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

BAKALÁŘSKÁ PRÁCE

Informovanost studentů Střední průmyslové školy a Vyšší odborné školy v Příbrami o problematice kybernetické kriminality

Autor práce: David Klemš

Studijní obor: Bezpečnostně právní činnost ve veřejné správě

Forma studia: Kombinovaná

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: David Klemš
Studijní program: Bezpečnostně právní činnost
Studijní obor: Bezpečnostně právní činnost ve veřejné správě
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Informovanost studentů Střední průmyslové školy a Vyšší *odborné školy v Příbrami o problematice kybernetické kriminality*

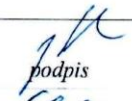
Název bakalářské práce v anglickém jazyce: Awareness of Students of the Secondary Industrial School in Příbram about the Issue of Cybercrime

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, titul): RNDr. Růžena Ferebauerová,
Datum zadání bakalářské práce (měsíc, rok): listopad 2021

Cíl bakalářské práce:
Hlavním cílem práce je zjistit, jaké mají studenti zkušenosti s kyberkriminalitou, jak je vnímána, zda vědí, jak problémy řešit popřípadě jim předejít.
Vedlejším cílem je analyzovat současný stav a trendy vývoje kyberkriminality, včetně ochrany před ní.

Student: David Klemš	5.12.21 *datum*	 *podpis*
Vedoucí práce: RNDr. Růžena Ferebauerová	5.12.21 *datum*	 *podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	24.1.2022 *datum*	 *podpis*
Prorektorka pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	26.1.2022 *datum*	 *podpis*
Pověřený rektor: doc. Ing. Jiří Dušek, Ph.D.	31.1.2022 *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 (ho) a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

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

ABSTRAKT

KLEMŠ, D. *Informovanost studentů Střední průmyslové školy a Vyšší odborné školy v Příbrami o problematice kybernetické kriminality: bakalářská práce*. Příbram: Vysoká škola evropských a regionálních studií, 2022. 76 s. Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová.

Klíčová slova: kyberkriminalita, kybernetický útok, kyberprostor

V bakalářské práci se autor zabývá základními pojmy, jako jsou kyberkriminalita, kyberprostor, kybernetický útok, počítačové sítě, dále legislativou, formy útoků a obranou a prevencí proti síťovým útokům.

Bakalářská práce je rozdělena do dvou částí. První část práce má 4 kapitoly a je zaměřena teoreticky. Druhá část bakalářské práce je zaměřena prakticky pomocí dotazníkového šetření u studentů střední průmyslové školy v Příbrami.

V praktické části práce se autor snaží zjistit, jaké mají studenti zkušenosti s kyberkriminalitou, jak je vnímána, zda vědí, jak problémy řešit popřípadě jim předejít na základě provedeného dotazníkového šetření.

ABSTRACT

KLEMŠ, D. *Awareness of Students of the Secondary Industrial School in Příbram about the Issue of Cybercrime: Bachelor thesis.* Příbram: The College of European and Regional Studies, 2022. 76 pages Supervisor: RNDr. Růžena Ferebauerová.

Keywords: cybercrime, cyber attack, cyberspace

In the bachelor's thesis, the author deals with basic concepts such as cybercrime, cyberspace, cyber attack, computer networks, legislation, forms of attacks and defense and prevention against network attacks.

The bachelor thesis is divided into two parts. The first part of the thesis has 4 chapters and is focused on theory. The second part of the bachelor's thesis is focused on practically using a questionnaire survey of students at a secondary industrial school in Příbram.

In the practical part of the work, the author tries to find out what students have experience with cybercrime, how it is perceived, whether they know how to solve problems or prevent them on the basis of a questionnaire surve

Obsah

Úvod 10

1 Cíl a metodika 11

2 Základní pojmy 12

2.1 Kyberkriminalita 12

2.2 Kyberprostor 14

2.2.1 Surface web 16

2.2.2 Deep web 16

2.2.3 Dark web 16

2.3 Kybernetický útok 17

2.4 Počítačové sítě 18

2.4.1 Dělení podle rozlohy 18

2.4.2 Dělení podle postavení síťových uzlů. 20

2.4.3 ISO/OSI model 21

2.4.4 TCP/IP model 23

2.4.5 IP ADRESA ' 24

3 Legislativa 26

3.1 Legislativní vývoj 26

3.2 Právní normy v ČR 30

3.3 Zákon o kybernetické bezpečnosti 32

4 Formy útoků 34

4.1 Malware 34

4.1.1 Adware 34

4.1.2 Spyware 34

4.1.3 Viry 35

4.1.4 Červi (Worms) 35

4.1.5 Trojské koně 35
4.1.6 Ransomware 36
4.2 Sociální inženýrství 36
4.3 Phishing 37
4.4 Podvodné webové stránky 37
4.5 Hacking 37
4.6 Cracking 38
4.7 Spam 38
4.8 Hoax 38
4.9 DoS, DDoS 38
5 Obrana a prevence proti síťovým útokům 40
5.1 Bezpečnostní protiopatření 40
5.1.1 Personální politika 40
5.1.2 Fyzická a technická ochrana 40
5.1.3 Záložní zdroje energie 40
5.1.4 Technická ochrana proti úmyslným útokům z Internetu 40
5.1.5 Kryptografická ochrana 40
5.1.6 Monitoring a bezpečnostní audit 41
5.1.7 Havarijní plán a plán obnovy funkčnosti 41
5.1.8 Pravidla a směrnice 41
5.1.9 Proškolování 41
5.2 Rozdělení sítě 41
5.2.1 Demilitarizované zóny 41
5.2.2 Virtuální LAN 42
5.3 IDS 42
5.4 IPS 42
5.5 Firewally 42

5.6 Antivirové programy 42
5.7 VPN 43
5.8 IPsec 43
5.9 Obecná doporučení 43
6 Empirické šetření 45
6.1 Příprava dotazníku a jeho realizace 45
6.1.1 Struktura dotazníkového šetření 45
6.1.2 Cíle a hypotézy výzkumu 46
6.2 Interpretace výsledků dotazníku 47
6.2.1 Výsledky hypotéz 58
Závěr 59
Literární zdroje 62
Elektronické zdroje 63
Legislativní dokumenty 65
Seznam zkratek 69
Seznam obrázků 71
Seznam grafů 71
Seznam příloh 72
Příloha č. I. – Formulář dotazníkového šetření 73

Úvod

Informační a komunikační technologie je jedno z nejrychleji a nejdynamičtěji se rozvíjejících odvětví. Dnes je téměř nepředstavitelný život bez nich, ještě před patnácti či dvaceti lety by nemožnost připojení se k Internetu a dalším ICT službám znamenala pouze to, že bychom šli dělat jinou práci, nebo se věnovali něčemu jinému. V současné době je otázkou, co bychom mohli dělat? Nebyli bychom schopni si najít užitečné informace na Internetu, nikomu bychom se nedovolali, začaly by problémy se službami, které ke své funkci informační a komunikační technologie potřebují např. telekomunikační služby, zdravotní péče, zajištění bezpečnosti občanů a státu, finanční transakce, přístup k informacím aj. Informační a komunikační technologie nemají pouze pozitivní vliv na společnost, mají spoustu negativních stránek, které v posledních letech s sebou přinášejí nová společensky škodlivá jednání, proto je kyberkriminalitě potřeba věnovat stále větší pozornost.

Toto téma bakalářské práce jsem si vybral, protože pracuji jako bezpečnostní správce informačních a komunikačních systémů. Zde se potkávám s různými formami útoků a kyberkriminalitou obecně. O tuto problematiku se zajímám už od střední školy a nyní prohlubuji své znalosti na různých seminářích a kurzech.

Bakalářská práce je rozdělena na dvě části, první část je zaměřena na teorii související s kyberkriminalitou a druhá část je zaměřena prakticky pomocí dotazníkového šetření u studentů střední průmyslové školy v Příbrami. V teoretické části budou vysvětleny pojmy jako kyberkriminalita, kyberprostor, kybernetický útok. Zároveň autor objasní právní výklad týkající se kyberkriminality, nejčastější formy útoků, obranu a možná preventivní opatření proti síťovým útokům. Praktická část bakalářské práce se zaměřuje na výzkum, pomocí dotazníkové šetření, který by měl zmapovat, jaké mají studenti zkušenosti s kyberkriminalitou, jak je kyberkriminalita vnímána a zda studenti vědí, jak problémy řešit popřípadě jim předejít.

1 Cíl a metodika

Hlavním cílem práce je zjistit, jaké mají studenti zkušenosti s kyberkriminalitou, jak je vnímána, zda vědí, jak problémy řešit popřípadě jim předejít. Vedlejším cílem je analyzovat současný stav a trendy vývoje kyberkriminality, včetně ochrany před ní.

Jedná se o práci praktickou, kdy bude využita kvantitativní strategie za využití metody dotazování a techniky dotazníku.

Hlavního cíle, tedy především zjistit, jaké mají studenti zkušenosti s kyberkriminalitou, jak je vnímána, zda vědí, jak problémy řešit popřípadě jim předejít, bude dosaženo analýzou dat získaných z dotazníkového šeření. Vedlejšího cíle bude dosaženo analýzou odborné literatury a analýzou právních předpisů.

Bakalářská práce je rozdělena do dvou částí. První část práce má 4 kapitoly a je zaměřena teoreticky. Druhá část bakalářské práce je zaměřena prakticky a bude zpracována pomocí kvantitativní, tj. dotazníkového šetření u studentů střední průmyslové školy v Příbrami.

V druhé kapitole budou vysvětleny základní pojmy, které mají napomoci k lepšímu porozumění. Především jde o kyberkriminalitu, kyberprostor, kybernetický útok a počítačové sítě.

Ve třetí kapitole bude představena legislativa. Především půjde o legislativní vývoj, právní normy v ČR a zákon o kybernetické bezpečnosti

Ve čtvrté kapitole budou vysvětleny nejčastější formy útoků. Především jde o malware, sociální inženýrství, phishing, podvodné webové stránky, hacking, cracking, spam, hoax a DoS/DDoS

V páté kapitole bude vysvětlena obrana a prevence proti síťovým útokům. Především jde o bezpečnostní protiopatření, rozdělení sítě, IDS, IPS, firewall, antivirové programy, VPN, IPsec a obecná doporučení.

V poslední, tedy v šesté kapitole budou na základě dotazníkového šetření podrobně znázorněny výsledky šetření pomocí grafů. V této kapitole budou stanoveny dvě hypotézy, které se po znázornění výsledků buď potvrdí, nebo vyvrátí.

V závěru bakalářské práce budou vyhodnoceny cíle bakalářské práce s možnými doporučeními.

2 Základní pojmy

2.1 Kyberkriminalita

Užíváni výpočetní techniky, informačních systémů a informačních technologií a jejich integrace do téměř všech odvětví lidské činnosti je pro dnešní dobu typické. Lze konstatovat, že nelze nalézt, anebo velmi obtížně oblast lidské činnosti, kde by se nevyužívala výpočetní technika. Tak jak roste využívání a rozvoj ICT, rostou i možnosti a četnost k jejich zneužívání k trestné činnosti

Pojem kyberkriminalita je těžko definovatelný, kvůli neustále se vyvíjejícím technologiím a s nimi i možnosti, které se dají páchat. Různí autoři a i různé právní normy si vykládají kyberkriminalitu odlišným způsobem.

Smejkal definoval kyberkriminalitu jako: „*je třeba chápat páchání trestné činnosti, v níž figuruje počítač jako souhrn hardwarového a softwarového vybavení data nevyjímaje, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět této trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako movité věci, nebo jako nástroje trestné činnosti.*“ [1]

Výše uvedená definice se vztahuje pouze na počítačové systémy.

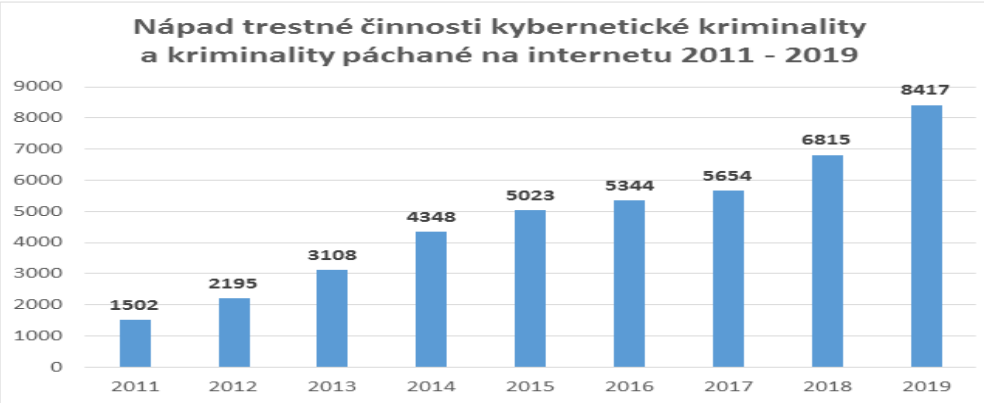
V dnešní době „Smart devices“ se může stát obětí kyberkriminality téměř každé zařízení, už nemusí být obětí pouze klasické PC, jako tomu bylo dřív. Dnes už je možné, aby se obětí stala například chytrá pračka nebo chytrá televize aj.[2]

Jirásek a spol. ve svém díle *Výkladový slovník kybernetické bezpečnosti* definovali kyberkriminalitu jako: „*Trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu té trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti.*“ [3]

[1] SMEJKAL, V., SOKOL, T., VLČEK, M. *Počítačové právo*. Praha, 1995, s. 99
[2] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 31 - 32.
[3] JIRASEK, P., NOVAK, L., POŽAR, J. *Výkladový slovník kybernetické bezpečnosti*. Praha, 2013, s. 57

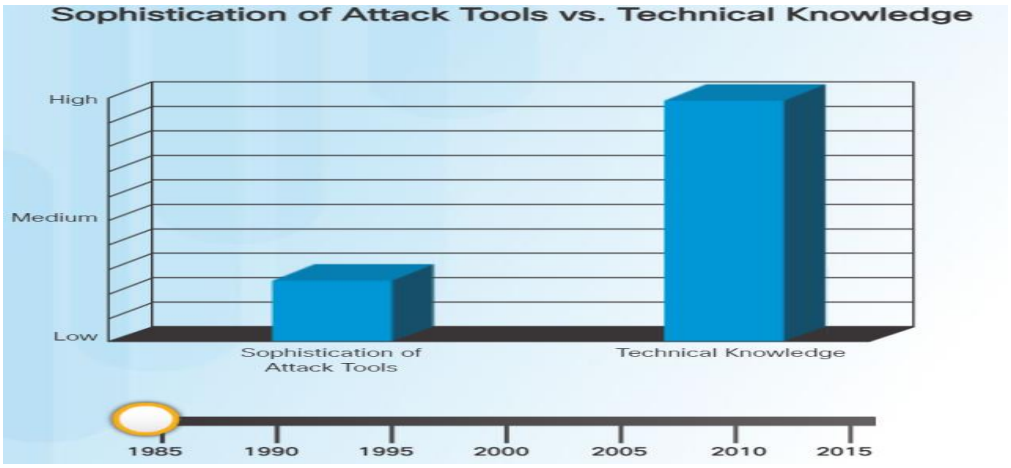
Nejobecněji lze definovat kyberkriminalitu jako: „*Veškerá trestná činnost, ke které dochází v prostředí informačních a komunikačních technologií.*“ [4]

Obrázek 1 Vývoj kybernetické kriminality mezi lety 2011-2019 [5]



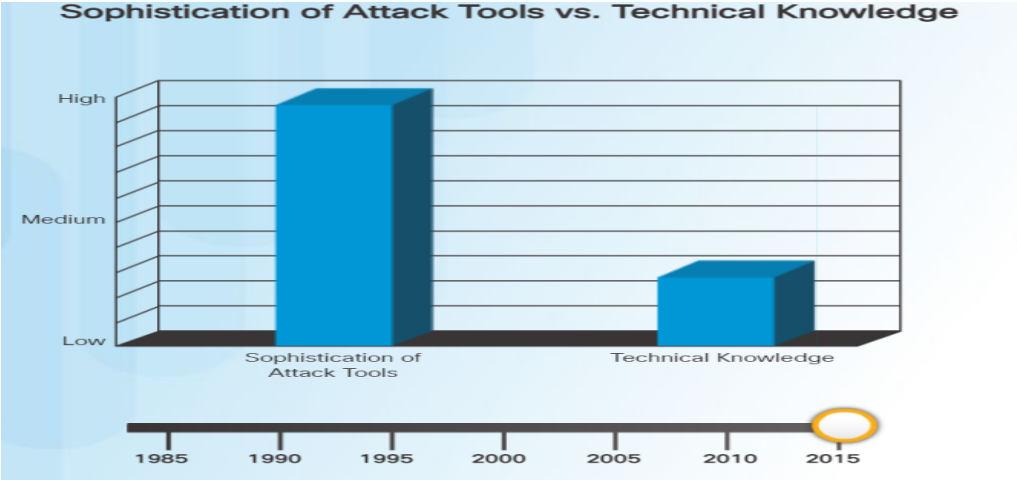
Výše uvedený graf znázorňuje vývoj kyberkriminality mezi lety 2011-2019 v ČR. Jak je z grafu zřejmé, kyberkriminalita roste, a proto je ji třeba věnovat stále vetší pozornost.

Obrázek 2 Sofistikovanost programů proti technickým znalostem uživatele [6]



[4] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity*. Praha, 2019, s. 83
[5] *Vývoj kybernetické kriminality a kriminality páchané na Internetu* [online]. 2021 [cit. 2022-13-01]. Dostupné z WWW: < https://www.policie.cz/clanek/kyberkriminalita.aspx >.
[6] *Interní materiály Cisco*

Obrázek 3 Sofistikovanost programů proti technickým znalostem uživatele [7]



Výše uvedené grafy znázorňují sofistikovanost programů a technické znalosti pachatelů (hackerů). Jak je možné vidět z grafu, v roce 1985 byly programy málo rozvinuté, ale znalost uživatelů musela být enormní, aby byly schopné obsluhovat tyto programy, v průběhu let se programy staly sofistikovanějšími a vysoce automatizovanými, což vyžaduje méně technických znalostí než v minulosti, což může způsobovat nárůst kyberkriminality.

2.2 Kyberprostor

Pojem kyberprostor byl poprvé použit v roce 1984 v románu *Neuromancer* od Williama Gibsona, ten definoval kyberprostor jako: *„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, …“* [8]

„Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts ... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non space of the mind, clusters and constellations of data. Like city lights, receding, …“ [9]

[7] *Interní materiály Cisco*
[8] KOLOUCH, J. *CyberCrime*, Praha, 2016, s. 42
[9] GIBSON, W. *Neuromancer*, New york, 1984, s. 37

Ačkoliv už uběhlo přes 30 let od prvního použití slova kyberprostor, stále nebyla vytvořena jednotná univerzální definice.

