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

BAKALÁŘSKÁ PRÁCE

NOVÉ TRESTNÉ ČINY - KYBERKRIMINALITA

Autor práce: Jiří Kopecký, DiS.

Studijní obor: Bezpečnostně právní činnost ve veřejné správě

Forma studia: Kombinovaná

Vedoucí práce: Ing. Mgr. Martin Černý

Katedra: Právních oborů a bezpečnostních studií

2020

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

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Jiří Kopecký

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

Název bakalářské práce: Nové trestné činy - kyberkriminalita

Název bakalářské práce v anglickém jazyce: New crimes - cybercrime

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, titul): Ing Mgr. Martin Černý

Datum zadání bakalářské práce: říjen 2019

CÍL BAKALÁŘSKÉ PRÁCE:

Hlavním cílem teoretické části bakalářské práce je vytvořit ucelený přehled o možnostech páchání kyberkriminality a její řešení českým a evropským právem. Mezi cíle bakalářské práce bude dále patřit zjištění, jakým způsobem veřejnost vnímá nebezpečí kyberkriminality, se kterým druhem se nejčastěji setkává a jak tuto hrozbu řeší. Zjištění těchto informací bude provedeno formou dotazníkového šetření a získané poznatky budou nadále vyhodnoceny a graficky znázorněny v empirické části. Vedlejším cílem je upozornit na nebezpečí a rozmanitost této trestné činnosti.

Student: Jiří Kopecký	4.11.2019 *datum*	 *podpis*
Vedoucí práce: Ing. Mgr. Martin Černý	*datum*	*podpis*

Ing. Mgr. Martin Černý
Digitálně podepsal Ing. Mgr. Martin Černý
Datum: 2019.11.04 06:23:44 +01'00'

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	19.11.19 *datum*	 *podpis*
Prorektorka pro studium a vnitřní záležitosti: RNDr. Růžena Ferebauerová	19.11.19 *datum*	 *podpis*
Pověřený rektor: doc. Ing. Jiří Dušek, Ph.D.	23.11.2019 *datum*	 *podpis*

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z.ú. ČESKÉ BUDĚJOVICE -2-

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 vedoucího 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 Ing. Mgr. Martinovi Černému za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

KOPECKÝ, J. *Nové trestné činy - kyberkriminalita: bakalářská práce.* České Budějovice : Vysoká škola evropských a regionálních studií, 2020. 67 s. Vedoucí bakalářské práce : Ing. Mgr. Martin Černý.

Klíčová slova: kyberkriminalita, internet, hacker, počítačový systém

Bakalářská práce pojednává o problematice nových forem trestných činů – kyberkriminality. Jejím cílem je seznámit se základy kyberkriminality a analyzovat, nakolik si lidé uvědomují rizika napadení jejich počítačových systémů a zda jsou ochotni investovat peněžní prostředky do ochrany svých dat.

Bakalářskou práci tvoří dvě části – teoretická a praktická. Teoretická část objasňuje základní pojmy kyberkriminality a popisuje některé druhy kybernetických útoků. Dále se věnuje základní evropské a české legislativě, která určuje a řeší, v jakých případech se jedná o kyberkriminalitu. Praktická část bakalářské práce zjišťuje, pomocí dotazníkového šetření, jak jsou v kyberprostoru uživatelé obezřetní ohledně kybernetických útoků a s jakými útoky mají sami zkušenost, případně jak tyto útoky řeší. Zjištěné poznatky jsou shrnuty v navrhovaných doporučeních.

ABSTRACT

KOPECKÝ, J. *New Crimes – Cybercrime : Bachelor Thesis.* České Budějovice : The College of European and Regional Studies, 2020. 67 p. Supervisor : Ing. Mgr. Martin Černý

Key words: cybercrime, internet, hacker, computer system

The bachelor thesis deals with the problematics of a new kind of crime – cybercrime. The goal is to get acquainted with basics of cybercrime and to analyse how much people realise the risks for their computers of being attacked and if they are willing to make investments to protect their data. The bachelor thesis consist of two parts – theoretical and practical.

The theoretical part clarifies basic terms of cybercriminality and describes some kinds of cybernetic attacks. Furthermore, it is dedicated to the basic european and czech legislation defining and solving the cases which are already understood as cybercrimes. Through a survey the practical part observes the discretion of the users in cyberspace regarding the cybernetic attacks and potentional experience of the users and how they proctect themselves. Gathered information is summarized into suggested recommendations.

Obsah

Úvod

V dnešní době bez velké nadsázky můžeme říct, že jakákoliv osoba může během dne udělat cokoliv. A jak je to možné? Možné je to rychlým nástupem a rozšířením moderních technologií, které nás obklopují skoro na každém kroku. Většina moderních technologií, která vznikla a stále vzniká je vytvářena především s úmyslem usnadnění každodenního života obyvatel této planety. Vždy se ovšem najdou osoby, které tyto moderní technologie nechtějí využívat jen za původním účelem pro které vznikly, ale začnou moderní technologie zneužívat k páchání různorodé nezákonné činnosti.

Proto cílem této bakalářské práce (dále jen „práce“) je upozornit na problematiku, která se týká v současné době většiny světové populace. Tento problém, který je v celosvětovém měřítku stále aktuálnější se nazývá kyberkriminalitou.

Člověk nejnovější technologie kolem sebe už ani nevnímá a bere je jako naprostou samozřejmost, která patří k jeho každodennímu životu. Používá je téměř při jakékoliv činnosti jako je relaxace, sport, výběr financí z bankomatu, platba v obchodech platební kartou, nakupování na internetu, používání tzv. chytrých telefonů a s nimi spojených aplikací, používání počítače v práci atd. Už si ani nepřipouštíme svou závislost na těchto technologiích a vzájemném propojení jednotlivých technologií mezi sebou.

Uživatel si mnohokrát ani neuvědomuje, kde všude musí zadávat své soukromé údaje, aby mohl moderní technologie využívat. A právě zde vzniká dané riziko, jelikož každý krok návštěvníka kyberprostoru je zaznamenáván a následně je snadno dohledatelný a zneužitelný. Rozhraní mezi tím, zda se někdo stane či nestane obětí kyberkriminality a zda bude úspěšným či neúspěšným pachatelem, závisí pouze na zkušenostech, znalostech a dovednostech jednotlivých uživatelů, kteří jsou na různých úrovních využívání moderních technologií. Pachatelé především využívají velké anonymity prostředí, rychlosti páchané trestné činnosti, která není omezena žádnou vzdáleností a následného špatného dohledávání a prokazování trestné činnosti dané osobě.

Jednou z hlavních obran uživatele proti pachatelům kyberkriminality by mělo být preventivní předcházení těmto útokům např. zakoupením antivirových programů, navštěvování pouze zabezpečených webových stránek, nereagovat na nevyžádanou elektronickou poštu, a především využívat sociální sítě s rozumem a maximální opatrností. Pokud k takovému útoku již dojde, neignorovat jej a situaci se snažit řešit. K tomuto by měl velkou měrou dopomáhat stát jak preventivním prováděním osvěty veřejnosti, tak správně nastavenou legislativou, která umožní řešit trestné činy kyberkriminality rychleji a snadněji.

1 Cíl a metodika bakalářské práce

Kyberkriminalita je fenoménem dnešní doby a mnoho lidí si neuvědomuje její sílu, rozmanitost a flexibilitu. Právě proto by měla tato práce prostřednictvím sběru informací především z odborné literatury poukázat na možnosti páchání kybekriminality a její dopady na oběti této trestné činnosti. Teoretická část má za cíl seznámit čtenáře s touto problematikou, kde budou především vymezeny a vysvětleny základní pojmy objektu zkoumání a budou představeny možnosti a styly jednotlivých druhů kyberktiminality. Dále se práce bude věnovat základní evropské a české legislativní úpravě a též bude zaměřena na základní rozdělení kybernetických útoků a protiprávních jednání.

Empirická část práce bude zaměřena na širokou veřejnost a formou kvantitativního šetření by měla ukázat, na kolik si lidé uvědomují možnost, že právě oni se mohou stát obětí kyberkriminality, s jakým druhem kyberkriminality se nejčastěji setkávají a jak tyto útoky řeší, eventuálně jakým způsobem se proti útokům brání. V empirické části budou stanoveny některé hypotézy, kdy cestou průzkumu budou potvrzeny či vyvráceny. Získané poznatky budou nadále vyhodnoceny a graficky znázorněny.

2 Vymezení pojmů

Tato kapitola by měla vymezit některé základní pojmy pro lepší pochopení celé problematiky kyberkriminality a lepší orientaci v ní. Je potřeba si definovat především pojmy kyberkriminalita, co je kyberprostor, ve kterém se tato činnost odehrává a určit jaké současné technologie jsou k páchání této trestné činnosti zapotřebí.

2.1 Kyberkriminalita

V současné době neexistuje žádná jednotná definice kyberkriminality. Většinou se používá více pojmů, které se mezi sebou zaměňují, nebo se předpokládá, že jsou tyto pojmy rovnocenné, přestože tomu tak není.[1]

Pojem kybernetická kriminalita, dříve označován jako informační kriminalita, lze chápat jako páchání trestné činnosti v prostředí informačních, komunikačních technologií a počítačových sítí, kdy tyto informační a komunikační technologie jsou samotným objektem trestné činnosti nebo jsou k této činnosti využívány.[2]

Mohlo by se zdát, že kybernetická kriminalita se dá páchat pouze na počítači nebo prostřednictvím počítače, ovšem v dnešní době díky vývoji mikroprocesorů a jejich miniaturizaci a následnému využití v jiných technických zařízeních, spousta těchto zařízení přebírá funkci osobního počítače, aniž by byly za počítač označovány.[3]

2.2 Kyberprostor

Jedná se o nehmotný svět s informacemi, který je propojen informačními a komunikačními systémy, především internetem, který s kyberprostorem bezprostředně souvisí. Tento svět není limitován žádnými hranicemi a není nijak omezen. Jeho omezení je pouze ze strany technologické vyspělosti společnosti. Kyberprostor funguje v celosvětovém měřítku, kdy dokáže zachovat, vytvářet, využívat a vzájemně si předávat informace prostřednictvím výpočetní techniky.[4]

---

[1] **ZAVRŠNIK, A**. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. str. 3. ISBN 978-80-7552-758-5.
[2] **Kyberkriminalita - Policie České republiky**. Úvodní strana - Policie České republiky [online]. [cit. 02.12.2019]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx
[3] **KOLOUCH, J**. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. str. 32. ISBN 978-80-88168-15-7.
[4] **KOLOUCH, J**. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. str. 43. ISBN 978-80-88168-15-7.

2.3 Internet

Internet se v současné době stal nezbytnou součástí našeho každodenního života. Je využíván ke komunikaci mezi lidmi i na druhém konci světa, dohledávání různých informací a služeb, nakupování, a to vše z pohodlí domova a během několika vteřin.[5]

Počátky samotného internetu sahají do 50. let 20. století v období tzv. Studené války mezi Spojenými státy a Sovětským svazem, kdy bylo prováděno testování a budování sítí propojených počítačů, což bylo děláno pro vědecké a vojenské účely. Dnešní Internet v podobě v jakého ho známe, byl vybudován na základech sítí ARPANET a NSFNET, ale vlastníkem samotného Internetu nebo nějakou hlavní institucí, která by Internet řídila, není nikdo.[6]

„Materiální (hmotnou) podstatou Internetu je jeho páteřní síť, která vede signál (data) vzduchem, kabely, či jinými přenosovými médii. Technicky se jedná o celosvětovou distribuovanou počítačovou síť složenou z jednotlivých menších sítí, které jsou navzájem spojeny pomocí protokolů IP a tím je umožněna komunikace, přenos dat, informací a poskytování služeb mezi subjekty navzájem. Tím je vlastně vytvořen dynamický, neustále se měnící a vyvíjející systém vázaný na hardware, avšak zároveň vytvářející těžko definovatelný a prakticky neomezený kyberprostor.“[7]

V Československé republice byly první neoficiální pokusy připojení k internetu provedeny během listopadu roku 1991 na ČVUT v Praze a to do internetového uzlu v Linci. Dne 13.2.1992 pak proběhlo oficiální připojení Československé republiky k internetu a to opět na ČVUT.[8]

2.4 Hacker

Historie samotného slova sahá do padesátých let minulého století, kde se ve skupině radioamatérů takto označoval člověk, který byl schopný si technicky přizpůsobit svůj vysílač tak, že zlepšoval jeho výkon a dosah a byl ochoten hledat další

[5] **HULANOVÁ, L**. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. str. 16. ISBN 978-80-7387-545-9.
[6] **KOLOUCH, J**. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. str. 42. ISBN 978-80-88168-15-7.
[7] **KOLOUCH, J**. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. str. 43. ISBN 978-80-88168-15-7.
[8] **HULANOVÁ, L**. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. str. 19. ISBN 978-80-7387-545-9.

cesty ke zlepšování parametrů a účinků vysílače.[9] V současné době, ale není úplně jednoduché určit pojem Hacker. Toto slovo se může vykládat několika způsoby. Podle internetového souboru Jargon File: The New Hackers Dictionary je hacker člověk, který rád zkoumá podrobnosti programovatelných systémů a ty se snaží vylepšit. Dále tento soubor popisuje hackera jako osobu,

- která je posedlá programováním a místo pouhých teoretických úvah raději zkouší
  programování v praxi
- je dobrá v rychlém programování nebo dokonale ovládá nějaký program
- osoba, která se vyzná v některém vědním oboru a je v tomto oboru expertem

Policie popisuje hackera jako osobu, která se snaží překonat nějaký chráněný systém, kdy ovšem této osobě nejde o žádný osobní prospěch, získání informací nebo dokonce o jejich zničení. Tento člověk překonává tyto systémy pouze pro svou zábavu, nebo aby si sám sobě dokázal, že má takové kvality a schopnosti, které dokáží obejít zabezpečovací systém. Dalo by se říct, že se jedná o jeho koníček.

Nejvíce zkreslenou představu, kdo je hacker, ukazují média. Osobu hackera vykreslují jako kriminálníka, který obchází zabezpečovací systémy a bez jakýchkoliv důvodů ničí internetové stránky, odcizuje důležitá a choulostivá data z informačních systémů, anebo přímo tyto informační systémy narušuje. Tyto mediální informace velmi ovlivňují představu veřejnosti, kdy hacker je představen pouze jako nějaký zloděj.[10]

V literatuře se také dočteme a dozvíme, že hackery můžeme dělit na několik typů.

Nejzákladnějším rozdělením je dělení podle aktivity hackera, a to na hackery a crackery.

Hacker - svojí činnost provozuje pouze pro zábavu a dokazováním svých schopností sám sobě nebo komunitě, ve které se pohybuje, nikoliv za účelem zisku.

Cracker – je to osoba, která se snaží škodit, ať už ve svůj nebo cizí finanční prospěch. Používá hackerské metody, kdy proniká do cizích systémů a snaží se prolamovat hesla

[9] **JIROVSKÝ, V**. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007. str.47. ISBN 978-80-247-1561-2.
[10] **JIROVSKÝ, V**. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007. str.51. ISBN 978-80-247-1561-2.

k licenčním mechanismům, odcizovat, pozměňovat nebo ničit data. Pokouší se do systémů zavádět různé druhy virů a tím získávat pro něj důležité informace.

