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

BAKALÁŘSKÁ PRÁCE

POČÍTAČOVÁ KRIMINALITA SE ZAMĚŘENÍM NA HACKING

Autor práce: David Knot

Studijní program: Bezpečnostně právní činnost

Forma studia: Prezenční

Vedoucí práce: doc. JUDr. Roman Svatoš, Ph.D.

Katedra: Katedra právních oborů a bezpečnostních studií

2022

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

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: David Knot

Studijní program: Bezpečnostně právní činnost
Studijní obor: Bezpečnostně právní činnost ve veřejné správě
Forma studia: Prezenční
Místo studia: České Budějovice

Název bakalářské práce: Počítačová kriminalita se zaměřením na hacking

Název bakalářské práce v anglickém jazyce: Cybercrime With a Focus on Hacking

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, titul):
doc. JUDr. Roman Svatoš, Ph.D.

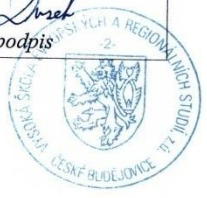
Datum zadání bakalářské práce (měsíc, rok): únor, 2021

Cíl bakalářské práce: Hlavním cílem bakalářské práce bude zjistit formy a četnost počítačové kriminality se zaměřením na hacking, její podmínky a příčiny, a navrhnout vhodná opatření k jejímu omezení.

Student: David Knot	11.2.2021 *datum*	 *podpis*
Vedoucí práce: doc. JUDr. Roman Svatoš, Ph.D.	12.3.2021 *datum*	 *podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	12.3.2021 *datum*	 *podpis*
Prorektorka pro studium a vnitřní záležitosti: RNDr. Růžena Ferebauerová	12.3.21 *datum*	 *podpis*
Pověřený rektor: doc. Ing. Jiří Dušek, Ph.D.	24.5.2021 *datum*	 *podpis*



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

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

.....

Rád bych poděkoval vedoucímu mé bakalářské práce panu doc. JUDr. Svatošovi,
Ph.D. za jeho rady a čas, který mi věnoval. Také bych rád poděkoval všem respondentům, kteří se podíleli na mém výzkumu.

ABSTRAKT

KNOT, D. Počítačová kriminalita se zaměřením na hacking: bakalářská práce. České Budějovice: Vysoká škola evropských a regionálních studií, 2022. 69 s. Vedoucí bakalářské práce: doc. JUDr. Roman Svatoš, Ph.D.

Klíčová slova: počítačová kriminalita, hacking, informační technologie, internet, kyberkriminalita

Bakalářská práce se zaměřuje na problematiku počítačové kriminality, která je stále více aktuální v dnešní době z důvodu dynamického rozvoje odvětví informačních technologií.

Cílem bakalářské práce je zjistit četnost počítačové kriminality, její formy, příčiny, a navrhnout vhodná opatření k jejímu omezení. Teoretická část převážně obsahuje analýzu literárních zdrojů o počítačové kriminalitě a hackingu. V praktické části jsou zpracovány výsledky dotazníkového šetření a poté navržena vhodná opatření k omezení počítačové kriminality.

ABSTRACT

KNOT, D. Cybercrime With a Focus on Hacking: Bachelor Thesis. České Budějovice: The College of European and Regional Studies, 2022. 69 p. Supervisor: doc. JUDr. Roman Svatoš PhD.

Key words: computer crime, hacking, information technology, internet, cybercrime

The bachelor thesis focuses on problematics of computer crime, which is still more current in these times, because of dynamic development information technology industry.

The main goal of the thesis is find out the frequency of computer crime, its forms, causes and suggest appropriate steps to reduce it. The chapter of the theoretical part mostly contains analysis of the literary sources about computer crime and hacking. In the practical part are processed results of the questionnaire investigation and then suggest appropriate steps to reduce computer crime.