„Kyberprostor je tvořen prvky informačních a komunikačních technologií, které vytvářejí pomocí protokolu TCP/IP celosvětovou, globální počítačovou síť, a jednotlivými počítačovými systémy, které jsou do této sítě připojeny a které v ní interagují. Vlastní interakce uvedených systémů samozřejmě není možná bez zásahu jednotlivých uživatelů (administrátorů či koncových uživatelů). Tím je vytvořen dynamický, neustále se měnící a vyvíjející systém vázaný na hardware, avšak zároveň vytvářející těžko definovatelný a prakticky neomezený kyberprostor. Kyberprostor je virtuální realitou, nemající konec ani začátek. Tato virtuální realita je však zcela závislá na materiální podstatě, tedy technologiích nacházejících se ve světě reálném.“ [10]

Legislativa v České republice definuje kyberprostor jako: *„Kybernetickým prostorem je digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací“* [11]

Americké ministerstvo obrany definovalo ve své publikaci kyberprostor jako: „*A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers“* [12]

„Globální doména v rámci informačního prostředí skládající se ze vzájemně provázané sítě infrastruktur informačních technologií a údajích o obyvatelích, včetně Internetu, telekomunikačních sítí, počítačových systémů a vestavěných procesorů a řadičů“

Kyberprostor si lze představit jako ledovec, kde špička ledovce představuje prostor, ve kterém se běžní uživatelé pohybují, a ponořená část ledovce je nedostupná pro běžný webový prohlížeč.[13]

[10] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity*. Praha, 2019, s. 36
[11] ČESKO. Zákon č. 181/2014 Sb. § 2 písm. a, o kybernetické bezpečnosti a o změně souvisejících zákonů, In Sbírka zákonů, Česká republika. 2014, částka 2, s. 1
[12] DEPARTMENT OF DEFENSE U.S. ARMY, *Joint Publication 1-02. Dictionary of Military and Associated Terms*. 2016. s. 58
[13] KOLOUCH, J. *CyberCrime*. Praha, 2016. s. 46-47

Obrázek 4 Rozdělení kyberprostoru [14]

Tento pomyslný ledovec lze rozdělit na 3 části:

1. Surface web
2. Deep web
3. Dark web

2.2.1 Surface web

Je část kyberprostoru, která je volně dostupná a lze se v ní pohybovat za použití standardních prostředků (např. webových prohlížečů aj.). Tato část obsahuje služby (stránky), jako jsou např. Google, Facebook, YouTube, Seznam aj. Surface web spadá do správy ICANN a má jasně danou strukturu.[15]

2.2.2 Deep web

Je část kyberprostoru, která už není veřejně dostupná. Například intranet je využíván jako firemní nebo podniková počítačová síť (síť, která umožnuje komunikaci, přenos dat aj. pouze uvnitř daného podniku) ale data z ní nejsou veřejně dostupná. Tím částečně vzniká Deep web. [16]

2.2.3 Dark web

Je část kyberprostoru, která není veřejně dostupná a k její návštěvě je zapotřebí speciální prohlížeč. Jeden z nejznámějších prohlížečů je Tor nebo Freenet. síť Tor, umožňuje uživatelům Internetu přistupovat ke službám, aniž by prozrazovali údaje, jako je IP adresa. Síť Tor se sestává z tisíců uzlů rozmístěných po celém světě. Tyto uzly

[14] *Rozdělení kyberprostoru* [online]. 2018 [cit. 2022-04-01]. Dostupné z WWW: < https://hackernoon.com/wtf-is-dark-web-358569fde822 >
[15] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 47-48
[16] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 48

umožňují zasílat zprávy z různých IP adres, než která je klientovi aktuálně přidělena. Pokud se uživatel rozhodne přistupovat přes Tor do Internetu, pak nejdříve musí sestavit okruh vedoucí přes několik uzlů sítě. Informace od uživatele jsou předávány postupně mezi uzly sítě až k tzv. výstupnímu uzlu. Výstupní uzel vytvoří běžné spojení TCP k serveru umístěnému v Internetu. Odpovědi od serveru jsou předávány po stejné cestě zpět směrem k uživateli. Server na Internetu nevidí v požadavcích IP adresu uživatele, ale IP adresu výstupního uzlu sítě. Veškerá komunikace uvnitř sítě je šifrovaná a uzly uvnitř sítě neznají skutečný cíl komunikace, pouze vstupní uzel sítě Tor zná IP adresu uživatele. Cílem několikanásobného předávání zpráv je promíchání provozu všech uživatelů sítě. Promícháním provozu dává síť Tor každému z uživatelů možnost popření autorství dat, protože není jednoduše zjistitelné, kdo která data vytvořil.[17]

Pro řadu uživatelů představuje darknet hrozbu, kde se prodávají zbraně, drogy, dětská pornografie aj., ale pak je tady druhá část uživatelů, pro kterou darknet představuje neregulované a necenzurované prostředí.[18]

Jedním z nejznámějších tržišť s nelegálním obsahem byl Silk Road, které vzniklo v roce 2011 a v roce 2013 bylo uzavřeno FBI. Transakce probíhali pomocí Bitcoinů a na tržišti se dalo sehnat téměř vše, například drogy, kradený software, přihlašovací údaje, falešné pasy, kreditní karty, zbraně aj. Ještě ve stejném roce, kdy byl Silk Road zavřen vznikl Silk Road 2.0, který byl zavřen o rok později v roce 2014. Po zavření Silk Roadu 2.0 téměř okamžitě vznikly jiné tržiště s obdobným obsahem a většinou s lepším zabezpečením. [19]

2.3 Kybernetický útok

„Útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků.“ [20]

Výše uvedená definice neuvádí všechny negativní aktivity uživatelů kyberprostoru a navíc slučuje poškození a získání dat. Útočníkovi může jít například pouze o získání informací pomocí sociálního inženýrství.

[17] POLČÁK, L., *Základní informace o síti Tor*. [online]. Brno: VUT FIT, 2017. [cit. 2022-05-01]. Dostupné z WWW: < https://www.fit.vut.cz/research/publication-file/?id=11513&file=%2Fpub%2F11513%2Ftr.pdf >.
[18] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 48
[19] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 49-51
[20] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti*. Praha, 2013, *s. 59*

„Kybernetický útok lze definovat jako jednání útočníka či skupiny útočníků, které využívá informační a komunikační technologie k útoku na jinou informační a komunikační infrastrukturu, ať už s cílem narušit dostupnost, důvěrnost nebo integritu dat.“ [21]

Tato definice je mnohem obecnější a přesnější. Autor zde dává na výběr, že útočník může narušit jednu ze tří základních bodů triády CIA.

2.4 Počítačové sítě

Jirásek a spol. ve svém díle *Výkladový slovník kybernetické bezpečnosti* definovali počítačovou síť jako: *„Soubor počítačů spolu s komunikační infrastrukturou (komunikační linky, technické vybavení, programové vybavení a konfigurační údaje), jejímž prostřednictvím si (počítače) mohou vzájemně posílat a sdílet data.“* [22]

Rozdělení:

1. Dle rozlohy.
2. Dle postavení síťových uzlů.

2.4.1 Dělení podle rozlohy

PAN

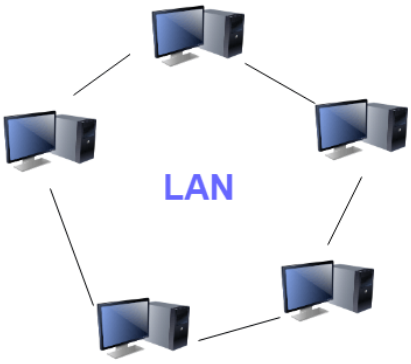
Personal Area Network neboli osobní síť. Je to velice malá síť, v okruhu několika metrů od zařízení používaná pro propojení osobních elektronických zařízení jako mobilní telefon, PDA, notebook příkladem je např. Bluetooth, ZigBee.

LAN

Local Area Network neboli lokální/místní síť. Pokrývá malé geografické území typicky uvnitř organizace, kampusu, ale také domácnosti, obvykle v okruhu 1 kilometru. Zařízení mohou být propojeny metalicky, opticky nebo bezdrátovými sítěmi. Nejjednodušším příkladem sítě LAN je propojení přes nějaký aktivní prvek (router, switch, AP) několika zařízení (PC, tiskárna, tablet aj.) v domácnosti.

[21] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity*. Praha, 2019, s. 83
[22] JIRÁSEK, P., NOVÁK, L., POŽÁR J. *Výkladový slovník kybernetické bezpečnosti*. Praha, 2013, *s. 73*

Obrázek 5 LAN [23]



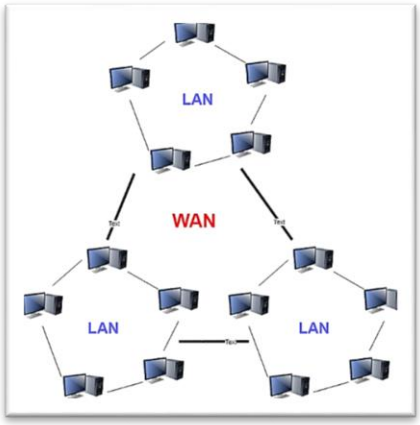
MAN

Metropolitan Area Network neboli metropolní síť. Propojuje LAN sítě v celém městě, nebo v malém regionu. Tento typ sítě je větší než LAN, která je většinou omezena na jednu budovu nebo místo. Umožňuje pokrýt oblast od několika kilometrů až do desítek kilometrů.

WAN

Wide Area Network neboli rozhlehlá/vzdálená síť. Je to síť, která propojuje geograficky vzdálené oblasti. Typicky se skládá z jednotlivých LAN a MAN. WAN obvykle pokrývá oblast státu, kontinentu.

Obrázek 6 WAN [24]



[23] *LAN* [online]. 2021 [cit. 2022-06-01]. Dostupné z WWW: < https://www.guru99.com/types-of-computer-network.html >

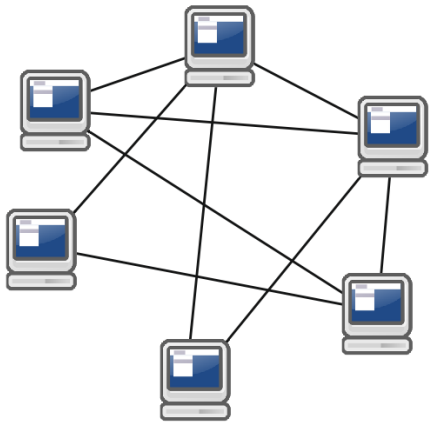
[24] *WAN* [online]. 2021 [cit. 2022-07-01]. Dostupné z WWW: < https://www.guru99.com/types-of-computer-network.html >

2.4.2 Dělení podle postavení síťových uzlů.

Peer to peer (P2P)

V peer-to-peer sítích může každé zařízení komunikovat v rámci sítě, pokud existuje přístup. V tomto případě jsou zařízení jak servery, tak klienti, protože sdílejí soubory v síti, ať už poskytují soubory (server) nebo používají soubory z jiného zařízení (klient). Obvykle je omezen počet zařízení připojených k síti peer to peer, protože čím více zařízení je v tomto typu sítě, tím pomaleji pracují. Sítě peer-to-peer jsou obecně méně bezpečné, protože každý uživatel zařízení se stará o své zabezpečení. Na P2P sítích funguje např. BitTorrent, Gnutella.[25]

Obrázek 7 Peer-to-peer [26]



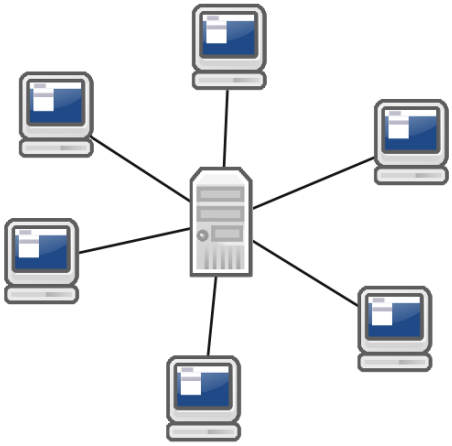
Klient - server

V síti klient/server mohou být zařízení buď klient, nebo server, obě být nemohou jako v P2P síti. Jak bylo uvedeno výše, servery poskytují soubory a informace, zatímco klienti používají informace poskytované servery. Se sítěmi typu klient/server jsou data bezpečnější než P2P sítě, protože se běžně používají ve velkých organizacích s důvěrnými informacemi, takže zabezpečení zajišťují správci systému. V sítích typu klient/server obslužná zařízení obvykle pracují rychleji a mají více úložného prostoru ve srovnání s P2P sítí. Síť klient/server může být mnohem větší než P2P. Klientská zařízení obvykle komunikují pouze s obslužnými zařízeními, protože potřebují pouze přijímat informace ze serverů a žádných jiných klientů. Klientská zařízení tak pracují

[25] BÁRTA, J., *Úvod do počítačových sítí*. České Budějovice, 1997, s. 26-28
[26] *Peer-to-peer* [online]. 2018 [cit. 2022-08-01]. Dostupné z WWW: < https://www.napocitaci.cz/33/peer-to-peer-p2p-site-uniqueidgOkE4NvrWuNY54vrLeM679zvh6YhHnhkpLpGVMy1prA/ >

rychleji, protože nemusí komunikovat s jakýmikoli jinými zařízeními kromě serverů.[27]

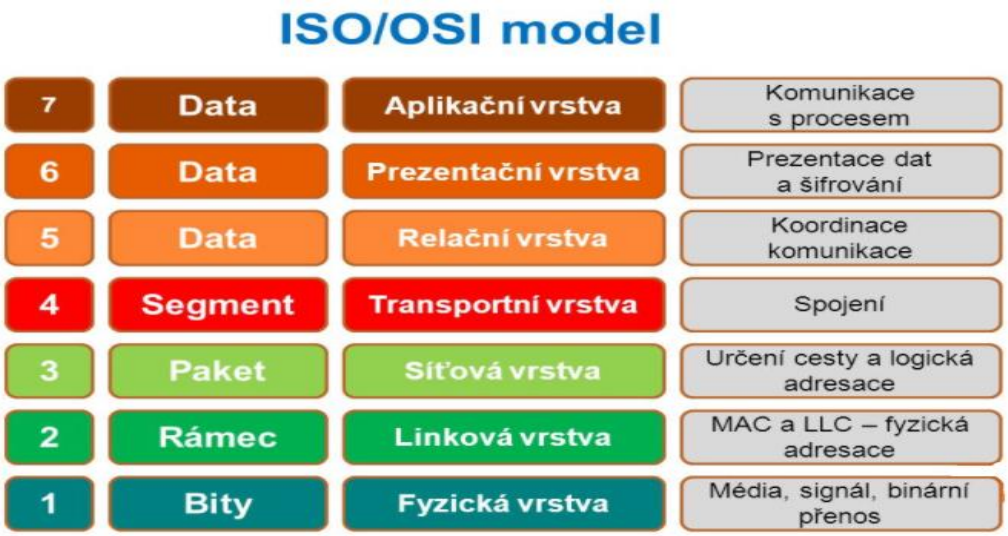
Obrázek 8 Klient-server [28]



2.4.3 ISO/OSI model [29]

ISO/OSI model je sedmivrstvý koncepční model, který charakterizuje a standardizuje komunikační funkce telekomunikačního nebo výpočetního systému.

Obrázek 9 ISO/OSI model [30]



[27] BÁRTA, J., *Úvod do počítačových sítí.* České Budějovice, 1997, s. 26-28
[28] *Klient-server* [online]. 2018 [cit. 2022-09-01]. Dostupné z WWW: < https://www.napocitaci.cz/33/peer-to-peer-p2p-site-uniqueidgOkE4NvrWuNY54vrLeM679zvh6YhHnhkpLpGVMy1prA/>
[29] PUŽMANOVÁ, R., *Moderní komunikační sítě od A do Z 2. vydání*. Brno, 2006, s. 50-81
[30] *ISO/OSI model* [online]. 2019 [cit. 2022-12-01]. Dostupné z WWW: < http://matureplus.4fan.cz/pos/3-model-isoosi-vrstvy >

FYZICKÁ VRSTVA

Je spodní vrstva modelu ISO/OSI, zabývá se přenosem a příjmem bitového toku přes fyzické médium. Popisuje elektrické, optické, mechanické a funkční parametry k fyzickému médiu a přenáší signály pro všechny vyšší vrstvy.

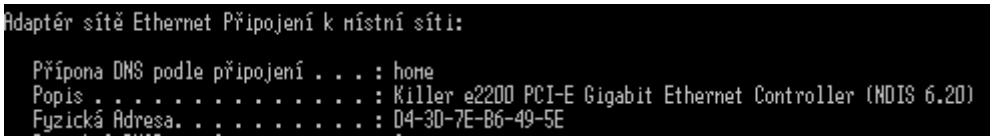
LINKOVÁ VRSTVA

Linková vrstva zajišťuje integritu toku dat z jednoho uzlu na druhý na stejné vrstvě, řízení toku dat a synchronizace. To znamená, že zprávy budou doručovány do správného zařízení v LAN pomocí hardwarových adres, a přeloží zprávy ze síťové vrstvy na bity, které fyzická vrstva přenese. Používá protokoly Ethernet, PPP, Frame Relay. Má dvě podvrstvy LLC a MAC.

LLC – Poskytuje rozhraní mezi přenosovým prostředkem a vyššími vrstvami, stará se o zapouzdřovaní paketů do rámců a doplňuje adresová a kontrolní pole.

MAC – Fyzická adresa zařízení/rozhraní, je mu přiřazena při výrobě. Zahrnuje přístupové protokoly, které umožní uzlům získat přístup ke společnému přenosovému prostředku. Je zodpovědná za hardwarovou adresaci MAC.

Obrázek 10 Fyzická adresa [31]



SÍŤOVÁ VRSTVA

Je zodpovědná za směrování dat přes síť do cíle, identifikaci zařízeních podle jejich logické adresy (IP adresy), určení nejlepší cesty k odeslání dat. Používá protokoly IPv4, IPv6, EIGRP, OSPF aj.

TRANSPORTNÍ VRSTVA

Poskytuje transparentní, spolehlivý přenos s požadovanou kvalitou a optimalizuje nejrůznější síťové služby. Transportní vrstva se nestará o směrování, ale poskytuje relační vrstvě transportní službu bez spojení (UDP) a transportní službu se spojením (TCP)

[31] *Vlastní zdroj*

TCP

Doručí adresátovi všechna přenášená data tak, jak je odesílatel vyslal (bez ztráty nebo zkreslení)

Skládá se ze tří částí:

1. Navázání spojení
2. Přenosu dat
3. Ukončení spojení

UDP

Používá se pro aplikace, pro které může být navázání spojení příliš zdlouhavé, a nebo si mohou dovolit ztratit nějaká data po cestě. Neobsahuje pole s informacemi o velikosti okna, čísla segmentů a potvrzení. Příkladem může být live stream.