Dalším typem dělení je tzv. kloboukové dělení, které má tři úrovně:

Bílé klobouky – jedná se o skupinu, která jedná zákonně. Tito lidé většinou pracují pro nějakou firmu, která se zabývá bezpečností systémů. Legálně se snaží nabourat a napadnout systém, aby zjistili jeho slabiny a tyto se dali odstranit. Vše probíhá na základě vědomí majitele systému.

Černé klobouky – tato skupina se snaží nabourat, napadnout a zjistit slabiny bezpečnostních systémů, kdy toto ovšem dělají za účelem získání některých výhod pro sebe nebo svého zaměstnavatele. Většinou pracují pro nějakou nelegální organizaci. Jedna z nejznámějších skupin je „H4H“ - Hacker for Hire. Skupina nabízí své služby právě některým z nelegálních organizací, které mají o tyto služby zájem.

Šedé klobouky – jedná se o skupinu, kde jsou převážně rodící se hackeři, kteří ještě neví, do jaké ze skupin se zařadí a jaký bude jejich úkol.

Skupina hackerů, která je naprosto samostatná, se nazývá **Brilantní programátoři**. Jedná se o osoby, které dokáží vyřešit jakýkoliv programátorský problém, ale často upravují program k obrazu svému a nepoužívají žádnou dokumentaci. Proto většinou tyto osoby pracují naprosto samostatně, neboť nedokážou pracovat ve skupině. Tato skupina se dělí na:

Guru – jedná se o osobu, která má velké a dlouhodobé zkušenosti, kdy se vyzná ve vzniklém problému. Své zkušenosti a znalosti dokáže při řešení tohoto problému využít.

Wizard (čaroděj) – jedná se o osobu, která se vyzná v daném problému a má excelentní znalosti a vzniklý problém dokáže vyřešit cestou, kterou ostatní nechápou. Problémem je, že takovéto řešení nemusí v extrémních případech správně fungovat.[11]

[11] **JIROVSKÝ, V**. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007. str.47-55. ISBN 978-80-247-1561-2.

2.5 Phreaker

Jedná se o spojení dvou slov „phone“ a „cracker“. Takto označená osoba protizákonně využívá telefonní sítě. Roku 1972 John Draper objevil, že může na píšťalce dosáhnout tónu o frekvenci 2 600 Hz, kdy tuto frekvenci v té době využívala společnost AT&T k přepojování meziměstských hovorů. Postupem času, kdy se dařilo této komunitě phreakerů získávat více informací, dokázali přehrát do telefonního přístroje tóny, kterými získali kredit, dařilo se odposlouchávat jiné hovory nebo odebírat 12 V z telefonní sítě. S přicházející se a rozvíjející se dobou počítačů se začal Phreaking měnit do jiných podob jako hacking a cracking a proto většina hackerů a crackerů pochází z Phreakerů.[12]

2.6 Darker

Je osoba, která se zabývá pro zábavu tzv. darkingem – temněním. *Jde o zábavu určitých osob spočívající v celoplošném odpojování elektrického proudu ničením úsečníků vysokého napětí.* První skupina, která tyto akce začala podnikat, vznikla v listopadu 2001 v České republice pod názvem Darkers Group No 1. Její první útoky byly směrovány na Český Telecom, a.s. a na společnost ČEZ. Největší nebezpečí těchto útoků spočívalo v odpojení od elektrické energie budovy veřejného zájmu především zdravotnická zařízení, kde byl ohrožen život nebo zdraví osob. Toto si ovšem členové skupiny neuvědomovali.[13]

[12] **SMEJKAL, V**. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. str.181-182. ISBN 978-80-7380-720-7.
[13] **SMEJKAL, V**. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. str.169. ISBN 978-80-7380-720-7.

3 Typy protiprávního jednání

V dnešní době existuje mnoho variant a podob kybernetických útoků, které se každým dnem zdokonalují a vyvíjí. Běžný uživatel se již těžko v těchto pojmech orientuje. Tato kapitola by měla objasnit výrazy a názvy kybernetických útoků, které používá pachatel při svém protiprávním jednání proti jeho oběti a vysvětlit jejich nebezpečí a specifika.

3.1 Projevy kyberkriminality

Přestože se zdá, že kyberkriminalita je považována za nový druh kriminality, není tomu tak, neboť vychází ze známých druhů protiprávních jednání, jako jsou podvody, šikana, vydírání aj. Toto jednání ovšem přešlo do prostředí kybernetického prostoru, kde ho lze konat rychleji, bez omezeného prostoru, v jakoukoliv dobu a stále oproti reálnému světu. Útoky, které se dají přímo považovat za kybernetické útoky, jsou například hacking, DoS a DDoS útoky, botnety aj. [14]

3.1.1 Sociální inženýrství (Sociotechnika)

Sociální inženýrství se samo o sobě nedá považovat za formu kybernetického útoku, ale je důležité k prováděným útokům. Jeho myšlenka je vyvolat v osobách pocit, že je vše jak má být. Jedná se o manipulaci s obětí, kde se jí útočník věrohodným způsobem snaží oklamat a donutit k prozrazení informací, které by jinak sama oběť neposkytla. Jedná se např. o poskytnutí hesel. Tato metoda je právě zaměřena na nejslabší článek celého systému, kterým je vždy samotný uživatel. Není využíváno žádných technických přístupů nebo prolamovačů hesel. Sociální inženýrství je směřováno jak na jednotlivce, tak na firmy. [15]

3.1.2 Hacking

Jedná se o delikt, kterým pachatel proniká do informačního systému neobvyklou cestou, kdy se snaží vyhnout zabezpečení tohoto systému tím, že ho obejde nebo se mu podaří prolomit bezpečnostní ochranu. Původní hacking nebyl provozován za účelem

[14] **KOLOUCH, Jan**. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. str. 181. ISBN 978-80-88168-15-7.
[15] **KOLOUCH, Jan**. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. str. 186. ISBN 978-80-88168-15-7.

obohacení, ale jen pro své potěšení a potvrzení svých informačních dovedností. Pokud se jedná o samostatný hacking, lze pouze těžko vyčíslit škodu, neboť se často stává, že správce systému ani netuší, že hacker v systému byl a tento nepáchá žádnou škodu.[16]

3.1.3 Kybernetické výpalné

V tomto případě se jedná o nátlak vyděrače na svou oběť. Vyděrač prezentuje, že pronikl do systému, kde se dostal k datům a souborům, které má nyní pod kontrolou. Žádá finanční prostředky pod pohrůžkou, že tyto data zveřejní, zablokuje nebo úplně zničí. Často se jedná pouze o klamavou informaci, kdy se pachatel snaží využít strachu a neznalosti oběti.[17]

3.1.4 Botnet

Botnet lze popsat jako síť „zotročených počítačů“, které ovládá správce sítě pro své účely. Tento systém se dá použít legálně pro různé distribuované výpočty, ale dá se také zneužít k nelegálním činnostem. Celý systém spočívá v nakažení počítače virem, který umožňuje využívat nějakou část výkonu ovládaného počítače. Tento odběr výkonu nemusí uživatel ani postřehnout při jeho běžné činnosti. Takto získané počítače se dají jednoduše zneužít např. k rozesílání spamů nebo dotazům na určité internetové stránky a tímto je vyřadit z provozu. V dnešní době existují počítačové systémy, které jsou schopny denně rozeslat až miliardy zpráv, ale jsou brzo dohledány podle IP adresy a jsou zablokovány z důvodu příliš velkého provozu v síti. Pokud ovšem útočník použije svou síť „zotročených počítačů“ mezi které se tato činnost rozdělí, nebude tato činnost vyhodnocena jako problematická. Tento systém se využívá především k provádění útoků jako phishing, DDoS, aj. z důvodu finančního zisku.[18]

3.1.5 Malware

Jedná se o jakýkoliv škodlivý software, který je schopen nějakým způsobem narušit počítačový systém a v něm negativně operovat. Dříve každý takovýto software byl označován různým termínem, v současné době se souhrnně označuje jedním termínem a

[16] **KOLOUCH, J**. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. str. 269-272. ISBN 978-80-88168-15-7.
[17] **JIROVSKÝ, V**. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007. str.102-103. ISBN 978-80-247-1561-2.
[18] **KOLOUCH, J**. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. str. 193-194. ISBN 978-80-88168-15-7.

to malware. Malware může mít spoustu podob, kdy především záleží, jakou činnost má škodlivý software vykonávat. Malware může vykonávat několik úkolů najednou, např. se může sám dále šířit pomocí e-mailů a zároveň získávat data ze systému. Přestože se převážně používá název malware, je možné se stále setkat s historickými názvy těchto škodlivých softwarů, kdy se jedná o skupiny:

Adware - v tomto případě se jedná o nejméně škodlivý software, který je ale velmi obtěžující. Jeho hlavním úkolem, jak už napovídá jeho plný název „advertising supported software" – software podporující reklamu, je v systému neustále uživateli zobrazovat reklamu například formou vyskakovacího okna.

Spyware - tento název pochází ze složení dvou anglických slov „spy" – špion a „software". Program dokáže získávat statistická data o činnosti na počítačovém systému a tyto data odesílat útočníkovi. Dokáže získávat informace osobního charakteru, navštívené webové stránky nebo spuštěné aplikace. Často si uživatel nevědomě, ale přitom dobrovolně nainstaluje tento software do svého systému při získávání volně dostupných aplikací, které nejsou nijakým způsobem nebezpečné. Tento spyware je v tomto případě ošetřen ve smluvních podmínkách EULA. Přestože, spyware bývá součástí instalačního balíčku dané aplikace, tak i po odinstalování této aplikace zůstává spyware v systému ukryt.

Viry - byly převážně používány v 80. a 90. letech 20. století. Existuje spousta druhů virů, kdy každý má jiný úkol od usazení se v systému s cílem dalšího šíření až po ničení souborů nebo celých systémů. Vir je program či závadný kód, který se sám připojí k nějakému funkčnímu souboru nebo dokumentu, a tak ho infikuje. Druhy virů se dají dělit podle toho, jaké soubory napadají, a to na bootviry (systémové oblasti), souborové viry (soubory), multiparitní viry (kombinace virů) a makroviry (útočí pomocí maker).

Červi - jejich úkol je podobný jako u virů a proto bývá i za vir označován. Červ ovšem na rozdíl od viru se nepotřebuje vázat na žádný spustitelný program a dokáže se šířit samostatně pomocí síťové komunikace. Tyto programy jsou schopny samy vyhodnocovat bezpečnostní systém a v tom následně vyhledávat a využívat slabiny tohoto systému.

Trojské koně a Backdoors - trojské koně jsou počítačové programy, které mají takové funkce, o kterých uživatel neví a ve svém systému je nechce. Jejich úkolem je ovlivňovat počítačový systém, kdy zde provádí blokace souborů nebo aplikací, mazání dat nebo narušují samotný běh počítačového systému, čímž umožňují lépe a snadněji proniknout do systému jiným škodlivým softwarům, v tomto případě jsou označovány jako Backdoor. Trojské koně často bývají připojeny k jinému bezpečnému programu a nejsou schopny se samostatně šířit a replikovat.

Rootkit - nejsou škodlivé programy, ale jedná se o technologii, která je schopna v napadeném systému zakrývat přítomnost malwaru a prodlužovat jeho životnost v systému tím, že napadají antivirové programy a ty ho následně nemohou v systému identifikovat a odstranit. Do systému se nejčastěji dostává v datově malých počítačových programech.

Keylogger - je systém, který dokáže zaznamenat, které klávesy byly použity v napadeném systému. Jeho hlavním úkolem je zjistit přihlašovací údaje do různých aplikací a systémů, které následně předá útočníkovi.

Ransomware - jedná se o tzv. vyděračský malware. Jedná se o systém, který se za pomoci červa nebo trojského koně dostane do systému uživatele. Trojský kůň nebo červ se usadí v počítačovém systému a následně dovolí stáhnout skutečný ransomware, který částečně nebo zcela dokáže zablokovat počítačový systém uživatele, dokud uživatel útočníkovi nezaplatí tzv. „výkupné“. Existují dva typy ransomware, které se dělí podle zásahu do chodu počítače. První typ blokuje celý systém počítače, přičemž druhý nechá systém funkční, ale blokuje data uživatele, jako jsou videa, fotky, textové soubory atd.[19]

3.1.6 Spam

Jedná se o označení nevyžádané komunikace, kterou v informačních technologiích můžeme rozdělit ve dvou rovinách, a to užším pojetím, kdy se jedná o nevyžádanou elektronickou poštu především reklamního charakteru a v širším slova

[19] **KOLOUCH, J**. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. str. 204-221. ISBN 978-80-88168-15-7.

smyslu jako jakoukoliv nevyžádanou zprávu včetně zpráv obsahující různé druhy malwarů.[20]

3.1.7 Phishing

Phishing využívá sociální inženýrství, kdy se snaží nastínit věrohodnou situaci a tímto způsobem se snaží svou oběť oklamat. Jedná se například o falešné přihlašovací stránky k internetovému bankovnictví, online obchodům aj. Takto získá od oběti potřebné informace jako je PIN, uživatelské jméno a heslo, údaje z kreditních karet atd., které může dále zneužít pro svůj prospěch.[21]

3.1.8 Pharming

Pharming je mnohem propracovanější forma phishing, kdy jde o útok na DNS (Domain Name System) server, na kterém dochází k překladu doménového jména na IP adresu. Samotný útok spočívá v tom, že uživatel zadá ve svém prohlížeči webovou stránku příslušného webového serveru, ale k tomuto přepojení nedojde a uživatel je přepojen na falešný webový server, který je většinou věrnou imitací skutečné stránky. Tento způsob je převážně používán na přihlašovací stránky internetového bankovnictví.

3.1.9 Spear Phishing

Jedná se o formu phishingového útoku, kdy na rozdíl od phishingu, který je prováděn spíše plošně, je tento realizován a zaměřen na přesný cíl nebo skupinu za účelem zjištění přesných specifických údajů vedených v daném systému.

3.1.10 Vishing

Jedná se o telefonický phishing, kdy se útočník, který se většinou představuje jako zástupce některé z bankovních institucí, pokouší za pomoci vymyšlené legendy od oběti získat citlivé údaje především k přihlašovacím údajům do internetového bankovnictví nebo čísla platebních karet.

[20] **KOLOUCH, J**. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. str. 231. ISBN 978-80-88168-15-7.
[21] **KOLOUCH, J**. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. str. 246. ISBN 978-80-88168-15-7.

3.1.11 Smishing

Tento systém se dá porovnat s vishingem a phishingem, kdy za použití SMS zprávy se snaží přimět oběť k zavolání na placenou linku, zaplatit dárcovskou SMS nebo zasílá podezřelé URL odkazy, kde je uživatel vyzván k zadávání citlivých údajů nebo k instalaci aplikací, které obsahují malware.[22]

3.1.12 Cracking

Obsahově je cracking především překonávání ochranných prvků počítačového systému, programů nebo aplikací za účelem následného neoprávněného užití. Cracking je též spojován s porušováním autorských práv, kdy se snaží obcházet ochranné prvky proti kopírování filmových a hudebních CD, DVD nebo nelegálního využívání softwarů.[23]

3.1.13 Internetové pirátství a Warez

Pojmem internetové pirátství je v obecné rovině zamýšlena protiprávní činnost, která porušuje práva duševního vlastnictví a autorského práva. V prostředí internetu se dá toto internetové pirátství rozdělit na dvě skupiny – softwarové pirátství, které porušuje práva k počítačovým programům a audiovizuální pirátství, které porušuje práva k audiovizuálním dílům. S internetovým pirátstvím je spojován pojem WAREZ, kdy se na internetu vytváří různá warezová fóra, do kterých je omezený přístup a komunikace probíhá pouze v privátních místnostech, kdy uživatelé mění svou IP adresu. Tato fóra slouží k získání cracků, keygenů, ale i filmů, seriálů, kompletních softwarových programů a hudby. Tyto upravené produkty se nazývají relase. A právě v dnešní době skoro neomezeného přístupu k internetu je tato protiprávní činnost v kyberprostoru nejrozšířenější.[24]

[22] **KOLOUCH, J**. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. str. 263-266. ISBN 978-80-88168-15-7.
[23] **KOLOUCH, J**. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. str. 276. ISBN 978-80-88168-15-7.
[24] **KOLOUCH, J**. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. str. 277-289. ISBN 978-80-88168-15-7.