Obsah

Úvod

Svou bakalářskou práci na téma „Počítačová kriminalita se zaměřením na hacking“ jsem si zvolil, protože je to stále velice nové a neprozkoumané téma. Z tohoto důvodu je počítačová kriminalita mezi lidmi velice podceňovaná a přehlížená. V dnešní době se celý svět díky technologiím stává stále více digitálním a tím také anonymním, toto platí také pro trestné činy. Většina lidí je již nějakým způsobem na technologiích závislá, protože všem ulehčují životy. Informační technologie dopomáhají k tomu, být v neustálém kontaktu se svými přáteli, klidně i z druhého konce světa. S připojením k internetu je možné sledovat neustálé novinky ze světa, využívat internetové bankovnictví či objednávat produkty z různých e-shopů. Dále je přes internet možné poslouchat hudbu, sledovat filmy, využívat internetové mapy atd. Toto lákavé digitální prostředí s sebou nese i různá rizika, kterých si lidé nejsou dostatečně vědomi a mylně si myslí, že jsou na internet u při využívání informačních technologií v bezpečí. Opak je pravdou, technologie jsou také nástroj pro kriminalitu a prostřednictvím nich je možné snadněji, než, kdy dříve, někomu vyhrožovat, od někoho vymáhat, nebo ukrást peníze či cenné materiály a informace.

Zkoumáním počítačové kriminality a pojmu hacking bych chtěl zjistit její formy, podmínky hackingu a nejčastější nástroje hackerů. Dále bych chtěl zjistit, zda každým rokem dochází k nárůstu případů počítačové kriminality a najít její možné příčiny. Důležitým cílem této práce je navrhnout vhodná opatření pro omezení počítačové kriminality. K tomu, abych mohl navrhnout vhodná opatření pro omezení počítačové kriminality, využiji nejdříve dotazníkové šetření, ve kterém bych chtěl mimo jiné zjistit od respondentů návrhy na opatření, která jsou podle nich vhodná pro omezení této kriminality, a ty následně využiji a zakomponuji do výsledku práce.

Práce bude rozdělena do dvou částí, ve kterých bude značná část věnována k objasnění pojmů počítačové kriminality a jejím podmínkám. Dále se bude práce věnovat formám hackingu a příčinám nebo četnosti počítačové kriminality. Následně bude využito dotazníkového šetření ke zjištění přehledu společnosti o počítačové kriminalitě a názor na prevenci proti ní. Dále chci také zjistit, jaké mají lidé zkušenosti s touto kriminalitou a navrhnout vhodná opatření k jejímu omezení.

1 Cíl a metodika bakalářské práce

Cílem této práce je zjistit četnost počítačové kriminality se zaměřením na hacking a její formy, proč k ní dochází, za jakých podmínek, a navrhnout opatření, která by vedla k jejímu omezení.

Bakalářská práce se dělí na dvě části. První část je teoretická. Pro tuto část bude jako zdroj využívána převážně odborná literatura, která se zaobírá kriminalitou související s informačními a komunikačními technologiemi. V této části dojde především k analýze těchto literárních zdrojů. Druhá část je část praktická, ve které bude využita kvantitativní strategie za pomoci dotazníkového šetření. V dotazníkovém šetření budou odpovídat respondenti z řad veřejnosti na otázky týkající se tématu a na otázky nezbytné k úspěšnému dosažení cílů práce.

2 Počítačová kriminalita – vymezení základních pojmů

Pro počítačovou kriminalitu není známá žádná přesná definice, ovšem dala by se popsat jako kriminalita, která je páchána na počítači nebo prostřednictvím počítače. To znamená, že počítač se dá využít v této problematice více způsoby. Dá se využít jako nástroj, prostřednictvím kterého je počítačová kriminalita páchána. Například prostřednictvím daného počítače je vypuštěn virus nebo posílán spam. Také se dá zneužít jako cíl počítačové kriminality, v tomto případě by byl virus nebo jiná forma počítačové kriminality nasměrována proti tomuto počítači.[1]

Pro počítačovou kriminalitu může být použit buď jeden počítač, pouze jeho komponent, nebo velké množství počítačů či počítačových sítí. Kromě počítačové kriminality existují také jiná odvětví kriminality, ve kterých počítače a počítačové sítě slouží jako vedlejší nástroje, které mají za úkol kriminální činnost usnadnit.[2]

