Univerzita Pardubice

Fakulta ekonomicko-správní

Počítačová kriminalita

Bakalářská práce

2019 Sára Škopová

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2018/2019**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Sára Škopová**
Osobní číslo:	**E16334**
Studijní program:	**B6202 Hospodářská politika a správa**
Studijní obor:	**Veřejná ekonomika a správa: Ekonomika pro kriminalisty a celníky**
Název tématu:	**Počítačová kriminalita**
Zadávající katedra:	**Ústav ekonomických věd**

Zásady pro vypracování:

Cílem práce je analýza počítačové kriminality a zhodnocení její hrozby v současném světě. Cílem je zjistit zda se respondenti setkali s nějakou formou počítačové kriminality, jak se před ní chrání, jestli používají sociální sítě, sdělují své osobní informace na internetu atd.

Osnova:
- Historie a druhy počítačové kriminality.
- Počítačová kriminalita ve světě.
- Prevence před počítačovou kriminalitou.
- Dotazníkové šetření a jeho analýza.

Rozsah grafických prací:

Rozsah pracovní zprávy: **cca 35 stran**

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

GŘIVNA, T., POLČÁK, R. Kyberkriminalita a právo. Vyd. 1. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4.
JIROVSKÝ, V. Kybernetická kriminalita. Vyd. 1. Praha: Grada, 2007. ISBN 978-80-247-1561-2.
KOLOUCH, J. CyberCrime. Vyd. 1. Praha: CZ.NIC, 2016. ISBN 978-80-88168-15-7.
POLČÁK, R. Internet a proměny práva. Vyd. 1. Praha: Auditorium, 2012. ISBN 978-80-87284-22-3.

Vedoucí bakalářské práce: **Ing. Simona Pichová, Ph.D.**
Ústav ekonomických věd

Datum zadání bakalářské práce: **3. září 2018**

Termín odevzdání bakalářské práce: **30. dubna 2019**

L.S.

doc. Ing. Romana Provazníková, Ph.D.
děkanka

doc. Ing. Jolana Volejníková, Ph.D.
vedoucí ústavu

V Pardubicích dne 3. září 2018

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.

Byla jsem seznámena s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 20. 11. 2019 Sára Škopová

PODĚKOVÁNÍ:

Tímto bych chtěla poděkovat vedoucí bakalářské práce Ing. Simoně Pichové, Ph.D., za vedení mé práce, konzultace a rady. Dále patří poděkování respondentům, kteří spolupracovali na dotazníkovém šetření.

ANOTACE

Tato práce se zabývá problematikou počítačové kriminality a pojmy s ní spojené. V první části jsou definovány pojmy počítačové kriminality, její typy a formy, způsoby prevence a vyšetřování těchto trestných činů. V další části se nachází dotazníkové šetření a jeho analýza.

KLÍČOVÁ SLOVA

počítač, počítačová kriminalita, trestný čin

TITLE

Cyber Crime

ANNOTATION

This thesis deal with matters of cyber crime and related concepts. First part define area of cyber crime, particular types and forms, possibilities of prevention and investigation these crimes. In the next part is questionnaire and its analysis.

KEYWORDS

computer, cyber crime, crime

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM ZKRATEK

ČSFR	Česká a Slovenská Federativní Republika
ČR	Česká republika
EU	Evropská unie
USA	Spojené státy americké
USD	Americký dolar
PdF UP	Pedagogická fakulta Univerzity Palackého
TŘ	Trestní řád
MŠMT	Ministerstvo školství, mládeže a tělovýchovy
SWAT	Zvláštní jednotka policejního oddělení v USA
ENIAC	Jeden z prvních elektronkových počítačů
IBM PC	První verze počítače
BBS	Systém elektronických nástěnek
BDO	Celosvětová síť poradenských společností
PC	Osobní počítač
IT	Informační technologie
MS Windows	Operační systém
URL	Jednotná adresa zdroje
ESET	Slovenská softwarová firma působící v IT bezpečnosti
DoS	Typ útoku – odepření služby (jeden strůjce)
DDoS	Typ útoku – odepření služby (více strůjců)
GCI	Celosvětový index kybernetické ochrany

ÚVOD

Cílem této bakalářské práce je poukázat na problematiku počítačové kriminality, její analýza a zhodnocení hrozeb v současném světě. Díky rostoucímu pokroku je většina činností prováděna prostřednictvím informačních technologií, s tím roste i možnost jejich zneužití a páchání trestných činů.

Nejdříve je zmíněna historie a vývoj kriminality, a to celkově po celém světě, tak i v České republice. Dále je definována počítačová kriminalita a pojmy s ní spojené. Mezi tyto pojmy patří kyberprostor, kybernetický útok, počítač a data. Vybrány jsou nejčastější typy a formy páchání počítačových trestných činů. V neposlední řadě jsou zde uvedeny možnosti prevence a vyšetřování kybernetické kriminality.

Jelikož se informační technologie stále rozvíjí a kybernetických útoků přibývá, je v další části uvedeno dotazníkové šetření, díky kterému bylo zjištěno, jak uživatelé informačních technologií reagují na hrozby počítačové kriminality. Šetření bylo prováděno mezi studenty a cílem bylo zjistit jejich celkový názor na počítačovou kriminalitu. Nejen jaký pohled na kriminalitu mají, ale zda s ní mají nějakou osobní zkušenost, jak se před ní chrání nebo jestli ji sami nějakým způsobem páchají.

V této době, kdy jsou technologie na vzestupu, by se měla tato problematika více probírat a řešit, aby co nejvíce lidí mělo představu o tom, co se může stát a jakým způsobem se lze chránit. Existují lidé, kteří například vůbec nevnímají počítačovou kriminalitu jako něco, co by mohlo ohrozit zrovna je, nebo si nejsou ani vědomi toho, že tento druh kriminality existuje a je velmi nebezpečný.

1 HISTORIE A VÝVOJ

Informační a počítačová kriminalita roste s rozvojem těchto technologií. Čím modernější a vyvinutější informační technologie byly, tím i větší prostor pro páchání trestné činnosti. Z toho vyplývá, že postupem času se trestné činy v této oblasti objevovaly častěji.

Mnohé zdroje se zabývají historií počítačové kriminality, a to z různých hledisek. V této práci je vybráno rozdělení podle klíčových událostí do tří období.

Obrázek 1: Historie počítačové kriminality

Zdroj: Vlastní zpracování

Pravěk

Pod pojmem prvního počítačového zločinu lze najít případ, který se v roce 1801 odehrál ve Francii [15]. Jednalo se o sestrojení zařízení, které automatizovalo a opakovaně provádělo činnosti při tkání látek. Toto zařízení tehdy sestrojil tkadlec Jacquard. Zaměstnanci manufaktury se ale báli o práci a proto sabotovali stroj a Jacquard už další vývoj neprovedl.

Další zmínkou můžou být chlapci, kteří měli na starost telefonní ústředny. Hovory náhodně přerušovali, smáli se do telefonu nebo spojovali nepříslušící hovory. Po mnoha stížnostech byli chlapci nahrazeni zodpovědnějšími dívkami a problém se již neopakoval.

Právě telefon se zasloužil o termín cyberprostor. Jde o neurčitý prostor nebo síť, kde dochází ke komunikaci, zábavě a neposledně ke zločinům. Druhý nutný přístroj potřebný k tomu, aby vznikl cyberprostor, byl osobní počítač, ten byl sestrojen až po půlstoletí déle. První počítač, jménem ENIAC byl sestrojen na univerzitě v Pensylvánii 14. února 1946 [3]. Tyto počítače byly velmi drahé a velké, proto musely být ve speciálních místnostech a nemohl si je dovolit každý. Počítače ve firmách byly velmi střeženým místem, a proto byla jen velmi malá možnost je zneužít ke kriminální činnosti.

Středověk

Nová éra v oblasti informačních technologií nastala zavedením počítače IBM PC na trh. Díky stavebnicovému uspořádání a cenové dostupnosti bylo možné pořídit počítač do každé domácnosti. Právě v tomto období došlo k propojení telefonní linky a počítače [5]. Počítače se díky modemům připojovaly do sítě, šlo o servery, na které se připojovalo přímou volbou čísla. Rozšířil se tím systém BBS, předchůdce současného internetu.

K rozvoji systému BBS přispěl také film War Games. Hlavní postavou byl mladý hacker, který téměř vyvolal 3. světovou válku tím, že se naboural do vojenského systému a měl problémy rozeznat virtuální svět od reálného. Film ukázal hackerům, čeho všeho je možné dosáhnout a byl lákadlem pro páchání trestných činů. Podobných filmů bylo v té době natočeno rovnou několik.

Éra středověku končí, když dochází ke změně typických pachatelů počítačových zločinů. Pachatelům už nejde pouze o slávu, ale především o zisk. Tím se z počítačových nadšenců stávají profesionálové.

Novověk

Charakteristikou novověku je především masové rozšíření počítačů, zejména těch na platformě PC se systémem Microsoft Windows. Dochází ke komercializaci internetu, pronikají na něj podnikatelé a stává se z něj obchodní nástroj. Díky tomu dochází k většímu přílivu peněz, což láká počítačové podvodníky. Počítačové podsvětí není ale ovládáno organizovanými skupinami zločinců, protože internet nelze ovládnout zcela a to například pro mafii není zajímavé. Organizované skupiny se proto zaměřují pouze na konkrétní okruh činností, tím jsou třeba útoky na finanční a bankovní systémy nebo zneužívání ukradených karet.

V roce 1995 byla zneužita harvardská univerzita z důvodu zjišťování hesel, díky kterým se dalo dostat do počítačů vlády. Díky soudnímu příkazu bylo možné sledovat policejní síť, a tím se také přišlo na viníka, kterým byl hacker z Argentiny. Šlo o první případ, kdy soud povolil odposlech na síti Internet v USA [15].

1.1 Situace v ČR

Počítače v České republice byly dostupné až koncem 80. let, proto počítačovou kriminalitu lze považovat za mladý obor. Málokterá domácnost měla do té doby vlastní počítač, přesto

se první případy kybernetických útoků staly už dříve, a to za pomoci ještě velkých počítačů, které zabíraly celou místnost.

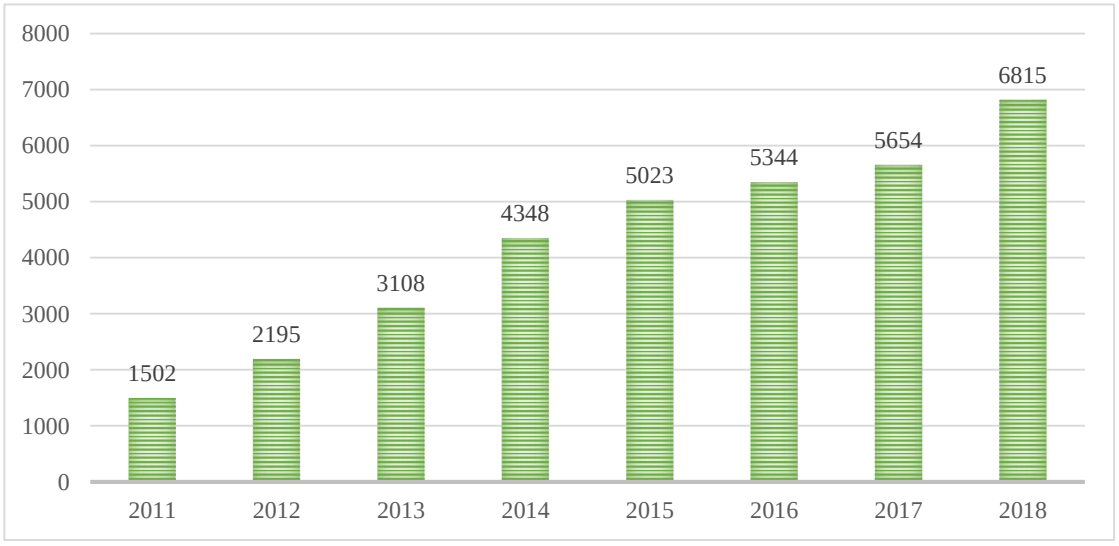
Prvním pachatelem, který byl za spáchání trestného činu pomocí počítače odsouzen, byl zaměstnanec Úřadu důchodového zabezpečení. Znehodnotil magnetické pásky a tím i záznamy na nich. Byl za tento čin odsouzen na více než 10 let vězení.

Další případ byl podobný, jednalo se o skupinku zaměstnanců, kteří také poškodili počítačové zařízení, a to proto, že chtěli vyměnit stávající systém za kvalitnější. Nejdříve byli stíhání za sabotáž, potom za porušení provozu v socialistické organici, poté za poškození majetku socialistického vlastnictví, a nakonec byla vyhlášena amnestie prezidenta a stíhání se zastavilo.