3.1.14 Sniffing

Sniffing je nezákonný odposlech dat, která procházejících počítačovou sítí při komunikaci dané služby s počítačovým systémem. Jde o nelegální činnost, o které uživatel neví a nechce ji. Pachatel je schopen se díky této metodě dostat k různým údajům jako jsou přístupy k různým aplikacím, elektronické komunikaci, používané služby a navštěvované internetové stránky atd.[25]

3.1.15 DoS, DDoS a DRDoS útoky

DoS jedná se o zkratku anglického výrazu „denial of service“ – popření služby. DoS, DDoS a DRDoS útoky jsou útoky, které mají stejný úkol, a to vyřadit z provozu internetovou službu, na kterou je útok cílený tím, že napadený počítačový systém je zahlcen požadavky na určité úkony, které postupně systém nestíhá vykonávat, čímž se zpomaluje nebo se úplně vyřadí z provozu. Rozdíl mezi uvedenými útoky je ve formě provedeného útoku.

DoS – jedná se o útok z jednoho zdroje. Proti takovému útoku není příliš složité se ubránit, kdy stačí zablokovat prováděné dotazy z tohoto zdroje.

DDoS (Distributed Denial of Service (distribuované odepření služby)) - k těmto útokům jsou využívány botnety, kdy útok je realizován z více počítačových systémů, které jsou různě rozmístěny po světě a tím zakrývají a znemožňují identifikaci primárního systému, čímž ho brání proti blokování.

DRDoS (Distributed Reflected Denial of Service (distribuované, odražené popření služby)) - z útočícího systému je na velké množství dalších počítačových systémů rozeslán podvržený požadavek, kdy tyto systémy na požadavek odpoví, ale odpověď již nejde k útočníkovi, ale k oběti. Zaslané požadavky totiž mají v sobě uvedenou zdrojovou adresu oběti. Oběť tedy následně dostává spoustu odpovědí, které ji vyřadí z provozu. [26]

[25] **KOLOUCH, J**. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. str. 294. ISBN 978-80-88168-15-7.
[26] **KOLOUCH, J**. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. str. 295-298. ISBN 978-80-88168-15-7.

3.1.16 Kyberterorismus

V současné době s nárůstem a rozšiřováním terorismu je kyberprostor především internet pro tyto organizace velmi účinným nástrojem. Skoro každá teroristická organizace má svoje webové stránky. Pomocí internetu se snaží získávat nové členy, sponzory, dělat propagandu své ideologii, zastrašovat, a hlavně je zde možnost se mezi sebou domlouvat a organizovat své útoky na jakoukoliv vzdálenost a v jakoukoliv denní dobu a to za možnosti utajené komunikace.

Samotný terorismus můžeme rozdělit na dvě skupiny, a to letální – kdy je využíváno běžných zbraní až po zbraně hromadného ničení a na skupinu neletální, která je především využívána v internetu. Tato forma neletálního terorismu je rozdělena na tři skupiny:

- Neozbrojený terorismus
- Kyberterorismus
- Mediální terorismus

3.1.17 Cybersquatting

Název pochází ze složení anglických slov „cybernetic“ a „squatting“. Jedná se o formu útoku, která v současné době už není moc využívána. Největší rozmach tohoto útoku byl při vstupu firem na internet. Pachatel si zaregistroval doménové jméno nějaké známé firmy nebo instituce např. www.bosch.cz a následně se pokusil tuto doménu prodat této firmě. Pokud subjekt odmítl stránku odkoupit, bylo mu vyhrožováno, že na tuto doménu bude umístěn nevhodný obsah jako třeba pornografie. [27]

3.2 Kybernetické útoky na sociálních sítích

Kybernetické útoky na sociálních sítích jsou trochu odlišnou skupinou kybernetických útoků, než jsou útoky malware, phishing atd., tyto útoky se odehrávají v celém kyberprostoru. Oproti tomu kybernetické útoky na sociálních sítích se z naprosté většiny odehrávají v prostoru sociálních sítí. Tyto útoky můžeme rozdělit na Kyberšikanu, Kybergrooming, Sexting, Kyberstalking.

[27] **KOLOUCH, J**. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. str. 323-326. ISBN 978-80-88168-15-7.

3.2.1 Kyberšikana

Jak už sám název napovídá, jedná se o šikanu, která se odehrává v kyberprostoru, ke které je nutné použít informační a komunikační technologie. Tato šikana má stejný úkol jako šikana reálná, tedy ponížit, ublížit, zesměšnit oběť šikany. Velkou „výhodou" kyberšikany oproti reálné šikaně je její trvanlivost v kyberprostoru. Je možné osobu šikanovat z jakéhokoliv místa, 24 hodin denně, opakovaně a přitom nezáleží, na jakém místě se právě oběť nachází. Nejčastější projevy kyberšikany jsou výhružky, zesměšnění, pomluvy, pořizování audiovizuálních nahrávek nebo fotografií s cílem tyto upravit a následně vystavit na internetu opět k zesměšnění osoby. K hlavním znakům kyberšikany patří:[28]

- pocit útočníka, že je v internetovém prostředí nedohledatelný
- neomezenost útoku, kdy může být veden opakovaně, bez nutnosti nějakého časového vymezení a vědět o oběti, kde se právě nachází
- neomezený okruh útočníků – útočník může být kdokoliv, nezáleží na žádných fyzických předpokladech
- neomezený prostor a prostředky – útočníkovi jsou poskytnuty skoro neomezené prostředky, jak s materiálem zacházet a měnit jeho obsah ke své potřebě, internet nabízí neomezený prostor webových stránek a sociálních sítí, kde takovéto materiály zveřejnit
- obtížná zjistitelnost – na oběti nejsou poznat žádné fyzické známky zranění, chybějících věcí atd., které by ukazovaly na šikanu
- trvalost – oproti klasické šikaně, která má vždy svůj začátek a konec útoku i když opakovaně, u kyberšikany stačí např. jedna fotografie, nahrávka, která je oběti stále připomínána.
- šikana nebo kyberšikana není trestným činem ani přestupkem, trestným činem nebo přestupkem se stává jednání, kterým je samotná šikana prováděna

3.2.2 Kybergrooming

Kybergrooming je za pomoci sociálního inženýrství útok na oběť pomocí informačních a telekomunikačních technologií, kdy se útočník snaží ve své oběti vzbudit důvěru k uskutečnění schůzky, kde je následně oběť fyzicky nebo sexuálně

[28] **KOLOUCH, J**. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. str. 309-310. ISBN 978-80-88168-15-7.

napadena. Obětí takového útoku se může stát dítě i dospělý člověk. Nejvíce ohroženy a nejčastějšími obětmi jsou mladé dívky ve věku 13 – 17 let. Vylákání oběti na takovou schůzku trvá útočníkovi přibližně od 3 měsíců až několik let. Doba, za jak dlouho je útočník schopen svou oběť vylákat na schůzku, záleží především na způsobu manipulace s obětí a její důvěřivostí. Kybergrooming má pět etap: [29]

„1*) Vzbuzení důvěry a snaha izolovat oběť od okolí (útočník mění svoji identitu, je velmi trpělivý)*

2) Podplácení dárky či různými službami, budování kamarádského vztahu

3) Vyvolání emoční závislosti oběti na osobě útočníka

4) Osobní setkání

5) Sexuální obtěžování, zneužití dítěte či jiný útok"

3.2.3 Sexting

Jedná se o složení slov „sex" a „texting". Jde o nahrání materiálů se sexuální tématikou na sociální sítě nebo jiná úložiště, a to samotným autorem nebo osobou, která získala přístup k takovému materiálu. Oběť nejčastěji sama dobrovolně takovýto materiál odešle osobě, které v té době důvěřuje a proto i oběť se tímto chováním podílí na činu. Ve chvíli odeslání ztrácí oběť kontrolu nad těmito materiály a pachatel (často bývalý partner), využívá těchto materiálů k vydírání oběti, zesměšnění na sociálních sítích nebo k vymáhání zaslání dalších podobných materiálů s pohrůžkou zveřejnění již obdržených materiálů. Samotný sexting – zaslání dat se sexuální tématikou není mezi dospělými osobami trestným činem, jelikož se jedná o dobrovolné přeposlání. Trestným činem se stává zneužití těchto dat útočníkem např. vystavením na sociálních sítích, vymáhání si zaslání dalších dat pod pohrůžkou zveřejnění atd.

Jinak je tomuto u dětí, které jsou pachatelem vyzývány k zasílání různých druhů materiálů se sexuální tématikou, kde se tyto děti objevují nahé, kdy se pachatel může dopustit nebo se dopouští trestného činu zneužití dítěte k výrobě pornografie.

3.2.4 Kyberstalking

Jedná se o složení slov „kyber" a „stalking". Kyberstalking je dlouhodobější, vytrvalé a stupňující se pronásledování oběti pomocí informačních a telekomunikačních

[29] **KOLOUCH, J**. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. str. 312-313. ISBN 978-80-88168-15-7.

technologií, kdy toto jednání v oběti vyvolává pocit strachu a obav o své soukromí, zdraví nebo dokonce život. Oběť kyberstalkingu může i nemusí pachatele znát. Pachatelé často dokáží měnit svou identitu, aby mohli svou oběť co nejvíce kontaktovat. V některých případech takovýto pachatel své oběti dokazuje sílu tím, že o ní zveřejňuje informace z jejího života na internetu.[30]

[30] **KOLOUCH, J**. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. str. 314-318. ISBN 978-80-88168-15-7.

4 Evropské a české právní předpisy o kyberkriminalitě

Postihování kyberkriminality je celosvětová záležitost, neboť tato kriminalita není ohraničena žádným prostorem. Každý stát má své vlastní právní normy, které určitým způsobem problematiku řeší. Existují i mezinárodní právní dokumenty, které se snaží sjednotit pohled na kyberkriminalitu a snaží se tuto činnost vymezit a uvést, co znamená kybernetická kriminalita.

4.1 Úmluva Rady Evropy č. 185 o kyberkriminalitě

Jedná se o nejdůležitější právní dokument vztahující se ke kyberkriminalitě. Tento dokument se snaží sjednotit jednotlivé právní úpravy členských států.

„Úmluvu o kyberkriminalitě schválil Výbor ministrů Rady Evropy na svém 109. zasedání dne 8. listopadu 2001. Úmluva o kyberkriminalitě byla otevřena k podpisu 23. listopadu 2001 v Budapešti. V platnost vstoupila tato úmluva dne 1. července 2004. Česká republika podepsala Úmluvu o kyberkriminalitě dne 9. února 2005 a ratifikovala ji 22. srpna 2013 s tím, že v ČR tato úmluva vstoupila v platnost 1. prosince 2013".[31]

Úmluva je dělena na preambuli, 4 kapitoly, ve kterých je celkem 48 článků – Kapitola 1 - Užití pojmů, Kapitola 2 – Opatření, která mají být přijata na vnitrostátní úrovni, Kapitola 3 – Mezinárodní spolupráce a Kapitola 4 – Závěrečná ustanovení.

Nejvíce zásadní částí této úmluvy je kapitola č. 2, která právně definuje a rozděluje 4 základních typy kybernetických útoků, čímž je umožněno tyto činy lépe identifikovat a stíhat. Tyto skupiny jsou rozděleny takto:[32]

1) Trestné činy proti utajování, integritě a dostupnosti počítačových dat a systémů
2) Trestné činy související s počítači
3) Trestné činy související s obsahem
4) Trestné činy související s porušováním autorských práv a práv souvisejících

[31] **KOLOUCH, J**. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. str. 332. ISBN 978-80-88168-15-7.
[32] Full list. *301 Moved Permanently* [online]. Copyright © Council of Europe 2019 [cit. 08.12.2019]. Dostupné z: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

4.2 Dodatkový protokol Rady Evropy č. 189 k Úmluvě o kyberkriminalitě

Jedná se o dodatek k Úmluvě o kyberkriminalitě, který byl přijat 28. ledna 2003. Skládá se z preambule a 4 kapitol s celkem 16 články. Jsou zde vypsány trestné činy, kterým se samotná Úmluva o kyberkriminalitě nevěnuje. V dodatku jsou tyto činy vypsány v 2. kapitole a jedná se o šíření rasistického a xenofobního materiálu skrze počítačový systém, rasisticky a xenofobně motivovaná výhrůžka, rasisticky a xenofobně motivovaná urážka, popírání, hrubé zlehčování, schvalování nebo ospravedlňování genocidy nebo zločinů proti lidskosti, napomáhání.[33]

4.3 GDPR v souvislosti s informačními technologiemi

Dne 25. května 2018 vstoupilo v účinnost nové evropské nařízení – Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), které je především známo pod zkratkou GDPR. Toto nařízení je velmi obsáhlé a mohlo by být zpracováno v samostatné práci. Nařízení je důležité z hlediska ochrany osobních údajů, které se stávají častým cílem protiprávních útoků a následným obchodem s těmito daty. My si v této kapitole uvedeme několik základních pojmů a oblastí, které Nařízení GDPR upravuje v souvislosti s informačními technologiemi a kyberprostorem.

Na začátku je důležité uvést koho se Nařízení GDPR týká a co upravuje.

Jak je již ze samotného názvu nařízení zřejmé, jedná se o nařízení, které má na území Evropské unie za úkol ochranu osobních údajů. Nařízení vzniklo na základě velkého a rychlého technologického progresu informačních a komunikačních technologií.[34]

Jedním ze stěžejních pojmů je osobní údaj, kdy se jedná o informace k identifikované nebo identifikovatelné fyzické osobě. Tato osoba se také nazývá subjektem údajů. Přes tyto údaje se dá osoba přímo nebo nepřímo identifikovat. Může

[33] Dodatkový protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů [cit. 12.12.2019]. Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804931bf

[34] **ŽŮREK, J**. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). str. 13. ISBN 978-80-7554-097-3.

se jednat například o identifikační číslo, rodné číslo, síťový identifikátor, ale i o fyziologické, genetické, ekonomické a jiné údaje. V praxi lze polemizovat, zda každý takový údaj je osobním údajem či nikoliv, jelikož není vždy jasné, k jaké osobě údaj směřuje. Proto v případě pochybností je lépe údaje považovat za osobní.[35]

Důležitým subjektem a zároveň pojmem v GDPR je správce a zpracovatel. Správcem může být jakákoliv osoba, kdy nerozhoduje její právní forma, která určuje účely a prostředky zpracování osobních údajů a za zpracování těchto údajů odpovídá. Oproti tomu zpracovatel je jakýkoliv subjekt, který pro správce zpracovává osobní údaje a může s nimi provádět pouze takové operace, kterými ho správce pověří a které po něm žádá.[36]

Z pohledu informačních technologií je mnoho možností zpracovávání osobních údajů, které mají tři typy dat:[37]

Strukturovaná data v informačních systémech

Nestrukturovaná data (e-mail, úložiště)

Fyzické dokumenty - archiv

Asi jedna z nejčastějších činností na internetu je navštěvování e-shopů, webů, blogů nebo stahování různých aplikací a i zde jsou nastaveny nařízením GDPR základní povinnosti:

-zpracování jen skutečně potřebných údajů

-zpracování údajů jen po nutně dlouhou dobu

-údaje se využívají jen pro účely, pro které byly získány

- údaje se musí chránit před zneužitím

Údaje subjekt údajů poskytuje dobrovolně a v případě, že není využit jiný právní titul pro zpracování osobních údajů, musí dát tzv. souhlas se zpracováním osobních údajů.[38]

[35] **ŽŮREK, J**. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9.