Odvětví informačních technologií by se dalo považovat za nejdynamičtěji rozvíjející se odvětví vůbec. Dnes by se nejspíš nenašel nikdo, kdo se kdy nesetkal s informačními technologiemi. Informační technologie jsou dnes již součástí lidského života. Jsou používány pro jeho usnadnění a jejich využití se dá najít téměř v každé lidské činnosti. Ovšem tyto výhody informačních technologií sebou nesou i své stinné stránky, jako jsou neustále zdokonalující se hrozby související s počítačovou kriminalitou.[3]

Dalo by se říct, že počítačová kriminalita se od jiných druhů kriminality podstatně liší, a je mnohem složitější ji pochopit. Důvodů může být hned několik. Hlavním důvodem je zajisté to, že se jedná o podstatně nové odvětví kriminality, které se neustále vyvíjí a je složitější pochopit pro běžnou populaci jeho problematiku, a to kvůli složitému porozumění stále vyvíjejícím se technologiím. Počítačové kriminalitě není věnována taková dávka pozornosti, kterou by si svou důležitostí zasloužila. Její problematika není příliš mnoho obsažena v knihách kriminologie či jiných odborných listech. Toto platí i přes to, že se jedná o nejrozšířenější a možná i nejvíce nebezpečné zločiny. Počítačová kriminalita je stále ještě páchaná lidmi, kteří hledají svou oběť, nebo jiný cíl za obrazovkou. Tudíž by do této kriminality měli více zasahovat, ať už za

[1] MATOUŠKOVÁ, I. *Aplikovaná forenzní psychologie*. Praha: Grada, 2013. s. 154.
[2] JIROVSKÝ, V. *Kybernetická kriminalita.* Praha: Grada, 2007. s. 271.
[3] KOLOUCH, J. *CyberCrime.* Praha: CZ.NIC, 2017. s. 31.

poznáním nebo přímým řešením, také psychologové a orgány činné v trestním řízení, a ne pouze počítačoví experti a kriminologové.[4]

2.1 Kyberprostor

Počítačová kriminalita by nemohla existovat bez jejího základního kamene, který se nazývá kyberprostor. Kybernetické útoky, kybernetická bezpečnost a jiné kybernetické záležitosti by neměly žádný význam bez kyberprostoru, ve kterém ke všem těmto akcím dochází. Kyberprostor je postaven na informačních technologiích. Bez těchto technologií nemá žádné využití a tím ztrácí svůj význam. To je dáno tím, že informační technologie vytvářejí v kyberprostoru globální síť. Tuto globální počítačovou síť drží při životě uživatelé, kteří ji využívají pomocí například svých počítačů či mobilních zařízení. Dalo by se říct, že tento systém je nekonečná virtuální realita, která je závislá pouze na informačních technologiích z vnějšího světa.[5]

Kyberprostor má několik svých důležitých vlastností, bez kterých by nemohl fungovat. První z těchto vlastností je bezpochyby jeho globální pokrytí za pomoci internetu, jehož sítě jsou rozprostřeny takřka ve všech koutech světa. Kyberprostor nemá žádného vedoucího, nikoho, kdo by ho celý řídil a měl na starost jako autorita. Tato vlastnost se nazývá decentralizace. Další důležitou vlastností kyberprostoru je jeho otevřenost. Do kyberprostoru má přístup každý, kdo chce. Není nic, co by jakémukoliv uživateli bránilo například se spojit s přáteli, nebo si v něm prostě dělat, co se mu zamane. Bohužel toto může být, a velice často bývá, zneužíváno.[6]

Informační technologie jsou logicky hlavním nástrojem pro konání počítačové kriminality. Jak už bylo výše řečeno, kyberprostor může přinášet uživatelům značnou dávku nového formátu zábavy a radosti, dále může vést k navýšení kvality v ekonomice a jiných odvětvích, ale také může vést i bohužel k opravdu velkému zdokonalení nebezpečných hrozeb, které existují. Příkladem těch nejhorších hrozeb, které kyberprostor přináší, je vydírání, špionáže na mezinárodní úrovni, loupeže nebo dokonce terorizmus.[7]