RELAČNÍ VRSTVA

Dohlíží na nastavení, údržbu a ukončení relace. Poskytuje správu více relací (každé připojení se nazývá relace) přiřazuje ID číslo každé relaci, aby datový tok zůstal oddělený. Používá protokoly SIP, PPTP.

PREZENTAČNÍ VRSTVA

Specifikuje, jak jsou data prezentována, formátována, transformována a kódována. Zajišťuje šifrování, dešifrování a kompresy dat. [32]

APLIKAČNÍ VRSTVA

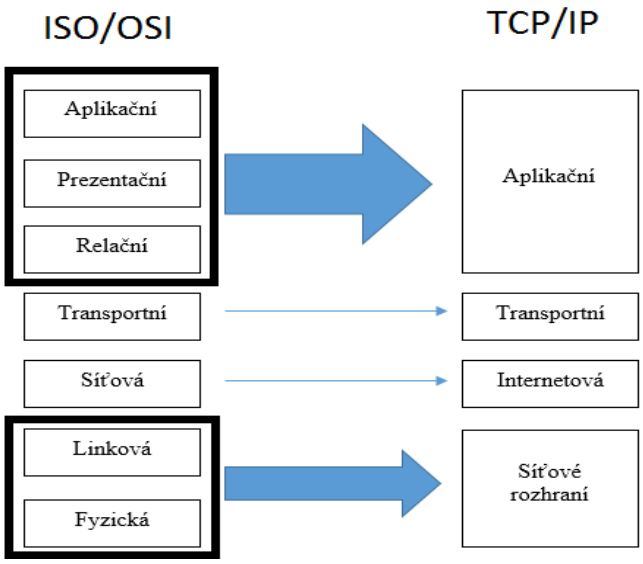
Definuje, jakým způsobem komunikují aplikace a služby se sítí. Používá protokoly HTTP, DNS, FTP.

2.4.4 TCP/IP model [33]

(Transmission Control Protocol and Internet Protocol) byl vyvinut v 70. letech na základě objednávky Defense Advanced Research Projects Agency (DARPA). Cílem bylo propojit vojenské, výzkumné a univerzitní počítače do jedné rozsáhlé sítě. Na rozdíl od ISO/OSI modelu má pouze čtyři vrstvy.

[32] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 72
[33] PUŽMANOVÁ, R., *Moderní komunikační sítě od A do Z 2. vydání*. Brno, 2006, s. 245-246

Obrázek 11 TCP/IP model [34]



Vrstva síťového rozhraní

Odpovídá nejnižším dvěma vrstvám ISO/OSI modelu (fyzické, linkové).

Internetová

Odpovídá síťové vrstvě ISO/OSI modelu.

Transportní

Odpovídá transportní vrstvě ISO/OSI modelu.

Aplikační

Odpovídá třem nejvyšším vrstvám ISO/OSI modelu (relační, prezentační, aplikační).

2.4.5 IP ADRESA [35, 36]

Internet protocol (IP) adresa je číselné označení, které je přiřazeno síťovým rozhraním zapojených do počítačové sítě. IP adresa má dvě hlavní funkce:

1. identifikace síťového rozhraní
2. adresování

IPv4 je 32 bitové číslo, které je definováno jako čtyři oktety. Každé číslo je zapisováno dekadicky a každý oktet je oddělen tečkou (např. 192.168.10.1). IPv4 má 2^{32}

[34] *Vlastní zdroj*
[35] DOSTÁLEK, L., KABELOVÁ, A., *Velký průvodce protokoly TCP/IP a systémem DNS 5. vydání*. Brno, 2012, s. 127 - 228
[36] SATRAPA, P., *IPv6 Internetový protokol verze 6 4. vydání*. Praha, 2019, s. 23 - 39

adres (4 294 967 296). Ovšem ne všechny jsou použitelné, protože některé adresy jsou rezervovány pro speciální účely, jako jsou např. privátní adresy (cca 18 miliónů adres), nebo skupinové adresy (cca 270 miliónů adres). To se mohlo zdát v 80. letech, jako velké množství adres, ovšem kvůli enormnímu rozmachu Internetu a výslednému vyčerpání veřejných adres, musel vzniknout nový systém adresování (IPv6), využívající 128 bitů, který byl vyvinut v roce 1995.

Ačkoliv jsou IP adresy uloženy jako binární čísla, jsou zobrazovány v dobře čitelné podobě, jako je např. 208.70.184.172 (pro IPv4) a 2001:db8:0:5224:0:423:1:1 (pro IPv6).

Aby si lidé nemuseli pamatovat dlouhá čísla, vznikl systém DNS, který překládá IP adresy do nám známe podoby (např. seznam.cz, google.com aj.)

Pro zpomalení vyčerpání vznikly privátní adresy, které definuje RFC 1918. Jsou to adresy, které nejsou směrovány na Internet a zařízení spolu komunikují pouze uvnitř jejich lokální sítě. Privátní adresy se často používají s překladači síťových adres (NAT) pro připojení k celosvětové síti Internet.

3 Legislativa

Tato kapitola se bude věnovat legislativnímu vývoji kybernetické bezpečnosti v ČR a základním právním předpisům, které problematiku kybernetické bezpečnosti upravují nebo s ní souvisí.

S příchodem nového druhu kriminality se stalo nutností vytvořit nový legislativní rámec, který by upravoval chování subjektů této trestné činnosti, zejména postih pachatele za konkrétní trestnou činnost a identifikaci toho, které činy skutečně kyberkriminalitou jsou a které ne. Kvůli rychle se vyvíjejícímu prostředí ICT je téměř nutností, aby státy, jak na domácí tak i na mezinárodní úrovni vytvářely a přijímaly nové právní úpravy pro efektivnější ochranu těchto technologií a obětí trestných činů.

3.1 Legislativní vývoj

Jedním z prvních strategických dokumentů, které zmiňovaly potřebu ochrany informačních technologií před trestnou činností byla: „*Koncepce boje proti organizovanému zločinu* [37]“ z roku 2000. Tento dokument byl primárně zaměřen na problematiku potírání trestné činnosti v oblasti IT. Ve stejném roce Ministerstvo vnitra přijalo *Koncepci boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření* [38], která představovala první dokument, který komplexněji řešil otázky zajištění bezpečnosti českého kyberprostoru především prostřednictvím opatření směřujících na potírání kyberkriminality a stanovila požadavek, aby byl vybudován CERT tým, nebo se zabývala ochranou kritické infrastruktury.[39]

V roce 2004 byl představen další významnější dokument *Státní informační a komunikační politika e-Česko 2006* [40]. Tento dokument definoval především: zajistit dostupné a bezpečné komunikační služby, informační vzdělanost, moderní veřejné služby on-line (e-government aj.) a vytvoření dynamického prostředí pro elektronické podnikání.[41]

---

[37] *Koncepce boje proti organizovanému zločinu* [online] 2000 [cit. 2022-02-01]. Dostupné z WWW: < https://www.dataplan.info/img_upload/7bdb1584e3b8a53d337518d988763f8d/koncepce-boje-proti-org.zlocinu.pdf >.

[38] *Koncepce boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření* [online] 2000 [cit. 2022-14-01]. Dostupné z WWW: <http://www.mvcr.cz/soubor/koncepce-pdf.aspx >.

[39] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity*. Praha, 2019, s. 87 - 88

[40] *Státní informační a komunikační politika e-Česko 2006* [online] 2004 [cit. 2022-12-01]. Dostupné z WWW: < https://www.esfcr.cz/documents/21802/761522/Státní+informační+a+komunikační+politika/9a6117ea-24a8-484f-8d08-07365057e12b >.

[41] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity*. Praha, 2019, s. 88 - 89

V roce 2005 vznikl dokument *Národní strategie informační bezpečnosti ČR* [42]. Gestorem bylo zpočátku Ministerstvo informatiky a po jeho zániku převzalo úkoly Ministerstvo vnitra, Ministerstvo průmyslu a obchodu, Ministerstvo pro místní rozvoj. Cílem této strategie bylo: zlepšení řízení informační bezpečnosti a řízení rizik, rozvoje znalostí o informační bezpečnosti, podpora národní a mezinárodní spolupráce v oblasti informační bezpečnosti, podpora používání nejlepší praxe v oblasti informační bezpečnosti, podpora ochrany lidských práv a svobod, podpora konkurenceschopnosti české ekonomiky.[43]

V roce 2010 bylo přijato usnesení vlády č. 205 [44], které řeší problematiku kybernetické bezpečnosti České republiky. Toto usnesení ustanovilo Ministerstvo vnitra gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. Ministerstvo měla plnit následující úkoly:

- koordinovat činnost státních institucí v oblasti kybernetické bezpečnosti a přispívat k zajištění plnění úkolů meziresortní povahy
- koordinovat zastupování České republiky v otázkách kybernetické bezpečnosti na mezinárodních fórech, včetně účasti státních orgánů na činnosti příslušných mezinárodních organizací,
- do 30. dubna 2010 předložit vládě ke schválení statut meziresortní koordinační rady pro kybernetickou bezpečnost,
- do 15. prosince 2010 předložit vládě strategii pro oblast kybernetické bezpečnosti,
- nejpozději k 31. prosinci 2010 zahájit zajišťování provozu vládního pracoviště CSIRT.[45]

V roce 2011 vláda České republiky přijala usnesení č. 781 [46], ve kterém ustanovila Národní bezpečnostní úřad (NBÚ) gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. Vláda uložila NBÚ řadu úkolů, ale jeden z nejvýznamnějších byl, aby do roku 2015 vzniklo plně funkční Národní centrum

[42] *Národní strategie informační bezpečnosti ČR* [online] 2005 [cit. 2022-12-01]. Dostupné z WWW: < https://moodle.unob.cz/pluginfile.php/20182/mod_resource/content/1/Národní%20strategie%20informační%20bezpečnosti%20ČR.pdf >.
[43] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity*. Praha, 2019, s. 89
[44] ČESKO. Usnesení vlády č. 205 ze dne 15. března 2010 o řešení problematiky kybernetické bezpečnosti České republiky, Dostupné z WWW: < https://apps.odok.cz/attachment/-/down/KORN97BQ9ASZ >.
[45] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity*. Praha, 2019, s. 90
[46] ČESKO. Usnesení vlády č. 781 ze dne 19. října 2011 o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast, Dostupné z WWW: < https://apps.odok.cz/attachment/-/down/KORN97BUKZ3E >.

kybernetické bezpečnosti a jako jeho součást vládní koordinační místo pro okamžitou reakci na počítačové incidenty (vládní CERT)[47]

Ve stejném roce byla přijata *Strategie pro oblast kybernetické bezpečnosti České republiky na období let 2011 až 2015* [48], ve které byly stanoveny následující cíle a opatření:

- vytvoření legislativního rámce,
- vybudování Národního centra kybernetické bezpečnosti a vládního pracoviště CERT,
- ochrana kritických informačních infrastruktur,
- posilování kybernetické bezpečnosti informačních a komunikačních systémů veřejné správy,
- zefektivnění potírání kriminality v kybernetickém prostoru,
- koordinace aktivit k zajištění kybernetické bezpečnosti v Evropě,
- používání spolehlivých a důvěryhodných informačních technologií,
- zvyšování povědomí o kybernetické bezpečnosti,
- odezva na kybernetické útoky.

28. června 2013 předložil NBÚ návrh zákona o kybernetické bezpečnosti Vládě České republiky. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů[49] (zákon o kybernetické bezpečnosti) vstoupil v platnost dne 29. srpna 2014 s účinností od 1. ledna 2015. V srpnu 2015 byl na základě požadavků stanovených v ZoKB vybrán provozovatel Národního CERT týmu. Tímto provozovatelem se stalo sdružení CZ.NIC. 18. prosince 2015 došlo k podpisu Veřejnoprávní smlouvy o zajištění činnosti Národního CERT a o spolupráci v oblasti kybernetické bezpečnosti. Tato smlouva byla uzavřena na dobu neurčitou. [50]

Významná novelizace ZoKB byla provedena zákonem č. 205/2017 Sb.,141 s účinností od 1. srpna 2017. Touto novelou byla do ZoKB implementována Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k

[47] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity*. Praha, 2019, s. 91
[48] *Strategie pro oblast kybernetické bezpečnosti ČR 2011-2015* [online] 2011 [cit. 2022-17-01]. Dostupné z WWW: < https://www.databaze-strategie.cz/cz/cr/strategie/strategie-pro-oblast-kyberneticke-bezpecnosti-cr-2011-2015?typ=struktura >.
[49] ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In Sbírka zákonů, Česká republika. 2014. Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/2014-181>
[50] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity*. Praha, 2019, s. 91 - 92

zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (NIS) a zároveň byl zřízen Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), který po NBÚ převzal práva a povinnosti v oblasti kybernetické bezpečnosti včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. NÚKIB je ve výše uvedených oblastech ústředním správním orgánem. Vedle těchto oblastí má NÚKIB na starosti také problematiku neveřejné služby v rámci družicového systému Galileo.

Současně s novelizací byla také přijata *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020* [51] a její *Akční plán* [52]. Jako hlavní cíle strategie si ČR stanovila:

- zajištění efektivity a posilování všech struktur, procesů a spolupráce při zajišťování kybernetické bezpečnosti,
- aktivní mezinárodní spolupráce,
- ochrana národní KII a VIS,
- spolupráce se soukromým sektorem,
- výzkum a vývoj / spotřebitelská důvěra,
- podpora vzdělávání, osvěta a rozvoj informační společnosti,
- podpora rozvoje schopností Policie České republiky vyšetřovat a postihovat informační kriminalitu,
- právní úprava pro kybernetickou bezpečnost (vytváření právního rámce), účast na tvorbě a implementaci evropských a mezinárodních pravidel.

V roce 2020 vznikla *Národní strategie kybernetické bezpečnosti České republiky na období 2020-2025* [53] a její *Akční plán* [54].

[51] *Národní strategie pro oblast kybernetické bezpečnosti ČR 2015-2020* [online] 2015 [cit. 2022-20-01]. Dostupné z WWW: < https://www.govcert.cz/download/gov-cert/container-nodeid998/nskb-150216-final.pdf. >.

[52] *Akční plán 2015-2020* [online] 2015 [cit. 2022-20-01]. Dostupné z WWW: < https://www.govcert.cz/download/gov-cert/container-nodeid967/akc48dnc3adplc3a1n-rkb-final-150408.pdf. >

[53] *Národní strategie pro oblast kybernetické bezpečnosti ČR 2020-2025* [online] 2020 [cit. 2022-20-01]. Dostupné z WWW: < https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/ >.

[54] *Akční plán 2020-2025* [online] 2020 [cit. 2022-20-01]. Dostupné z WWW: < https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/ >

Jako hlavní cíle strategie si NÚKIB stanovila:

- Celonárodní přístup s důrazem na sdílení informací, koordinaci a spolupráci
- Rozvoj schopností a kapacit státu v kybernetické bezpečnosti
- Posílení zabezpečení a odolností infrastruktury
- Rozvoj schopností predikce, detekce a agilní reakce na kybernetický útok
- Účinná strategická komunikace
- Prevence a potírání kybernetické kriminality
- Efektivní mezinárodní spolupráce
- Tvorba spojenců
- Prosazování zájmů ČR v zahraničí
- Vytváření dialogu v mezinárodním prostředí
- Podpora otevřeného a bezpečného chování v kyberprostoru
- Export know-how
- Zajištění bezpečnosti digitalizace státní správy
- Kvalitní systém vzdělávání
- Osvětová činnost
- Spolupráce státu, soukromé sféry a občanů
- Vytváření expertní základny

3.2 Právní normy v ČR

V současné době je problematika kybernetické bezpečnosti ošetřena zákonem o kybernetické bezpečnosti, avšak dílčí aspekty ochrany České republiky je možné nalézt i v jiných právních předpisech. Z pohledu kybernetické bezpečnosti jsou nejdůležitější následující dokumenty:

Ústavní zákony

- Ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů
- Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů
- Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky

Zákony

- zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů
- zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů
- zákon č. 240/2000 Sb., o krizovém řízení a změně některých zákonů (krizový zákon), ve znění pozdějších předpisů
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů
- zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů
- zákon č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů
- zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
- zákon č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů
- zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů
- zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů
- zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů
- zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim
- zákon č. 89/2012 Sb., občanský zákoník
- zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
- zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce

Prováděcí předpisy

- nařízení vlády č. 522/2005 Sb., kterým se stanoví seznamy utajovaných informací, ve znění pozdějších předpisů
- vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění pozdějších předpisů
- vyhláška č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy)
- nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury
- vyhláška 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů
- vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích
- vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby
- vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

3.3 Zákon o kybernetické bezpečnosti

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti (Zákon o kybernetické bezpečnosti) vstoupil v platnost 29. srpna 2014 s účinností od 1. ledna 2015

ZoKB má za cíl zajistit bezpečné fungování české informační společnosti, tj. zajištění základního práva na informační sebeurčení a ochranu nedistributivních práv státu. ZoKB nezakládá civilní ani trestní odpovědnost pachatelů kybernetických útoků, ale vytváří systém bezpečnostních opatření, která mají incidentům předcházet. Má zajistit, že případný kybernetický bezpečností incident neohrozí celkové fungování

informačních a komunikačních systémů nebo fungování kriticky důležitých společenských informačních funkcionalit.[55]

V roce 2017 proběhly dvě obsahově významné novely zákona o kybernetické bezpečnosti, a to prostřednictvím zákona č. 104/2017 Sb. s účinností od 1. července a zákona č. 205/2017 Sb. s účinností od 1. srpna 2017. K aktuálnímu datu proběhly ještě následující novelizace tohoto zákona – novelizace zákonem č. 183/2017 Sb., zákonem 35/2018 Sb., zákonem č. 111/2019 Sb., č. 12/2020 Sb. a aktuálně poslední novelizace zákonem č. 261/2021 Sb.[56]

[55] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity*. Praha, 2019, s. 133
[56] *Zákon o kybernetické bezpečnosti* [online]. Praha: NUKIB, 2021 [cit. 2022-16-01]. Dostupné z WWW: < https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/>.

4 Formy útoků

Tato kapitola se bude věnovat nejčastějším formám útoků.