[36] *Praktický manuál GDPR pro každého: vše, co potřebujete vědět o novém nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně osobních údajů v praktickém kompletu s webem, e-bookem a aktualizačním servisem*. Bratislava: DonauMedia, 2018. str. 13. ISBN 978-80-8183-049-5.

[37] **STAŇKOVÁ, L.** *GDPR snadno a přehledně*. Praha: Mladá fronta, 2018. str.201. ISBN 978-80-204-5108-8.

[38] **STAŇKOVÁ, L.** *GDPR snadno a přehledně*. Praha: Mladá fronta, 2018. str.214-215. ISBN 978-80-204-5108-8.

Používáním internetu se do našich informačních systémů dostávají soubory tzv. Cookies, kdy tyto krátké textové sobory umožňují odlišit jednotlivé uživatele a ukládají o nich konkrétní údaje. Existují i tzv. autentizační Cookies, které slouží například pro uložení potvrzení na sociálních sítích, e-shopů atd.
I tyto Cookies mají vzhledem k GDPR prioritní povinnost vůči subjektu a to náležitě subjekt údajů poučit o používání Cookies souborů.[39]

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

Zákon o kybernetické bezpečnosti vstoupil v účinnost dne 1.1.2015. Důvodem jeho vzniku byl především razantní nárůst používání informačních technologií celou společností ve všech oblastech a narůstající závislosti společnosti na těchto informačních technologiích. S touto závislostí začalo přibývat i sofistikovanějších útoků na informační systémy jednotlivce nebo celých korporací, kdy tyto útoky mohou být prováděny jak jednotlivcem, tak organizovanými skupinami.[40]

Samotná působnost tohoto zákona je vymezena na oblast kybernetické bezpečnosti, kde jsou upraveny práva a povinnosti osob a pravomoc a působnost orgánů veřejné moci. Samotný zákon se ovšem nevztahuje na informační a komunikační systémy, které pracují s utajovanými informacemi. Zákon dále upravuje, kdo jsou v tomto případě povinné subjekty. Ty můžeme pomyslně rozdělit do dvou základních skupin. První skupina jsou poskytovatelé služeb a elektronických komunikací a subjekty, které zajišťují významné sítě. Druhá skupina lze specifikovat jako správce informačního nebo telekomunikačního systému.[41]

Zákon dále upravuje např. reaktivní a ochranná opatření, varování, evidenci kybernetický útoků, rozděluje povinnosti a pravomoci národního a vládního CERTu (Computer Emergency Respone Team), ovšem nutné je upozornit v tomto zákoně na

[39] **STAŇKOVÁ, L**. *GDPR snadno a přehledně*. Praha: Mladá fronta, 2018. str.220-221. ISBN 978-80-204-5108-8.
[40] **MAISNER, M**. *Zákon o kybernetické bezpečnosti: komentář*. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR). str. 1. ISBN 978-80-7478-817-8.
[41] **MAISNER, M**. *Zákon o kybernetické bezpečnosti: komentář*. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR). str. 74. ISBN 978-80-7478-817-8.

§ 7, který vymezuje kybernetické bezpečnostní události a kybernetický bezpečnostní incident.

Hlavním rozdílem mezi těmito zdánlivě stejnými pojmy je, že *„kybernetickou bezpečnostní událostí je událost bez reálného negativního následku pro daný komunikační nebo informační systém, kybernetickým bezpečnostním incidentem je pak samotné narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací“.*[42]

Pokud je událost vyhodnocena jako kybernetický bezpečnostní incident, nastává povinnost předat informaci příslušnému pracovišti CERT.[43]

4.5 Nejčastější projevy kybernetické kriminality s odkazem na zákon č. 40/2009 Sb.

Kybernetické trestné činy podle trestního zákoníku se dají dělit více způsoby, jeden ze způsobů dělení je na:

a) trestné činy, při jejichž páchání představují prostředky informačních a komunikačních technologií předmět ochrany

§ 182 Porušení tajemství dopravovaných zpráv

§ 183 Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí

§ 207 Neoprávněné užívání cizí věci

§ 228 Poškození cizí věci

§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací

§ 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

§ 234 Neoprávněné opatření, padělání a pozměnění platebního prostředku

§ 264 Zkreslení údajů a nevedení podkladů ohledně vývozu zboží a technologií dvojího užití

§ 267 Zkreslení údajů a nevedení podkladů ohledně zahraničního obchodu

[42] **MAISNER, M.** *Zákon o kybernetické bezpečnosti: komentář*. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR). str. 100. ISBN 978-80-7478-817-8.

[43] **MAISNER, M.** *Zákon o kybernetické bezpečnosti: komentář*. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR). str. 100. ISBN 978-80-7478-817-8.

s vojenským materiálem

§ 270 Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi

§ 290 Získání kontroly nad vzdušným dopravním prostředkem, civilním plavidlem a pevnou plošinou

§ 291 Ohrožení bezpečnosti vzdušného dopravního prostředku a civilního plavidla

§ 311 Teroristický útok

§ 317 Ohrožení utajované informace

b) trestné činy, při jejichž páchání jsou prostředky informačních a komunikačních technologií užity ke spáchání trestného činu

§ 180 Neoprávněné nakládání s osobními údaji

§ 181 Poškození cizích práv

§ 182 Porušení tajemství dopravovaných zpráv

§ 184 Pomluva

§ 191 Šíření pornografie

§ 192 Výroba a jiné nakládání s dětskou pornografií

§ 193 Zneužití dítěte k výrobě pornografe

§ 193b Navazování nedovolených kontaktů s dítětem

§ 205 Krádež

§ 209 Podvod

§ 213 Provozování nepoctivých her a sázek

§ 214 Podílnictví

§ 216 Legalizace výnosů z trestné činnosti

§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací

§ 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

§ 234 Neoprávněné opatření, padělání a pozměnění platebního prostředku

§ 236 Výroba a držení padělatelského náčiní

§ 268 Porušení práv k ochranné známce a jiným označením

§ 269 Porušení chráněných průmyslových práv

§ 272 Obecné ohrožení

§ 276 Poškození a ohrožení provozu obecně prospěšného zařízení

§ 287 Šíření toxikomanie

§ 316 Vyzvědačství

§ 345 Křivé obvinění

§ 348 Padělání a pozměnění veřejné listiny

§ 353 Nebezpečné vyhrožování

§ 354 Nebezpečné pronásledování

§ 355 Hanobení národa, rasy, etnické nebo jiné skupiny osob

§ 356 Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod

§ 357 Šíření poplašné zprávy

§ 361 Účast na organizované zločinecké skupině

§ 364 Podněcování k trestnému činu

§ 365 Schvalování trestného činu

§ 400 Genocidium

§ 403 Založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka

§ 407 Podněcování útočné války

Vzhledem ke skutkovým podstatám samotných trestných činů je možné některé zařadit do obou kategorií.[44]

4.6 Vybrané trestné činy ve zvláštní části trestního zákoníku

V této kapitole jsou dle mého názoru uvedeny nejvíce páchané trestné činy dle zák. č. 40/2009 Sb.

§ 180 Neoprávněné nakládání s osobními údaji

V dnešní době rozšiřování informačních technologií je spousta citlivých údajů uloženo na různých nosičích dat. Právě o tyto informace, které především obsahují osobní data občanů nebo hospodářsky využitelná data, mají pachatelé enormní zájem.[45] K neoprávněnému nakládání s osobními údaji, která mohou být zveřejněny, sděleny,

[44] **KOLOUCH, J**. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. str. 340-341. ISBN 978-80-88168-15-7.

[45] **SMEJKAL, V**. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. str. 254. ISBN 978-80-7380-720-7.

zpřístupněny nebo může být s nimi jinak lze využít např. tisky, film, rozhlas, ale i veřejně přístupnou počítačovou síť. K protiprávnímu jednání postačí i nedbalost. [46]

§ 181 Poškození cizích práv

Pachatel se snaží způsobit vážnou újmu oběti tím, že o ní prostřednictvím informačních systémů zveřejní takové informace, které mohou uvést někoho v omyl, nebo využije něčího omylu. Takovým příkladem může být zveřejnění nepravdivého inzerátu s erotickým podtextem, kdy je oběti ublíženo na cti a je obtěžována zaslanými odpověďmi na tento inzerát.[47]

§ 182 Porušení tajemství dopravovaných zpráv

V dnešní době přešla osobní komunikace mezi lidmi především do elektronické komunikace ve formě textové, hlasové, obrazové, zvukové. Uvedené ustanovení by mělo chránit tuto komunikaci před porušením ze strany pachatele. [48]

§ 183 Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí

Jedná se o nový trestný čin, který doplňuje § 182. Toto ustanovení chrání písemnosti osobní i profesní povahy, které musí být nějakým způsobem uzamčeny, uzavřeny nebo jinak chráněny proti přístupu dalších osob, musí být uchovávané v soukromí[49].

§ 184 Pomluva

Podle ust. § 184 odst. 2 lze čin spáchat tiskem, filmem, rozhlasem, TV, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem. Pachatel v tomto případě zveřejňuje v internetovém prostoru informaci o oběti, o které zcela jistě ví, že není pravdivá. Tato pomluva může oběti způsobit problémy v zaměstnání, snížit vážnost u spoluobčanů, snížit její důvěryhodnost atd.[50]

---

[46] **VANTUCH, P.** *Trestní zákoník s komentářem: k ...* Olomouc: ANAG, 2011-. Právo (ANAG). str. 622 – 625. ISBN 978-80-7263-677-8.

[47] **SMEJKAL, V**. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. str.208 – 209. ISBN 978-80-7380-720-7.

[48] **SMEJKAL, V**. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. str. 315. ISBN 978-80-7380-720-7.

[49] **SMEJKAL, V**. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. str. 360. ISBN 978-80-7380-720-7.

[50] **SMEJKAL, V**. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. str. 382. ISBN 978-80-7380-720-7.

§ 191 Šíření pornografie

Šíření filmového, počítačového, grafického aj. materiálu se sexuálním obsahem, ve kterém je projevováno násilí a neúcta k člověku nebo je zde zobrazován pohlavní styk se zvířetem. O pornografickém charakteru díla rozhoduje jeho celý obsah, nikoliv jen určitá část. Vladimír Smejkal podotýká, „*že vnímání, co je a co není pornografie, je závislé na místu, čase, kontextu a vyvíjí se tak, jak se vyvíjí i lidská společnost, jak se vyvíjí většinový náhled na žádoucí chování člověka*.“[51]

§ 192 Výroba a jiné nakládání s dětskou pornografií

Dětská pornografie není novodobou záležitostí, ale s příchodem internetu se její množství zvýšilo, jelikož internet pachatelům slouží jako dobrý pomocník s výrobou, distribucí a prohlížením tohoto závadového materiálu. Internet umožňuje pachatelům lepší, rychlejší a anonymnější komunikaci s obětí.[52] Toto ustanovení by mělo chránit všechny děti bez rozdílu pohlaví a přispívat k jejich správnému tělesnému a duševnímu vývoji dítěte a zabránit přechovávání, vytváření, prodávání, zprostředkování a jiné činnosti s obsahem, který zobrazuje dětskou pornografii. [53]

§ 193b Navazování nedovolených kontaktů s dítětem

Toto ustanovení bylo vytvořeno vzhledem k jednání pachatelů na sociálních sítích, a to především na Facebooku.[54] „*Kdo navrhne setkání dítěti mladšímu patnácti let v úmyslu spáchat trestný čin podle § 187 odst. 1, § 192, 193, § 202 odst. 2 nebo jiný sexuálně motivovaný trestný čin, bude potrestán odnětím svobody až na dvě léta“*. [55]

§ 207 Neoprávněné užívání cizí věci

Toto ustanovení se vztahuje pouze na fyzické nakládání se zařízením ICT. Nelze aplikovat na dálkový přístup do cizího informačního systému.[56]

---

[51] **SMEJKAL, V**. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. str. 266-267. ISBN 978-80-7380-720-7.
[52] **HULANOVÁ, L**. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. str. 59. ISBN 978-80-7387-545-9.
[53] **VANTUCH, P**. *Trestní právo. 2., dopl. a přeprac*. vyd. Brno: Rašínova vysoká škola, 2010. str. 167. ISBN 978-80-87001-17-2.
[54] **SMEJKAL, V**. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. str. 314. ISBN 978-80-7380-720-7.
[55] *Trestní předpisy: redakční uzávěrka ... Česko*. Ostrava: Sagit, 2010- . ÚZ: úplné znění
[56] **SMEJKAL, V**. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. str. 184. ISBN 978-80-7380-720-7.

§ 209 Podvod

Podvod patří na internetu k jedné z nejrozšířenějších trestných činností, kdy je zde možnost podvod páchat na dálku, za skrytou identitou, v neomezeném množství. Podvody mohou spočívat ve vymazání či přemazání údajů, uvedení v omyl jinou osobu, využije něčího omylu aj. Pachatelé jsou v této trestné činnosti velmi úspěšní.[57]

§ 228 Poškození cizí věci

Ke vztahu k výpočetní technice toto ustanovení rozděluje počítačový systém na hardware a software, kdy může být způsobena škoda na jedné nebo obou částech. Poškození se dělí do tří kategorií – zničení, poškození nebo učinění neupotřebitelnou. Aby se jednalo o protiprávní jednání, musí se jednat o cizí věc a být způsobena škoda nikoli nepatrná.[58]

§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací

Jedná se o paragraf, který vychází z původního § 257a zák. č. 140/1961 Sb. Z tohoto paragrafu byly vytvořeny dva nové paragrafy a to § 230 a § 231. Tímto rozdělením došlo k rozsáhlejší úpravě a popisu protiprávních jednání.[59] § 230 je složen z pěti odstavců, které slouží pro ochranu informací v počítačovém systému nebo předmětném datovém nosiči, kdy popisují jednotlivé skutkové podstaty s nakládáním získaných dat a způsobenou újmu.[60]

§ 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

Jedná se ryze o nové ustanovení trestního zákoníku, kdy předchozí trestní zákon toto ustanovení neobsahoval. Na základě tohoto ustanovení není nutné přímo proniknout do počítačového systému nebo se zmocnit neoprávněně nějakých údajů. K samotné trestnosti stačí „pouze“ přechovávat takové zařízení, program, heslo nebo přístupový kód, kterým lze zneužít jiný počítačový systém nebo z něj získat data. V

[57] **SMEJKAL, V**. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. str. 186-187. ISBN 978-80-7380-720-7.
[58] **SMEJKAL, V**. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. str. 177. ISBN 978-80-7380-720-7.
[59] **SMEJKAL, V**. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. str. 556. ISBN 978-80-7380-720-7.
[60] **VANTUCH, P.** *Trestní zákoník s komentářem: k ...* Olomouc: ANAG, 2011-. Právo (ANAG). str. 829 – 839. ISBN 978-80-7263-677-8.

tomto případě by se mohlo na celou věc pohlížet jako na přípravu k trestnému činu, který má být těmito prostředky spáchán.[61]

§ 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

Toto ustanovení bylo do trestního zákoníku zakotveno na základě požadavků orgánů činných v trestním řízení, kdy z praxe bylo zjištěno, že pachatelům se těžko dokazuje úmysl v jednání, přestože z povahy jednání a postavení samotného pachatele úmysl byl zřejmý. Zároveň se nešlo hojit na takovém zaměstnanci, který hrubě svou nedbalostí způsobil zaměstnavateli milionové škody nebo ohrozil celou organizaci. Aby osoba mohla být pro tento § trestně stíhaná, musí způsobit škodu z nedbalosti v minimální výši 500 000,- Kč (značná škoda), která je uvedena v 1. odstavci. Pro možnost vyššího udělení trestu, který je uveden v 2. odstavci, by osoba musela způsobit škodu v rozsahu minimálně 5 000 000,- Kč (škoda velkého rozsahu).[62]

§ 270 Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi

Porušování autorských práv v oblasti ICT se dá rozdělit na dvě větve:

- neoprávněné užívání (a/nebo šíření) počítačových programů
- neoprávněné užívání (a/nebo šíření) jiných autorských děl, zejména pak audiových a audiovizuálních děl (hudba, filmy).