[4] SHAW, J. *Zlo: Věda o temných stránkách lidství*. Přeložil Petra Miketová. Praha: Paseka, 2020. s. 123.
[5] KOLOUCH, J., BAŠTA, P. *CyberSecurity*. Praha: CZ.NIC, 2019. s. 35-36.
[6] JIROVSKÝ, V. *Kybernetická kriminalita.* Praha: Grada, 2007. s. 33-34.
[7] DRMOLA, J. *Protidžihádistický vigilantismus v kyberprostoru.* Brno: Masarykova univerzita. Fakulta sociálních studií, 2018. s. 9.

2.2 Kybernetická bezpečnost

Stejně tak jako u počítačové kriminality, tak i u kybernetické bezpečnosti platí to, že přijít se správným vymezením tohoto pojmu může být velký problém a způsobit velké nejasnosti. Lidé, kteří se nepohybují nijak zvláštně v oblasti ICT a IT, než jen tím způsobem, že využívají své mobilní telefony nebo osobní počítače, by si v téhle problematice jen těžce dokázali správně vysvětlit tento pojem. Většina by si pomyslela, že je kybernetická bezpečnost určena pouze pro IT odborníky, kteří pracují v tomto odvětví. Pravda je ovšem taková, že kybernetickou bezpečnost řeší všichni, kdo využívají některá z těchto osobních zařízení. Jestliže by kterákoliv firma, ať už velký státní podnik, nebo malá soukromá firma, podcenila kybernetickou bezpečnost, mohlo by to zapříčinit fatální dopad na její finance či dokonce na její existenci. Fyzické osoby, které podcení tuto problematiku, mohou přijít například o svůj osobní bankovní účet, nebo mohou být odcizeny jejich citlivé údaje.[8]

K tomu, aby byla řádně zajištěna kybernetická bezpečnost všech osobních či firemních počítačů, nesmí chybět nainstalování firewallu či průběžné provádění antivirové kontroly. Dále by měly být na těchto zařízení zajištěny bezpečnostní aktualizace, které mají za úkol přinášet a obnovovat nové bezpečností aplikace. Tyto aktualizace by se měly provádět automaticky. Tím nevznikne to, že by se na ně zapomnělo. Dále tyto aktualizace mají za úkol chránit systém před všemi možnými složkami nebezpečí, a to stahováním nejnovějších zabezpečení, či nejnovějšími opravami systému. Každý IT správce, který má na starost v dané firmě počítačová zařízení, by měl být pověřen svými nadřízenými k tomu, aby na počítačích byla zpřístupněna možnost takových úkonů, které jsou nezbytné pro pracovní výkon zaměstnanců, a nedocházelo například k odcizování či sdílení různých hesel nebo údajů, při jejichž ztrátě by mohlo dojít k velkým škodám. Počítačová zařízení by měla také mít své pravidelné zálohování, které je využíváno k tomu, abychom nepřišli o všechna uložená data v počítači, jestliže dojde k jejich zničení nebo ztrátě.[9]

2.3 Kybernetický útok

Jeden ze základních pojmů počítačové kriminality je kybernetický útok. Zneužití kybernetického útoku se stále zvyšuje souměrně s tím, jak roste využití informačních technologií, která jsou stále vyvíjeny a zlepšovány. Vymezení pojmu kybernetického útoku je poněkud složité, protože je velmi rozsáhlý a může být vždy založen na jiném

[8] KOLOUCH, J., BAŠTA, P. *CyberSecurity*. Praha: CZ.NIC, 2019. s. 39-40.
[9] NEZMAR, L. *GDPR: Praktický průvodce implementací*. Praha: Grada, 2017. s. 78.