Největší technologický rozmach nastal po roce 1989, kdy se otevřely hranice a počítačová technika byla ve velkém dovážena, a poté v roce 1992, kdy se ČSFR připojila k internetu [16]. Díky tomuto technologickému vývoji se nejen zlepšily informační a komunikační technologie, ale také se zvětšil prostor pro trestné činy.

Vývoj kybernetické kriminality

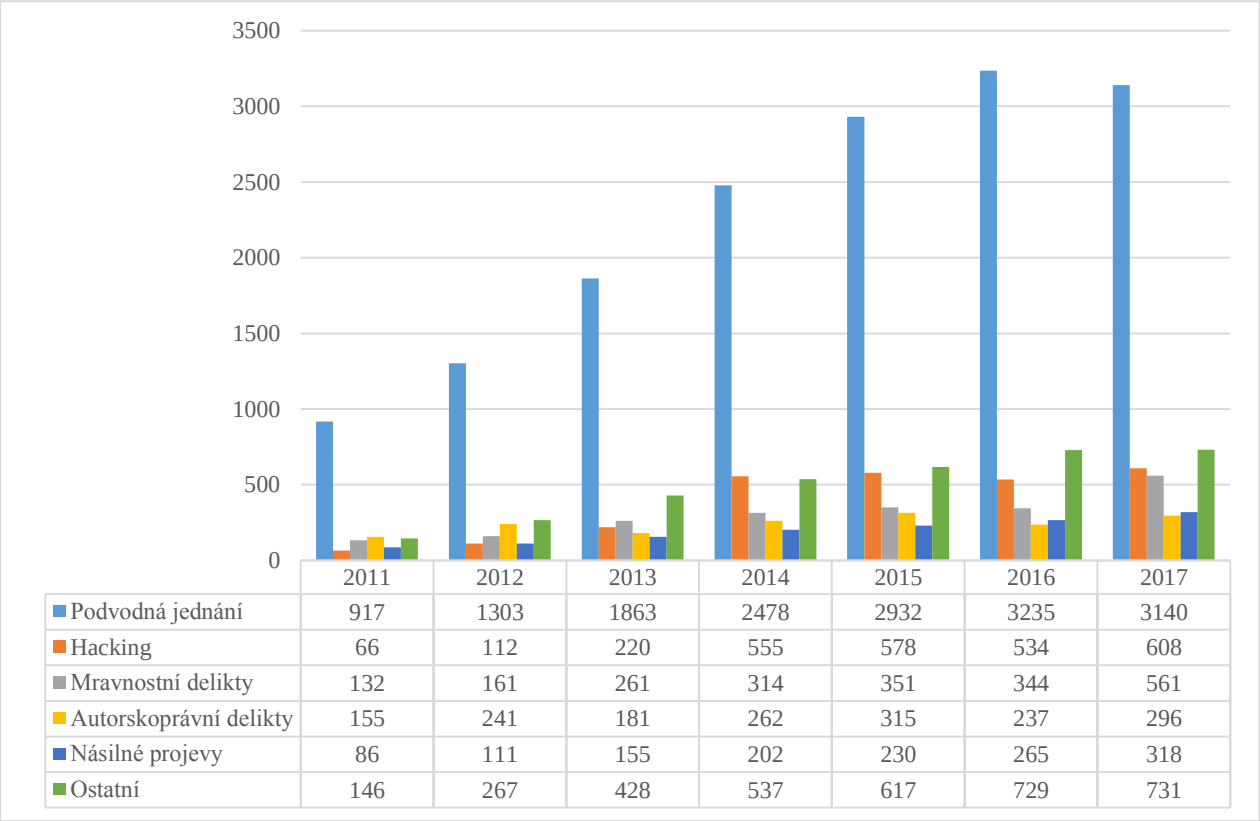
V roce 2018 klesla celková kriminalita v České republice o 7,3 %, což je o 15 860 méně trestných činů. Kybernetická kriminalita oproti ostatním ale stále vzrůstá, v roce 2018 bylo zaznamenáno 6815 trestných činů.



Obrázek 2: Kybernetická kriminalita v ČR *Zdroj: Vlastní zpracování podle [6]*

Za 7 let od roku 2011 vzrostla počítačová kriminalita o celých 353,73 %. Podle poradenské služby BDO je nejčastějším útokem phising, novým trendem jsou i útoky na mobilní telefony a čím dál častěji jsou vidět útoky na univerzity. Nejvíce ohroženy jsou stále banky, státní správa a firmy z oblasti energetiky.

V nejvyšším počtu trestných činů vedou ve všech letech podvodná jednání, ty byly nejvyšší v roce 2016. Pod podvodným jednáním si lze představit podvodné eshopy, které slouží k vylákání finančních prostředků, nebo obdobné podvodné inzeráty. Následuje hacking, který hlavně v posledních letech převyšuje mravnostní delikty. Předposlední se umístily autorskoprávní delikty a nejmenší počet tvoří násilné projevy.



	2011	2012	2013	2014	2015	2016	2017
Podvodná jednání	917	1303	1863	2478	2932	3235	3140
Hacking	66	112	220	555	578	534	608
Mravnostní delikty	132	161	261	314	351	344	561
Autorskoprávní delikty	155	241	181	262	315	237	296
Násilné projevy	86	111	155	202	230	265	318
Ostatní	146	267	428	537	617	729	731

Obrázek 3: Struktura počítačových trestných činů

Zdroj: Vlastní zpracování podle [8]

1.2 Kybernetická kriminalita ve světě

Počítačová kriminality roste nejen v České republice, ale i všude po světě. Na tento nárůst reaguje také trh s kybernetickou bezpečností, kterému roste byznys. V budoucnu by se měla do počítačové bezpečnosti zapojovat čím dál více umělá inteligence, která bude mít uplatnění ve všech segmentech, to však útočníkům umožní ještě větší prostor k útokům.

Minulý rok kybernalita způsobila globální škodu ve výši 600 miliard USD, to je o 150 miliard více než v roce 2014, kdy byla prováděna poslední studie. Předpokládá se, že některé firmy útok ani nehlásí, proto čísla nemusí být úplná. Tímto nastává velký potenciál pro pojišťovny, které se budou snažit sbírat pečlivěji aktuální data pro lepší ocenění rizik [18].

Kybernetická ochrana předvídá, že do roku 2022 bude 6 bilionů uživatelů internetu a více než 7,5 bilionu do roku 2030 [12]. Podobně jako pouliční zločiny narůstají s růstem populace, tak i počítačová kriminalita roste s lepším vybavením a zvýšením počtu potencionálních obětí.

Každoročně je sestavován index, který hodnotí, jak se jednotlivé státy staví k IT bezpečnosti. Tento index nese název Global Cybersecurity Index, neboli GCI. Index vyhodnocuje 5 oblastí internetové bezpečnosti, je to oblast právní, technická, organizační, edukační a kooperativní. Čím vyšší skóre země získá, tím lépe na tom je. V tabulce je pro představu uvedeno pár zemí s jejich indexem, ČR je zhruba uprostřed, což je takový průměr.

Tabulka 1: GCI vybraných zemí

Země	**GCI**
Singapore	0,925
USA	0,919
Austrálie	0,824
Francie	0,819
Velká Británie	0,783
Nizozemsko	0,760
Německo	0,679
Rakousko	0,639
Itálie	0,626
Polsko	0,622
Česká republika	0,609
Chorvatsko	0,590
Maďarsko	0,534
Španělsko	0,519
Portugalsko	0,508
Slovensko	0,362

Zdroj: Vlastní zpracování podle [4]

2 CHARAKTERISTIKA POČÍTAČOVÉ KRIMINALITY

Počítačová kriminalita neboli kybernetická a internetová kriminalita, kyberkriminalita a kybernalita. Definování počítačové kriminality je velmi obtížné. Neexistuje žádná univerzální definice, která by specifikovala počítačovou kriminalitu v plném rozsahu. Ale v zásadě se jedná o trestné činy, kde je počítač využíván jako nástroj nebo cíl trestné činnosti. Samozřejmé ne vždy je právě počítač nutný k spáchání činu, hlavní roli zde hraje síť, bez které by tato činnost nebyla možná. Tyto trestné činy mají společný charakter, nejvýznamnější charakterem je počítač nebo program. Kriminalita v této oblasti je také zajímavá tím, že poškozený někdy ani nezaznamená, že proti němu byl spáchán trestný čin.

Zde je uvedeno rozdělení podle budapešťské úmluvy [27]:

- Neoprávněný přístup – Za neoprávněný přístup je považován průnik do počítačového systému a dat bez souhlasu nebo vědomí oprávněné osoby. Takový průnik může být jen příprava pro další čin. Příkladem je zničení nebo poškození informací. V tomto případě je objektem ochrana bezpečnosti počítačového systému a dat, přístup do systému je objektivní stránkou.
- Neoprávněné zachycení informací – Bezpečnost soukromé datové komunikace je objektem, objektivní stránkou je zaznamenání neveřejných[1] přenosů dat. Komunikace zaměstnanců ve firmě má také znaky neveřejných přenosů a je chráněna.
- Zásah do dat – Ochrana počítačových programů a dat před způsobením škody je objektem, jedná se o porušování integrity nebo neoprávněné užívání počítačových dat. Objektivní stránkou zde je změna, poškození a vymazání dat. Tuto činnost představují viry a jiné zásahy, například trojský kůň.
- Zásah do systému – Hlavním smyslem je ochrana uživatelů a operátorů telekomunikačních a informačních systému, toto se dá také označit jako počítačová sabotáž. Spadá sem narušování nebo zničení počítačových dat. Jedná se o narušení systému takovým způsobem, že způsobuje uživateli problémy. Pomocí škodlivých virů a odepření služby dochází k narušení nebo zpomalení chodu systému a zablokování komunikačních cest.

[1] Neveřejné přenosy v tomto případě znamenají způsob přenosu, ne obsah přenosu.

- Zneužití zařízení – Toto jednání působí v materiální povaze jako přípravná činnost pro páchání dalšího trestního činu v kyberprostoru. Ohrožení zájmu společnosti a jednotlivce vychází z nekontrolovatelné výroby, prodeje a distribuce, které napomáhají trestné činnosti v kyberprostoru.
- Falšování údajů spojené s počítači – Jde o ochranu elektronických dat, které můžou způsobit důsledky v právních vztazích. Falešné údaje vznikají v důsledku vymazání, změny nebo vložení dat. Obdobou falšování údajů je padělání hmotných dokumentů.
- Podvody spojené s počítači – Nepatřičná manipulace a zpracování dat s cílem nezákonně získat cizí vlastnictví.
- Trestné činy spojené s dětskou pornografií – Ochrana dětí před podněcováním ke skutečnému sexuálnímu zneužívání. Rovněž i tvorba a zasílání odkazů s dětskou pornografií.
- Trestné činy spojené s porušením autorského práva a práv jemu příbuzných – Jedná se o porušení autorského práva a práv příbuzných autorskému právu, pokud k tomuto jednání došlo díky počítačovému systému.

Kyberprostor

Kyberprostor lze chápat jako virtuální svět, ve kterém probíhají informační a telekomunikační činnosti. V tomto světě jsou vymezena vlastní pravidla, ačkoliv zde působí podobné rysy jako v reálném světě [23]. Někteří jedinci si virtuální prostor natolik oblíbili, že v něm žijí více než ve svém vlastním životě.

S kyberprostorem souvisí internet, bez jeho vymezení nelze kyberprostor definovat. Internet je nenahmatatelná síť, která je propojena po celém světě. Díky tomu člověk může s kýmkoliv a kdekoliv komunikovat a přenášet data. Jednou z vlastností internetu je i možnost pracovat utajeně v anonymním režimu, což přímo nahrává kybernetickým zločincům.

Kybernetický útok

Nezákonné jednání v kybernetickém prostoru, které má za cíl získat, poškodit či změnit počítačové informace a tím poškodit zájem dané osoby. Aby byl kybernetický útok trestným činem, nemusí dojít až ke konečnému dokonání, stačí příprava nebo pokus o spáchání útoku.

Ze zákona o počítačové bezpečnosti lze využít i definici pojmů počítačová bezpečnostní událost a bezpečnostní incident. Počítačovou bezpečnostní událost lze definovat jako událost,

která prozatím nepředstavuje reálný negativní následek pro daný systém, ale pohlíží se na ni jako na hrozbu, která je reálná.

Počítačový bezpečnostní incident je narušení bezpečnosti informačních systémů, elektronických komunikací nebo bezpečnosti, které mají negativní dopad [27].

Počítač

Počítač je elektronický přístroj, který přijímá, zpracovává a poté vytváří výsledky podle vytvořeného programu. Uživatel počítač ovládá, dává mu vstupní data ke zpracování a počítač z toho poté vytvoří výstupy. Počítač má technické a programové vybavení, neboli hardware a software.