Takovéto jednání může být způsobeno jak fyzicky, což znamená přímé předání nějakého nosiče, který obsahuje nelegální software. Může být ovšem způsobeno i nefyzickým způsobem, kdy takovýto software je zaslán elektronickou poštou, je sdělen link, kde se software nachází nebo je uložen na některém serveru, který funguje jako úložiště. Z praxe je možné softwarové pirátství rozdělit do čtyř skupin:[63]

- nelegální zásahy do softwaru
- nelegální výroba počítačových programů
- nelegální šíření softwaru
- nelegální užívání počítačových programů

[61] **SMEJKAL, V**. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. str. 580. ISBN 978-80-7380-720-7.
[62] **SMEJKAL, V**. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. str. 585. ISBN 978-80-7380-720-7.
[63] **SMEJKAL, V**. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. str. 491. ISBN 978-80-7380-720-7.

Za zmínku v souvislosti s porušováním autorských práv jistě stojí volně přístupná úložiště v prostoru internetu, které slouží pro ukládání především filmových, hudebních, ale i textových děl chráněných autorským zákonem. K těmto dílům má přístup omezený, ale většinou neomezený okruh uživatelů.[64]

§ 355 Hanobení národa, rasy, etnické nebo jiné skupiny osob

Toto jednání by se dalo zařadit do skupiny, která využívá informační systémy k šíření zpráv směřujících proti určitým osobám nebo celým skupinám osob.[65] Pachatel za pomoci veřejné počítačové sítě hanobí některý národ, jazyk, příslušnost k rase nebo některé z etnických skupin, politické nebo náboženské přesvědčení. Chráněny v tomto případě jsou především základní lidská práva.[66]

§ 356 Podněcování k nenávisti vůči skupině osob nebo k omezování práv a svobod

Toto jednání by se dalo stejně jako § 355 zařadit do skupiny, která využívá informační systémy k šíření zpráv směřujících proti určitým osobám nebo celým skupinám osob.[67] Pachatel za pomoci počítačové sítě „*veřejně podněcuje k nenávisti k některému národu, rase, etnické skupině, náboženství, třídě nebo jiné skupině osob nebo k omezování práv a svobod jejich příslušníků*“.[68]

§ 357 Šíření poplašné zprávy

V současné době se dá šířit poplašná zpráva prostřednictvím internetové komunikace, kdy pachatel prostřednictvím webových stránek nebo e-mailu rozesílá zprávy, kterými může znepokojit část obyvatelstva. Tyto informace rozesílá nebo zveřejňuje, přestože se nezakládají na pravdě. Pachatel se většinou snaží získat tímto jednáním nějaký prospěch pro svou nebo cizí osobu.[69]

---

[64] **SMEJKAL, V**. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. str. 504. ISBN 978-80-7380-720-7.
[65] **SMEJKAL, V**. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. str. 473. ISBN 978-80-7380-720-7.
[66] **KRUPKA, V**. *Trestní právo hmotné - zvláštní část: (vybrané skutkové podstaty trestných činů a souvisejících přestupků).* Praha: Armex, 2012. Skripta pro střední a vyšší odborné školy. str. 119. ISBN 978-80-87451-12-0.
[67] **SMEJKAL, V**. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. str. 473. ISBN 978-80-7380-720-7.
[68] **VANTUCH, P.** *Trestní zákoník s komentářem: k ...* Olomouc: ANAG, 2011-. Právo (ANAG). str. 1237. ISBN 978-80-7263-677-8.
[69] **SMEJKAL, V**. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. str. 375 - 377. ISBN 978-80-7380-720-7.

5 Kvalitativní výzkumné šetření

5.1 Cíl praktické části

Praktická část bakalářské práce s názvem „Nové trestné činy - kyberkriminalita“ je zaměřena na širokou veřejnost bez konkrétní specifikace.

Cílem praktické části bakalářské práce bylo zobrazit postupný nárůst počtu případů kyberkriminality a metodou dotazníkového šetření zjistit chování obětí kyberkriminality a způsoby, kterými se snaží těmto napadením předcházet eventuálně analyzovat bezpečný pohyb osob v internetovém prostoru, především stahování neznámých příloh do počítačového systému a samotné zabezpečení vlastního informačního systému.

5.1.1 Stanovení předpokladů

Pro praktickou část bakalářské práce byly stanoveny tři předpoklady. Předpoklady byly ověřovány dotazníkovým šetřením.

■ Předpoklad č. 1

Lze předpokládat, že min 70% respondentů se již setkalo s protiprávním jednáním proti své osobě, které bylo uskutečněno prostřednictvím počítačových systémů.

■ Předpoklad č. 2

Lze předpokládat, že více jak 70% respondentů své informační systémy a data chrání pouze základním volně dostupným antivirovým systémem.

■ Předpoklad č. 3

Lze předpokládat, že více jak 60% respondentů napadení svého počítačového systému ignoruje.

5.2 Průběh průzkumu

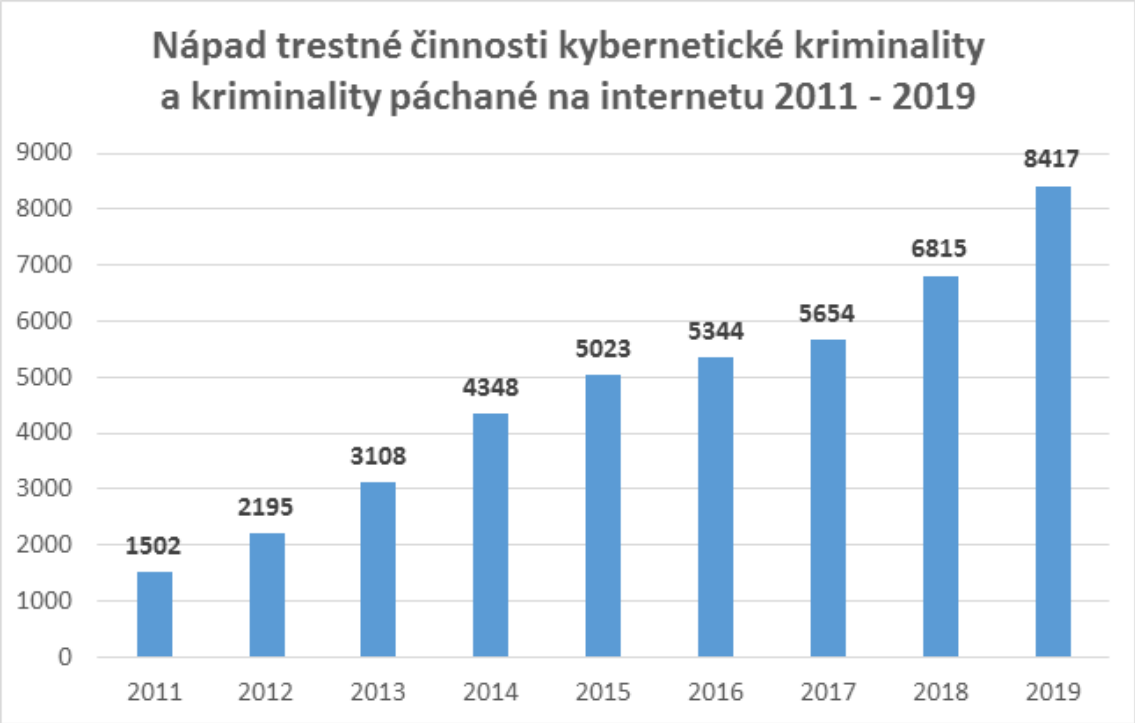
Realizace průzkumu v praktické části bakalářské práce byla prováděna prostřednictvím serveru www.survio.cz, který je specializovaný na tvorbu dotazníků. Zde bylo vytvořeno 14 otázek, které měly směřovat k potvrzení nebo vyvrácení určených předpokladů případně zjistit nové poznatky v oblasti kyberkriminality.

Samotný odkaz na tento dotazník byl následně několikrát sdílen mezi veřejnost, a to prostřednictvím sociálních sítí. Dotazník bylo možnost vyplnit v období od 8.1.2020 do 20.2.2020. Za tuto dobu dotazník vyplnilo 238 respondentů.

5.3 Nápad trestné činnosti kybernetické kriminality a kriminality páchané na internetu 2011 - 2019

Jak ukazuje níže uvedený graf od roku 2011 do roku 2019 kybernetická kriminalita je každým rokem na vzestupu a ročně pomocí počítačových systémů se uskutečňuje více a více protiprávních jednáních. Největší nárůst byl právě zaznamenán mezi posledními hodnocenými roky 2018 a 2019, kdy se počet skutků zvýšil o 23,5%. Toto byl jeden z důvodů níže vytvořeného dotazníkového šetření a zjištění jak osoby na kyberkriminalitu reagují.

Graf č. 1 – Nápad trestné činnosti kybernetické kriminality

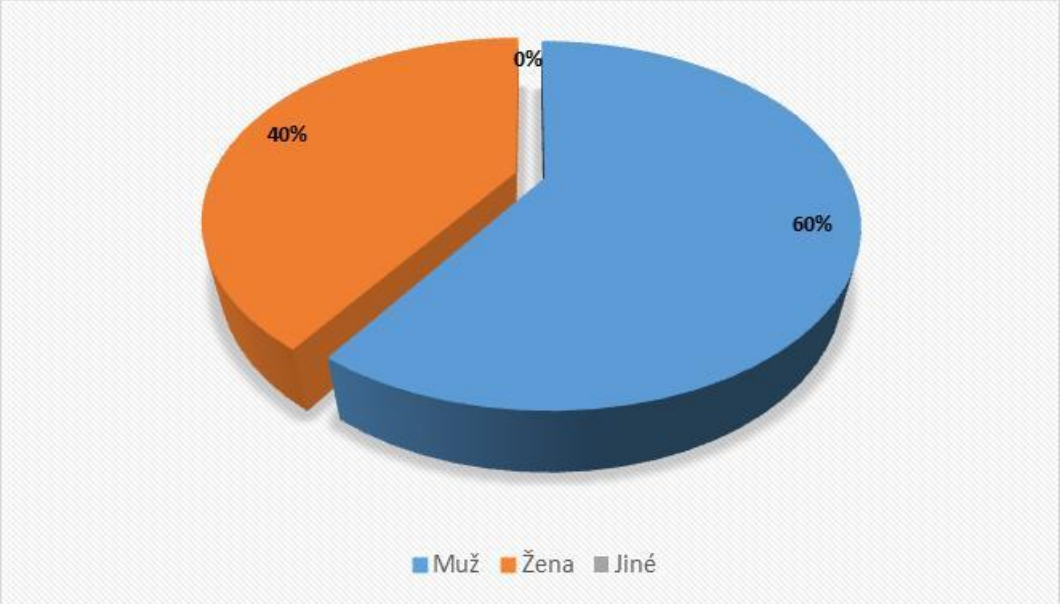


zdroj: https://www.policie.cz/clanek/kyberkriminalita.aspx

5.4 Výsledky dotazníkového šetření a jejich interpretace

Pohlaví respondentů

Graf č. 2 – Pohlaví respondentů



Tabulka č. 1 – Pohlaví respondentů

Pohlaví	Počet	%
Muž	142	60
Žena	96	40
Jiné	0	0

Otázka č. 1 byla zaměřena na zjištění pohlaví respondentů. Z výsledku vyplynulo, že dotazník vyplnilo dohromady 238 respondentů. Z tohoto počtu jsou muži zastoupeni počtem 142 respondentů, tj. 60%, ženy v počtu 96 respondentů, tj. 40 % nikdo z respondentů neuvedl, že by se považoval za jiné pohlaví.

Nejvyšší dosažené vzdělání respondentů

Graf č. 3 – Nejvyšší dosažené vzdělání respondentů

Tabulka č. 2 – Nejvyšší dosažené vzdělání respondentů

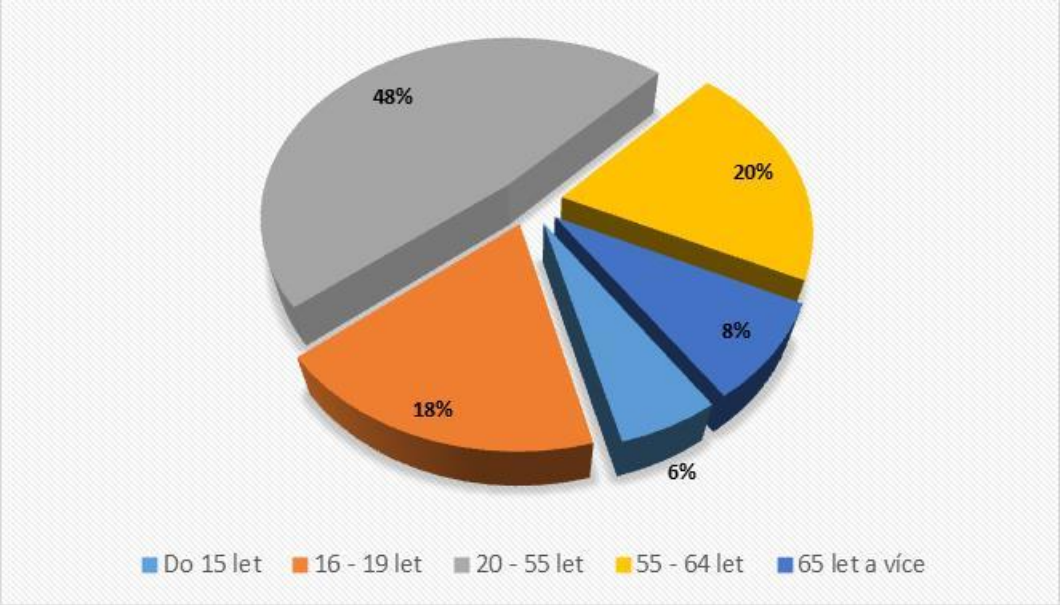
Nejvyšší dosažené vzdělání	Počet	%
Neukončené základní vzdělání	13	5
Základní	37	16
Střední odborné s výučním listem	48	20
Střední s maturitou	70	29
Vyšší odborné	11	5
Vysokoškolské	59	25

Otázka č. 2 byla zaměřena na zjištění nejvyššího dosažené vzdělání respondentů. Z výsledku dotazníkového šetření vyplynulo, že největší zastoupení z odpovídajících osob dosáhlo středního vzdělání s maturitou v celkovém zastoupení 70 osob, tj. 29%. Druhou největší skupinou odpovídajících jsou osoby s vysokoškolským vzděláním

v zastoupení 59 osob, tj. 25%. Dále jsou v menším zastoupení za sebou sestupně seřazeny osoby se středním odborným vzděláním s výučním listem v počtu 48 osob, tj. 20%, základním vzděláním v počtu 37 osob, tj. 16%, neukončené základní vzdělání v počtu 13 osob, tj. 5% a vyšší odborné vzdělání v počtu 11 osob, tj. 5%.