postupu. Pravdou však je, že jde o jednání za pomoci informačních technologií, které má nějakým způsobem poškodit jinou osobu. Dalo by se říct, že kybernetický útok je často zaměňován nebo spojován s kybernetickým bezpečnostním incidentem. Ovšem tyto dva pojmy se od sebe velice liší. Za zaviněním kybernetického útoku vždy stojí nějaká osoba, která chce tímto útokem něco získat, nebo někoho poškodit, tudíž je to pouze úmyslná činnost. Zatímco kybernetický bezpečnostní incident, za kterým také stojí nějaká osoba, je možné spáchat úmyslně nebo také pouze nedbalostí.[10]

Útočník vede proti svému cíli kybernetické útoky prostřednictvím informačních technologií a jejich dat. Kybernetické útoky lze považovat za jistý druh zbraní, ovšem proti klasickým zbraním se značně liší. Největší odlišnost je v tom, že klasické zbraně jsou smrtící a ze značné části také nerozlišují své cíle. Zatímco počítače, kterými jsou prováděny kybernetické útoky, například prostřednictvím různých virů nebo červů, jsou stále považovány za systémy, jejichž úkolem není vzít něčí život, ale pouze zaútočit na systémy jednotlivých osob či firem. V tomto tvrzení může být výjimka v tom, že daný vir může být ukryt v některých ze smrtících zbraní, které nerozlišují své cíle. Také o kybernetických útocích také platí to, že útočník, který je provádí, bývá velice přesný a spíše se nemůže stát, že by minul a zasáhl svým útokem jiný cíl. V jistých normách mezinárodního práva jsou tvrzení o tom, že využití kybernetického útoku je rozumnější, a je schvalováno spíše než využití klasických zbraní z důvodu omezení ztrát na životech.[11]

2.4 Historie počítačové kriminality

Dle dostupných zdrojů, které máme, spadá historie počítačové kriminality do let, kdy ještě nebyl ani postaven první počítač, a to až do roku 1801. V tomto roce bylo sestaveno jednoduché zařízení se systémem, který znatelně vedl k ulehčení práce dělníků v továrně na výrobu látek. Tento systém totiž dokázal tkát látky za dělníky, a to automaticky a s lepším výkonem. Stvořitel tohoto zařízení byl po nějaké době donucen upustit od dalšího vylepšování tohoto zařízení. Poté byl nucen dokonce zařízení zlikvidovat, protože se dělníci báli, že je tento vynález, který tolik vše ulehčuje, nahradí, a přijdou o práci. Další případ, který se stal, byl v druhé polovině devatenáctého století v tamním podniku, a to za pomoci telefonů, s nimiž chlapci, kteří měli povinnost starat se o hovory, je využívali k jednoduchým žertíkům. Náhodně ukončovali nebo s různými zvuky přerušovali hovory a spojovali k sobě hovory, které k sobě nepatřily. K dalšímu

[10] KOLOUCH, J., BAŠTA, P. *CyberSecurity*. Praha: CZ.NIC, 2019. s. 82.
[11] POLČÁK, R., GŘIVNA, T. *Kyberkriminalita a právo.* Praha: Auditorium, 2008. s. 56.

nelegálnímu využívání telefonů docházelo začátkem 20. století. Dalo by se říci, že právě hovory za pomoci telefonů stojí za vznikem kyberprostoru, protože se na dálku setkávají a komunikují spolu dvě nebo více osob. Druhou a také hlavní složkou kyberprostoru byl osobní počítač, který byl ovšem vytvořen až v roce 1971.[12]