Hardware

Fyzické vybavení, díky kterému počítač může fungovat. Lze říci, že hardware je vše, co není software. V souvislosti s hardwarem můžeme rozlišit dvě skupiny, a to vnitřní počítačové vybavení a rozšiřující vybavení.

Vnitřní vybavení je nutné, protože by bez něj počítač nemohl fungovat. Jde o základní desku, procesor a paměť, kromě tohoto standardního vybavení sem patří i grafická karta, harddisk, mechanika paměťových médií, televizní a zvuková karta.

Rozšířené vybavení není nutností pro fungování, ale rozšiřuje možné využití počítače. Sem se řadí monitor, klávesnice, paměťová zařízení, tiskárna, datový projektor, scanner, joystick.

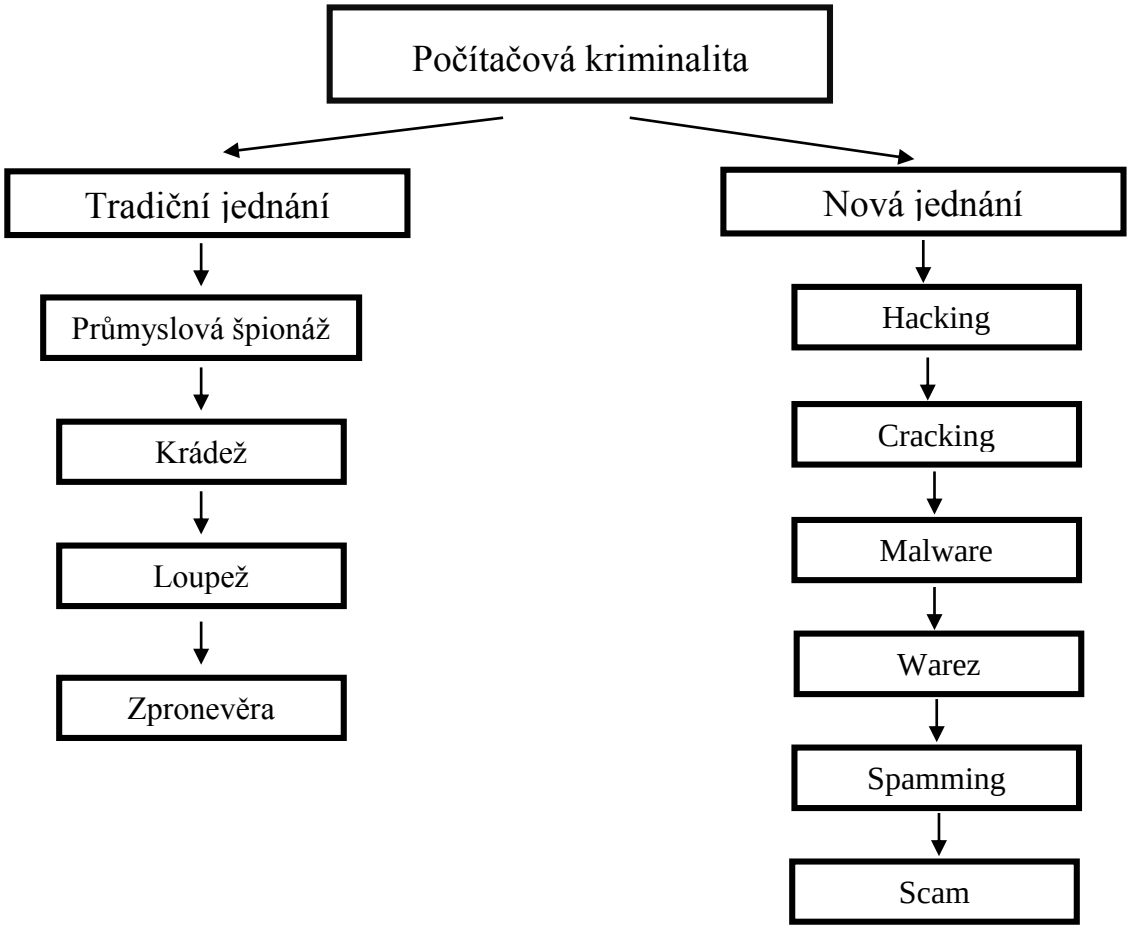
Software

Software je veškeré netechnické vybavení, díky kterým počítač pracuje a zpracovává data a informace. Obsahuje základní vstupní/výstupní sytém, operační systém (nejčastějším je MS Windows), grafické rozhraní a všechny aplikace.

3 TYPY POČÍTAČOVÉ KRIMINALITY

Počítačová kriminalita se dá rozdělit na tradiční jednání a nová jednání. Ačkoliv toto dělení může v dnešní době vypadat poněkud zastarale, protože nová jednání dnes už nejsou tak nová.

V případě tradičního jednání se jedná o počítačovou kriminalitu v širším slova smyslu, počítač není nástrojem pro páchání trestné činnosti, nýbrž jeho předmětem. V případě krádeže počítače jako hardwaru se počítače týká, ale jen v podobě předmětu trestné činnosti. Druhou zmíněnou skupinou je nové jednání, což jsou nové typy trestných činů, které přišly s rozvojem technologií.



Obrázek 4: Typy počítačové kriminality *Zdroj: Vlastní zpracování*

3.1 Hacking

Pojem hacking a hacker vznikl v 50. letech 20. století v USA [28]. Označuje osobu, která je technicky nadaná a objevuje nová řešení problému. Veřejnost si pod tím představuje veškeré

činnosti a pachatele, kteří získávají nelegální přístupu do cizího systému. Je velký rozdíl mezi vnímáním tohoto pojmu z pohledu veřejnosti a z pohledu hackera samotného.

Podle motivace k dané činnosti a pozdějším nakládáním se získanými daty, lze hackery rozdělit do tří skupin:

- White Hats – Pronikají do systémů s cílem zjistit bezpečnostní slabiny a mezery a podle toho vytvořit takový mechanismus, který zabrání případným útokům. Často jsou to zaměstnanci nebo spolupracovníci společnosti, která podniká v oblasti informačních technologií.
- Black Hats – Opak hackerů White Hats. Jejich cílem je průnik do cizích systémů a způsobení škody nebo újmy napadenému uživateli.
- Grey Hats – Jde o osoby, které nepatří ani do jedné z výše uvedených skupin. Občas svým jednáním způsobí porušení práv nebo morální škodu, ale není to jejich primární zájem.

Hlavním faktorem pro posouzení hackera je tedy to, co ho k dané činnosti vede. V některých případech, kdy je narušena bezpečnost systému počítače, jde o reálnou hrozbu. Kdežto v dalších případech může jít o zlepšení bezpečnosti počítačového systému.

3.2 Cracking

Často je pojem cracking spojován s hackingem, někdy jsou i nesprávně zaměňovány. V crackingu jde především o pachatele patřící do skupiny Black Hats, tedy o ty, kteří pronikají do cizího systému se záměrem způsobit škodu nebo újmu uživateli systému a sebe popřípadě obohatit.

Cracking je také spojován s porušováním autorských práv a práv souvisejících s právem autorským. Jedná se o nedodržení ochranných prvků, formou vytváření kopií, nelegální stahování a používání počítačových programů a filmových či hudebních produktů.

3.3 Malware

Malware je jakýkoli software, který je využit k narušení činnosti počítače, získává informace a využívá je k přístupu do systému počítače. Je schopný plnit více funkcí, může se e-mailem šířit dál nebo získávat adresy z napadeného počítače.

Pod současným pojmem malware dříve existovalo více termínů pro software [15]:

- adware – Software, který podporuje reklamu. Je výnosnou reklamou, ale také nejméně nebezpečnou. Reklama je zobrazována v podobě vyskakovacích oken v operačním systému nebo na webových stránkách.
- spyware – Získávání statistických dat o aktivitě počítačového systému a následně jsou odesílány do datové schránky pachatele. Spyware může být nainstalován jako malware nebo je součástí jinak bezproblémového programu.
- viry – Program nebo škodlivý kód, který se připojuje k spuštěnému souboru nebo otevřenému dokumentu. Účelem virů je se usídlit v co největším počtu počítačových systémů a pak je využít k útoku.
- červi – Lze je řadit mezi viry. Podobně jako viry nepotřebují hostitele, ale rozdílem je, že mohou vyhledávat mezery v bezpečnostních systémech.
- trojské koně – Počítačové systémy, ve kterých jsou skryty funkce, se kterými by uživatel nesouhlasil, pokud by o nich věděl. Trojské koně na rozdíl od virů nemají tu schopnost se šířit bez pomoci uživatele. Pokud dojde k aktivaci trojského koně, může být počítačový systém mazán, blokován, změněn nebo narušen.
- rootkity – Díky rootkitům dochází k maskování malwaru v počítači. Příkladem jsou antivirové programy, ty kvůli napadení nemůžou malware odstranit, a tím se prodlužuje jeho přítomnost v počítači.
- keylogger – Software, který zaznamenává klávesové stisky na konkrétním počítači. Nejčastěji využívání k získání přihlašovacích údajů a hesel k účtům uživatele, data jsou odesílána pachateli.
- ransomware – Jde o vyděračský malware. Ransomware omezuje užívání počítače do té doby, než uživatel zaplatí výkupné.

3.4 Warez

Warez se rozmohl díky rozmachu internetu, pachatel v tomto případě není pouze jeden, ale skupina lidí. Skupina se skládá z lidí, kteří prolamují a obcházejí ochranu proti kopírování v programech, ostatní propagují své produkty na internetových stránkách a snaží se získat finance na jejich fungování.

Často k prodeji získaných produktů ani nedochází a je možné je získat zdarma. Finance na provoz tedy získávají umisťováním různých erotických a pornografických odkazů na svých

stránkách. Například při spuštění videa se pořád otvírají nová okna s touto tématikou a uživatel se toho nemůže zbavit. Při hledání na internetu se uživatel ani k hledanému softwaru nedostane a je pouze zahlcen otevírajícími se okny [23].

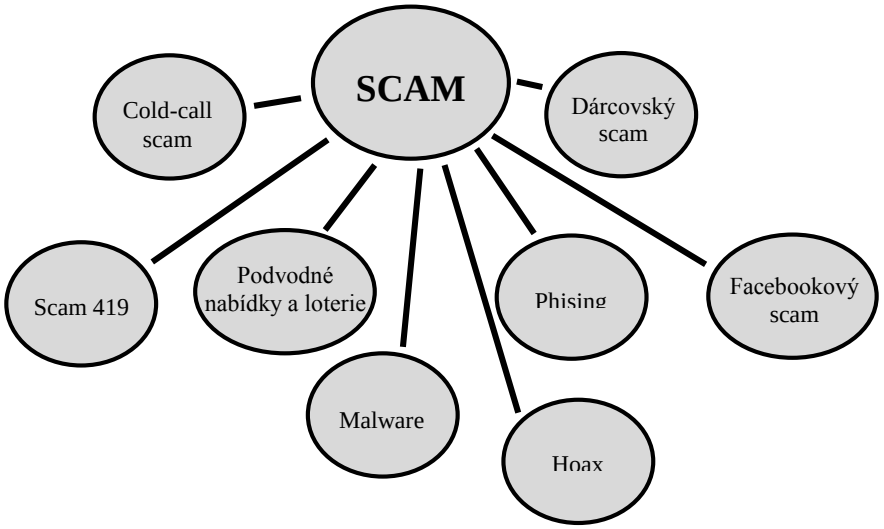
3.5 Spamming

Znakem spammingu je především to, že jde o sdělení, které je zasíláno elektronicky, je zasláno všem příjemcům hromadně a jedná se o nevyžádanou poštu. Tato nevyžádaná elektronická pošta má obvykle reklamní nebo propagační obsah, ale je možné se setkat i s nabídkami finančními, náboženskými nebo pornografickými. Pokud jde o spam, který obsahuje kriminální nebo podvodný obsah, hovoří se potom o scamu [15].

Marketingové společnosti využívají spam jako přímý marketing, kterým většinou příjemce jen obtěžují. Společnosti získávají elektronické adresy příjemců různými způsoby, nejčastěji to jsou www konference, blogy, diskuzní fóra nebo při službách zdarma, kde se musí vyplňovat osobní údaje. Boj proti spammingu není příliš úspěšný, protože spammeři počítají s tím, že se budou snažit jejich adresy blokovat a tak si je jednoduše modifikují.

3.6 Scam

Jak už bylo zmíněno výše, scam je spam, který má kriminální či podvodný obsah. Se scamem se v současné době lze setkat velmi často, snaží se získat důvěru příjemce a vést ho k činnosti, která obohatí pachatele, nejčastěji jde o navštívení adresy URL nebo zobrazení přijaté přílohy.



Obrázek 5: Rozdělení scamu *Zdroj: Vlastní zpracování*

Do scamu lze zařadit malware, phising, hoax, scam 419, dárcovský scam, cold-call scam, podvodné nabídky a loterie, facebookový scam.