Věk respondentů

Graf č. 4 – Věk respondentů



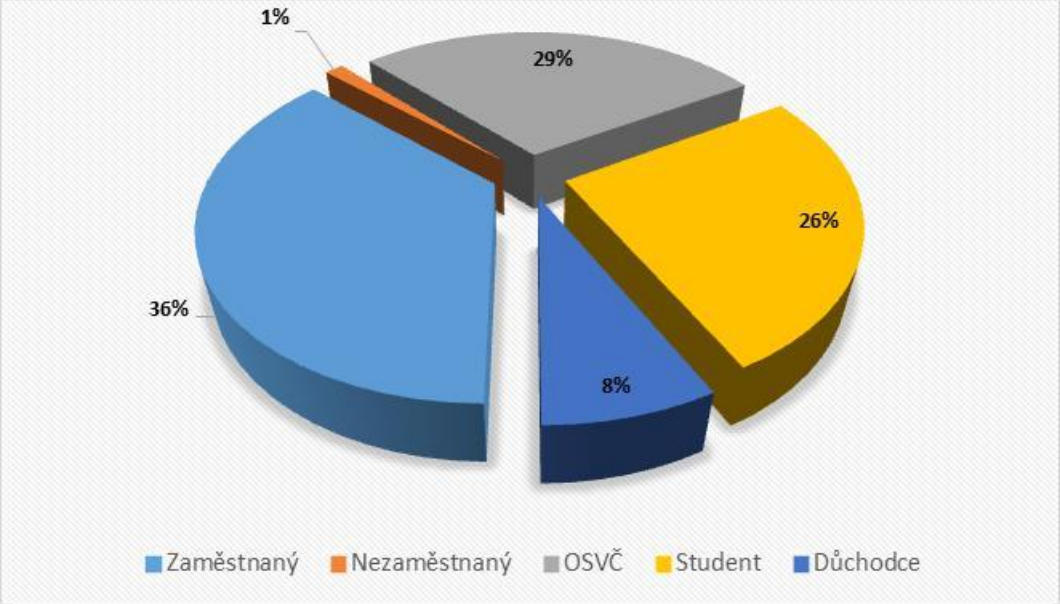
Tabulka č. 3 – Věk respondentů

Věk	Počet	%
Do 15 let	13	6
16 – 19 let	43	18
20 – 55 let	114	48
56 – 64 let	48	20
65 let a více	20	8

Otázka č. 3 byla zaměřena na zjištění věku respondentů. Z výsledku dotazníkového šetření vyplynulo, že největší zastoupení z odpovídajících osob dosáhlo věku v rozmezí mezi 20 až 55 lety v celkovém zastoupení 114 osob, tj. 48%. Za touto skupinou následuje věková skupina 55 až 64 let v zastoupení 48 osob, tj. 20%. S mírným odstupem následuje věková skupina 16 až 19 let, kterou uvedlo celkem 43 osob, tj. 18%. K věkové skupině 65 let a více se přihlásilo celkem 20 osob, tj. 8% a nejméně zastoupenou skupinou byly osoby do 15 let v počtu 13 osob, tj. 6%.

Sociální status respondentů

Graf č. 5 - Sociální status respondentů



Tabulka č. 4 - Sociální status respondentů

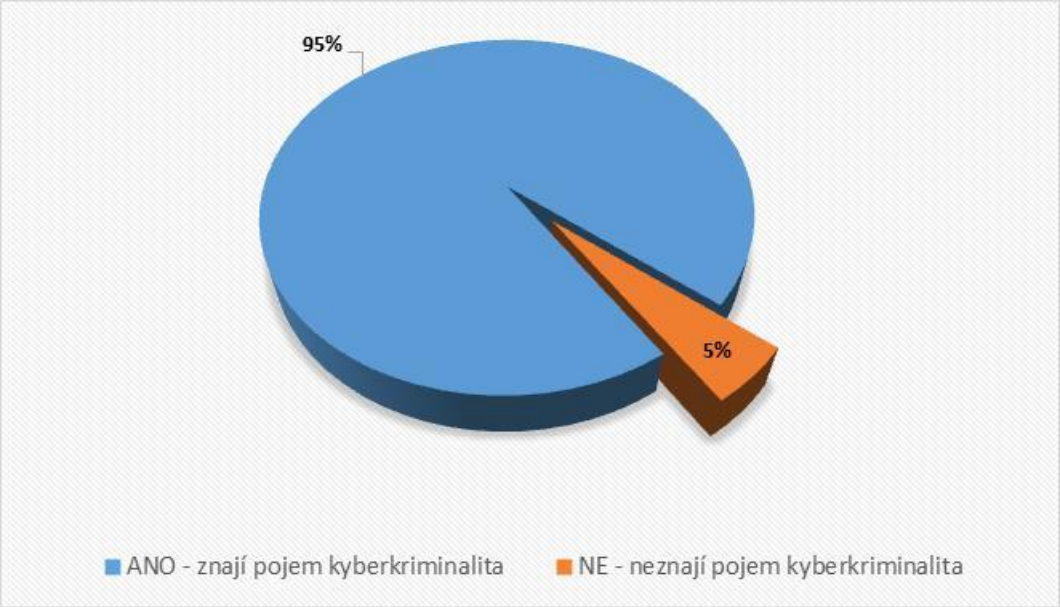
Sociální status	Počet respondentů	%
Zaměstnanec	87	36
OSVČ	68	29
Student	62	26

Důchodce	18	8
Nezaměstnaný	3	1

Otázka č. 4 byla zaměřena na zjištění sociálního statusu respondentů. Z výsledku dotazníkového šetření vyplynulo, že nejvíce respondentů je v zaměstnaneckém poměru, tato kategorie je v zastoupení 87 osob, tj. 36%. Druhou nejpočetnější kategorií je skupina osob OSVČ v zastoupení 68 osob, tj. 29%. S menším odstupem následuje třetí skupina, a to studenti v počtu 62 osob, tj. 26%. Výrazně v nižším zastoupení oproti předešlým skupinám je skupina důchodce, kde je zaznamenáno 18 osob, tj. 8%. Poslední a nejméně zastoupenou skupinou je skupina nezaměstnaných s počtem 3 osoby, tj. 1%.

Znalost pojmu kyberkriminalita

Graf č. 6 - Znalost pojmu kyberkriminalita



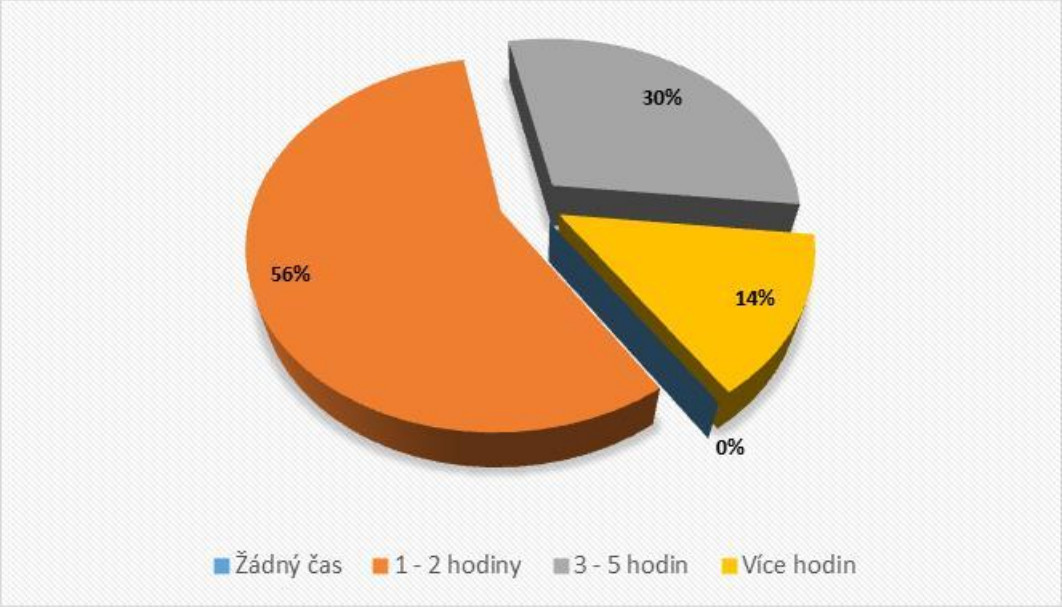
Tabulka č. 5 - Znalost pojmu kyberkriminalita

Znalost pojmu – kyberkriminalita	Počet respondentů	%
ANO, zná pojem	226	95
NE, nezná pojem	12	5

Otázka č. 5 byla zaměřena na zjištění, zda se respondenti někdy setkali s pojmem kyberkriminalita, která se v poslední době stává velkým tématem dnešní společnosti. Zde jednoznačný počet 226 osob, tj. 95%, odpovědělo, že již pojem kyberkriminalita slyšely. Přesto se našlo 12 osob, tj. 5%, které uvedly, že se s pojmem kyberkriminalita ještě nesetkaly.

Čas strávený na internetu

Graf č. 7 - Čas strávený na internetu



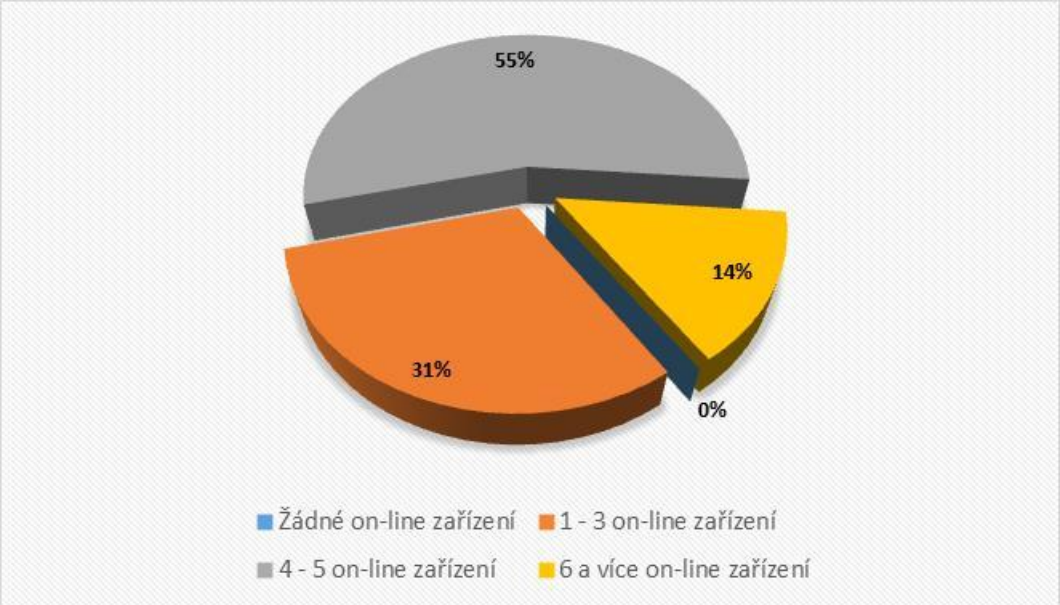
Tabulka č. 6 - Čas strávený na internetu

Čas strávený na internetu	Počet respondentů	%
Žádný	0	0
1-2 hodiny	134	56
3-5 hodin	71	30
Více jak 5 hodin	33	14

Otázka č. 6 byla zaměřena na zjištění, kolik času denně respondenti tráví na internetu. Největší skupinu tvoří 134 osob, tj. 56 %, které tráví na internetu 1 až 2 hodiny denně. Druhou skupinou jsou osoby, které tráví na internetu 3 až 5 hodin denně, kdy se jedná o 71 osob, tj. 30%. Nejvíce hodin na internetu denně, což je 5 hodin a více tráví 33 respondentů, tj. 14%. V kategorii osob, které netráví na internetu žádný čas, se nikdo neobjevil.

Počet on-line připojených zařízení v domácnosti

Graf č. 8 - Počet on-line připojených zařízení v domácnosti



Tabulka č. 7 - Počet on-line připojených zařízení v domácnosti

Počet on-line připojených zařízení v domácnosti	Počet respondentů	%
Žádné	0	0
1-3 ks	73	31
4-5 ks	131	55
6 a více ks	34	14

Otázka č. 7 byla zaměřena na zjištění, kolik počítačových systémů má respondent ve své domácnosti připojených do datové sítě tzv. on-line. Nejvíce početnou skupinu tvoří 131 osob, tj. 55%, kdy tyto osoby uvedly, že mají připojeny 4 až 5 počítačových systémů. Druhou nejpočetnější skupinou je skupina s 1 až 3 počítačovými systémy, kterou tvoří 73 osob, tj. 31%. Šest a více počítačových systémů ve své domácnosti má připojeno 34 osob, tj. 14%. Z dotazovaných osob nikdo neodpověděl, že by neměl doma ani jeden připojený počítačový systém.

Druh použité ochrany počítačového systému

Graf č. 9 - Druh použité ochrany počítačového systému

Tabulka č. 8 - Druh použité ochrany počítačového systému

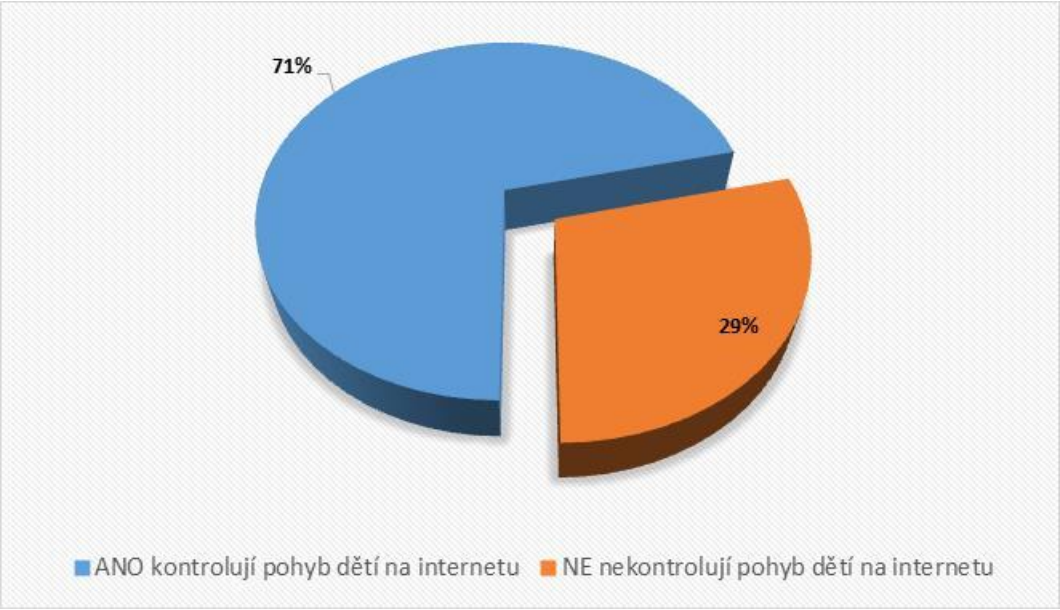
Druh použité ochrany počítačového systému	Počet respondentů	%
Žádný	29	12
Volně dostupný antivirový program	191	80
Placený antivirový program	18	8

Otázka č. 8 byla zaměřena na zjištění, jakým způsobem mají respondenti chráněný svůj počítačový systém, aby ochránily svá data před případným napadením nebo v případě již uskutečněného napadení. Z výsledku dotazníkového šetření vyplynulo, že 191 osob, tj. 80%, používá pouze základní antivirový program. Investici do ochrany svého počítačového systému a dat provedlo 18 osob, tj. 18% a 29 osob z dotazovaných, tj. 12%, uvedlo, že žádnou antivirovou ochranu ve svém počítačovém systému nepoužívá.