Velmi často je kyberkriminalita považována za nový druh kriminality, nicméně značná část kyberkriminality využívá či přenáší známé druhy protiprávního jednání (např. podvody, porušování práv autorských, krádeže, šikanu aj.) do prostředí digitálního, ve kterém je lze páchat lépe, rychleji, efektivněji než ve světě reálném. Mezi ryze kybernetické útoky je možné zařadit např. hacking, DoS a DDoS útoky, botnety aj.[57]

4.1 Malware

Malware vznikl složením dvou anglických slov „malicious software“ (škodlivý software). Malware je jakýkoli software využitý k narušení standardní činnosti počítačového systému, zisku informací (dat), nebo k získání přístupu k počítačovému systému. Malware může mít celou řadu podob, přičemž mnohé druhy malware jsou pojmenovány podle toho, jakou činnost provádějí.[58, 59]

4.1.1 Adware

Adware je zkratka z anglického slovního spojení „advertising supported software“ (software podporující reklamu). Zobrazuje otravná vyskakovací okna (např. pop-up okna v operačním systému nebo na webových stránkách, reklamy zobrazované společně se software aj.), aby svému autorovi generovala příjmy. Adware primárně „pouze“ obtěžuje uživatele neustálými reklamními sděleními, která „vyskakují“ na obrazovce, ale společně se spyware může sledovat činnost uživatele a odcizit důležité informace. [60]

4.1.2 Spyware

Pojem spyware je složeninou anglických slov „spy“ (špion) a „software“. Pomocí spyware jsou získávána data o provozu počítačového systému a bez vědomí a souhlasu uživatele odesílána k útočníkovi. Součástí těchto dat mohou být i osobního informace, informace o navštívených webových stránkách, o spuštěných aplikacích apod. Spyware může být instalován jako samostatný malware, nebo může být i součástí jiných, volně šířených a jinak zcela bezpečných programů. Charakteristickou vlastností spyware je, že většinou zůstávají nainstalovány v počítači i poté, co hlavní program byl odinstalován. [61]

[57] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 181
[58] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 204
[59] JOHNSON, A. *31 Days Before Your CCNA Exam. New Jersey*, 2020, s. 625 - 626
[60] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 205
[61] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 207

4.1.3 Viry

Virus je typ malwaru, který se šíří vložením své kopie do jiného programu. Po spuštění programu se viry šíří z jednoho počítače na druhý a infikují počítače. Většina virů vyžaduje k šíření lidskou pomoc. Například, když někdo připojí infikovaný USB disk ke svému PC, virus se dostane do PC. Virus pak může infikovat nový USB disk a rozšířit se do nových počítačů. Viry mohou ležet v nečinnosti po delší dobu a poté se aktivovat v určitý čas a datum. Viry mohou být neškodné, například ty, které zobrazují obrázek na obrazovce, nebo mohou být naopak destruktivní, například ty, které upravují nebo mažou soubory na pevném disku. Většina virů se nyní šíří pomocí USB paměťových jednotek, CD, DVD, souborů sdílených na Internetu a e-mailu. E-mailové viry jsou nejběžnějším typem virů. [62]

4.1.4 Červi (Worms)

Červi nepotřebují žádného hostitele, tedy žádný spustitelný soubor. Tyto programy se na rozdíl od virů, které bývají připojeny jako součást jiného programu, šíří zpravidla samostatně. Napadený systém je následně červem využit k odeslání kopií sebe sama dalším uživatelům pomocí síťové komunikace. Tímto způsobem se velmi rychle rozšiřuje, což může vést až k zahlcení počítačové sítě, a tím i celé infrastruktury. Na rozdíl od virů jsou tyto programy schopny analyzovat bezpečnostní slabiny v zabezpečení, proto bývají využívány i k vyhledávání bezpečnostních mezer v systémech nebo v poštovních programech. [63, 64]

4.1.5 Trojské koně

Za trojské koně jsou obecně označovány počítačové programy, které obsahují skryté funkce, s jejichž užitím uživatel nesouhlasí nebo o nich neví, a které jsou potenciálně nebezpečné pro další fungování systému. Stejně jako v případě virů mohou být tyto programy připojeny k jinému, bezpečnému programu či aplikaci nebo mohou samy vypadat jako neškodný počítačový program. Trojské koně, na rozdíl od klasických virů, nejsou schopny se replikovat a ani se šířit bez „pomoci“ uživatele. V případě, že je trojský kůň aktivován, může být využit například k mazání, blokování, modifikaci, kopírování dat či například narušování běhu počítačového systému, či počítačových sítí.

[62] SANTOS, O. *Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide.* New Jersey, 2021, s. 65, 122, 125, 802,
[63] SANTOS, O. *Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide*. New Jersey, 2021, s. 114, 122, 125, 802 - 805
[64] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 208

Některé trojské koně po své aktivaci bez vědomí uživatele otevírají komunikační porty počítače, čímž výrazným způsobem zjednodušují další napadání takto zasaženého systému jinými škodlivými programy, popřípadě usnadňují přímé ovládnutí napadeného počítače na dálku. S užitím trojských koní bývá často též spojeno užití různých skenovacích programů, což jsou programy, které slouží zejména ke zjištění, které komunikační síťové porty počítače jsou otevřené, jaké služby jsou na nich spuštěné a zda je přes ně možno realizovat útok na takový systém. [65, 66, 67]

4.1.6 Ransomware

Ransomware je vyděračský malware (ransom - výkupné). Ransomware brání či omezuje uživatele v užívání počítačového systému do doby, než dostane útočník zaplaceno výkupné. Ransomware se nejčastěji dostane do počítače pomocí trojského koně, nebo červa, který je umístěn na webových stránkách, nebo je přílohou e-mailu. Obecně je možné rozlišovat dva typy ransomware podle toho, jak moc zasahují do vlastního chodu počítačového systému. Prvním typ, omezí funkčnost celého počítačového systému a neumožní uživateli tento systém vůbec využívat např. zabráněním spuštění operačního systému či zablokováním systémové obrazovky. Druhý typ ponechá počítačový systém funkční, avšak dochází k uzamčení a znepřístupnění dat uživatele.[68, 69]

4.2 Sociální inženýrství

Sociální inženýrství nelze považovat přímo za kybernetický útok, nicméně je předpokladem pro to, aby byla řada kybernetických útoků úspěšná. Pokud bychom chtěli definovat pojem sociální inženýrství, bylo by možné říci, že jde o ovlivňování, přesvědčování či manipulaci s lidmi s cílem je donutit provést určitou akci, či od nich získat informace, které by jinak neposkytli. Hlavní myšlenkou sociálního inženýrství je nevyužívat ryze technické přístupy, nebo nástroje například k prolomení hesla, když mnohem jednodušší je uvést oběť v omyl, ve kterém sama dobrovolně toto heslo prozradí. Nejslabším článkem bezpečnostního systému je a vždy bude člověk (uživatel). Jelikož na světě nemůže existovat počítačový systém, který by alespoň v nějaké fázi nebyl závislý

[65] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 208
[66] JIROVSKÝ, V., *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, 2007, s. 63 - 64
[67] PUŽMANOVÁ, R., *Moderní komunikační sítě od A do Z 2. vydání*. Brno, 2006, s. 372
[68] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 221
[69] SANTOS, O. *Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide.* New Jersey, 2021, s. 124, 804

na člověku (zprovoznění, nastavení, údržba počítačového systému), proto je nejjednodušší cestou získat potřebné informace právě od člověka. Pro sociální inženýrství je jedním z klíčových faktorů zisk co největšího množství informací o cíli. Mnohdy dochází k dlouhodobému působení na osobu a budování „důvěry" mezi útočníkem a obětí před vlastním útokem, přičemž útočník typicky využívá lidské neopatrnosti, důvěřivosti, ochoty pomoci jiným, lenosti, slabosti, strachu (např. aby se osoba nedostala do problémů), neodpovědnosti, aj. [70, 71]

4.3 Phishing

Pojmem phishing se nejčastěji označuje podvodné či klamavé jednání, jehož cílem je získat informace o uživateli, jako jsou např. uživatelské jméno, heslo, číslo kreditní karty, PIN aj. Phishing představuje jednání, které po uživateli vyžaduje navštívení podvodné stránky (zobrazující např. webovou stránku Internetového bankovnictví, online obchodu aj.) a následné vyplnění přihlašovacích informací.[72]

4.4 Podvodné webové stránky

Na Internetu se lze setkat s celou řadou webových stránek prezentujících úžasné výhry, nebo nabízejících různé zboží za velmi výhodné ceny. Útočníci využívají sociálního inženýrství a spoléhají primárně na důvěřivost a neopatrnost lidí. Vlastní činnost útočníka pak může mít typicky dvojí podobu. V prvním případě se útočník snaží vylákat citlivé údaje (např. jméno, příjmení, doručovací adresa, e-mail, telefonní číslo a heslo) typicky za účelem registrace, doručení zboží, výhry aj. Všechny tyto údaje zadává uživatel sám a dobrovolně. Útočník se tak dostává k údajům, které může, stejně jako v případě phishingu, využít k celé řadě aktivit. Například na základě zadaného hesla a dalších údajů o uživateli se útočník může pokusit získat přístup k dalším službám, které uživatel používá. V druhém, mnohem častějším případě se pak jedná o aktivity, které spočívají v podvodném vylákání finančních prostředků z uživatele.[73, 74]

4.5 Hacking

Hacking se dá definovat jako jakýkoliv neoprávněný průnik do počítačového systému z vnějšku, nejčastěji v rámci sítě Internet a osoba, jež tento čin páchá, se označuje jako hacker. Nebezpečí hackerských aktivit spočívá mimo jiné i v tom, že vedle vlastního

[70] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 186 - 187
[71] JOHNSON, A. *31 Days Before Your CCNA Exam. New Jersey*, 2020, s. 629 - 630
[72] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 246
[73] SMEJKAL, V. *Kybernetická kriminalita. 2. rozšířené a aktualizované vydání*. Plzeň, 2018, s. 187
[74] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 266 - 267

získání neoprávněného přístupu do napadeného systému (bez ohledu na motivaci hackera) tyto osoby k realizaci těchto útoků vytvářejí a užívají vysoce efektivní softwarové prostředky, jejichž zdrojové kódy jsou často zveřejněny např. na Darknetu. To může vést k dalšímu hromadnému zneužívání těchto programů uživateli, kteří sami neovládají programování na takové úrovni, aby tyto programy vytvořili, ale kvůli existenci těchto nástrojů mohou potenciálně způsobovat jiným uživatelům poměrně značné škody. [75, 76]

4.6 Cracking

Pojem cracking znamená prolamování nebo obcházení ochranných prvků počítačového systému, programů nebo aplikací, s cílem jejich následného neoprávněného užití. Cracking je spojen zejména s porušováním autorských práv a práv souvisejících s právem autorským. Za cracking je označováno jednání spočívající v obcházení ochranných prvků, které brání vytváření kopií či nelegálnímu užívání počítačových programů a hudebních nebo filmových produktů.[77, 78]

4.7 Spam

Jedná se o všechny doručené nevyžádané zprávy, tedy i např. o zprávy obsahující viry, trojské koně apod. Pro spam je typické, že se jedná o sdělení, které je zaslané elektronicky, hromadně a bez vyžádání. Spam využívá různé komunikační kanály k odesílání nevyžádaných zpráv (e-mail, Skype, SMS, MMS, sociální sítě, aj.).[79]

4.8 Hoax

Snaží se svým obsahem vyvolat dojem důvěryhodnosti. Informuje např. o šíření virů nebo útočí na sociální cítění adresáta. Může obsahovat škodlivý kód nebo odkaz na Internetové stránky se škodlivým obsahem [80]

4.9 DoS, DDoS

DoS je zkratkou z anglického spojení slov „Denial of Service“, což lze do českého jazyka přeložit jako popření či odepření služby. Cílem DoS a DDoS útoků je vyřazení z činnosti nebo snížení výkonu napadeného zařízení. Tento útok je realizován zahlcením napadeného počítačového systému (či prvku sítě) pomocí opakujících se požadavků,

[75] MATĚJKA, M. *Počítačová kriminalita*. Praha, 2002, s. 53 - 54
[76] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 269 - 274
[77] MATĚJKA, M. *Počítačová kriminalita*. Praha, 2002, s. 73
[78] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 276
[79] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 231 - 235
[80] JIRASEK, P., NOVAK, L., POŽAR, J. *Výkladový slovník kybernetické bezpečnosti*. Praha, 2015, s. 88

které má počítačový systém vykonat. Systém napadený DoS útokem se projevuje zejména neobvyklým zpomalením služby, celkovou nebo chvilkovou nedostupností služby (např. webových stránek) apod. Rozdíl mezi DoS a DDoS útoky je především v tom, jakým způsobem je útok veden. V případě DoS je zdroj útoku jeden. Tomuto typu útoku se poměrně snadno brání, protože je možné zablokovat provoz ze zdroje útoku. U DDoS (Distributed Denial of Service - distribuované odepření služby) dochází k zahlcení cílového počítačového systému odesíláním paketů z více počítačových systémů, které jsou různě geograficky umístěny, což ztěžuje obranu a identifikaci útočníka. DoS a DDoS útoky velmi často využívají chyby například v operačním systému, spuštěných programech, nebo síťových protokolech. Cílem útoků typu DoS/DDoS není infikovat počítačový systém, nebo překonat bezpečnostní ochranu např. heslem, které ho chrání, ale pomocí série opakovaných požadavků ho buď zahltit, či dočasně vyřadit z provozu. Typicky tak dojde k omezení či zablokování přístupu ke službám. DDoS útok nemusí být pokaždé úmyslný, může jít například o normální činnost uživatelů Internetu, kteří se v jeden okamžik snaží připojit např. na webový server společnosti, která prodává elektroniku a oznámila, že od 15:00 hod dojde k plošnému snížení cen elektroniky o 50 %. Pokud je cílový počítačový systém nedostatečně dimenzován, nebo je špatně nakonfigurován (není schopen odbavit požadovanou sumu přístupů), dojde k jeho „kolapsu“ obdobně, jako tomu je u cíleného DDoS útoku. [81, 82, 83]

[81] SMEJKAL, V. *Kybernetická kriminalita*. Plzeň, 2015, s. 534 – 539
[82] PUŽMANOVÁ, R., *Moderní komunikační sítě od A do Z 2. vydání*. Brno, 2006, s. 372
[83] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 295 - 304

5 Obrana a prevence proti síťovým útokům

5.1 Bezpečnostní protiopatření [84]

Jsou všechny prostředky, které jsou nasazeny ke zmírnění nebo znemožnění útoku na integritu, důvěrnost nebo dostupnost (CIA), k minimalizaci následků porušení funkcí informačního systému, k minimalizaci následků kybernetických útoku a k rychlému obnovení funkčnosti. To se týká i následků, které mají svůj původ v přírodních jevech, technických selháních a neúmyslných hrozbách.

Oblasti kde lze uplatnit bezpečnostní protiopatření:

5.1.1 Personální politika

Výběr a prověření vhodných pracovníků IS a uživatelů, stanovení jejich práv a povinností, rozsah přístupu k informacím. Stanovit požadavky na personální kvality pracovníků IS podle citlivosti informací, se kterými pracovník smí přijít do styku. Analýzy bezpečnostních incidentů se shodují, že cca 80% incidentů s vážnými následky způsobují útoky „zevnitř".

5.1.2 Fyzická a technická ochrana

Zabezpečit příslušný stupeň ochrany objektů, prostor, zařízení, komunikačních tras, ve kterých je provozován IS s důrazem na klíčová zařízení (např. servery, paměťová média, regulace pohybu osob v objektech aj.)

5.1.3 Záložní zdroje energie

Zajistit záložní zdroje energie, zálohování dat, proti případným živelným pohromám.

5.1.4 Technická ochrana proti úmyslným útokům z Internetu

Instalace antivirových programů, volba firewallu, instalace proxy serveru pro vytvoření demilitarizované zóny, instalace automatického průběžného monitoringu s nastavitelnou bezpečnostní politikou aj.

5.1.5 Kryptografická ochrana

Slouží proti možnému poškození, odcizení informací během přenosu, nebo během zpracování a uložení na paměťových médiích. Pro zajištění volit certifikované

[84] FEREBAUEROVÁ, R., PEKÁREK, O. *Aplikovaná informatika*. 1. vydání. České Budějovice, 2014, s. 68 - 70

prostředky, zavedení elektronického podpisu a využívání certifikační autority, zřizování virtuálních privátních sítí (VPN) aj.

5.1.6 Monitoring a bezpečnostní audit

Zajistit důsledný provozní monitoring a bezpečnostní audit, vyšetřit každý bezpečnostní incident, provádět penetrační testy pro odhalení slabin systémů. Obsahem bezpečnostního auditu je vyhodnocení auditu, prošetřování příčin bezpečnostních incidentů, přijímání protiopatření k minimalizaci následků a zdokonalování bezpečnosti informačního systému.

5.1.7 Havarijní plán a plán obnovy funkčnosti

Nastavit pravidla pro různé typy havárií a připravit postupy a plány pro rychlé obnovení funkčnosti IS.

5.1.8 Pravidla a směrnice

Vytvoření souboru pravidel a směrnic pro práci s IS, která mají za cíl udržet IS v bezpečném provozu. Tato pravidla pak tvoří bezpečnostní politiku IS.

5.1.9 Proškolování

Provádět pravidelná školení personálu.

5.2 Rozdělení sítě [85]

Správné rozdělení sítě je z pohledu kybernetické bezpečnosti velmi důležité a je to jeden ze základních prvků bezpečnosti. Při rozdělování sítě je vhodné se zaměřit na:

- Oddělení systémů se zvýšeným potenciálním rizikem útoku od zbytku sítě a na to se použijí demilitarizované zóny
- Rozdělení provozu v síti (oddělit provoz jednotlivých oddělení, informačních systémů aj.) Dále je vhodné oddělit provoz přicházející z veřejné Wi-Fi sítě určené např. pro návštěvy od ostatního síťového provozu. V případě rozdělování provozu sítě si obvykle vystačíme s logickým rozdělením sítě pomocí Virtuální LAN (VLAN).

5.2.1 Demilitarizované zóny

Demilitarizovaná zóna (DMZ) je podsíť, která se nachází mezi veřejným Internetem a privátními sítěmi. Cílem DMZ je umožnit organizaci přístup k nedůvěryhodným sítím, jako je Internet, a zároveň zajistit, aby její privátní síť nebo LAN

[85] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity*. Praha, 2019, s. 426 - 428

zůstaly bezpečné. Obvykle jsou v DMZ umístěny servery, na kterých jsou provozované služby (webový server, mail server, FTP server aj.), které mají být dostupné uživatelům z jiných sítí. Smyslem DMZ je ochránit lokální síť v případě, kdy se útočníkovi podaří kompromitovat některý z veřejně dostupných serverů. Demilitarizovaná zóna se zpravidla implementuje pomocí firewallu, který oddělí jednotlivé sítě.

5.2.2 Virtuální LAN

Virtuální místní síť (VLAN) umožňuje provést logické rozdělení sítě nezávisle na jejím fyzickém uspořádání (např. potřebuji oddělit jednotlivá oddělení, IP telefony aj.). Počítačové systémy mohou přímo komunikovat pouze s jinými počítačovými systémy, které jsou ve stejné VLAN (pro komunikaci do jiné VLAN musí být provoz vyveden do routeru a ten jej přesměruje do příslušné VLAN).