Scam 419

Scam 419 označuje podvodné e-maily, které lze také najít pod názvem Nigerijské dopisy. Tyto podvody představují přenesení kriminality z reálného světa do toho virtuálního.

Ačkoliv pro někoho může být tento pojem neznámý, tak podvody tohoto typu existovaly již dříve, příkladem jsou faxy nebo dopisy. Podvody se časem nijak nezměnily, pouze se díky moderní době rozšířily. Spousta lidí se již setkala s tím, že jim přišel e-mail, ve kterém mu byla slíbena odměna za to, že pomůže pachateli převést ze země zděděný nebo získaný majetek. Oběť, která se nechala napálit, neustále platila různé administrativní poplatky a převod majetku se stále oddaloval.

Podvodné nabídky

Zasílání podvodných nabídek pomocí e-mailů nebo různých sociálních sítí se stalo velmi úspěšné. Nabídky se zasílají buď hromadně, nebo individuálně. V minulosti bylo snazší podvodné sdělení rozpoznat, jelikož pachatelé psali zvláštní češtinou nebo i cizím jazykem, často rusky nebo anglicky. Dnes už se snaží přesvědčit příjemce, že se jedná o důvěryhodnou a seriózní nabídku, a tak si dávají záležet na úpravě sdělení.

Hromadně rozesílána může být nabídka výhodné práce z domova, skvělé a vyzkoušené zhodnocení peněz, půjčka s nízkými úroky. V případě cíleného rozesílání se lze setkat i s jednáním, kde dochází k jednání s uživatelem, který nabídku přijal, jedná se o aukční podvody.

Phising

Při phisingu dochází k získání osobních a tajných informací o uživateli, které jsou později zneužity. Při opravdu dobrém phisingu lze dosáhnout vysoké míry úspěšnosti, v roce 2014 bylo úspěšných 45 % [17].

K získání potřebných informací musí uživatel buď navštívit podvodnou stránku (například internetové bankovnictví nebo online obchod) a přihlásit se pomocí svých údajů. V druhém případě uživatel nemusí dělat nic, pouze dostane e-mail nebo je přesměrován na podvodnou stránku, kde je malware, který získá osobní informace sám. V reálném světě také existuje phising, ale ve virtuálním je provádění těchto podvodů mnohem snazší, rozesílání je možné ve velkém množství a to bez velké námahy.

4 VYŠETŘOVÁNÍ KYBERNALITY

Kyberkriminalita je mířena proti počítači, jeho hardwaru, softwaru a síti. Nebo může být počítač využíván jako nástroj k spáchání trestného činu. Je velmi obtížné tuto kriminalitu sledovat, protože se veškeré jednání odehrává ve virtuálním světě, takže sledování této činnosti lze pouze pomocí počítače.

Lze říci, že značná část trestných činů pochází z reálného světa, je jen rozšířena do světa virtuálního, kde je tato činnost páchána rychleji a efektivněji. Jde o porušování autorských práv, šikanu, krádeže či podvody. Pak jsou tu činy, které vznikly až s příchodem počítačů, tam se řadí hacking, botnety, DoS a DDoS útoky [14].

Kyberkriminalita je zcela výjimečná oblast, která se nepodobá normální kriminalitě. Proto bylo potřeba vyvinout nové metodiky, které pomohou s dokazováním a upřesněním. Tyto metodiky jsou neustále modernizovány, protože i oblast kybernetiky a kybernetických útoků se každým dnem rozvíjí.

4.1 Digitální stopa

Každé zařízení, které získává, zpracovává a vyhodnocuje data, zanechává určitou stopu svých činností. Digitální stopa tedy pomáhá určit záměr uživatele, v případě páchání trestného činu záměr pachatele.

Tato stopa je důkazem a soudy připouští využívání digitálních důkazů v soudním řízení. Důkazem mohou být e-maily, elektronické dokumenty, historie internetového prohlížeče, počítačová paměť. Oproti klasickým stopám je většinou více objemná, může se nacházet kdekoliv v kybernetickém prostoru, její trvání může být krátké a dochází k její ztrátě. Kvůli těmto vlastnostem často dojde k neobjasnění kyberzločinu.

V současnosti je počítačová stopa začleněna v ustanovení § 112 odst. 1 či odst. 2 TŘ [26].

4.2 Předmět vyšetřování

U počítačové kriminality je potřeba zjišťovat:

- zda jde o jeden či více skutků
- informace o vlastním útoku – Zda byly zdroje a aktivity útočníka zaznamenány, délka a typ útoku, jak dlouho trvalo zajištění počítačových systémů a médií, způsobenou škodu.

- informace o počítačovém systému – Který počítač je koncovým připojeným bodem a na kterém bylo spácháno protiprávní jednání, důležité informace o napadeném systému, jakým způsobem byl počítač zapojen do počítačové sítě.
- informace o datech – Povaha napadených dat, obsah paměťových médií, uložená data a případná manipulace s nimi.
- informace o pachateli – Kolik osob se na nelegálním jednání podílelo a jakým způsobem k němu došlo, rozsah pachatelových znalostí, motiv pachatele.
- události, které umožnily spáchání trestného činu
- míra oprávnění pro přistup k počítačovému systému, uložišti, jednotlivým službám.

4.3 Přijetí trestního oznámení a jeho prověření

Trestní řízení začíná sepsáním záznamu o zahájení úkonů trestního řízení, provedením neodkladných úkonů, které mu bezprostředně předcházely. O spáchání trestného činu se činné orgány nejčastěji dozví na základě přijetí trestního oznámení.

Oznámení je klíčové, protože by bez něco nemohlo začít trestní řízení. Důležitým faktorem oznámení je perfektní zpracování, zajištění důkazů a prvotních informací. Zajištění dat by mělo v co nejkratší době, aby nedošlo k jejich změně, lepší jsou originální e-maily nebo paměť počítače než pouze kopie a printscreeny.

Z podaného oznámení musí být dle § 59 odst. 4 TŘ patrné [26]:

- který orgán činný v trestním řízení organu je k dané věci určen,
- kdo jej činí,
- které věci se týká a co sleduje,
- musí být podepsáno a datováno.

4.4 Dokazování kriminality

Důkazem je vše, co přispívá k objasnění věci, zejména jde o výpovědi svědků a obviněného, znalecký posudek, důležité věci a listiny pro řízení. Důkaz může vyhledat, předložit nebo navrhnout každá ze stran.

Nejčastěji jsou důkazy:

- věcné - Jedná se o předměty, na kterých nebo kterými byl trestný čin spáchán. Tyto důkazy mohou přispět k odhalení objasnění a odhalení činu, pachatele nebo dalších stop. V případě této kriminality jsou věcným důkazem počítačové systémy a paměťová média.
- listinné – Pokud je záznam v elektronické podobě, jedná se o důkaz věcný, po vytisknutí dokumentu se stává důkazem listinným. Trestní řád nedefinuje vlastní pojem listina, ale za listinu lze považovat předmět, na kterém je možné zachytit písemný nebo grafický projev.

4.5 Mezinárodní spolupráce při vyšetřování

Vzhledem ke stále zvyšující se propojenosti počítačů a počítačových sítí, se může stát, že trestný čin byl spáchán na území více států. Při vyšetřování spolu tedy musí orgány činné v trestním řízení spolupracovat.

Formálně tato spolupráce spočívá v právní pomoci (Interpol), nebo neformálně, kde se potřebné informace poskytují přímo orgánům daného státu. Pro úspěšnou spolupráci států je potřeba souhlas orgánů zúčastněných států. Vzájemná pomoc v případě této kriminality je mnohem důležitější než u té klasické, může totiž dojít k ztrátě důkazů, v případě že nejsou zajištěny rychle.

Pro vyšetřování trestných činů v této oblasti jsou potřeba kvalifikovaní odborníci, kteří mají zvláštní soudní a technické znalosti. Proto je potřeba znalosti neustále rozvíjet a zlepšovat, následně je sdílet s ostatními státy.

4.6 Orgány činné v trestním řízení

V okamžiku, kdy oznamovatel předá informace orgánům činným v trestním řízení, tak vyšetřování přechází na ně a oznamovatel se stává pouze svědkem. Předání vyšetřování je manažerským rozhodnutím, vychází z různých pohnutek [11]:

- Pokud jde o organizaci, která má státní nebo politické pozadí, mají manažeři obavu z toho, že pokud předá vyšetřování policii, tak dojde k publicitě, která může mít nepříznivé důsledky na fungování organizace.
- Vzhledem k rozsahu případu nepovažují za nutné předat vyšetřování. Vyšetřování by pravděpodobně nikam nevedlo z důvodů nedostatečným prostředků v této sféře.

Je důležité zpracovat bezpečnostní politiku organizace, díky které se předběžně stanoví, kdy je nutné podat oznámení činným orgánům.

- Častým případem je, že se činů dopouští zaměstnanci firmy (administrátoři), a to z důvodu nespokojenosti na své pozici a poškození firmy. Pokud dojde k poškození organizace zevnitř, manažer pak nechce takové selhání zveřejňovat.

Pokud dojde k předání vyšetřování činným orgánům, ve firmě se často zhorší celková atmosféra, jak komunikace, tak se zvýší i podezřívavost mezi kolegy.

4.7 Vyšetřovací tým

Při každém vyšetřování je nutné mít schopný tým. Není obvyklé, aby manažeři sestavovali tyto týmy, ale dříve či později se většina firem s počítačovým narušením setká. Oblastí kyberkriminality se zabývají americké speciální jednotky SWAT, v České republice se lze setkat s označením Cyber.

Nejdříve je nutné zjistit příčiny počítačového incidentu, na základě kterého se vytvářejí vyšetřovací analýzy a plány. Také dochází k vyslýchání svědků, zjišťují se provedené průniky do systému a rozsah škod.

Ve větších organizacích jsou tvořeny vyšetřovací týmy z pracovníků bezpečnostních složek, pro které je vyšetřování potencionálních rizik náplní práce. Každý člen týmu by měl v tomto oboru být specialistou a měl by mít možnost pracovat s potřebnými nástroji umožňujícími vyšetřování počítačového incidentu [13].

4.8 Zpráva o vyšetřování internetové kriminality

Nejčastějším trestným činem ve struktuře kybernetické kriminality je podvodné jednání, v rámci toho přetrvávají podvodné internetové obchody a využívání virtuálních měn pro převádění podvodných finančních prostředků. Přetrvává vzrůst phishingových útoků i hackingu. Dále se zvyšují počty i jiných trestných činů v této oblasti, jde například o mravnostní trestné činy, násilné a nenávistné projevy nebo krádeže identit a odcizení osobních údajů. V ČR klesá celková kriminalita, předpokládá se, že dochází k jejímu přemístění právě do kyberprostoru [16].

5 PREVENCE POČÍTAČOVÉ KRIMINALITY

Fenomén současné doby je používání internetu, zejména sociálních sítí, které propojují lidi z celého světa a umožňují jim sdílet informace. Tyto sítě jsou skvělým nástrojem, který ne jednomu člověku ulehčuje život, ale je třeba si dávat pozor na svou bezpečnost a svoje soukromí. Podvodů spáchaných prostřednictvím sociálních sítí narůstá. Pachatelé, díky neopatrnosti uživatele, získávají jeho osobní informace, přihlašovací údaje a hesla do bankovnictví. Tyto informace jsou potom zneužity, oběť může přijít o své finance nebo je jeho jménem smluven závazek.

Prevenci lze rozdělit na psychologickou a technologickou, navzájem se doplňují. Psychologická prevence znamená mít povědomí o tom, co je trestné a co se nesmí dělat, někteří uživatelé internetu si nemusejí ani uvědomovat, že to, co dělají je trestné. Proto je potřeba zvyšovat toto povědomí o počítačové kriminalitě například pomocí různých kampaní nebo sdělovacích prostředků. V případě technologické prevence jde o technologické zabezpečení. Jsou to nejrůznější elektronická zabezpečení nebo antivirové programy.

Stop online

Jedná se o nízkoprahové kontaktní centrum, které přijímá hlášení ohledně nelegálního obsahu na internetu, zejména jde o dětskou pornografii a kyberšikanu dětí. Úkolem centra je co nejrychleji odstranit nelegální obsah z internetu. Stop online spolupracuje s Policií ČR, mezinárodními horkými linkami a provozovateli webových stránek.

