sbirka/1991/sb104-91.pdf>. ISSN 1210-0005.
2. Zákon č. 127/2005 Sb., o elektronických komunikacích. *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Copyright © AION CS, s.r.o. 2010 [cit. 09.11.2021]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2005-127>.

3. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti. *Zákony pro lidi – Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Copyright © AION CS, s.r.o. 2010 [cit. 09.11.2021]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2014-181>.
4. Zákon č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákon.... *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Copyright © AION CS, s.r.o. 2010 [cit. 09.11.2021]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2017-205>.
5. 40/2009 Sb. Trestní zákoník. *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Copyright © AION CS, s.r.o. 2010 [cit. 31.03.2022]. Dostupné z:<https://www.zakonyprolidi.cz/cs/2009-40>

Ostatní zdroje

Kromě výše uvedených zdrojů byly při zpracování bakalářské práce využity následující materiály:

- <https://www.fi.muni.cz/usr/jkucera/pv109/xsmysit.html>.

Seznam zkratek

SSSR	-	Sovětský svaz
USA	-	Spojené státy americké
ARPA	-	Advanced Research Project Agency
UCLA	-	University of California Los Angeles
UCSB	-	University of California Santa Barbara
SRI	-	Stanford Research Institute
NÚKIB	-	Národní úřad pro kybernetickou a informační bezpečnost
GUI	-	Grafické Uživatelské Rozhraní
ROM	-	Read Only Memory
DoS	-	Denial of Services
DDoS	-	Distributed Denial of Services

Seznam tabulek a grafů

Přílohy

Dotazník Kybernetická bezpečnost.

1. Jakého jste pohlaví?

- ☐ Muž
- ☐ Žena

2. V jaké věkové kategorii se nacházíte?

- ☐ 6-15
- ☐ 16-20
- ☐ 21-40
- ☐ 41–60
- ☐ 61 a více

3. Jaké je vaše vzdělání?

- ☐ Základní
- ☐ Středoškolské s maturitou
- ☐ Středoškolské s výučním listem
- ☐ Vysokoškolské

4. Z hlediska používání PC jste:

- ☐ Začátečník
- ☐ Běžný uživatel
- ☐ Pokročilý
- ☐ Specialista

5. Jaké pojmy znáte?

- ☐ Kybernetická bezpečnost
- ☐ Kybernetická hrozba
- ☐ Kybernetická kriminalita
- ☐ Neznám žádný

6. Myslíte, že by každý, kdo používá počítač měl znát nástrahy virtuálního prostředí?

Povinná otázka, respondant musel zvolit jednu z nabízených odpovědí a podle toho se mu zobrazily další otázky [Souhlasím, Spíše souhlasím, Nevím – otázka č. 8; Spíše nesouhlasím , Nesouhlasím – otázka č. 7].

- ☐ Souhlasím
- ☐ Spíše souhlasím
- ☐ Nevím
- ☐ Spíše nesouhlasím
- ☐ nesouhlasím

7. Proč myslíte, že není potřeba znát nástrahy?

8. Jaké hrozby virtuálního prostředí (internetu) znáte? Zvolit můžete více odpovědí.

☐ DoS,DDos útok ☐ Kybergrooming ☐ Kyberšikana ☐ Phishing ☐ Ransomware
☐ Sexting ☐ Sexuální predátorství ☐ Sniffing ☐ Spam ☐ Virus, Červ

9. Máte osobní zkušenost s kybernetickou kriminalitou?

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí a podle toho se mu zobrazily další otázky [Ano – otázka č. 10, Nevím, Ne – otázka č. 11].

☐ Ano ☐ Ne ☐ Nevím

11. Poslal/a jste nebo zveřejnil/a někdy svou intimní fotografii?

☐ Ano ☐ Ne

12. Používáte sociální sítě?

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí a podle toho se mu zobrazily další otázky [Ano – otázka č. 13, Ne – otázka č. 14].

☐ Ano ☐ Ne

13. Jaké sociální sítě používáte? Vybrat můžete více odpovědí.

☐ Facebook ☐ Instagram ☐ Skype ☐ Snapchat ☐ TikTok ☐ Twitter
☐ WhatssApp ☐ YouTube ☐ ICQ ☐ Lide.cz

14. Používáte ochranu proti kybernetickým hrozbám?

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí a podle toho se mu zobrazily další otázky [Ano – otázka č. 15, Ne – otázka č. 16].

☐ Ano ☐ Ne

15. Jakou ochranu svého zařízení používáte?

☐ Antivirus placený ☐ Antivirus Zdarma ☐ Hesla ☐ VPN

☐ Jiné zabezpečení: _____

16. Do emailu vám přišla tato zpráva, co uděláte?

☐ Nebudu platit nic, email ignoruji.

☐ Zaplatím požadovanou částku, z důvodu možné pokuty pošty

☐ Jiné řešení: _____

17. Od uživatele ve vašem seznamu přátel vám přijde tato zpráva, jak budete reagovat?

- ☐ Kód v žádném případě neposílám
- ☐ Obdržený kód zašlu, mám ho v přátelích, nemůže se nic stát.
- ☐ Jiné řešení: _____

18. Jaký druh internetové kriminality je podle vás nejvíce nebezpečný?

- ☐ Dětská pornografie, Sexuální predátorství
- ☐ Hacking (Neoprávněný přístup do počítače.
- ☐ Kyberšikana
- ☐ Podvodné jednání
- ☐ Stalking (Nebezpečné pronásledování)
- ☐ Jiná: _____

20. Myslíte si, že zvládnete rozpoznat hrozbu na internetu?

☐ ano ☐ nevím ☐ ne

21. Měl by se Stát více věnovat prevenci v oblasti kybernetické kriminality?

☐ ano ☐ ne

22. Seznámil/a jste se někdy ve škole, zaměstnání, informačním letáku či kurzu o doposud známých kybernetických hrozbách?

☐ ano ☐ ne

23. Měl/a byste zájem získávat pravidelné informace o nových hrozbách v internetu a možných způsobech ochrany?

☐ ano ☐ ne