V tomto bodě byl plně potvrzen předpoklad č. 2 - lze předpokládat, že více jak 70% respondentů své informační systémy a data chrání pouze základním volně dostupným antivirovým systémem. Zde uvedlo 80% respondentů a zároveň potencionálních obětí, že používá pouze základní volně dostupný antivirový program, který je schopen detekovat pouze základní kybernetické hrozby. Vlastní data např. soubory různých obrazových, textových a audiových typů, případně samotné přístupy k různým sociálním sítím, bankovním účtům a i vlastní soukromí je v tomto případě velmi ohroženo, přestože je nějakým alespoň částečným způsobem počítačový systém chráněn. Velkým překvapením bylo, že 12% osob vůbec žádnou ochranu svého počítačového systému nepoužívá. Tento hazard s vlastními daty by se dal přirovnat k předání klíčů od svého bytu neznámé osobě.

Kontrola pohybu dětí na internetu do 15 let

Graf č. 10 – Kontrola pohybu dětí na internetu do 15 let



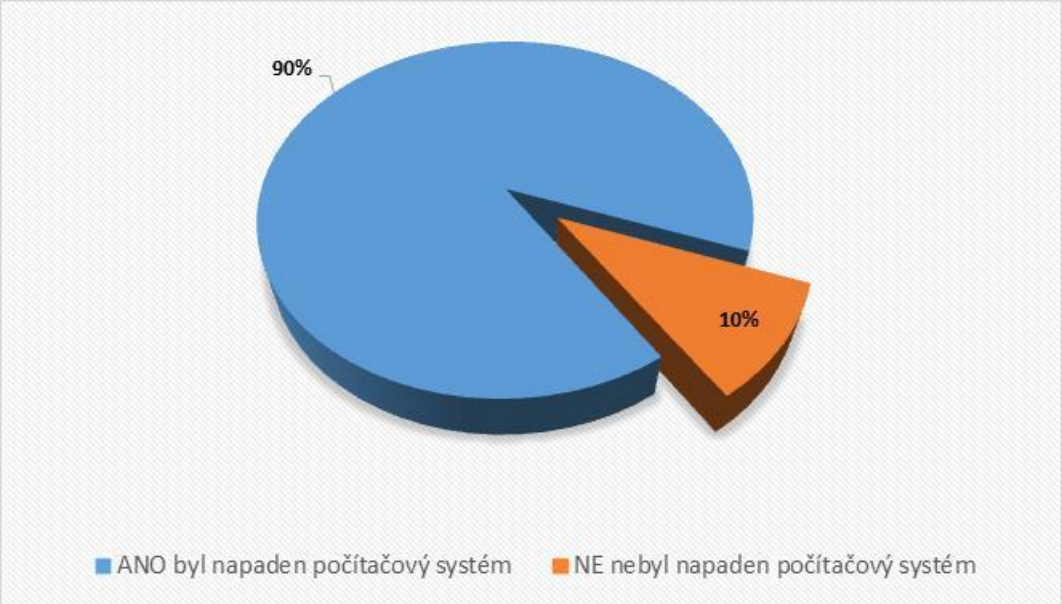
Tabulka č. 9 – Kontrola pohybu dětí na internetu do 15 let

Rodiče, kteří kontrolují nebo nekontrolují pohyb svých dětí na internetu	Počet respondentů	%
ANO – kontrolují	31	69
NE – nekontrolují	14	31

Otázka č. 9 byla zaměřena na zjištění, zda rodiče kontrolují pohyb svých dětí na internetu. Otázka byla určena jen pro rodiče s dětmi do 15 let. Na tuto otázku odpovědělo z celkového počtu respondentů 45 osob. Odpovědi na dotazník ukázaly, že více jak 2/3 rodičů pohyb svých dětí v prostředí internetu kontroluje, a to konkrétně 31 osob, tj. 69%, zbylých 14 osob, tj. 31% uvedlo, že své děti nekontroluje při jejich pohybu v prostředí internetu.

Napadení počítačového systému

Graf č. 11 - Napadení počítačového systému



Tabulka č. 10 - Napadení počítačového systému

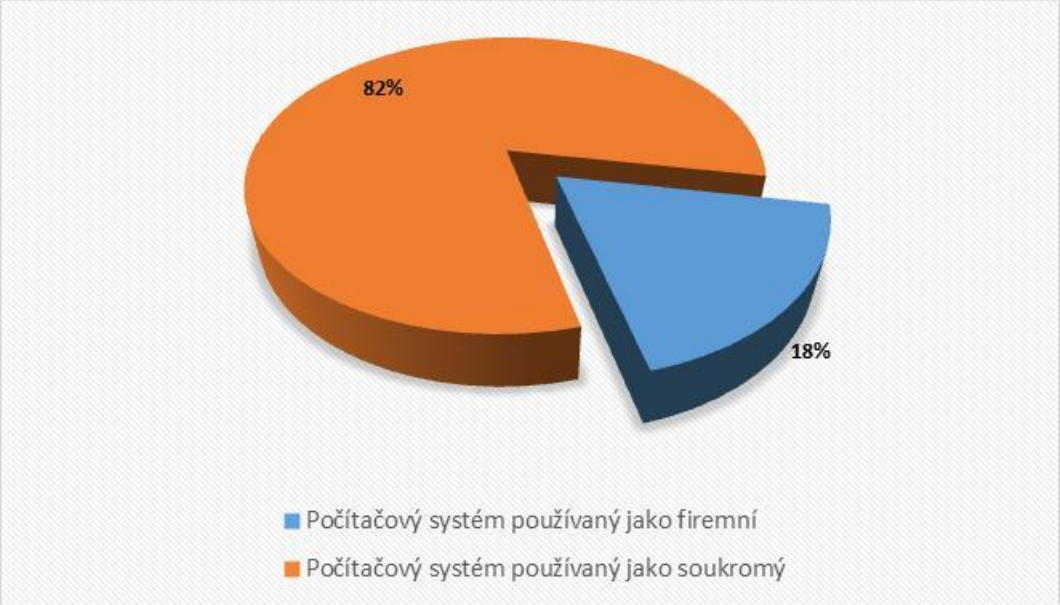
Byl napaden Váš počítačový systém	Počet respondentů	%
ANO, byl napaden	214	90
NE, nebyl napaden	24	10

Otázka č. 10 byla zaměřena na pouhé zjištění, zda se respondenti už setkali přímo s napadením jejich počítačového systému. Celých 90%, tj. 214 osob odpovědělo, že jejich počítačový systém už napaden byl. Oproti tomu 24 osob, tj. 10% odpovědělo, že jejich počítačový systém napaden nebyl.

V tomto případě byl naprosto potvrzen a velkou měrou přesažen daný předpoklad č. 1 – (lze předpokládat, že více jak 70% respondentů se již setkalo s protiprávním jednáním proti své osobě, které bylo uskutečněno prostřednictvím počítačových systémů). Za zmínku v tomto bodě stojí, že při bližším zkoumání jednotlivých odpovědí respondentů bylo zjištěno, že několik osob, které uvedly svůj stav jako důchodový, nikdy neslyšely pojem kyberkriminalita a zároveň uvedly, že jejich počítačový systém nebyl nikdy napaden. Zde by se dalo předpokládat, že tyto osoby si neuvědomují, že na ně byl směrován některý z kybernetických útoků a též si nedokáží tento útok přiřadit pod pojem kyberkriminalita. Vzhledem k této skutečnosti může být procentuální číslo napadených některým z kybernetických útoků ještě vyšší.

Druh napadeného počítačového systému

Graf č. 12 - Druh napadeného počítačového systému



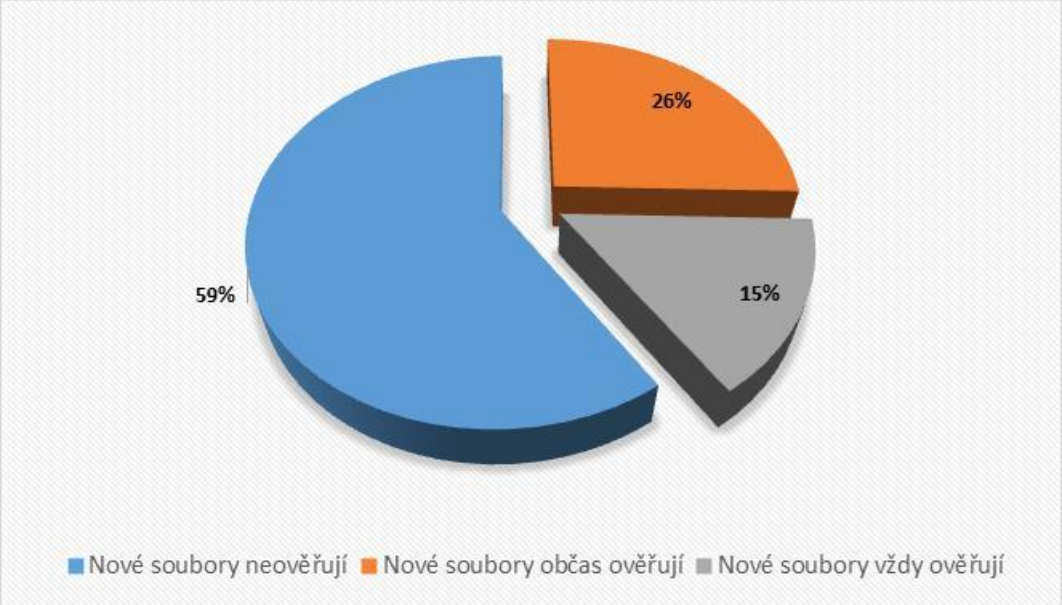
Tabulka č. 11 - Druh napadeného počítačového systému

Pro jaké účely byl používán napadený počítačový systém	Počet respondentů	%
Soukromý	175	82
Firemní	39	18

Otázka č. 11 byla zaměřena na zjištění, zda počítačový systém, který respondent používá, byl napaden jako soukromý nebo firemní. Z otázky vyplynulo, že z celkového počtu 214 napadených počítačových systémů bylo 175, tj. 82 %, používáno jako soukromý počítačový systém (útok byl směrován proti soukromé osobě) a 39 počítačových systémů bylo napadeno jako firemní počítačový systém, tj. 18% (útok byl směrován proti firmě).

Ověření nových souborů

Graf č. 13 - Ověření nových souborů



Tabulka č. 12 - Ověření nových souborů

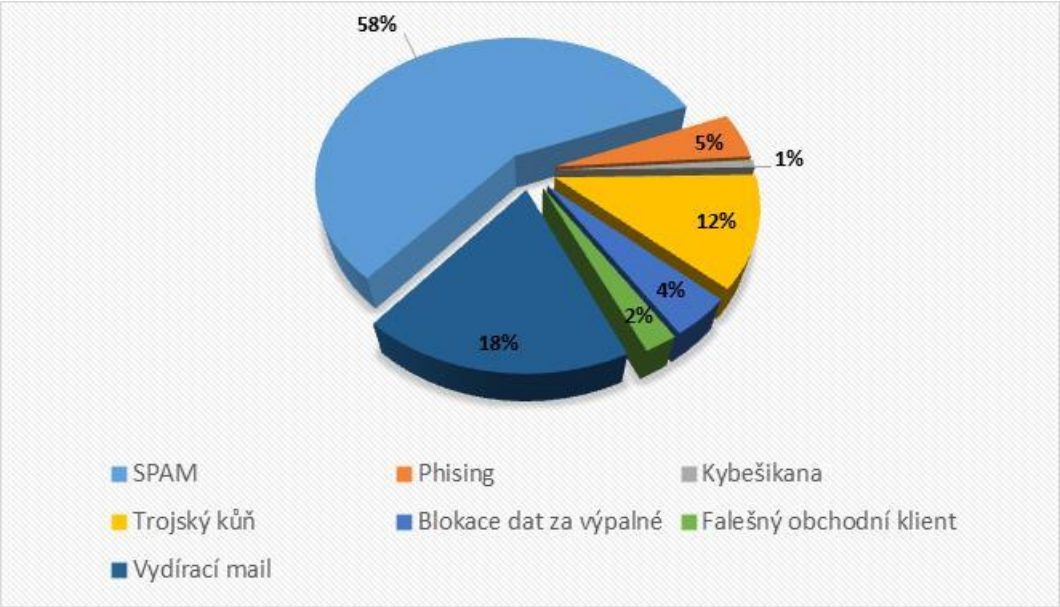
Ověřování nových stažených souborů	Počet respondentů	%
Nikdy soubor neověřují	141	59
Soubor ověřují občas	61	26
Vždy soubor ověřují	36	15

Otázka č. 12 byla zaměřena na zjištění, zda respondenti se chovají obezřetně vzhledem ke stahování a následnému otevírání nových souborů v počítačovém systému. Otázka přesně zjišťovala, zda si nový stažený soubor respondent vždy ověří před otevřením nebo ho ověří pouze občas nebo nikdy otevíraný soubor neověřuje. Z dotazníku bylo zjištěno, že nejvíce osob 141, tj. 59%, stahovaný a následně otevíraný soubor nikdy neověřuje, 61 osob, tj. 26%, nově stažený soubor do svého počítačového

systému občas ověří a nejmenší část tvoří 36 osob, tj. 15%, kdy tyto osoby vždy nově stažený soubor ověří před jeho otevřením.