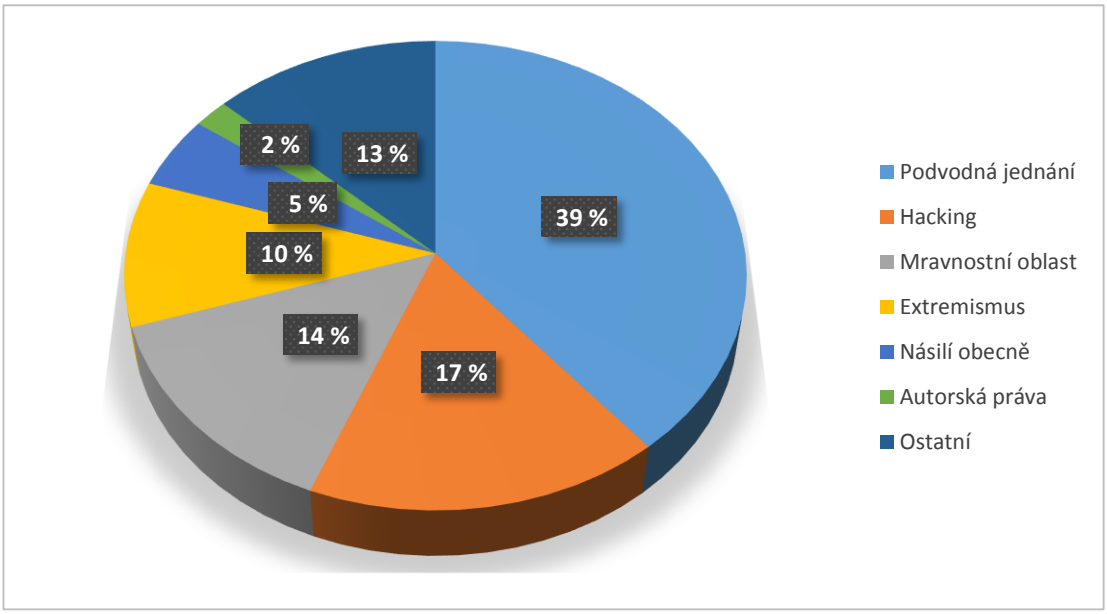
Hlášení se podává pomocí formuláře, vše je anonymní, není nutné vyplňovat žádné osobní informace, pouze v případě, že chce oznamovatel být zpětně informován. Přijatá oznámená jsou analyzována, a pokud jsou opodstatněné, tak jsou předána dalším složkám – Policii ČR, mobilním operátorům, poskytovatelům internetových služeb.

O nelegálním nahlášeném obsahu může v České republice rozhodnout pouze soud. Některý nelegální obsah může být z kyberprostoru smazán na základně vnitřních pravidel mobilních operátorů a poskytovatelů internetu. Linka tedy negarantuje odstranění a znepřístupnění nelegálního obsahu.

Policejní internetová linka HotLine

Od 1. srpna 2012 do 24. června 2018 byla zřízena internetová policejní linka HotLine, na kterou se mohlo nahlásit závadný obsah a aktivity na internetu. Hlášení bylo rozděleno do

7 oblastí, v roce 2016 bylo přijato celkem 3 378 oznámení, z toho nejpočetnější skupinu tvořilo podvodné jednání.



Obrázek 6: Hlášení linky HotLine v roce 2016 *Zdroj: Vlastní zpracování podle [21]*

Online helpline

Jde o poradenské centrum, provozuje ho Národním centrem bezpečnějšího internetu. Jejich specializací je problematika zneužívání Informačních technologií, kterými jsou internet a mobilní telefony. Pomoc je poskytována dětem a mladistvým, u kterých hrozí nebezpečí kyberšikany, stalkingu, groomingu a dalších negativních projevů, které mohou děti a mladistvé negativně ovlivnit. Dalšími osobami, kterým je pomoc poskytována, jsou senioři, kteří mají těžkou životní situaci kvůli používání informačních technologií.

Svůj problém může na tuto linku poslat každý na e-mail, tato služba je anonymní, ale lze uvést adresu pro případ zaslání odpovědi.

Poradna e-bezpečí

Poradna lze nalézt v Centru prevence rizikové virtuální komunikace PdF UP v Olomouci. Poradenství je zdarma a anonymní. Poradna spolupracuje se společností O_2, Google, Microsoft, ESET, Policii ČR, MŠMT, Ministerstvem vnitra ČR, Statutárním městem Olomouc [8].

Projekt bezpečný internet.cz

Projekt vznikl s cílem poukázat na rizika spojená s internetem a také na způsoby prevence a obrany. V současnosti je na internetu mnoho informací, které se věnují rizikům na internetu, ale jsou popisována v konkrétní podobě a jsou směřována pouze pro určitou skupinu lidí. Tento projekt tedy míří na rozsáhlejší cílové skupiny a snaží se pomoci lidem s bezpečným používáním internetu. Poskytují rady, návody a zkušenosti spojené s internetem, a to zcela zdarma.

Lidé se na internetu mohou denně setkat s nespočtem nástrah, ať už je to používání komunikačních kanálů nebo plateb přes internet. Čím více budou lidé vědět o možných rizicích, tím rychleji budou schopni se bránit a reagovat na útoky.

V roce 2013 byl proveden výzkum rizikového chování dětí na internetu a bylo zjištěno, že 51 % dětí má nějaké zkušenosti s kyberšikanou. Nejčastěji se děti setkávají s verbálními útoky, vyhrožování a zastrašování nebo krádeží identit. Výzkum také ukázal, že děti si nejen píší s cizími lidmi, ale značná část dětí by s nimi šla i na osobní schůzku. Další oblastí výzkumu byla intimita na internetu, 75 % dětí si uvědomuje rizika, ale přes 7 % uvedlo, že na internet umístily svou nahou fotku nebo video [2].

6 DOTAZNÍKOVÉ ŠETŘENÍ

Cílem bylo zjistit, jaký pohled mají studenti na počítačovou kriminalitu, zda se s ní nějakým způsobem setkali, jestli ji oni sami jsou součástí. Za účelem provedení této analýzy byla zvolena kvantitativní metoda výzkumu, konkrétně použití dotazníkového šetření. Záměrem dotazníkového šetření bylo také zjistit, zda se cítí bezpečně při využívání internetových služeb, a jakým způsobem by případně změnili kontrolu a ochranu internetu.

6.1 Informace o získaných datech

Dotazník byl vytvořen pomocí internetové stránky Google dotazník. Je anonymní a obsahuje 17 otázek, a to otevřených i uzavřených. Šetření bylo provedeno na Univerzitě Pardubice, celkem bylo získáno 210 odpovědí. Vyplňovat dotazník bylo možné na internetových stránkách, ke kterým měli respondenti přístup pomocí odkazu, který byl zveřejněn na stránkách školy na sociální síti. Potencionálních respondentů tedy bylo zhruba 300, návratnost dotazníků je 70 %. Nejvíce respondentů bylo z fakulty ekonomicko-správní z prvního ročníku bakalářského studia (78 %), vyšší zastoupení měli i studenti z navazujícího studia (15 %). Odpovídajícími byly v nadpoloviční většině ženy (75 %).

6.2 Výsledky dotazníkového šetření

1. Přichází Vám nevyžádaná pošta (spam) do e-mailové schránky?

Nevyžádaná pošta přichází většině respondentů. Více jak polovina dostává spam jen občas, 43 % respondentům přichází často a pouze 3 % uživatelů se s nevyžádanou poštou nesetkává vůbec. V dnešní době je téměř nemožné se vyhnout nevyžádané poště, proto není překvapující, že 97 % odpovědělo, že jim spam přichází.

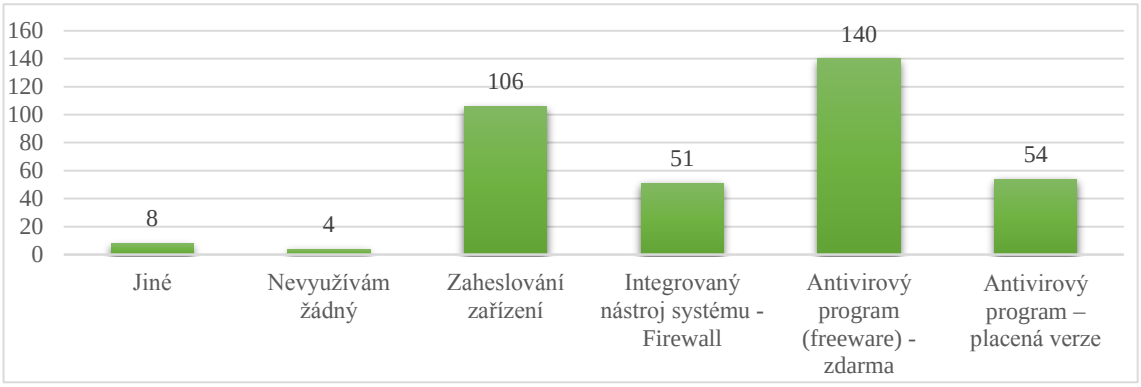
Tabulka 2: Nevyžádaná pošta

Odpověď	n_i	p_i
Ano, často	90	43 %
Ano, ale jen občas	112	54 %
Ne	7	3 %
Celkem	209	100 %

Zdroj: Vlastní zpracování

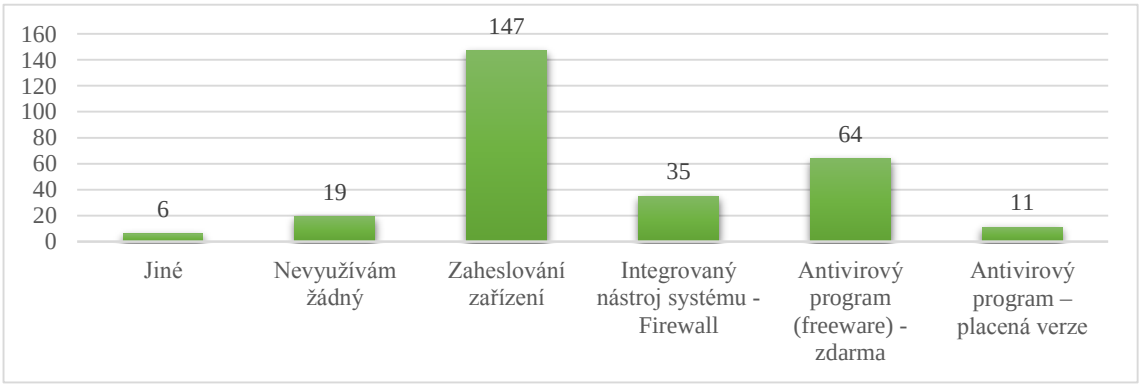
2. – 3. Jaké zabezpečení používáte na ochranu svého PC a tabletu & telefonu?

Při ochraně PC a tabletu respondenti nejčastěji využívají antivirový program, který je poskytován zdarma, další častou ochranou je zaheslování zařízení. Téměř na stejné úrovni uživatelé využívají, jak placenou verzi antivirového programu, tak integrovanou ochranu v systému zařízení. 1 % uživatelů nevyužívá žádnou ochranu. Jako další zabezpečení, které respondenti uvedli, jsou tisky prstů nebo integrovaná ochrana v systému Apple.



Obrázek 7: Zabezpečení PC a tabletu *Zdroj: Vlastní zpracování*

V případě zabezpečení mobilního telefonu uživatelé nejčastěji využívají jeho zaheslování. Poté 23 % respondentů svůj telefon chrání antivirovým programem poskytovaným zdarma, 12 % integrovanou ochranou v systému telefonu a 4 % placenou verzí antivirového programu. Oproti zabezpečení počítače nebo tabletu, respondenti chrání své mobilní telefony méně, 7 % z nich odpovědělo, že nevyužívá žádnou ochranu. Z jiných možností bylo uvedeno zaheslování aplikací, biometrické údaje a pravidelné aktualizace.

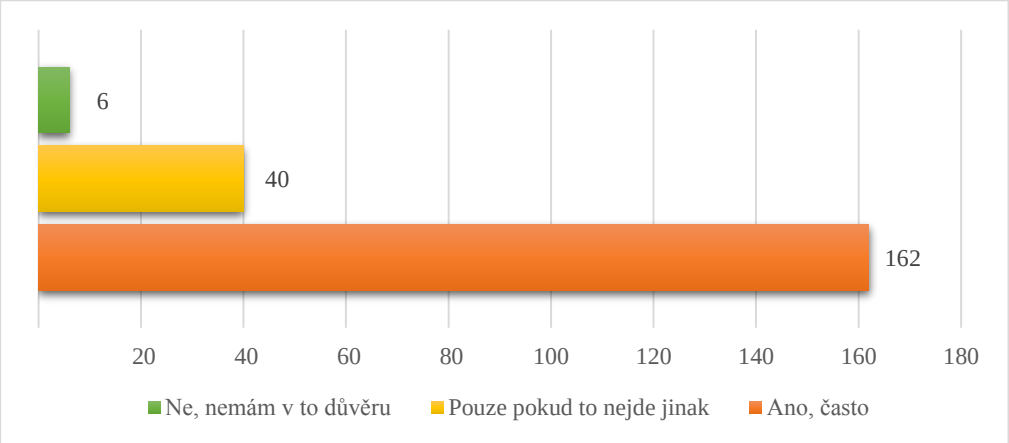


Obrázek 8: Zabezpečení mobilního telefonu *Zdroj: Vlastní zpracování*

V obou případech, jak u zabezpečení počítače i mobilního telefonu, se velmi často objevuje zaheslování zařízení. V tomto případě jde o zaheslování zařízení jako fyzické věci, například pomocí otisku prstu nebo pinu. Toto zabezpečení ale nezabrání pachateli v tom, aby se dostal do konkrétního počítače nebo mobilního telefonu.