5.3 IDS

Intrusion detection system (IDS) je systém, který se na základě sledování síťového provozu, nebo na základě chování procesů a operačního systému, snaží identifikovat případné pokusy o útok a další podezřelé jevy. IDS dokáže zjistit pokusy o skenování portů, exfiltraci dat, exploitaci zranitelností aj.[86, 87]

5.4 IPS

Intrusion Prevention System (IPS) je systém, který na rozdíl od IDS dokáže sám zasáhnout proti rozpoznanému útoku, například resetováním síťového spojení, zablokováním provozu z podezřelé IP adresy, nebo zahozením závadných paketů.[88]

5.5 Firewally

Firewall má za úkol zabránit nechtěné síťové komunikaci mezi dvěma různými zónami, kterými mohou být dvě či více různých počítačových sítí, nebo rozhraní sítě a koncového počítačového systému. Rozhodnutí, jaká komunikace bude povolena či zakázána se řídí bezpečnostní politikou, jejíž pravidla jsou aplikována na každý paket, procházející firewallem. [89]

5.6 Antivirové programy

Antivirové programy (antiviry) jsou programy vytvořené pro vyhledávání a ničení počítačových virů. Aby správně fungovaly je potřeba mít aktuální virovou databázi, kvůli

[86] SANTOS, O. *Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide.* New Jersey, 2021, s. 114 - 120, 224, 274 - 278
[87] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity*. Praha, 2019, s. 460
[88] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity*. Praha, 2019, s. 461
[89] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity*. Praha, 2019, s. 455 - 457

které program ví, co je a není virem. Dříve byl antivirový program určen pouze k jednomu účelu, vyhledat a zničit veškeré viry v počítači. Později se krom virů zaměřily také na trojské koně a červy. Moderní antivirové programy mají rezidentní ochranu (umístěna v RAM, kterou také sleduje), standartní štít, webový a e-mailový štít, siťový štít. Veškerá konfigurace záleží na tom, jaký antivirový program používáme. Mezi antivirové programy patří například Avast, AVG, Norton aj. Antivirové programy lze rozšířit o další funkce jako je například: antispam, antispyware aj.[90]

5.7 VPN

K zabezpečení síťového provozu mezi weby a uživateli používají organizace virtuální privátní sítě (VPN) k vytvoření end-to-end privátních síťových připojení. VPN je virtuální v tom, že přenáší informace v rámci privátní sítě, ale tyto informace jsou ve skutečnosti přenášeny přes veřejnou síť. VPN je privátní, protože provoz je zašifrován, aby byla data při přenášení přes veřejnou síť důvěrná.[91]

5.8 IPsec

IPsec je ucelený soubor standardů (definován RFC 2401-2412) pro kryptografické zabezpečení síťového přenosového protokolu IP. Kromě kryptografického zabezpečení samotného IP protokolu se automaticky zajišťuje i bezpečnost všech protokolů, jejichž datové jednotky jsou v tělech IP paketů přenášeny. V praxi se zejména jedná o transportní protokoly TCP i UDP a pak i o všechny aplikační protokoly, které služby protokolů TCP a UDP využívají. IPsec může chránit provoz od vrstvy 3 až po vrstvu 7. [92]

5.9 Obecná doporučení [93]

Následující podkapitola se bude věnovat obecným doporučením chování v kyberprostoru. Samozřejmě nikdo nikdy nezaručí, že pokud budete dodržovat doporučení tak se vám nic nestane v kyberprostoru, ale alespoň tím výrazně snížíte riziko různých kyber útoků. Zde je pár nejzákladnějších doporučení:

- Nevěřte všemu, co se na Internetu dozvíte. Informace ověřujte z více zdrojů.
- Nezveřejňujte o sobě na Internetu žádné citlivé informace.

[90] *Antivir* [online]. [cit. 2022-23-01]. Dostupné z WWW: < http://iki.ktkadan.cz/soubory/viry_antiviry.pdf >
[91] PUŽMANOVÁ, R., *Moderní komunikační sítě od A do Z 2. vydání*. Brno, 2006, s. 388 - 389
[92] BURDA, K. *Kryptografie okolo nás.* Praha, 2019, s. 53
[93] *Doporučení* [online]. [cit. 2022-23-01]. Dostupné z WWW: < https://www.nukib.cz/cs/infoservis/doporuceni/>

- Nikomu neposílejte své intimní fotografie. Ani je veřejně nesdílejte
- Dávejte pozor na podezřelé zprávy, přílohy, videa a odkazy.
- Ověřte si totožnost člověka, se kterým komunikujete.
- Pro přístup do informačních systémů s citlivými informacemi vždy používejte vícefaktorovou autentizaci.
- Nikomu nesdělujte své přihlašovací údaje. Pravidelně je aktualizujte. Používejte silná a unikátní hesla. (silné heslo: minimálně 8 znaků, kombinace písmen, číslic a speciálních znaků, unikátní heslo: použito pro přístup pouze k jednomu účtu nebo zařízení.)
- Na veřejných počítačích (na univerzitě, v knihovně, v kavárně) nikdy nepřistupujte k důvěrným sítím nebo datům a neukládejte hesla a přihlašovací údaje do paměti prohlížeče.
- Udržujte své antivirové zabezpečení aktualizované. Své zařízení pravidelně testujte.
- Zálohujte soubory ve svém zařízení na externí disky nebo do cloudu. V případě potřeby můžete svá data kdykoli obnovit.
- Neotevírejte obsah nalezených paměťových zařízení na svém počítači.
- Když používáte nezabezpečenou veřejnou Wi-Fi síť, nikdy na ní nenakupujte, nekontrolujte své účty ani nepřistupujte k důvěrným sítím nebo datům.
- Zapínám Wi-Fi, bluetooth, NFC a další bezdrátové technologie, jen pokud je využívám.
- Protože je obtížné zapamatovat si všechna hesla, využívám správce hesel.

6 Empirické šetření

6.1 Příprava dotazníku a jeho realizace

Hlavním cílem práce je zjistit, jaké mají studenti zkušenosti s kyberkriminalitou, jak je vnímána, zda vědí, jak problémy řešit popřípadě jim předejít. Aby tento cíl bakalářské práce mohl být splněn, bylo provedeno dotazníkové šetření probíhající od 14. 2. 2022 do 25. 2. 2022. Empirické šetření se zabývá vyhodnocením dat prostřednictvím studentů Střední průmyslové školy a Vyšší odborné školy v Příbrami. Dotazníkové šetření bylo možné vyplnit pouze v tištěné podobě, kvůli rychlejší návratnosti dotazníků. Celkem bylo osloveno 120 respondentů a 106 (88,3%) respondentů na dotazník odpovědělo.

6.1.1 Struktura dotazníkového šetření

Dotazníkové šetření obsahuje celkem 16 otázek a je umístěno na konci mé bakalářské práce v příloze č. I. Šetření se skládá ze 14 otázek – 9 otázek je uzavřených, 5 otázek je polouzavřených / polootevřených (s možností jiné) a 2 otázky jsou otevřené. V otevřených otázkách mohou respondenti vyjádřit svůj názor, (viz. v dotazníkovém šetření, odpověď – pokud ano, „stručně vysvětlete“). Z celkových 14 otázek (polouzavřené + uzavřené), jsou 4 otázky s výběrem z více možností.

Otázka č. 1 a č. 2 slouží pro identifikaci respondenta, který vyplňuje dotazníkové šetření. Otázka č. 3 je otevřená a respondenti se mohli vyjádřit, co znamená pojem kybernetická kriminalita. V otázce č. 4 šlo o zjištění, jakou má respondent osobní zkušenost s kyberkriminalitou. Varianty odpovědí byly – podvodné webové stránky (emaily), odcizení citlivých dat (foto, videa, aj.), odcizení profilu (Facebook, Instagram, aj.), vyhrožování, vydírání, urážení, podvodné jednání, vir, červ, bootnet, trojský kůň, spam, sexting (zprávy se sexuálním obsahem), jiné. Otázka č. 5 byla zaměřená na to, jakou respondenti používají ochranu proti malware. Varianty odpovědí byly – základní (součást továrního nastavení), antimalwarové/antivirové programy zdarma (freeware), placené programy (Premium verze), žádná varianta. V otázce č. 6 bylo zjišťováno, v jaké oblasti kyberkriminality vidí respondenti největší hrozbu. Varianty odpovědí byly – hacking (získání neoprávněného přístupu do zařízení), DoS, DDoS (odepření služby, znefunkční a znepřístupní např. server), malware (škodlivé programy, např. viry, sledovací programy, aj.), phishing (podvodné stránky, jejíž cílem je získat informace, jako jsou např. uživatelské jméno, heslo, číslo kreditní karty, PIN), hoax (zpráva, která se snaží šířit paniku), sexting (zprávy se sexuálním obsahem), podvodné jednání, jiné. Otázka č. 7 zjišťovala, jak by respondent jednal, pokud by jeho zařízení bylo infikováno

malwarem. Varianty odpovědí byly – vyhledám odborníka, zeptám se kamaráda, někoho z rodiny, koupím nové zařízení, zkusím to vyřešit sám, půjdu na policii, jiné. Otázka č. 8 zjišťovala, zda si respondent zálohuje data. Respondenti mohli odpovědět – ano, ne. Otázka č. 9 zjišťovala, jak by respondent jednal, pokud by mu přišla zpráva, ve které stojí, že vyhrál jeden milion korun. Varianty odpovědí byly – hned ji smažu, přečtu si jí, ignoruji jí, přečtu si ji a kliknu na uvedený odkaz ve zprávě, abych si vyzvedl výhru. Otázka č. 10 měla zjistit, jak si respondenti volí heslo. Respondenti mohli odpovědět – generátor náhodných hesel, podle známých věcí (jména mazlíčků, datum narození, přezdívka, aj.), jedno univerzální, jiné. Otázka č. 11 zjišťovala, zda respondent používá nelegální software. Varianty odpovědí byly – ano, ne. Otázka č. 12 zjišťovala, zda respondent sdílí osobní informace na sociálních sítích. Varianty odpovědí byly – ano, ne. Otázka č. 13 zjišťovala, jakým způsobem se respondenti brání proti kyberútokům. Varianty odpovědí byly – silné unikátní heslo (silné heslo: minimálně 8 znaků, kombinace písmen, číslic a speciálních znaků, unikátní heslo: použito pro přístup pouze k jednomu účtu nebo zařízení.), používám antimalware/antiviroré programy, neotevírám přílohy z neznámých zdrojů, pravidelně aktualizuji systém a antivirové zabezpečení, zálohuji si svá data, používám VPN, když používám nezabezpečenou veřejnou WiFi síť, tak na ní nenakupuji, nepřihlašuji se do systému s citlivými informacemi (bankovnictví aj.), zapínám Wi-Fi, bluetooth, NFC a další bezdrátové technologie, jen pokud je využívám, nezveřejňuji o sobě na Internetu žádné citlivé informace, nepoužívám žádnou ochranu proti kyberútokům. Otázka č. 14 zjišťovala, jaká je podle respondenta procentuální úspěšnost při odhalování kyberkriminality. Varianty odpovědí byly – do 20%, 21-40%, 41-60%, 61-80%, 81-100%. Otázka č. 15 zjišťovala, jestli by měli respondenti zájem získávat pravidelné informace o nových hrozbách kyberkriminality a možných způsobech ochrany. Varianty odpovědí byly – ano, ne. Na závěr otázka č. 16, která je otevřená a respondenti se mohli vyjádřit, v čem by viděli zlepšení do budoucna.

6.1.2 Cíle a hypotézy výzkumu

Hlavním cílem výzkumu bylo zjistit, jaké mají studenti zkušenosti s kyberkriminalitou, jak je vnímána, zda vědí, jak problémy řešit popřípadě jim předejít. Výzkum byl zvolen na základě dotazníkového šetření. Dále byly sestaveny dvě hypotézy, které se na základě výsledků vyvrátí či potvrdí.

Stanovené hypotézy:

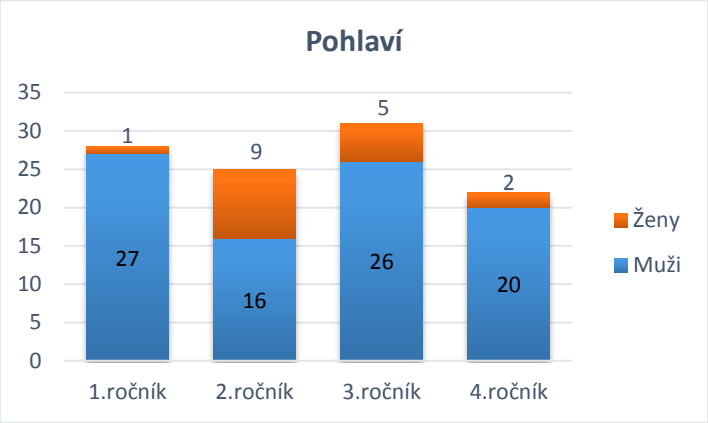
H1: Více jak 90% respondentů odpovědělo, že používá nějakou ochranu proti kyberútokům.

H2: Maximálně 60% respondentů uvedlo, že sdílí osobní informace na sociálních sítích.

6.2 Interpretace výsledků dotazníku

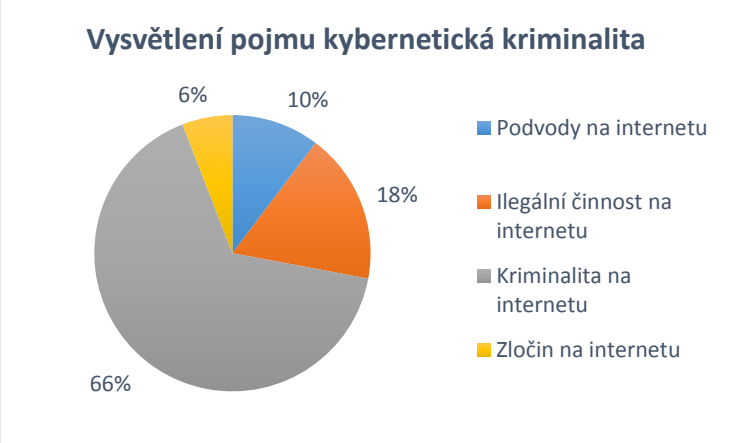
V následujících bodech jsou uvedeny výsledky výzkumu, které jsou pro přehlednější orientaci čtenáře znázorněny graficky.

Graf 1 Pohlaví [94]



Dotazníkové šetření se zúčastnilo 16% žen a 84% mužů. Na dotazník odpovídalo více mužů z důvodu, že se jedná o střední průmyslovou školu, kde je převážně mužské zastoupení. Graf č. 2 vyjadřuje porovnání pohlaví mezi ročníky.

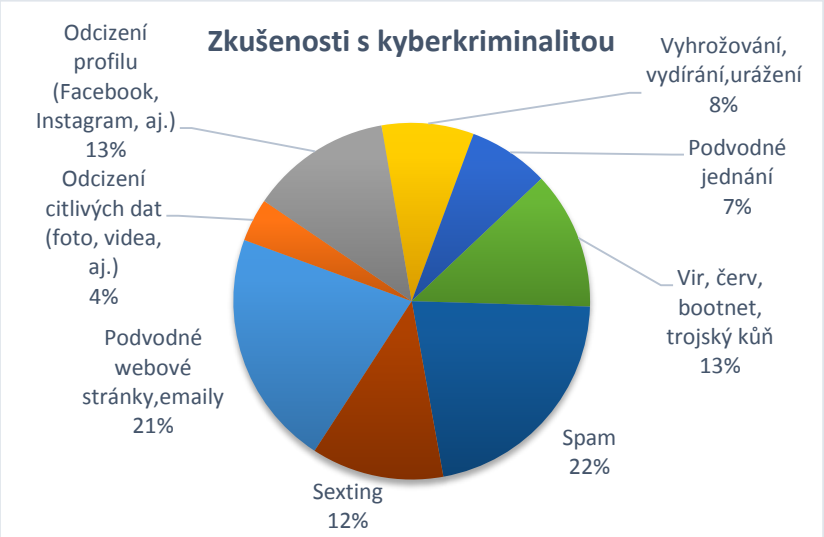
Graf 2 Vysvětlení pojmu kybernetická kriminalita [95]



[94] *Vlastní zdroj*
[95] *Vlastní zdroj*

Graf č. 2 zobrazuje, co si respondenti myslí, že je kybernetická kriminalita. Otázka byla otevřená a každý respondent mohl napsat odpověď svými slovy. Z celkových 106 dotázaných odpovědělo na otázku 68 (64,2%), 45 respondentů (66%) odpovědělo, že je to kriminalita na Internetu, 12 respondentů odpovědělo (18%), že je to ilegální činnost na Internetu, 7 respondentů (10%) odpovědělo, že to jsou podvody na Internetu a 4 respondenti (6%) odpověděli, že je to zločin na Internetu.

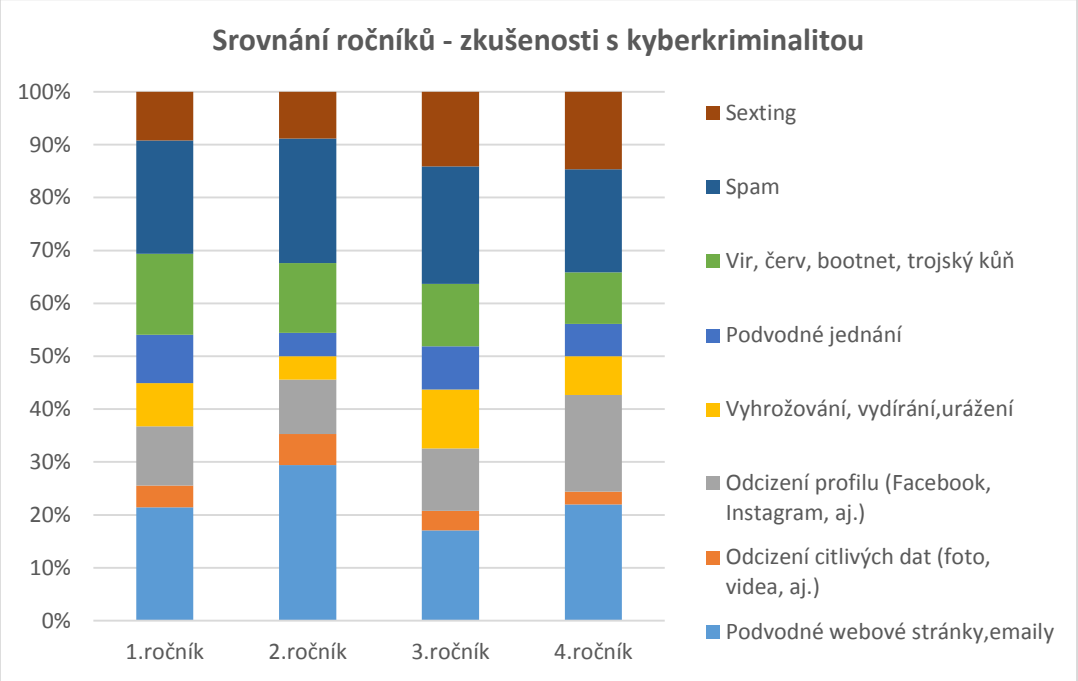
Graf 3 Zkušenosti s kyberkriminalitou [96]



Graf č. 3 vyjadřuje, jaké mají respondenti zkušenosti s kyberkriminalitou. Respondenti mohli vybrat více odpovědí. Nejčastěji se respondenti potýkali se spamem 83 respondentů (22%), následovaly podvodné webové stránky 82 respondentů (21%), poté bylo odcizení profilu 49 respondentů (13%), poté s viry, červy, bootnety a trojskými koni 48 respondentů (13%), následoval sexting 46 respondentů (12%), dále vyhrožování, vydírání a urážení 32 respondentů (8%), poté s podvodným jednáním 28 respondentů (7%). Nejméně se respondenti potýkali s odcizením citlivých dat 15 respondentů (4%).