Typ kybernetického útoku

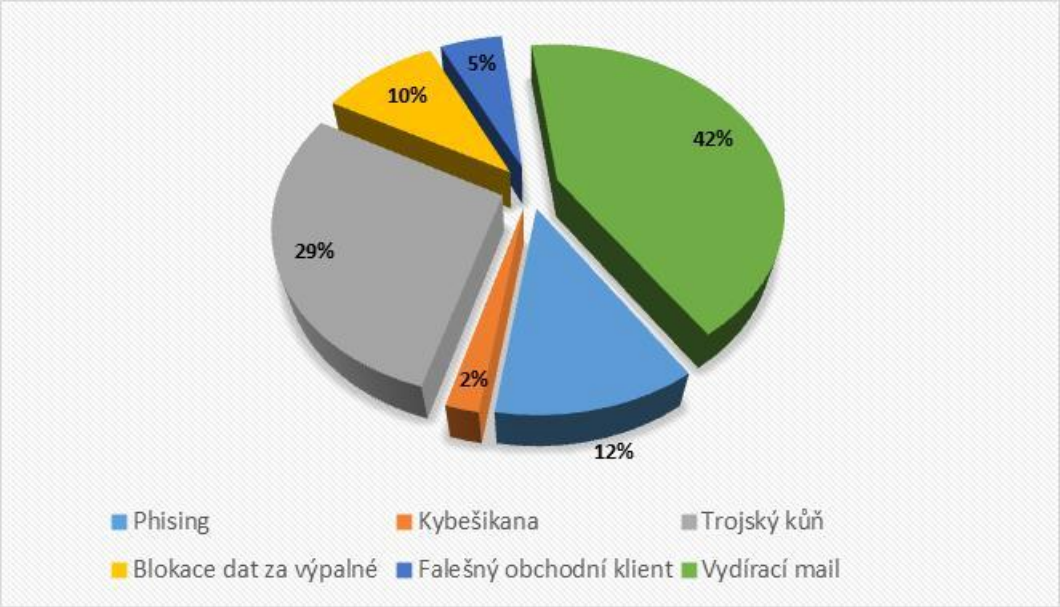
Graf č. 14a - Typ kybernetického útoku (včetně SPAMU)



Tabulka č. 13a - Typ kybernetického útoku (včetně SPAMU)

Typ napadení počítačového systému	Počet respondentů	%
SPAM	206	58
Vydírací mail	64	18
Trojský kůň	43	12
Phishing	18	5
Blokace disku	15	4
Falešný obchodní klient – faktura	8	2
Kyberšikana	3	1

Graf č. 14b - Typ kybernetického útoku (bez SPAMU)



Tabulka č. 13b - Typ kybernetického útoku (bez SPAMU)

Typ napadení počítačového systému	**Počet respondentů**	**%**
Vydírací mail	64	42
Trojský kůň	43	29
Phishing	18	12
Blokace disku	15	10
Falešný obchodní klient – faktura	8	5
Kyberšikana	3	2

Otázka č. 13 byla zaměřena na zjištění, jakým způsobem byl počítačový systém respondentů napaden. U této otázky mohl respondent uvést v jedné odpovědi více druhů napadení. Z celkového počtu 214 respondentů, kteří měli nějakým způsobem svůj počítačový systém napaden, bylo celkem uvedeno 357 napadení. Nejvíce napadení tzv. SPAMEM, bylo uvedeno téměř u každého z odpovídajících respondentů, tj. 206 respondentů, tj. 58%. Druhým nejvíce početným napadením přes operační systém bylo uváděno zaslání tzv. vydíracího e-mailu, kdy takto odpovědělo 64 respondentů, tj. 18 %.

Dalším útokem uvedeným 43 respondenty, tj. 12 %, je aplikování trojského koně do počítačového systému. Dále sestupně dle počtu uvedení jsou tyto napadení Phishing v počtu 18, tj. 5%, 15 x blokování dat na operačním disku, tj. 4%, 8 x falešný obchodní klient – faktura, tj. 2% a posledním případem v zastoupení, nikoliv ve vážnosti napadení, byla od 3 respondentů uvedena kyberšikana.

Jelikož bylo v dotazníku několikrát uvedeno, že napadení SPAMEM je každodenní záležitostí, je v uvedeném grafu ukázáno procentuální zastoupení napadení bez napadení SPAMEM. V tomto případě se výrazně mění procentuální zastoupení jednotlivých kybernetických protiprávních jednání. Tyto protiprávní jednání jsou následně sestupně seřazena takto: 64x vydírací e-mail, tj. 42 %, 43x aplikován trojský kůň, tj. 29 %, 18x Phishing blokování dat na operačním disku, tj. 12 %, 15x blokování dat na operačním disku, tj. 10%, 8x falešný obchodní klient – faktura, tj. 5% a 3x kyberšikana, tj. 2%.

Výše uváděná procenta jsou vždy procenta z celkového počtu napadení, tedy v případě grafu, který je uváděn se SPAMEM, je to z celkového počtu 357 napadení a v případě grafu, který je uváděn bez SPAMU, je to z celkového počtu 151 napadení.

Řešení kybernetického útoku

Graf č. 15 - Řešení kybernetického útoku

Tabulka č. 14 Řešení kybernetického útoku

Způsob řešení kybernetického útoku	Počet respondentů	%
Ignorování napadení	197	67
Přeinstalování operačního systému	43	14
Pořízení antivirového programu	27	9
Splnění požadavků útočníka	12	4
Předání IT specialistům	11	4
Oznámení příslušným orgánům	6	2

Otázka č. 14 byla určena pro zjištění, jakým způsobem respondenti řeší napadení svého počítačového systému. Odpověď umožňovala zapsat respondentovi více druhů řešení, ale bylo požadováno zapsání alespoň nejzásadnějšího řešení. Celkem odpovědělo 214 respondentů, kdy uvedli 296 odpovědí. U prováděného dotazníkového šetření bylo 197x, tj. 67%, odpovězeno, ignorování napadení, dalších 43 odpovědí, tj. 14%, uvádělo přeinstalování operačního systému. Dále bylo 27x uvedeno pořízení nového antivirového programu. S téměř stejným počtem odpovědí je za sebou 12x, tj. 4% splnění požadavků útočníka a 11x, tj. 4% předání věci IT specialistům. Šest odpovědí, tj. 2% uvádělo, že věc byla nahlášena příslušným orgánům.

V tomto bodě by se z prvotních údajů mohlo zdát, že byl potvrzen předpoklad č. 3 - lze předpokládat, že více jak 60% respondentů napadení svého počítačového systému ignoruje. Zde opravdu v největším procentuálním zastoupení 67% bylo odpovězeno, že je napadení ignorováno. Pokud ovšem odpovědi analyzujeme důkladněji, zjistíme, že většina odpovědí, kde bylo uvedeno, že napadení bylo ignorováno, byl uváděn jako útok napadení SPAM. V naprosté většině dalších druhů kybernetických útoků byl nějakým způsobem ze strany respondenta útok řešen a respondent na něj reagoval. Například u vydíracího mailu byl z 64 útoků požadavek útočníka splněn 4x, u patnácti blokací dat na operačním disku byl požadavek splněn 2x. Pouze šest případů bylo nahlášeno

příslušným orgánům, a to v případě tří falešných obchodních faktur, dvou kyberšikany a jednoho phishingu. V ostatních případech se respondenti snažili věc vyřešit vlastními silami, a to přeinstalováním operačního systému, pořízením antivirového programu nebo předáním specialistovi. Z těchto údajů bylo zjištěno, že pokud se jedná o některý ze specifičtějších kybernetických útoků, napadená osoba většinou věc neignoruje, a naopak na útok nějakým způsobem reaguje.

5.4.1 Celkové zhodnocení dotazníku

Z výše uvedených grafů a dat se dá odvodit více závěrů než pouze udělat závěry na uvedené předpoklady. Ovšem pro lepší představu o celé situaci, je potřeba si dotazníkové šetření vzít jako celek a některé odpovědi důkladněji analyzovat, případně mezi sebou i propojit.

Z dotazníku vyplývá, že v dnešní tzv. počítačové době bychom jen těžko hledali některou věkovou skupinu, která by neměla alespoň minimální zkušenost s nějakým počítačovým systémem a nezáleží ani na jejím pohlaví nebo, zda je osoba zaměstnána, student či je již důchodového věku ani na stupni nejvyššího dosaženého vzdělání. Celkem 100% odpovídajících uvedlo, že tráví každý den alespoň nějaký minimální čas na internetu, kdy 30% odpovědělo, že tráví 3 až 5 hodin denně na internetu a 14%, že zde tráví více jak 5 hodin, tzn., že v průměru 44% lidí tráví na internetu 4 hodiny denně. Z produktivní části dne (kdy je člověk vzhůru) se jedná poměrně o podstatný časový úsek. Nadpoloviční většina respondentů uvedla, že mají ve své domácnosti připojeno 4 až 5 počítačových systémů, kdy každý z těchto počítačových systémů se může stát pro útočníka pomyslnou vstupní branou do soukromí jejich uživatelů. Přestože většina domácností nabízí více možností pro kybernetický útok a lidé tráví mnoho času ve virtuálním světě, kam se často svěřují s věcmi ze svého soukromí, ukládají zde pro sebe velmi důležité soubory a data, ke kterým mívají citové vazby a někdy jsou pro ně i existenčně důležité jako například peníze na bankovním účtu, nemají svá data řádně zabezpečena. Najdou se i osoby, které používají počítačové systémy, ale vůbec žádným způsobem svá data nechrání. Většina uživatelů používá základní antivirový program, který nedokáže detekovat novější a více specifičtější kybernetické hrozby. Z tohoto vyplývá, že se pohyb v kyberprostoru stal každodenní součástí života, přesto se někteří lidé domnívají, že pro ochranu počítačového systému je postačující pouze volně

dostupný antivirový program a nejsou ochotni investovat své finanční prostředky pro jeho lepší ochranu, případně tím alespoň ztížit pachateli provedení jeho kybernetického útoku. Lidé se pohybují často po kyberprostoru velmi nerozvážně a věří, že jim se kybernetický útok vyhne a věci řeší až po provedeném útoku. Z tohoto je zřejmé, že útočníkům se vyplatí na své oběti útočit, neboť 4% napadených, tj. každá 20 osoba, jak bylo zjištěno v tomto dotazníkovém šetření, splní požadavky útočníka a v celkovém součtu se může jednat o velkou sumu peněz, ke které si pachatel za minimálního úsilí a při minimálním riziku přijde, protože kybernetické útoky bývají příslušným orgánům hlášeny pouze v minimálních případech.

Závěr

Téma bakalářské práce „Nové trestné činy - kyberkriminalita“ je tématem velice obsáhlým. Značný rozvoj informačních technologií vnesl do společnosti nový fenomén škodlivého jednání a v poslední době je nezbytné tomuto věnovat stále větší pozornost. Bakalářská práce se proto pokusila zmapovat základní problematiku kybernetické trestné činnosti.

Cílem teoretické části bakalářské práce je definování kyberkriminality, objasnění základních pojmů s ní souvisejících a zmapování toho, kdo a proč páchá tuto nezákonnou činnost. Dále se teoretická část snažila přiblížit a upozornit na některé základní i specifičtější způsoby kybernetických útoků proti počítačovým systémům. Je zde též uvedena základní právní úprava kyberkriminality.

Druhá část bakalářské práce je věnována dotazníkovému šetření a jeho vyhodnocení. Cílem bylo pomoci dotazníku zjistit, zda si lidé při používání kyberprostoru uvědomují, že jsou vystaveni riziku napadení svých počítačových systémů a považují-li jejich zabezpečení za dostačující. Za účelem šetření byl vytvořen dotazník obsahující 14 otázek. Dotazník byl vytvořen na serveru www.survio.cz a zveřejněn na sociálních sítích v období od 8.1.2020 do 20.2.2020. Na otázky odpovídala anonymně široká veřejnost, v konečném součtu se šetření zúčastnilo 238 osob.

Na základě vyplněných dotazníků je možné částečně odvodit potvrzení či vyvrácení stanovených předpokladů. Šetřením byl potvrzen předpoklad č. 1, že více jak 70% respondentů se již setkalo s protiprávním jednáním proti své osobě, které bylo uskutečněno prostřednictvím počítačových systémů.

Byl potvrzen předpoklad č. 2, že více jak 70% respondentů své informační systémy a data chrání pouze základním, tudíž volně dostupným antivirovým systémem a z prvotních více neanalyzovaných odpovědí byl potvrzen též předpoklad č. 3, že více jak 60% respondentů napadení svého počítačového systému ignoruje, ovšem po bližší analýze odpovědí by se dal tento předpoklad považovat za nepotvrzený.

V průběhu zpracování předložené bakalářské práce byla získána řada nových poznatků o problematice kyberkriminality a bylo zjištěno, že tato problematika je

natolik rozsáhlá, že v rámci jedné bakalářské práce není možno veškerou problematiku pojmout. Přestože se v šetření část respondentů s kyberkriminalitou nesetkala, lze předpokládat, že obětí plošně přibývá. Práce poukazuje, že někteří lidé se stávají cílem útoku v kyberprostoru opakovaně a snadno, jelikož k napadení jsou využívány nejen základní, ale i velmi specifické kybernetické útoky. Tyto útoky se nevyhýbají fyzickým ani právnickým osobám, nezáleží na pohlaví, věku, ani na stupni nejvyššího dosaženého vzdělání. Internetový prostor využívá stále více jednotlivců či organizovaných skupin k páchání trestných činů, umožňuje jim to nejen rychlý vývoj technologií a snadná dostupnost sociálních sítí, ale především lidská důvěřivost a neznalost této problematiky. Kyberkriminalitu bohužel vymýtit zcela nejde a jak bylo zobrazeno její činnost je stále na vzestupu a dá se předpokládat, že tyto data jsou ještě mnohem vyšší, jelikož latentní kriminality v tomto ohledu bude několika násobek uváděných statistických čísel. Kyberkriminalitě lze ale účinně předcházet nebo ztěžovat její páchání. Bylo by vhodné mezi širokou veřejností zvýšit osvětu o nebezpečí kybernetických útoků. Lidé by měli věnovat větší pozornost zabezpečení svého počítačového systému, více investovat do ověřených antivirových programů. Pečlivě třídit a vyhodnocovat informace, které se k nim internetovým prostorem dostávají a v případě podezření na páchání trestné činnosti si plnit svou ohlašovací povinnost. V dnešní době existuje jediná možnost, aby se člověk nestal obětí kyberkriminality, a to být off-line.

Seznam použitých zdrojů

Literární zdroje

1. **HULANOVÁ, Lenka**. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012.ISBN 978-80-7387-545-9.
2. **JIROVSKÝ, Václav**. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007. ISBN 978-80-247-1561-2.
3. **KOLOUCH, Jan**. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.
4. **KRUPKA, Vladimír**. *Trestní právo hmotné - zvláštní část: (vybrané skutkové podstaty trestných činů a souvisejících přestupků).* Praha: Armex, 2012. Skripta pro střední a vyšší odborné školy. ISBN 978-80-87451-12-0.
5. **MAISNER, Martin**. *Zákon o kybernetické bezpečnosti: komentář*. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-817-8.
6. *Praktický manuál GDPR pro každého: vše, co potřebujete vědět o novém nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně osobních údajů v praktickém kompletu s webem, e-bookem a aktualizačním servisem*. Bratislava: DonauMedia, 2018. ISBN 978-80-8183-049-5.
7. **SMEJKAL, Vladimír**. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7.
8. **STAŇKOVÁ, Lucie.** *GDPR snadno a přehledně*. Praha: Mladá fronta, 2018. ISBN 978-80-204-5108-8.
9. **VANTUCH, Pavel.** *Trestní zákoník s komentářem: k zákonu č. 40/2009 Sb., ve znění pozdějších předpisů.* Olomouc: ANAG, 2011-. Právo (ANAG). ISBN 978-80-7263-677-8.
10. **ZAVRŠNIK, Aleš**. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. ISBN 978-80-7552-758-5.
11. **ŽŮREK, Jiří**. *Praktický průvodce GDPR*. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3.

12. **ŽŮREK, Jiří**. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9.

Elektronické zdroje

1. *Dodatkový protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů* [cit. 12.12.2019].
   Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804931bf
2. *Full list. 301 Moved Permanently* [online]. Copyright © Council of Europe 2019 [cit. 08.12.2019].
   Dostupné z: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
3. *Kyberkriminalita - Policie České republiky*. Úvodní strana - Policie České republiky [online]. [cit. 02.12.2019]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

Seznam grafů

Seznam tabulek