4. Využíváte internet pro práci s choulostivými daty (bankovnictví, účetnictví)?

Jen 3 % uživatelů nemá důvěru používat internet pro práci s choulostivými daty. Ostatní internet pro tyto účely využívají, 78 % často a 19 % jen pokud to nejde jinak. Například internetové bankovnictví je skvělá věc, která ušetří spoustu času, ale stále k ní nemá dost lidí důvěru. Není divu, právě internetové bankovnictví je jedním z nejčastějších terčů hackerů.



Obrázek 9: Práce s choulostivými daty *Zdroj: Vlastní zpracování*

5. Sdílíte na sociálních sítích (Facebook, Twitter, Instagram apod.) nebo jinde na internetu své osobní údaje, fotky atd.?

Největší počet respondentů odpověděl, že sdílí na sociálních sítích své fotky a údaje jen v malé míře. 12 % nemá problém se sdílením informací a fotek na sociálních sítích, 10 % má strach, že by toho mohl někdo zneužít a 1 % procentu nevyužívá nic, kde by mohl zveřejňovat své fotky a údaje.

Tabulka 3: Sociální sítě

Odpověď	n_i	p_i
Ano, nevidím v tom problém	26	12 %
Ano, ale pouze v malé míře	160	77 %
Ne, mohl by to někdo zneužít	21	10 %
Nepoužívám nic, kde bych mohl/a zveřejňovat své fotky apod.	2	1 %
Celkem	209	100 %

Zdroj: Vlastní zpracování

6. Přijde Vám internet dostatečně kontrolován a chráněn?

Nejvíce respondenti souhlasí s tím, že internet není dostatečně chráněn a kontrolován, takto odpovědělo 85 % uživatelů. S tím, že internet je dostatečně bezpečný, souhlasí 9 % respondentů, zbylých 7 % se o to nezajímá.

Tabulka 4: Kontrola a ochrana internetu

Odpověď	n_i	p_i
Ano, opatření jsou dostatečná	19	9 %
Ne, opatření nejsou dostatečná	174	84 %
Je mi to jedno	14	7 %
Celkem	207	100 %

Zdroj: Vlastní zpracování

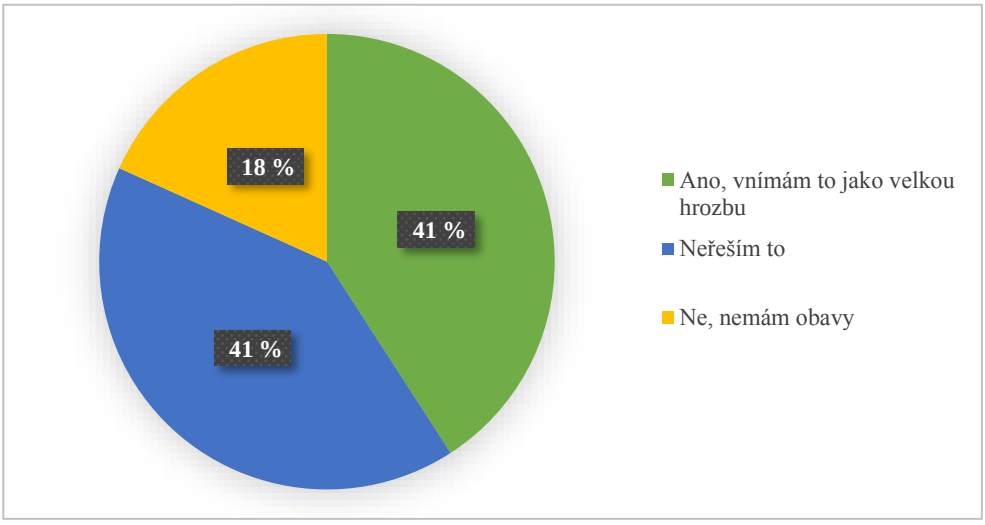
7. Máte obavy, že byste se mohl/a stát terčem kriminality na internetu?

41 % uživatelů odpovědělo, že mají obavy z toho, že by se mohli stát obětí počítačové kriminality. Stejné množství respondentů vůbec neřeší tuto možnost. Zbylých 18 % si nedělá starosti s tím, že by se jich počítačová kriminalita mohla dotknout.

Tabulka 5: Obavy z počítačové kriminality

Odpověď	n_i	p_i
Ano, vnímám to jako velkou hrozbu	85	41 %
Neřeším to	85	41 %
Ne, nemám obavy	38	18 %
Celkem	208	100 %

Zdroj: Vlastní zpracování



Obrázek 10: Obavy z počítačové kriminality

Zdroj: Vlastní zpracování

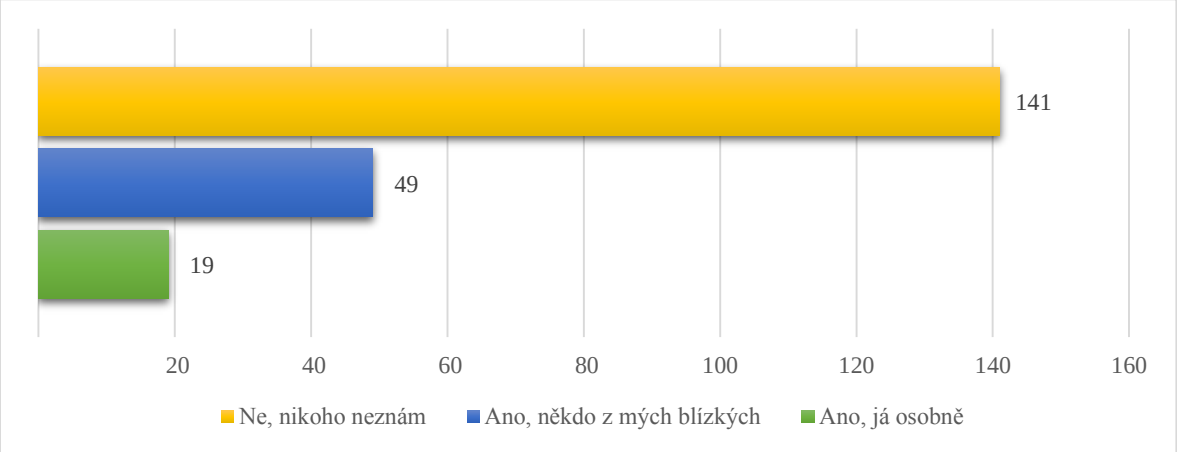
8. Stali jste se Vy nebo někdo z vašeho okolí obětí kriminality na internetu?

Uživatelé, kteří se nestaly obětí kriminality ani nikdo z jejich blízkých je 67 %. 9 % respondentů mělo s počítačovou kriminalitou osobní zkušenost, ostatních 23 % odpovědělo, že někdo z jejich blízkých se stal terčem kybernality. Asi třetina má tedy nějakou zkušenost s kybernetickým útokem, což není úplně malá část.

Tabulka 6: Zkušenosti s počítačovou kriminalitou

Odpověď	**n_i**	**p_i**
Ano, já osobně	19	9 %
Ano, někdo z mých blízkých	49	23 %
Ne, nikoho neznám	141	67 %
Celkem	209	100 %

Zdroj: Vlastní zpracování



Obrázek 11: Zkušenosti s počítačovou kriminalitou *Zdroj: Vlastní zpracování*

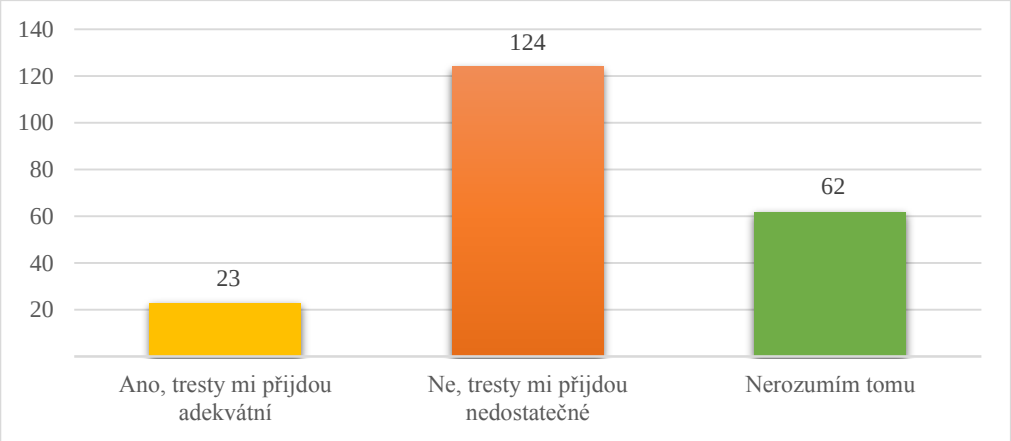
9. Přijde Vám kriminalita páchaná na internetu dostatečně trestána?

Tresty přijdou adekvátní 11 % uživatelů. S tím, že jsou tresty nedostatečně, souhlasí více než polovina respondentů. Zbylých 30 % odpovědělo, že tomu nerozumí.

Tabulka 7: Trestání počítačové kriminality

Odpověď	**n_i**	**p_i**
Ano, tresty mi přijdou adekvátní	23	11 %
Ne, tresty mi přijdou nedostatečné	124	59 %
Nerozumím tomu	62	30 %
Celkem	209	100 %

Zdroj: Vlastní zpracování



Obrázek 12: Trestání počítačové kriminality *Zdroj: Vlastní zpracování*

10. Berete zasílání nevyžádané pošty, stahování nelegálních softwarů, muziky, her atd. také jako počítačovou kriminalitu?

Pro většinu respondentů není zasílání nevyžádané pošty, stahování nelegálních softwarů atd. tak vážné, ostatních 23 % na to pohlíží jako na zločin.

Tabulka 8: Pohled na kybernetickou kriminalitu

Odpověď	n_i	p_i
Ano	49	23 %
Ne, nepřijde mi to tak vážné	160	77 %
Celkem	209	100 %

Zdroj: Vlastní zpracování

11. Pácháte Vy sami nějakým způsobem kriminalitu přes internet?

93 % respondentů se dopouští páchání počítačové kriminality, z toho více jak polovina pouze výjimečně. 7 % uživatelů se nedopouští kriminality, protože to berou jako zločin. Téměř všichni tedy nějakým způsobem páchají počítačovou kriminalitu a nejsou za to nijak trestání. To už vypovídá o tom, že by měl být například ztížen přístup k nelegálnímu softwaru.

Tabulka 9: Páchání kriminality na internetu

Odpověď	n_i	p_i
Ano, často	75	36 %
Ano, ale pouze výjimečně	119	57 %
Ne, je to zločin	15	7 %
Celkem	209	100 %

Zdroj: Vlastní zpracování

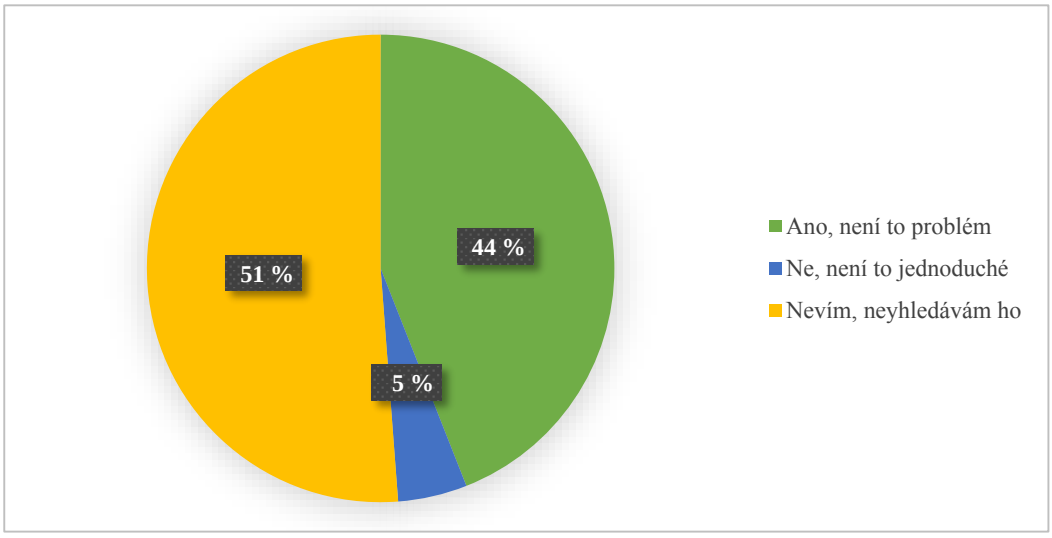
12. Přijde Vám jednoduché dostat se k nelegálnímu softwaru na internetu?