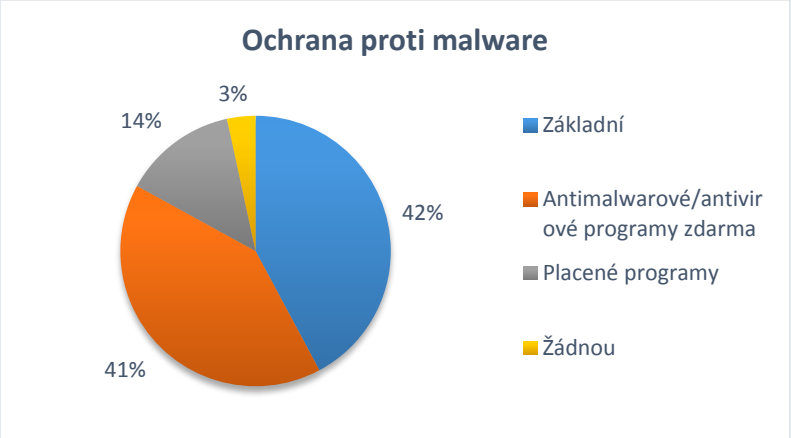
[96] *Vlastní zdroj*

Graf 4 Srovnání ročníků - zkušenosti s kyberkriminalitou [97]



Graf č. 4 vyobrazuje zkušenosti s kyberkriminalitou mezi ročníky. Z grafu je možné vypozorovat, že respondenti napříč ročníky měli velice podobné odpovědi.

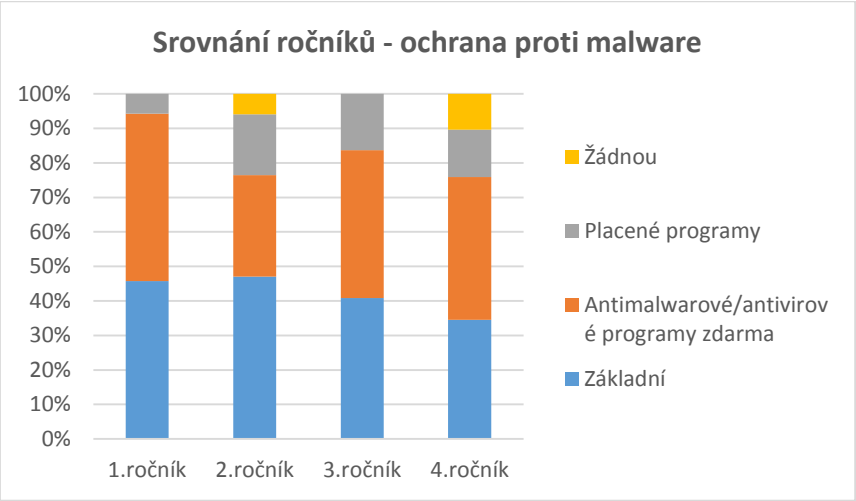
Graf 5 Ochrana proti malware [98]



Graf č. 5 znázorňuje jakou ochranu proti malware respondenti používají. Na otázku mohli respondenti vybrat více odpovědí. Nejčastěji používají respondenti základní ochranu 62 respondentů (42%), nebo antimalwarové/antivirové programy zdarma 60 respondentů (41%). Placené programy využívá 20 respondentů (14%) a pouze 5 respondentů (3%) uvedlo, že nepoužívá žádnou ochranu proti malware.

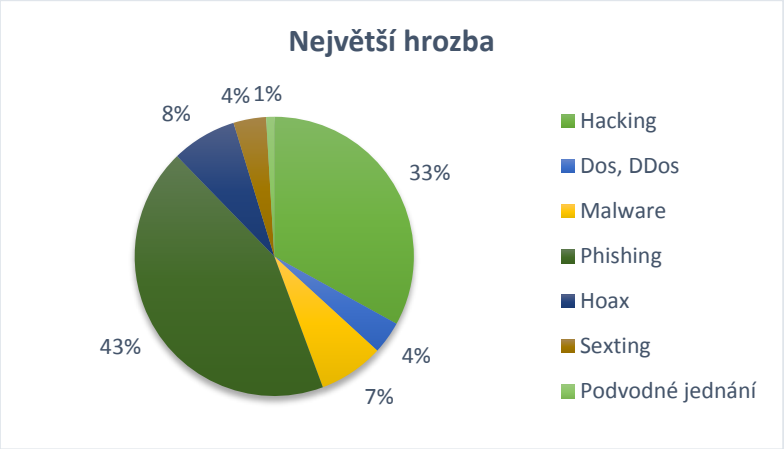
[97] *Vlastní zdroj*
[98] *Vlastní zdroj*

Graf 6 Srovnání ročníků - ochrana proti malware [99]



Graf č. 6 zobrazuje, jakou ochranu proti malware používají respondenti napříč ročníky. Respondenti odpovídali přibližně stejně až na druhý ročník, kde 2 respondenti uvedli, že nepoužívají žádnou ochranu a čtvrtý ročník, kde 3 respondenti uvedli, že také nepoužívají žádnou ochranu.

Graf 7 Největší hrozba [100]

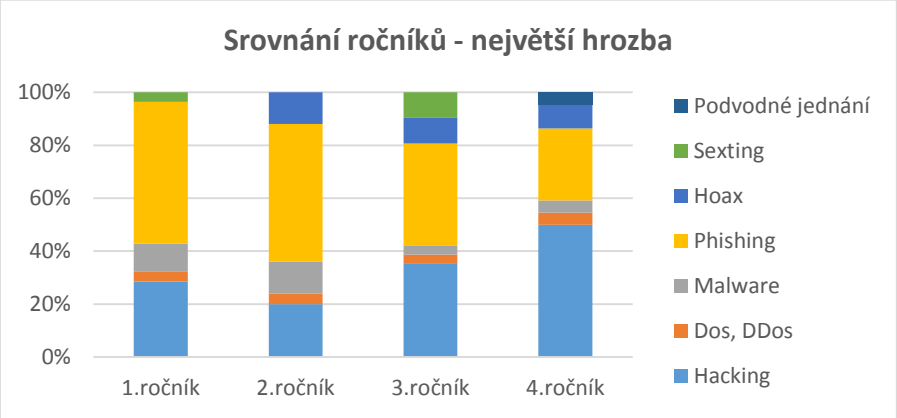


Graf č. 7 zobrazuje v jaké oblasti kyberkriminality vidí respondenti největší hrozbu. Do grafu není zahrnuta odpověď spam, protože ji žádný z respondentů nevybral. Největší hrozbu vidí respondenti ve phishingu 46 respondentů (43%). Na druhém místě je hacking, který vybralo 35 respondentů (33%), poté je hoax a malware každý po 8 respondentech (8%), 4 respondenti (4%) vybrali DoS, DDoS. Stejný počet respondentů

[99] *Vlastní zdroj*
[100] *Vlastní zdroj*

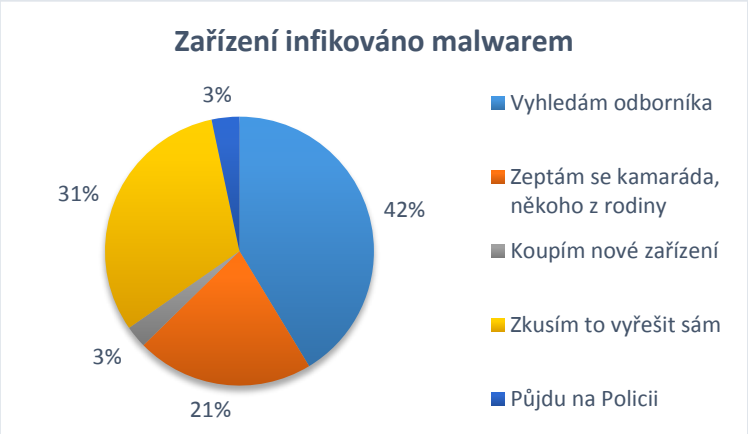
vybral sexting (4%) a pouze 1 respondent vybral jako největší hrozbu podvodné jednání (1%).

Graf 8 Srovnání ročníků - největší hrozba [101]



Graf č. 8 zobrazuje srovnání ročníků na otázku, v jaké oblasti vidí respondenti největší hrozbu. Odpovědi respondentů napříč ročníky se příliš nelišily, v 1. a 2. ročníků nejčastěji respondenti vybírali odpověď phishing, ve 3. ročníků byla nejčastější odpověď phishing, ale pouze o jednoho respondenta méně volilo hacking, ve 4. ročníků dominovala odpověď hacking.

Graf 9 Zařízení infikováno malwarem [102]

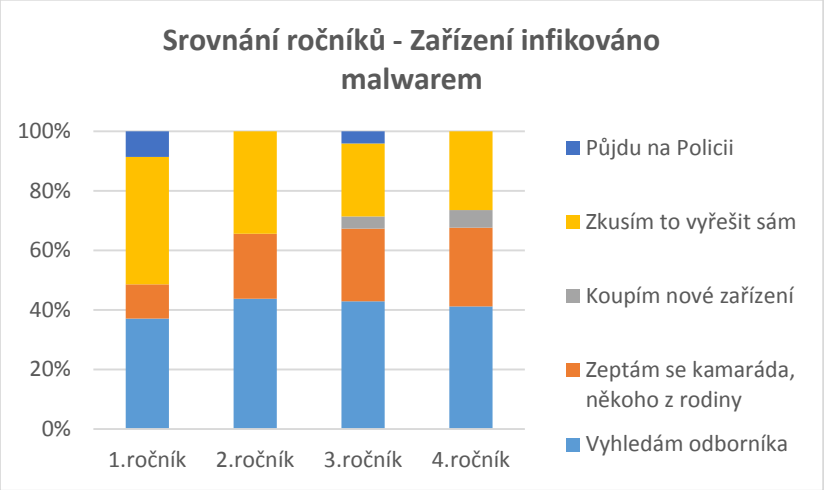


Graf č. 9 zobrazuje, jak by respondenti reagovali, pokud by jejich zařízení bylo infikováno malwarem. Respondenti mohli vybrat více odpovědí. Nejčastěji by respondenti vyhledali odborníka 62 respondentů (42%), problém by se pokusilo vyřešit samo 47 respondentů (31%). Třetí nejčastější odpověď byla zeptám se kamaráda, nebo

[101] *Vlastní zdroj*
[102] *Vlastní zdroj*

někoho z rodiny 32 respondentů (21%), pouze 5 respondentů (3%) by šlo problém řešit na policii a 4 respondenti (3%) by koupili nové zařízení.

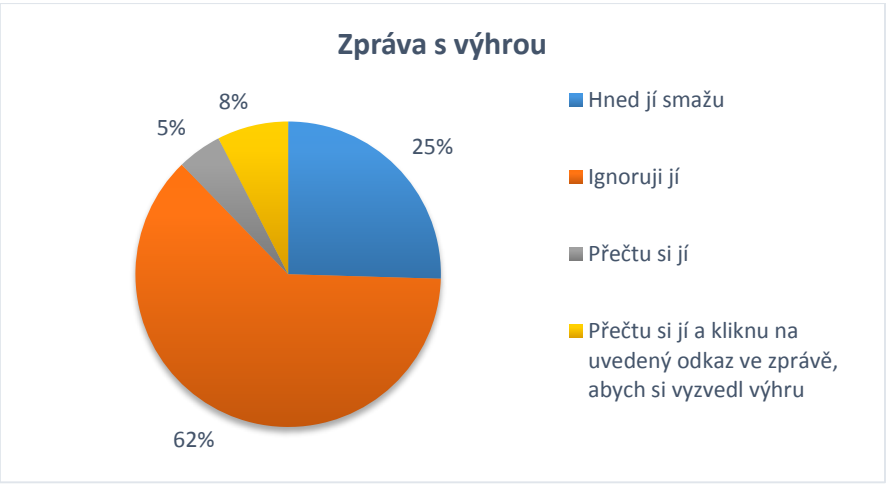
Graf 10 Srovnání ročníků - Zařízení infikováno malwarem [103]



Graf č. 10 vyjadřuje srovnání ročníků, jak by respondenti reagovali, pokud by jejich zařízení bylo infikováno malwarem. Odpovědi respondentů z druhého až čtvrtého ročníku byly velice podobné. U respondentů z prvního ročníků dominovala odpověď zkusit to vyřešit sám.

Zálohujete si data? Tak zněla otázka č. 8. 73 respondentů (69%) uvedlo, že si svá data zálohuje a 33 respondentů (31%) uvedlo, že ne.

Graf 11 Zpráva s výhrou [104]

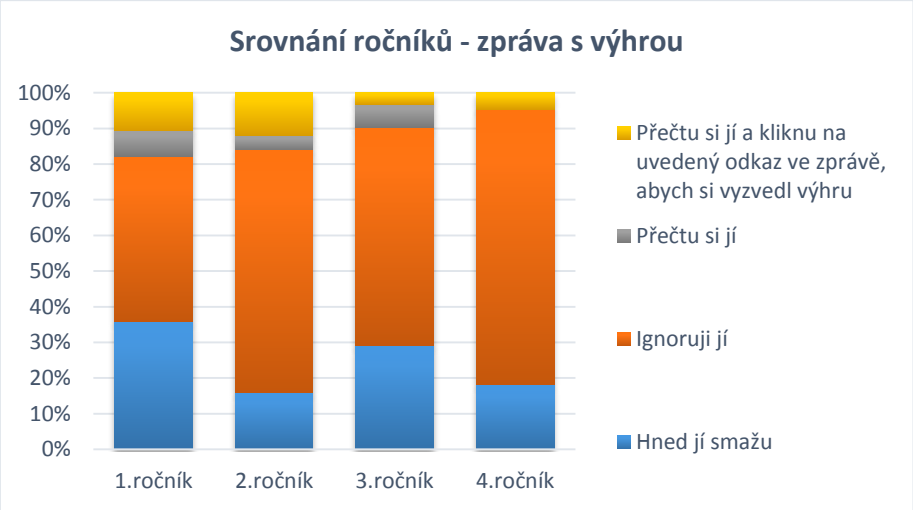


Z grafu č. 11 je možné vidět, že nejčastější odpověď na otázku, co by respondenti udělali, pokud by jim přišla zpráva, ve které stojí, že vyhráli jeden milion korun, byla, že

[103] *Vlastní zdroj*
[104] *Vlastní zdroj*

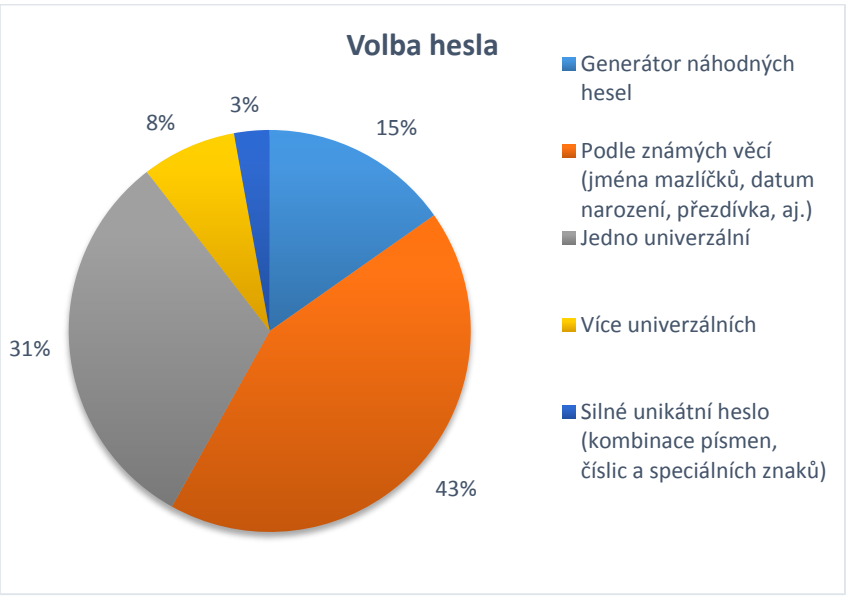
ji budou ignorovat 66 respondentů (62%), druhá nejčastější odpověď byla, že ji hned smažou 27 respondentů (25%), 8 respondentů (8%) uvedlo, že by si zprávu přečetli a klikli na uvedený odkaz ve zprávě, aby si vyzvedli výhru a 5 respondentů by si zprávu pouze přečetlo.

Graf 12 Srovnání ročníků - zpráva s výhrou [105]



Z grafu č. 12 je zřejmé, že ve všech ročnících převažovala odpověď ignorovat zprávu.