Více jak polovina uživatelů nevyhledává nelegální software na internetu, tudíž neví, jestli je to jednoduché nebo ne. 44 % si myslí, že vyhledat a dostat se k nelegálnímu softwaru není problém a zbylých 5 % se domnívá, že přístup je těžký.

Tabulka 10: Přístup k nelegálnímu softwaru

Odpověď	n_i	p_i
Ano, není to problém	92	44 %
Ne, není to jednoduché	10	5 %
Nevím, nevyhledávám ho	107	51 %
Celkem	209	100 %

Zdroj: Vlastní zpracování



Obrázek 13: Přístup k nelegálnímu softwaru *Zdroj: Vlastní zpracování*

13. Jak vnímáte situaci kriminality na internetu v ČR? (v porovnání s ostatními zeměmi)

Více jak polovina, konkrétně 61 % respondentů nemá představu o tom, jak je na tom počítačová kriminalita v České republice. 29 % respondentů smýšlí pozitivně o situaci počítačové kriminality a tvrdí, že Česká republika je na tom lépe než ostatní země. Zbytek odpovídajících si myslí, že ostatní země na tom jsou lépe než Česká republika.

Z pohledu rizikovosti vůči počítačové kriminalitě je Česká republika asi uprostřed s 35 %. Mezi nejrizikovější země patří Malta, Řecko, Rumunsko nebo Slovensko, tyto země mají 40 %

a více. Na druhé straně mezi nejméně rizikové patří Nizozemsko, Finsko, Německo a Estonsko, ty mají 30 % a méně.

Tabulka 11: Situace počítačové kriminality v ČR

Odpověď	n_i	p_i
Situace v ČR mi připadá lepší než v jiných zemích	60	29 %
Situace v ČR mi připadá horší než v jiných zemích	21	10 %
Nemám představu o tom, jaká je situace v ČR	127	61 %
Celkem	208	100 %

Zdroj: Vlastní zpracování

14. Pokud Vám přijde řešení počítačové kriminality nedostatečné nebo chybné, jak byste to řešili vy?

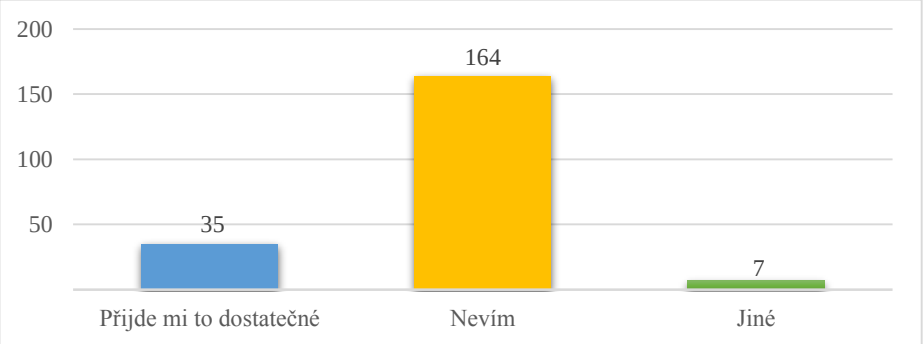
Respondentů, kterém přijde řešení počítačové kriminality dostatečné, je 17 %. Poměrně vysoké procento, téměř většina odpovídajících, neví, jakým způsobem by zlepšili stav počítačové kriminality.

Ostatní uvedli například přísnější tresty a větší opatření, vyšší kontrolu sociálních sítí, lepší systém pro nahlášení počítačové kriminality, více monitorovat a hlídat počítačový prostor. Objevil se i názor, že nic takového nelze udělat, internet je příliš široké místo a nejde ho regulovat v jedné zemi jedním způsobem.

Tabulka 12: Řešení počítačové kriminality

Odpověď	n_i	p_i
Přijde mi to dostatečné	35	17 %
Nevím	164	80 %
Jiné	7	3 %
Celkem	206	100 %

Zdroj: Vlastní zpracování



Obrázek 14: Řešení počítačové kriminality *Zdroj: Vlastní zpracování*

6.3 Shrnutí výsledků dotazníkového šetření

Cílem dotazníkového šetření bylo zjistit, jaký názor mají studenti na počítačovou kriminalitu, a to konkrétně v následujících oblastech:

- zda se někdy setkali s jakoukoli formou počítačové kriminality
- jak se před kybernetickou kriminalitou chrání
- jestli používají sociální sítě
- zda sdělují své osobní informace na internetu.

Odpovědi na tyto otázky byly zodpovězeny díky dotazníkovému šetření a jeho následné analýze.

Z tohoto šetření vyplývá, že všichni respondenti využívají internet, takže všichni mohou být potencionálními obětmi. Jen malá většina se vůbec nesetkává s nevyžádanou poštou, často právě při otevření spamu může dojít nějakým způsobem k ohrožení zařízení. V dnešní době není překvapující, že téměř každý má účet na nějaké sociální síti, kde uvádí informace ze svého soukromí nebo fotky, které mohou být zneužity. Například internetové bankovnictví je téměř nezbytné, i když mnozí mu stále zcela nedůvěřují. Právě bankovnictví přes internet je jedním z nejčastějších terčů kybernetické kriminality.

Uživatelé chrání nejčastěji svá zařízení pomocí antivirového programu poskytovaného zdarma i jeho placenou verzi. Velká část má zařízení také zaheslováno nebo mají antivirovou ochranu integrovanou přímo v mobilu nebo počítači. Způsoby ochrany počítače a mobilního telefonu se liší, ale stále většina uživatelů alespoň nějakou ochranu využívá.

Většina respondentů vnímá internet jako nedostatečně kontrolován a chráněn, mnozí si myslí, že tresty nejsou tak vysoké jaké by měly být, přitom ale zasílání nevyžádané pošty, stahování nelegálních softwarů nebo muziky neberou jako počítačovou kriminalitu a velké procento odpovídajících se ji samo dopouští.

Z výsledků vyplývá, že uživatelé informačních technologií zaznamenávají existenci počítačové kriminality, jsou si vědomi hrozby, která může nastat, ale stále hodně z nich doufá, že zrovna jim se to nestane. Pokud se někdo stal obětí kybernetické kriminality nebo alespoň někdo z jeho blízkých, je už větší pravděpodobnost, že se dotyčný bude více chránit a bude tento problém brát mnohem vážněji.

ZÁVĚR

Cílem práce byla analýza počítačové kriminality a zhodnocení její hrozby v současném světě. Vytyčeny byly hlavní cíle, které měly být v práci obsaženy. Cíle se týkají historie a druhů počítačové kriminality, kybernetická kriminalita ve světě, prevence před kriminalitou na internetu a dotazníkové šetření. Tyto body byly naplněny a zde je shrnutí celé práce.

Historie počítačové kriminality je popsána od samého začátku, kdy vznikl první počítač, od pravěku přes středověk a novověk až dodnes. Tento druh kriminality se od dob jeho vzniku velmi rozšířil a stále roste, a to jak v České republice, tak i všude po světě. Je popsána současná situace kriminality globálně, u nás v ČR a v jiných státech EU. Uvedena je i struktura trestných činů v oblasti kybernetické kriminality za posledních pár let.

Pro lepší chápání kybernetické kriminality je uvedena její charakteristika a popis pojmů, které jsou důležité pro tuto oblast. Uvedeno je rozdělení, které se především zabývá novým jednáním, které přišlo s novými technologiemi a nyní se s nimi lze setkat nejčastěji.

Pro lepší boj s kriminalitou na internetu je potřeba sledovat stále nové technologie a pokrok. Tuto práci můžou vykonávat pouze specialisté na tento obor a je nutné, aby se neustále zdokonalovali. Je popsáno jakým způsobem probíhá vyšetřování této kriminality, jak se zajišťují důkazy, aby nedošlo k jejich ztrátě. Důležité je i podání a přijetí trestního oznámení a náležitosti, které musí obsahovat. Dokazování trestného činu je často obtížné právě kvůli rychlé změně důkazního materiálu. Při vyšetřování je nezbytné, aby bylo prováděno schopným týmem, který má speciální dovednosti a umí pracovat s nástroji, které jsou pro vyšetřování incidentu potřebné. Trestné činy mohou být spáchány i na území více států, v takovém případě tyto státy musí spolupracovat a zjištěná data a znalosti.

Asi nejdůležitějším tématem v této práci je prevence před počítačovou kriminalitou. Spousta uživatelů internetu se stane obětí této kriminality právě z toho důvodu, že si nejsou vědomi rizika a hrozeb, které mohou nastat. Proto existují různé semináře a školení, které se zabývají touto problematikou. Velmi zranitelné jsou děti, které si plně neuvědomují závažnost kybernetických trestných činů, mnozí z nich se s některým z činů setkaly, přitom asi polovina rodičů nemá tušení, čemu jsou jejich děti na internetu vystavovány.

Z analýzy dotazníkového šetření vyplývá, že téměř každý nějakým způsobem využívá internet, ať už to je na sociální sítě, internetové bankovnictví nebo pro zábavu. Většina uživatelů se snaží svoje zařízením alespoň nějakým způsobem chránit, ale přesto ne všichni jsou si plně

vědomi rizika, které přichází s používáním informačních technologií. Málokdo má vůbec představu jak na tom je celkově Česká republika v oblasti počítačové kriminality. Měla by se globálně zlepšit informovanost občanů, například formou školení nebo různých sdělení.

Kriminalita páchána prostřednictvím internetu je vykonávána stále na dokonalejší úrovni a je nebezpečnější každým dnem, díky technologickým pokrokům stále narůstá. Neměla by tedy být brána na lehkou váhu, ať už se s ní dotyčný setkal nebo naopak, potkat to může opravdu kohokoliv a ochrana svého zařízení a soukromí je důležitá. Díky takovému technologickému rozmachu by v budoucnu mělo být i více možností a zbraní jak s kybernetickou kriminalitou bojovat a bránit se před ní.

POUŽITÁ LITERATURA

[1] AUTOLOGISTIKA.CZ. *BDO: počítačová kriminalita dramaticky roste* [online]. 2019 [cit. 2019-11-01]. Dostupné z: https://www.autologistika.cz/bdo-pocitacova-kriminalita-roste/?fbclid=IwAR3Jucqdx7Rjh1lv2r2rs_OvFZsmVx7CBDWFDGYIsAjMtGW-wV7TYVlSBCE

[2] BEZPEČNÝ INTERNET. Videa a dokumenty ke stažení. *Výzkum rizikového chování českých dětí v prostředí internetu 2013* [online]. 2019 [cit. 2019-11-01]. Dostupné z: http://www.bezpecnyinternet.cz/ke-stazeni/default.aspx

[3] CHM. Birth of the Computer. *ENIAC* [online]. 2019 [cit. 2019-11-01]. Dostupné z: https://www.computerhistory.org/revolution/birth-of-the-computer/4/78

[4] CITADELO. *Počítačová kriminalita - jsme často oběťmi hackerských útoků?* [online]. 2019 [cit. 2019-11-01]. Dostupné z: https://citadelo.com/cz/blog/pocitacova-kriminalita-jsme-casto-obetmi-hackerskych-utoku/?fbclid=IwAR2XYlaLZqXPldTQbfOrFC88KM7EUq0qGSU0chBoTWM5lQ_uauLZbHbIpl8

[5] CNEWS.CZ. *Před 35 roky byl uveden IBM PC, moderní stolní počítač pro každého* [online]. 2019 [cit. 2019-11-01]. Dostupné z: https://www.cnews.cz/pred-35-roky-byl-uveden-ibm-pc-moderni-stolni-pocitac-pro-kazdeho/

[6] ČTK. České noviny. *NCOZ: Vzrostla kybernetická kriminalita i nelegální obchody se zbraněmi* [online]. 2019 [cit. 2019-11-01]. Dostupné z: https://www.ceskenoviny.cz/zpravy/ncoz-vzrostla-kyberneticka-kriminalita-i-nelegalni-obchody-se-zbranemi/1780890

[7] DATA CONNECTORS. *21 Terrifying Cyber Crime Statistics* [online]. 2019 [cit. 2019-11-01]. Dostupné z: https://dataconnectors.com/technews/21-terrifying-cyber-crime-statistics/

[8] E-BEZPEČÍ. *Vývoj kybernetické kriminality (2008-2017)* [online]. 2019 [cit. 2019-11-01]. Dostupné z: https://www.e-bezpeci.cz/index.php/z-jinych-webu/1355-vyvoj-kyberneticke-kriminality-2008-2017?fbclid=IwAR2WGsfa98BcjGrx0KwlOVHDGX76JLZk5fktkuumlsWG8iNBkCEuYrIgG3k)

[9] EUROSTAT. European Commission. *Database* [online]. 2019 [cit. 2019-11-01]. Dostupné z: https://ec.europa.eu/eurostat/data/database

[10] ITU. Cybersecurity. *Global Cybersecurity Index* [online]. 2019 [cit. 2019-11-01]. Dostupné z: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[11] GŘIVNA, Tomáš, POLČÁK, Radim. *Kyberkriminalita a právo.* Vyd. 1. Praha - Auditorium, 2008, 220 s. ISBN 978-80-903786-7-4.

[12] HERJAVEC GROUP. *2019 Official Annual Cybercrime Report* [online]. 2019 [cit. 2019-11-01]. Dostupné z: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

[13] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Vyd. 1. Praha – Grada, 2007, 284 s. ISBN 978-80-247- 1561-2.

[14] KOLOUCH, Jan. *CyberCrime*. Praha - CZ-NIC, 2016, 524 s. ISBN 978-80-88168-18-8.

[15] MATĚJKA, Michal. *Počítačová kriminalita*. Vyd. 1. Praha - Computer Press, 2002, 106 s. ISBN 80-7226-419-2.

[16] MVČR. Dokumenty – kybernetické hrozby [online]. 2019 [cit. 2019-11-01]. Dostupné z: https://www.mvcr.cz/clanek/o-nas-bezpecnost-a-prevence-dokumenty-bezpecnost-a-prevence-dokumenty-kyberneticke-hrozby.aspx

[17] NCKB. Informační servis. *Phishing - stále aktuální hrozba* [online]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/doporuceni/2325-phishing-stale-aktualni-hrozba/

[18] OPOJIŠTĚNÍ.CZ. Pojistný trh. *Kybernetická kriminalita stála svět 600 miliard dolarů* [online]. 2019 [cit. 2019-11-01]. Dostupné z: https://www.opojisteni.cz/pojistny-trh/kyberneticka-kriminalita-stala-svet-600-miliard-dolaru/c:14163/

[19] POLČÁK, Radim. *Internet a proměny práva*. Praha - Auditorium, 2012, 388 s. ISBN 978-80-87284-22-3.

[20] POLICIE ČESKÉ REPUBLIKY. *Kyberkriminalita*. [online]. 2019 [cit. 2019-01-20]. Dostupné z: https://www.policie.cz/kyberkriminalita.aspx

[21] POLICIE ČESKÉ REPUBLIKY. Kyberkriminalita. *Policejní internetova HotLine* [online]. 2019 [cit. 2019-11-01]. Dostupné z: https://www.policie.cz/clanek/policejni-internetova-hotline.aspx

[22] PREVENCE KRIMINALITY V ČESKÉ REPUBLICE. Prevence se musí vyplatit. *Prevence kriminality* [online]. 2019 [cit. 2019-01-20]. Dostupné z: http://www.prevencekriminality.cz/prevence-kriminality/

[23] SPRÁVA-SÍTĚ.EU. Správa sítě - slovník pojmů. *Zabezpečení sítí* [online]. 2019 [cit. 2019-11-01]. Dostupné z: https://www.sprava-site.eu/zabezpeceni-site-ostatni/

[24] WEBSITE BUILDER EXPERT. *Which EU Country Is Most Vulnerable To Cybercrime?* [online]. 2019 [cit. 2019-11-01]. Dostupné z: https://www.websitebuilderexpert.com/blog/eu-cybercrime-risk/

[25] WORLD ECONOMIC FORUM. Cybersecurity. *Here are the biggest cybercrime trends of 2019* [online]. 2019 [cit. 2019-11-01]. Dostupné z: https://www.weforum.org/agenda/2019/03/here-are-the-biggest-cybercrime-trends-of-2019/

[26] Zákon č. 141/1961 Sb. ze dne 29. listopadu 1961, o trestním řízení soudním. In *Sbírka zákonů České republiky*. 1961, částka 66, s. 513-576

[27] ZAVRŠIK, Aleš. *Kyberkriminalita.* Praha - Wolters Kluwer ČR, 2017, 148 s. ISBN 978-80-7552-758-5.

[28] ŽIVĚ.CZ. Živě.cz – O počítačích, IT a internetu. *Hacking* [online]. 2019 [cit. 2019-11-01]. Dostupné z: https://www.zive.cz/hacking/sc-381/default.aspx

SEZNAM PŘÍLOH

Příloha A - Dotazníkové šetření

Vážený pane/paní,
žádám Vás o vyplnění tohoto dotazníku za účelem zjištění situace mezi studenty v problematice počítačové kriminality (počítačovou kriminalitou se nazývají trestné činy, které míří proti počítačům nebo jsou díky počítačům páchány).

Data z dotazníku budou anonymizována a použita jako podklad pro analýzu v bakalářské práci.

U každé otázky zaškrtněte, prosím, pouze jednu odpověď (pokud není určeno jinak).

Děkuji.

Sára Škopová
Fakulta ekonomicko-správní
Univerzita Pardubice

1. Přichází Vám nevyžádaná pošta (spam) do e-mailové schránky?

a) Ano, často	
b) Ano, ale jen občas	
c) Ne	

2. Jaké zabezpečení používáte na ochranu svého PC nebo tabletu? (více možností)

a) Antivirový program – placená verze	
b) Antivirový program (freeware) - zdarma	
c) Integrovaný nástroj systému - Firewall	
d) Zaheslování zařízení	
e) Nevyužívám žádný	
f) Jiné, prosím uveďte	

3. Jaké zabezpečení používáte na ochranu svého mobilního telefonu? (více možností)

a) Antivirový program – placená verze	
b) Antivirový program (freeware) - zdarma	
c) Integrovaný nástroj systému - Firewall	
d) Zaheslování zařízení	
e) Nevyužívám žádný	
f) Jiné, prosím uveďte	

4. Využíváte internet pro práci s choulostivými daty (bankovnictví, účetnictví)?

a) Ano, často	
b) Pouze pokud to nejde jinak	
c) Ne, nemám v to důvěru	

5. Sdílíte na sociálních sítích (Facebook, Twitter, Instagram apod.) nebo jinde na internetu své osobní údaje, fotky atd.?

a) Ano, nevidím v tom problém	
b) Ano, ale pouze v malé míře	
c) Ne, mohl by to někdo zneužít	
d) Nepoužívám nic, kde bych mohl/a zveřejňovat své fotky apod.	

6. Přijde Vám internet dostatečně kontrolován a chráněn?

a) Ano, opatření jsou dostatečná	
b) Ne, opatření nejsou dostatečná	
c) Je mi to jedno	

7. Máte obavy, že byste se mohl/a stát terčem kriminality na internetu?

a) Ano, vnímám to jako velkou hrozbu	
b) Neřeším to	
c) Ne, nemám obavy	

8. Stali jste se vy nebo někdo z vašeho okolí obětí kriminality na internetu?

a) Ano, já osobně	
b) Ano, někdo z mých blízkých	
c) Ne, nikoho neznám	

9. Přijde Vám kriminalita páchaná na internetu dostatečně trestána?

a) Ano, tresty mi přijdou adekvátní	
b) Ne, tresty mi přijdou nedostatečné	
c) Nerozumím tomu	

10. Berete zasílání nevyžádané pošty, stahování nelegálních softwarů, muziky, her atd. také jako počítačovou kriminalitu?

a) Ano	
b) Ne, nepřijde mi to tak vážné	

11. Pácháte vy sami nějakým způsobem kriminalitu přes internet? (např. stahování filmů z internetu, hudby, her, zasílání nevyžádané pošty)

a) Ano, často	
b) Ano, ale pouze výjimečně	
c) Ne, je to zločin	

12. Přijde Vám jednoduché dostat se k nelegálnímu softwaru na internetu?

a) Ano, není to problém	
b) Ne, není to jednoduché	
c) Nevím, nevyhledávám ho	

13. Jak vnímáte situaci kriminality na internetu v ČR? (v porovnání s ostatními zeměmi)

a) Situace v ČR mi připadá lepší než v jiných zemích	
b) Situace v ČR mi připadá horší než v jiných zemích	
c) Nemám představu o tom, jaká je situace v ČR	

14. Pokud Vám přijde řešení počítačové kriminality nedostatečné nebo chybné, jak byste to řešili vy?

a) Přijde mi to dostatečné	
b) Nevím	
c) Uveďte prosím Vaše řešení	

15. Na které fakultě studujete?

a) Dopravní fakulta Jana Pernera	
b) Fakulta ekonomicko-správní	
c) Fakulta elektrotechniky a informatiky	
d) Fakulta chemicko-technologická	
e) Fakulta filozofická	
f) Fakulta restaurování	
g) Fakulta zdravotnických studií	

16. V jakém ročníku studujete?

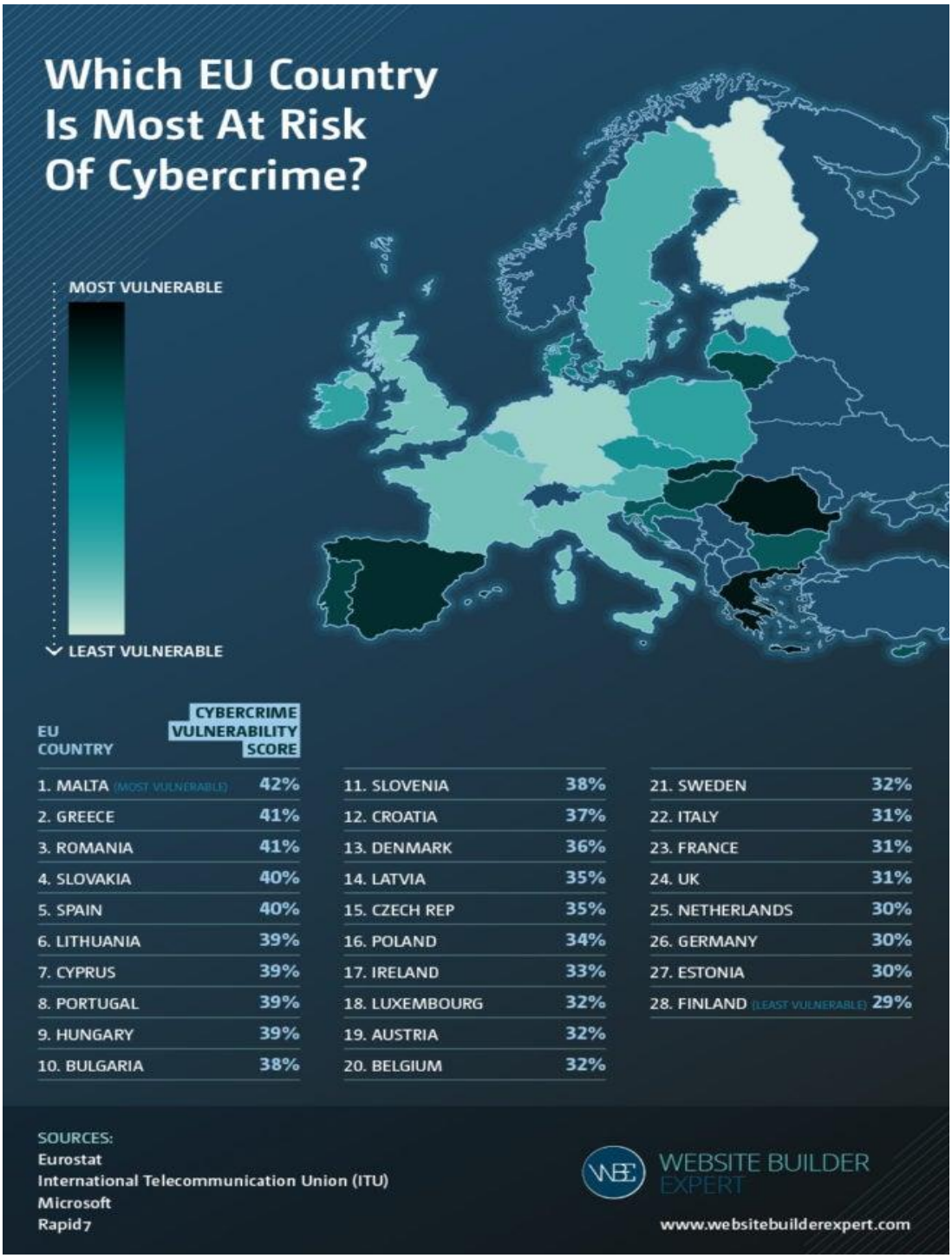
a) 1. ročník	
b) 2. ročník	
c) 3. ročník	
d) Navazující studium	

17. Vaše pohlaví?

a) Muž	
b) Žena	

Děkuji Vám mnohokrát za ochotu při vyplňování dotazníku.

Příloha B - Riziko kyberzločinu v zemích EU



Zdroj: [22]