Graf 13 Volba hesla [106]

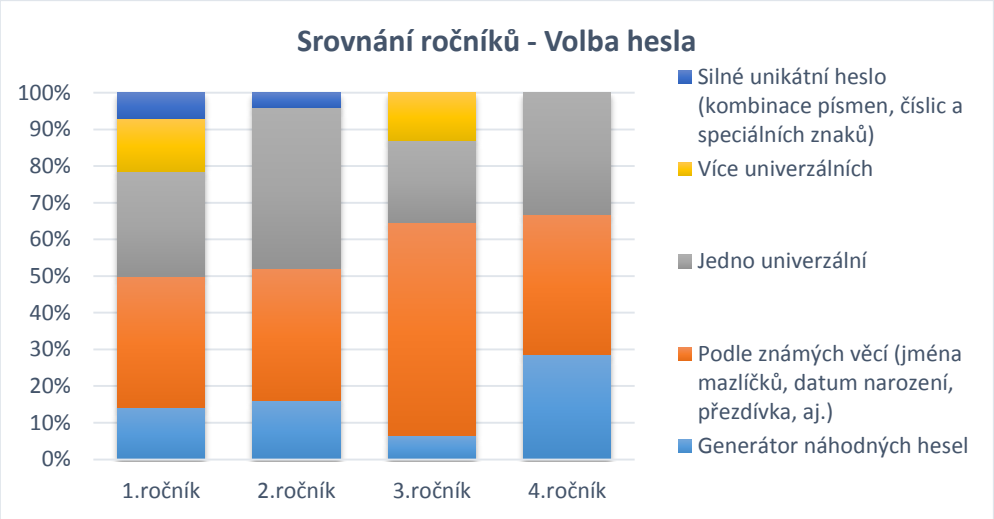


Graf č. 13 zobrazuje, jak si respondenti volí heslo. 45 respondentů (43%) uvedlo, že si volí heslo podle známých věcí, 33 respondentů (31%) má jedno univerzální, 16

[105] *Vlastní zdroj*
[106] *Vlastní zdroj*

respondentů (15%) používá pro tvorbu hesla generátor náhodných hesel a 11 respondentů zvolilo možnost jiné, kde 8 respondentů (8%) uvedlo, že používá více univerzálních a 3 respondenti (3%) uvedli, že si volí silné unikátní heslo (kombinace písmen, číslic a speciálních znaků).

Graf 14 Srovnání ročníků - volba hesla [107]



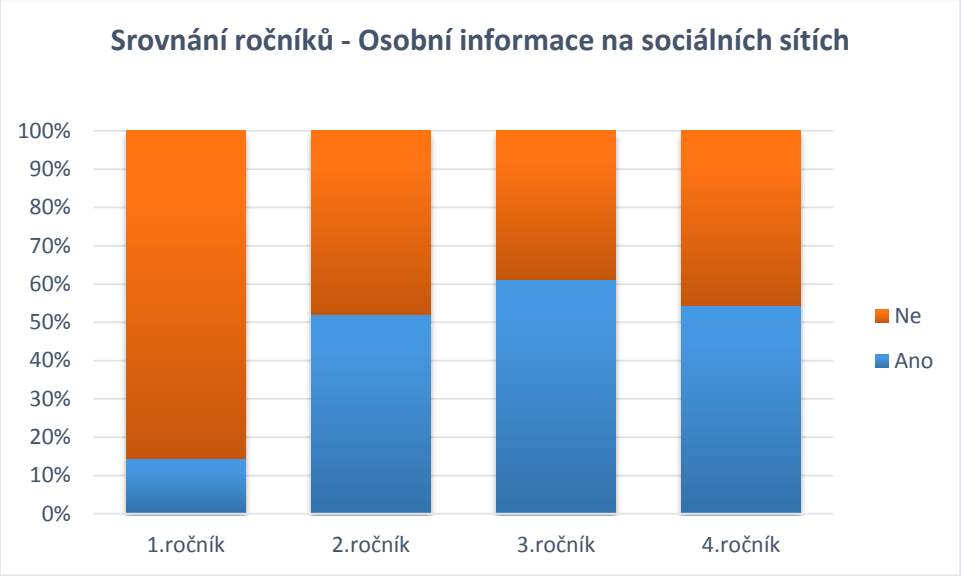
Graf č. 14 znázorňuje, jak si respondenti volí heslo napříč ročníky.

Používáte nelegální software (cracknuté hry/programy, stažené filmy, písničky,aj.)? Tak zněla otázka č. 11. 88 respondentů (83%) odpovědělo, že používá nelegální software, 18 respondentů (17%) uvedlo, že nelegální software nepoužívá.

Sdílíte osobní informace na sociálních sítích? Tak zněla otázka č. 12. 58 respondentů (55%) uvedlo, že nesdílí a 48 respondentů (45%) uvedlo, že osobní informace sdílí.

[107] *Vlastní zdroj*

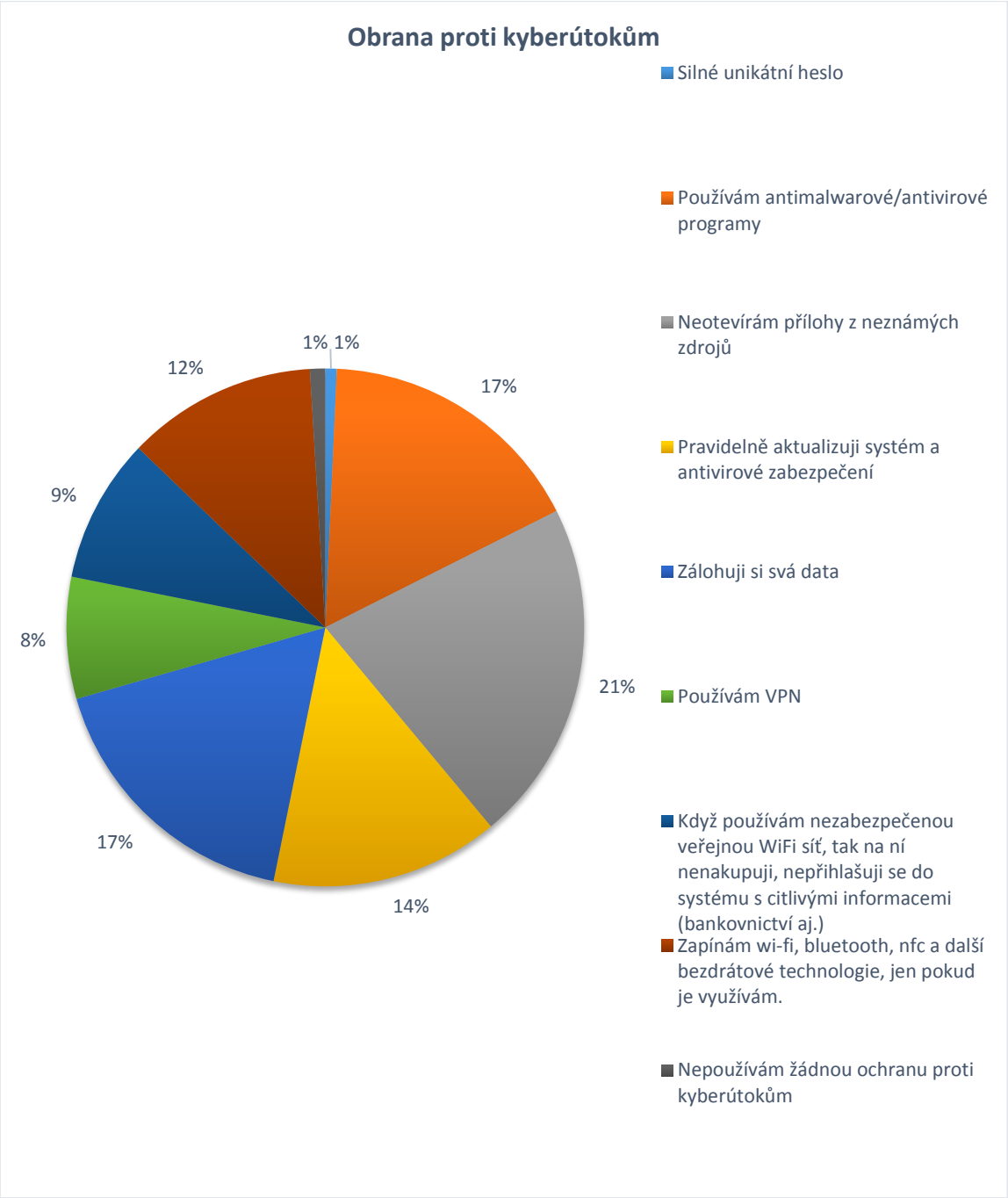
Graf 15 Srovnání ročníků - Osobní informace na sociálních sítích [108]



Graf č. 15 zobrazuje srovnání ročníků, jak respondenti sdílí osobní informace na sociálních sítích. U druhého až čtvrtého ročníku uvedlo více jak 50% respondentů, že osobní informace na sociálních sítích sdílí, zatímco u prvního ročníku to bylo pouze 14%.

[108] *Vlastní zdroj*

Graf 16 Obrana proti kyberútokům [109]

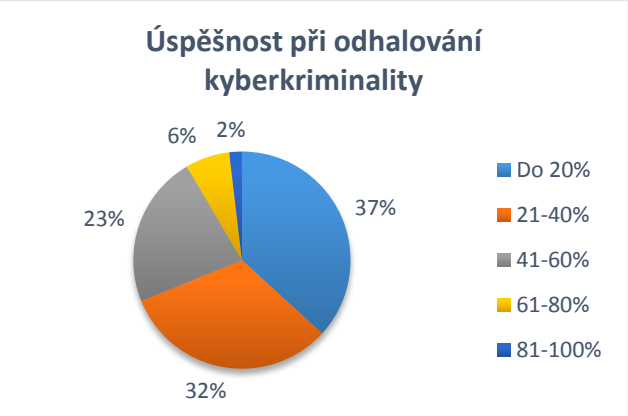


Graf č. 16 představuje, jakým způsobem se respondenti brání proti kyberútokům. Respondenti mohli vybrat více odpovědí. 90 respondentů (21%) odpovědělo, že neotevírají přílohy z neznámých zdrojů, 73 respondentů (17%) odpovědělo, že si zálohuje svá data, 71 respondentů (17%) používá antimalwarové/antivirové programy, 60 respondentů (14%) pravidelně aktualizuje systém a antivirové zabezpečení, 50 respondentů (12%) zapíná Wi-Fi, bluetooth, NFC a další bezdrátové technologie, jen

[109] *Vlastní zdroj*

pokud je využívá, 38 respondentů (9%) nenakupuje na nezabezpečené veřejné Wi-Fi a nepřihlašují se do systému s citlivými informacemi (bankovnictví aj.), 32 respondentů (8%) používá VPN, 3 respondenti (1%) mají silné unikátní heslo a pouze 4 respondenti (1%) uvedli, že nepoužívají žádnou ochranu proti kyberútokům.

Graf 17 Úspěšnost při odhalování kyberkriminality [110]



Graf č. 17 zobrazuje, jaká je podle respondentů procentuální úspěšnost při odhalování kyberkriminality. 39 respondentů (37%) odpovědělo do 20%, 34 respondentů (32%) odpovědělo 21-40%, 24 respondentů (23%) odpovědělo 41-60%, 7 respondentů (6%) odpovědělo 61-80% a 2 respondenti (2%) odpověděli 81-100%.

Měli byste zájem získávat pravidelné informace o nových hrozbách kyberkriminality a možných způsobech ochrany? Tak zněla otázka č. 15. 62 respondentů (58%) odpovědělo, že by mělo zájem dostávat pravidelné informace o nových hrozbách kyberkriminality a možných způsobech ochrany, 44 respondentů (42%) uvedlo, že by neměli zájem.

V čem byste viděli zlepšení do budoucna? Tak zněla otázka č. 16, která byla otevřená, a každý respondent mohl napsat odpověď svými slovy. Z celkových 106 dotázaných odpovědělo pouze 28 (26,4%), 20 respondentů (71%) by chtělo zlepšit základní zabezpečovací programy, 8 respondentů (29%) by chtělo více přednášek, aby si zlepšili povědomí o problematice kyberkriminality.

[110] *Vlastní zdroj*

6.2.1 Výsledky hypotéz

Stanovenou hypotézu č. 1: „Více jak 90% respondentů odpovědělo, že používá nějakou ochranu proti kyberútokům.“ definuje otázka č. 5. Tato hypotéza se potvrdila.

Stanovenou hypotézu č. 2: „Maximálně 60% respondentů uvedlo, že sdílí osobní informace na sociálních sítích“ definuje otázka č. 12. Tato hypotéza se potvrdila.

Závěr

Práce se zabývala problematikou kybernetické kriminality u studentů střední školy v Příbrami. Pomocí dotazníkového šetření se autor snažil přiblížit tento velký problém. Cílem této práce bylo zjistit, jaké mají studenti zkušenosti s kyberkriminalitou, jak je vnímána, zda vědí, jak problémy řešit popřípadě jim předejít.

Z práce vyplývá, že studenti ve všech ročnících mají téměř stejnou zkušenost s různými druhy kyberkriminality. Nejčastěji se studenti potýkali se spamem, který není tak nebezpečný, jako spíš otravný. Nejjednodušším řešením, jak se zbavit spamu je, že si zablokujete konkrétní e-mailové adresy. Na druhém místě se studenti nejvíce potýkali s podvodnými webovými stránkami nebo emaily. To už může být velký problém, protože správně provedený phishingový útok může napáchat velké škody jak materiální tak, psychické. Proti phishingu se dá bránit tak, že budete obezřetní a nebudete klikat na odkazy v nevyžádané poště, nebo na sociálních sítích, nebudete otevírat přílohy z nevyžádané pošty, nikomu nebudete sdělovat své citlivé osobní údaje, budete si všímat detailů (např. banka má webové stránky končící .cz, zatímco v podvodném emailu, který je naprosto stejný jako ten od banky s tím rozdílem že je od podvodníka, je koncovka .com) a pravidelně budete aktualizovat operační systém, prohlížeč a antivirus. Na třetím místě se studenti potýkali s viry, červy, bootnety a trojskými koni. Nejlepší obranou je mít aktualizovaný operační systém a antivirus, mít neustále zapnutý firewall a nestahovat z neznámých a neověřených zdrojů. Čtvrtým nejčastějším jevem, se kterým se studenti potýkali, byl sexting. Sexting může způsobit značné psychické problémy, které mohou vést v těch nejhorších případech až k sebevraždě, proto se musí tyto problémy řešit co nejdříve a svěřovat se s nimi. Útočníci často vyhrožují tím, že intimní fotografie zveřejní na sociálních sítích, a proto oběť často přistoupí k dalším mnohem horším skutkům. Jediná a účinná obrana proti zveřejnění sextingového obsahu je taková, že nikomu takový obsah nebudete posílat a když už opravdu musíte, nebo chcete, tak alespoň tak, aby nebylo poznat, kdo na fotografii je. Zbytek druhů kyberkriminality, se kterými se studenti potýkali, byl v řádech jednotek procent.

Dalším cílem BP bylo zjistit, jak studenti vnímají kyberkriminaltu. Jako největší hrozbu studenti vnímají phishing. Obrana proti phishingu je zmíněna o odstavec výše a jako druhé hacking. Proti hackerům je nejúčinnější ochrana portů pomocí firewallu, aby se nikudy nemohli dostat do PC a mít aktualizovaný operační systém a antivirus. Všechny druhy kyberkriminality, které měli studenti na výběr, jsou velice nebezpečné a myslím si,

že naprosto klíčovým faktorem při výběru odpovědi bylo, jak se na to daný jedinec podívá. Z pohledu jedince není například útok DoS, DDoS závažný, protože se uživateli na chvíli vypne PC a bude muset svojí práci přerušit nebo odložit na jiný den. Z pohledu např. nemocnice to je obrovský problém, protože se musí odložit naplánované operace, příjem pacientů je zpomalen atd. Proto si myslím, že ostatní druhy kriminality nebyly pří výběru odpovědí až tak oblíbené.

Dalším cílem BP bylo zjistit, zda studenti vědí, jak problémy řešit. Otázka č. 7 a 9 měla za úkol zjistit, jak by studenti jednali, pokud by jejich zařízení bylo infikováno malwarem a pokud by jim přišla zpráva/email, ve které stojí, že vyhráli milion korun. Více jak 80% studentů by si zprávu ani nepřečetlo, protože by jim bylo hned jasné, že se jedná o podvod, což nemusí být úplně pravda. Pravděpodobnost, že Vám přijde zpráva, ve které stojí, že jste vyhrál milion korun, a nebude se jednat o podvod, je mizivá, proto si myslím, že jednání více jak ¾ studentů je správné. Na otázku, jak by student reagoval, pokud by zjistil, že je jeho zařízení infikováno malwarem, všichni odpověděli, že by problém nějakým způsobem řešili, nejčastěji by vyhledali odborníka, nebo se problém pokusili vyřešit sami.

Posledním cílem bakalářské práce bylo zjistit, jestli studenti vědí jak problémům předejít. Otázky nebyly položeny přímo a byly zaměřeny na různé druhy preventivních opatření, kterými se dá útokům předejít. Otázka č. 5 zjišťovala, jakou ochranu proti malware studenti používají, 42% studentů uvedlo, že používá základní ochranu, což může být v některých případech nedostačující, 41% uvedlo, že používá freeware programy, které mají jen omezené funkce, což už je lepší druh obrany, ale proti sofistikovanějším druhům útoku to může být stále málo, 14% uvedlo, že používá placené programy s dostupností všech funkcí, co daná aplikace nabízí, to je ta nejlepší možná volba ochrany, ale ne každý si ji může dovolit a pouze 3% uvedli že nepoužívají žádnou ochranu, nebo o ní nevědí. To je ta nejhorší možná varianta a vystavují se tím zbytečnému bezpečnostnímu riziku. Otázka č. 10 měla za úkol zjistit, jak si studenti volí heslo. 43% uvedlo, že si volí heslo podle známých věcí, jako jsou například jména mazlíčků, datum narození aj., to je považováno za velmi slabé heslo, protože propracovaný útok s použitím sociálního inženýrství ho velmi snadno a rychle odhalí. 31% uvedlo, že používá jedno univerzální heslo. Většina útočníku potom, co uhádne heslo k jednomu účtu, ho hned vyzkouší na jiný účet v naději, že uživatel používá stejné heslo i k jiným účtům. Proto i tato varianta je nedostačující. 8% má více hesel. 15% používá generátor náhodných hesel

a 3% používají silné unikátní heslo, to je za mě ta nejlepší možná varianta, jak si zvolit heslo. Možností, jak si zvolit heslo je mnoho, samozřejmě si nejde zapamatovat 50 silných unikátních hesel, ale existují password managery, do kterého si stačí zapamatovat pouze jedno silné heslo a zbytek bude uložený tam. Otázka č. 13 měla za úkol zjistit, jakým způsobem se studenti brání proti kyberútokům. 99% dotázaných se nějakým způsobem brání, v čemž shledávám značné pozitivum, protože tím dávají najevo, že je pro ně kyberútok velkou hrozbou a snaží se před ním chránit.

Závěrem je nutno říci, že svět IT se rozvíjí neskutečným tempem a přináší s sebou spoustu nových hrozeb, které je třeba eliminovat. Určitě by bylo vhodné, aby se na školách pořádalo více přednášek na tuto problematiku, aby studenti mohli včas a správně reagovat na tyto hrozby.

Literární zdroje

1. BÁRTA, J., *Úvod do počítačových sítí*. České Budějovice: KOPP, 1997, 204 s. ISBN: 80-7232-002-5.
2. BURDA, K. *Kryptografie okolo nás.* Praha: CZ.NIC z. s. p. o., 2019, 131 s. ISBN 978-80-88168-52-2
3. DEPARTMENT OF DEFENSE U.S. ARMY. *Joint Publication 1-02 Dictionary of Military and Associated Terms*. 2016. 480 s.
4. DOSTÁLEK, L., KABELOVÁ, A., *Velký průvodce protokoly TCP/IP a systémem DNS 5. vydání.* Brno: Computer Press a. s., 2012, 488 s. ISBN: 978-80-251-2236-5.
5. FEREBAUEROVÁ, R., PEKÁREK, O. *Aplikovaná informatika*. 1. vydání. České Budějovice: Vysoká škola evropských a regionálních studií, 2014, 151 s. ISBN 978-80-87472-74-3.
6. GIBSON, W. *Neuromancer*. New york: Berkley Publishing Group, 1984, 271 s. ISBN: 0-441-56958-7.
7. JIRÁSEK, P., NOVAK L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti*. Praha: Policejní akademie ČR, 2015, 240 s. ISBN 978-80-7251-436-6.
8. JIRÁSEK, P., NOVAK L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti*. Praha: Policejní akademie ČR, 2013, 200 s. ISBN 978-80-7251-397-0.
9. JIROVSKÝ, V., *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, 2007, 284 s. ISBN: 978-80-247-1561-2.
10. JOHNSON, A. *31 Days Before Your CCNA Exam. New Jersey:* Cisco Press, 2020, 862 s. ISBN: 978-0-13-596408-8
11. KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC z. s. p. o., 2016. 524 s. ISBN 978-80-88168-15-7.
12. KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity*. Praha: CZ.NIC z. s. p. o., 2019, 560 s. ISBN 978-80-88168-31-7.
13. MATĚJKA, M. *Počítačová kriminalita*. Praha: Computerpress, 2002, 106 s. ISBN: 80-722-6419-2.

14. PUŽMANOVÁ, R., *Moderní komunikační sítě od A do Z 2. vydání*. Brno: Computer Press a. s., 2006, 430 s. ISBN: 80-251-1278-0.
15. SANTOS, O., *Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide.* New Jersey: Cisco Press, 2021. 668 s. ISBN: 01-3680-783-6.
16. SATRAPA, P., *IPv6 Internetový protokol verze 6 4. vydání*. Praha: CZ.NIC z. s. p. o., 2019, 460 s. ISBN: 978-80-88168-46-1.
17. SMEJKAL, V. *Kybernetická kriminalita. 2. rozšířené a aktualizované vydání*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, 936 s. ISBN 978-80-7380-720-7.
18. SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. ISBN 978-80-7380-501-2.
19. SMEJKAL, V., SOKOL T., VLČEK, M. *Počítačové právo.* Praha: C. H. Beck, 1995, 264 s. ISBN 80-7179-009-5.

Elektronické zdroje

1. *Akční plán 2015-2020* [online] 2015 [cit. 2022-20-01]. Dostupné z WWW: < https://www.govcert.cz/download/gov-cert/container-nodeid967/akc48dnc3adplc3a1n-rkb-final-150408.pdf. >
2. *Akční plán 2020-2025* [online] 2020 [cit. 2022-20-01]. Dostupné z WWW: < https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/ >
3. *Antivir* [online]. [cit. 2022-23-01]. Dostupné z WWW: < http://iki.ktkadan.cz/soubory/viry_antiviry.pdf >
4. *Doporučení* [online]. [cit. 2022-23-01]. Dostupné z WWW: < https://www.nukib.cz/cs/infoservis/doporuceni/>
5. *ISO/OSI model* [online]. 2019 [cit. 2022-12-01]. Dostupné z WWW: < http://matureplus.4fan.cz/pos/3-model-isoosi-vrstvy >
6. *Klient-server* [online]. 2018 [cit. 2022-09-01]. Dostupné z WWW: < https://www.napocitaci.cz/33/peer-to-peer-p2p-site-uniqueidgOkE4NvrWuNY54vrLeM679zvh6YhHnhkpLpGVMy1prA/ >
7. *Koncepce boje proti organizovanému zločinu* [online] 2000 [cit. 2022-02-01]. Dostupné z WWW: < https://www.dataplan.info/img_upload/7bdb1584e3b8a53d337518d988763f8d/koncepce-boje-proti-org.zlocinu.pdf >.

8. *Koncepce boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření* [online] 2000 [cit. 2022-14-01]. Dostupné z WWW: <http://www.mvcr.cz/soubor/koncepce-pdf.aspx >.
9. *LAN* [online]. 2021 [cit. 2022-06-01]. Dostupné z WWW: < https://www.guru99.com/types-of-computer-network.html >
10. *Národní strategie informační bezpečnosti ČR* [online] 2005 [cit. 2022-12-01]. Dostupné z WWW: < https://moodle.unob.cz/pluginfile.php/20182/mod_resource/content/1/Národní%20strategie%20informační%20bezpečnosti%20ČR.pdf >.
11. *Národní strategie pro oblast kybernetické bezpečnosti ČR 2015-2020* [online] 2015 [cit. 2022-20-01]. Dostupné z WWW: < https://www.govcert.cz/download/gov-cert/container-nodeid998/nskb-150216-final.pdf. >.
12. *Národní strategie pro oblast kybernetické bezpečnosti ČR 2020-2025* [online] 2020 [cit. 2022-20-01]. Dostupné z WWW: < https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/ >.
13. *Peer-to-peer* [online]. 2018 [cit. 2022-08-01]. Dostupné z WWW: < https://www.napocitaci.cz/33/peer-to-peer-p2p-site-uniqueidgOkE4NvrWuNY54vrLeM679zvh6YhHnhkpLpGVMy1prA/ >
14. POLČÁK, L., *Základní informace o síti Tor*. [online]. Brno: VÚT FIT, 2017. [cit. 2022-05-01]. Dostupné z WWW: < >.
15. *Rozdělení kyberprostoru* [online]. 2018 [cit. 2022-04-01]. Dostupné z WWW: < https://hackernoon.com/wtf-is-dark-web-358569fde822 >
16. *Státní informační a komunikační politika e-Česko 2006* [online] 2004 [cit. 2022-12-01]. Dostupné z WWW: < https://www.esfcr.cz/documents/21802/761522/Státní+informační+a+komunikační+politika/9a6117ea-24a8-484f-8d08-07365057e12b >.
17. *Strategie pro oblast kybernetické bezpečnosti ČR 2011-2015* [online] 2011 [cit. 2022-17-01]. Dostupné z WWW: < https://www.databaze-strategie.cz/cz/cr/strategie/strategie-pro-oblast-kyberneticke-bezpecnosti-cr-2011-2015?typ=struktura >.

18. *Vývoj kybernetické kriminality a kriminality páchané na Internetu* [online]. 2021 [cit. 2022-13-01]. Dostupné z WWW: < https://www.policie.cz/clanek/kyberkriminalita.aspx >
19. *WAN* [online]. 2021 [cit. 2022-07-01]. Dostupné z WWW: < https://www.guru99.com/types-of-computer-network.html >

Legislativní dokumenty

1. ČESKO. VLÁDA. *Usnesení vlády č. 205 ze dne 15. března 2010 o řešení problematiky kybernetické bezpečnosti České republiky*, Dostupné z WWW: < https://apps.odok.cz/attachment/-/down/KORN97BQ9ASZ >.
2. ČESKO. VLÁDA. *Usnesení vlády č. 781 ze dne 19. října 2011 o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast*, Dostupné z WWW: < https://apps.odok.cz/attachment/-/down/KORN97BUKZ3E >.
3. ČESKO. zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In *Sbírka zákonů České republiky*. 2014. Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/2014-181>
4. ČESKO. zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů. In *Sbírka zákonů České republiky*. 1999. Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/1999-106>
5. ČESKO. zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů. In *Sbírka zákonů České republiky*. 2000. Dostupné z WWW: < https://www.zakony.cz/zakony/2000/101/zakon-121-2000-Sb-SB2000121 >
6. ČESKO. zákon č. 240/2000 Sb., o krizovém řízení a změně některých zákonů (krizový zákon), ve znění pozdějších předpisů. In *Sbírka zákonů České republiky*. 2000. Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/2000-240>
7. ČESKO. zákon č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů. In *Sbírka zákonů České republiky*. 2000. Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/2000-365>

8. ČESKO. zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů. In *Sbírka zákonů České republiky*. 2004. Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/2004-480>
9. ČESKO. zákon č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů. In *Sbírka zákonů České republiky*. 2005. Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/2005-127>
10. ČESKO. zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. In *Sbírka zákonů České republiky*. 2005. Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/2005-412>
11. ČESKO. zákon č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů. In *Sbírka zákonů České republiky*. 2006. Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/2006-69>
12. ČESKO. zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů. In *Sbírka zákonů České republiky*. 2008. Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/2008-300>
13. ČESKO. zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. In *Sbírka zákonů České republiky*. 2009. Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/2009-40>
14. ČESKO. zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů. In *Sbírka zákonů České republiky*. 2009. Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/2009-111>
15. ČESKO. zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim. In *Sbírka zákonů České republiky*. 2011. Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/2011-418>
16. ČESKO. zákon č. 89/2012 Sb., občanský zákoník. In *Sbírka zákonů České republiky*. 2012. Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/2012-89>

17. ČESKO. zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce. In *Sbírka zákonů České republiky*. 2016. Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/2016-297>
18. ČESKO. VLÁDA. nařízení vlády č. 522/2005 Sb., kterým se stanoví seznamy utajovaných informací, ve znění pozdějších předpisů. 2005. Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/2005-522>
19. ČESKO. vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění pozdějších předpisů. 2005. Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/2005-523>
20. ČESKO. vyhláška č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy). 2006. Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/2006-529>
21. ČESKO. VLÁDA. nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. 2010. Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/2010-432>
22. ČESKO. vyhláška 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů. 2012. Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/2012-357>
23. ČESKO. vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. 2014. Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/2014-317>
24. ČESKO. vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby. 2017. Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/2017-437>
25. ČESKO. vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). 2018. Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/2018-82>

26. ČESKO. Ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů. 1993 Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/1993-1>
27. ČESKO. Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů. 1993 Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/1993-2>
28. ČESKO. Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky. 1998 Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/1998-110>

Seznam zkratek

AP	Access Point
CD	Compact Disk
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity, Availability. (Důvěrnost, Integrita, Dostupnost)
DARPA	Defense Advanced Research Projects Agency
DDoS	Distributed denial of service
DMZ	Demilitarized zone
DNS	Domain Name System. Hierarchický systém doménových jmen
DoS	Denial of service
DVD	Digital Video Disc
EIGRP	Enhanced Interior Gateway Routing Protocol
EU	Evropská unie
FBI	Federal Bureau of Investigation
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol. Internetový protokol určený pro výměnu hypertextových dokumentů ve formátu HTML.
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Informačni a komunikačni technologie
IDS	Intrusion detection system
IPS	Intrusion Prevention System
IP	Internet Protocol
IS	Informační systém
IT	Informační technologie
KII	Kritická informační infrastruktura

LAN	Local Area Network
LLC	Logical Link Control
MAC	Media Access Control
MAN	Metropolitan Area Network
MMS	Multimedia Messaging Service
NAT	Network Adress Translation. Překlad síťových adres.
NBÚ	Národní bezpečnostní úřad
NFC	Near Field Communication
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OSPF	Open Shortest Path First
P2P	Peer-to-peer
PAN	Personal Area Network
PC	Personal Computer. Osobní počítač.
PDA	Personal Digital Assistant
PIN	Personal identification number
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
RAM	Random Access Memory
SIP	Session Initiation Protocol
SMS	Short message service
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol over Internet Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus
VIS	Významné informační systémy

VLAN	Virtual Local Area Network
VPN	Virtuální privátní síť
WAN	Wide Area Network
ZoKB	Zákon o kybernetické bezpečnosti

Seznam obrázků

Obrázek 1 Vývoj kybernetické kriminality mezi lety 2011-2019 13
Obrázek 2 Sofistikovanost programů proti technickým znalostem uživatele 13
Obrázek 3 Sofistikovanost programů proti technickým znalostem uživatele 14
Obrázek 4 Rozdělení kyberprostoru 16
Obrázek 5 LAN 19
Obrázek 6 WAN 19
Obrázek 7 Peer-to-peer 20
Obrázek 8 Klient-server 21
Obrázek 9 ISO/OSI model 21
Obrázek 10 Fyzická adresa 22
Obrázek 11 TCP/IP model 24

Seznam grafů

Graf 1 Pohlaví 47
Graf 2 Vysvětlení pojmu kybernetická kriminalita 47
Graf 3 Zkušenosti s kyberkriminalitou 48
Graf 4 Srovnání ročníků - zkušenosti s kyberkriminalitou 49
Graf 5 Ochrana proti malware 49
Graf 6 Srovnání ročníků - ochrana proti malware 50
Graf 7 Největší hrozba 50
Graf 8 Srovnání ročníků - největší hrozba 51
Graf 9 Zařízení infikováno malwarem 51
Graf 10 Srovnání ročníků - Zařízení infikováno malwarem 52
Graf 11 Zpráva s výhrou 52
Graf 12 Srovnání ročníků - zpráva s výhrou 53

Graf 13 Volba hesla 53
Graf 14 Srovnání ročníků - volba hesla 54
Graf 15 Srovnání ročníků - Osobní informace na sociálních sítích 55
Graf 16 Obrana proti kyberútokům 56
Graf 17 Úspěšnost při odhalování kyberkriminality 57

Seznam příloh

Příloha č. I. – Formulář dotazníkového šetření 73

Příloha č. I. – Formulář dotazníkového šetření

Milí respondenti.

Jsem student třetího ročníku Vysoké školy evropských a regionálních studií v Příbrami, obor Bezpečnostně právní činnost. Rád bych Vás tímto požádala o vyplnění následujícího dotazníku, který je určen lidem různých věkových kategorií a ve kterém se zaměřuji na průzkum jejich znalostí a názorů, tykajících se kyberkriminality. Výsledky dotazníkového šetření jsou anonymní a budou sloužit výhradně jako podklad k vypracování mé bakalářské práce na téma: „Informovanost studentů Střední průmyslové školy a Vyšší odborné školy v Příbrami o problematice kybernetické kriminality“.

Děkuji Vám za ochotu David Klemš

1. Pohlaví
   - ◯ Muž
   - ◯ Žena
   - ◯ Jiné: _____

2. Studovaný ročník
   - ◯ První
   - ◯ Druhý
   - ◯ Třetí
   - ◯ Čtvrtý

3. Víte co znamená pojem kybernetická kriminalita? (pokud ano, zkuste jednoduše vysvětlit)

_____

4. Jaké máte zkušenosti s kyberkriminalitou? *Zaškrtněte všechny platné možnosti.*

- [ ] Podvodné webové stránky, emaily
- [ ] Odcizení citlivých dat (foto, videa, aj.)
- [ ] Odcizení profilu (Facebook, Instagram, aj.)
- [ ] Vyhrožování, vydírání, urážení
- [ ] Podvodné jednání
- [ ] Vir, červ, bootnet, trojský kůň
- [ ] Spam
- [ ] Sexting (zprávy se sexuálním obsahem)
- [ ] Jiné: _____

5. Jakou ochranu proti malware (malware = škodlivý program, např. viry, sledovací programy, aj.) používáte? *Zaškrtněte všechny platné možnosti.*

- [ ] Základní (součást továrního nastavení)
- [ ] Antimalwarové/antivirové programy zdarma (freeware)
- [ ] Placené programy (premium verze)
- [ ] Žádnou
- [ ] Jiné:

6. V jaké oblasti kyberkriminality vidíte největší hrozbu? *Označte jen jednu elipsu.*

- ◯ Hacking (získání neoprávněného přístupu do zařízení)
- ◯ Dos, DDos (odepření služby, znefunkční a znepřístupní např. server)
- ◯ Malware (škodlivé programy, např. viry, sledovací programy, aj.)
- ◯ Phishing (podvodné stránky, jejíž cílem je získat informace, jako jsou např. uživatelské jméno, heslo, číslo kreditní karty, PIN)
- ◯ Hoax (zpráva, která se snaží šířit paniku)
- ◯ Spam
- ◯ Sexting (zprávy se sexuálním obsahem)
- ◯ Podvodné jednání

Jiné: _____

7. Co byste dělali pokud by jste zjistili, že je Vaše zařízení infikováno malwarem ? (malware = škodlivý program, např. viry, sledovací programy, aj.) *Zaškrtněte všechny platné možnosti.*

- [ ] Vyhledám odborníka
- [ ] Zeptám se kamaráda, nebo někoho z rodiny
- [ ] Koupím nové zařízení
- [ ] Zkusím to vyřešit sám
- [ ] Půjdu na Policii
- [ ] Jiné:

8. Zálohujete si data? *Označte jen jednu elipsu.*

- Ano
- Ne

9. Pokud Vám přijde zpráva/email, ve které stojí, že jste vyhrál milion korun, co s ní uděláte? *Označte jen jednu elipsu.*

- Hned ji smažu
- Ignoruji jí
- Přečtu si jí
- Přečtu si ji a kliknu na uvedený odkaz ve zprávě, abych si vyzvedl výhru

10. Jak si volíte heslo? *Označte jen jednu elipsu.*

- Generátor náhodných hesel
- Podle známých věcí (jména mazlíčků, datum narození, přezdívka, aj.)
- Jedno univerzální

Jiné:

11. Používáte nelegální software? (cracknuté hry/programy, stažené filmy, písničky, aj.) *Označte jen jednu elipsu.*

- Ano
- Ne

12. Sdílíte osobní informace na sociálních sítích? *Označte jen jednu elipsu.*

Ano

Ne

13. Jakým způsobem se bráníte proti kyberútokům? *Zaškrtněte všechny platné možnosti.*

Silné unikátní heslo (Silné heslo: minimálně 8 znaků, kombinace písmen, číslic a speciálních znaků.) (Unikátní heslo: použito pro přístup pouze k jednomu účtu nebo zařízení.)

Používám antimalware/antivirové programy

Neotevírám přílohy z neznámých zdrojů

Pravidelně aktualizuji systém a antivirové zabezpečení

Zálohuji si svá data

Používám VPN

Když používám nezabezpečenou veřejnou Wi-Fi síť, tak na ní nenakupuji, nepřihlašuji se do systému s citlivými informacemi (bankovnictví aj.)

Zapínám Wi-Fi, bluetooth, NFC a další bezdrátové technologie, jen pokud je využívám. Nezveřejňuji o sobě na Internetu žádné citlivé informace

Nepoužívám žádnou ochranu proti kyberútokům

14. Jaká je dle Vašeho názoru procentuální úspěšnost při odhalování kyberkriminality? *Označte jen jednu elipsu.*

Do 20%

21-40%

41-60%

61-80%

81-100%

15. Měli byste zájem získávat pravidelné informace o nových hrozbách kyberkriminality a možných způsobech ochrany? *Označte jen jednu elipsu.*

Ano

Ne

16. V čem byste viděli zlepšení do budoucna?