V roce 1969 vznikla první verze internetu, ke kterému byly v roce 1972 připojeny pouze armádní počítače. Poté se pro internet nacházeli další oblasti využití počínaje akademickými pracovišti. V této době o počítačové kriminalitě nebylo ještě ani zmínky. Roku 1980 byla poprvé v historii první verze internetu zahlcena virem. O rok později se jako prvnímu člověku, který byl za počítačovou kriminalitu potrestán, povedlo dostat do nepřístupného systému americké IT firmy s názvem American Telephone and Telegraph. Tento systém zmátl a převrátil celé dění tak, aby systém nebyl schopen rozpoznat, jestli jsou účtovány sazby za noční nebo denní tarif. Roku 1988 byl vypuštěn první virový červ, který zahltil několik tisíc počítačů. Poté byla za pomoci počítače vykradena americká banka a pachatelé si tak přišli na 10 milionů dolarů. K počítačové kriminalitě mezi běžnými uživateli informačních technologií začalo docházet, až když se internet více rozšířil a začalo ho využívat stále více uživatelů, do té doby to byla spíše aktivita, která byla páchána na větších společnostech.[13]

2.5 Internet

Bylo by dobré alespoň z části rozvést pojem Internet, protože bez něj by počítačová kriminalita nemohla fungovat. V dnešní době by se asi zřídka našel někdo, ke komu se alespoň nedonesl název Internet. Jedná se o globální počítačovou síť, kterou jak již bylo řečeno, využívali především armádní složky nebo pracovníci vědeckých či pedagogických oblastí. V dnešní době je to tak neopomenutelná technologie, že bez ní by si dnešní děti, dospělí lidé, nebo i velká část důchodců nedokázala představit žít. Internet neboli z anglického překladu Network, je globální síť, která efektivně dokáže spojit za pomocí internetových protokolů velké množství menších sítí jednotlivých počítačů. Pro běžnou veřejnost největším využitím Internetu je, že za pomoci přenášení informací umožňuje využívat chat a video chat, klidně s někým, kdo je připojen k Internetu na druhém konci planety, a to zcela okamžitě.

[12] MATĚJKA, M. *Počítačová kriminalita.* Brno: Computer Press, 2002. s. 18-19.
[13] MATOUŠKOVÁ, I. *Aplikovaná forenzní psychologie.* Praha: Grada, 2013. s. 154.

Umožňuje navštěvování webových stránek, a to odkudkoliv, využívání online médií, nebo třeba hraní různých her.[14]

Každý uživatel počítače musí přiznat, že nebýt Internetu, tak by byl počítač využíván podstatně méně. K tomu, aby počítač mohl být připojen k síti, musí mít svou jedinečnou a originální IP adresu, která je mu přidělena buď nastálo, nebo ji dostane při každém novém připojení do sítě. Každý uživatel má možnost si svou IP adresu přes jisté programy nechat skrýt, aby nebylo možné ji přes jiný počítač vyhledat a popřípadě zaměřit. Jinak je IP adresa každého počítače zcela zjistitelná, protože ji každý počítač využívá pro spojení se s jiným počítačem. IP adresy se řadí do dvou druhů, a to do starší a dříve zavedené IP verze 4 a do novější IP verze 6, která postupně nahrazuje starší verzi. Starší verze IPv4 stále využívá 32bitové adresy. Pouze čtyři čísla jsou obsažena v této verzi IP adresy. Hodnota těchto čísel je maximálně 255 a jednotlivá čísla jsou od sebe oddělena tečkou. Jako příklad této adresy je možno uvést 78.250.108.222, nebo 91.243.58.119. Zatímco takováto adresa je chybná: 135.324.68.169. IP verze 4 bohužel obsahovala vyčerpatelné množství přístupných adres, tudíž muselo dojít k modernizaci, a to přestupem na verzi 6. Ovšem tento přestup na novější verzi nemohl být hotový hned a ještě nějakou dobu potrvá, než dojde k absolutnímu využívání, do té doby tyto dvě verze fungují dohromady. Novější IP verze 6 obsahuje až 2 128 adres a na rozdíl od své předešlé verze se v množství bitů rozrostla na 128 a zapisuje se v šestnáctkové soustavě jako třeba: 2103:2:7af4:453c:b8:1bdd:fa15.[15]

[14] PROCHÁZKA, D. *První kroky s internetem - 3 vydán.* Praha: Grada. 2010. s. 11.
[15] KOLOUCH, J. *CyberCrime.* Praha: CZ.NIC, 2017. s. 74-75.

3 Hacking

Podle Matějky se tento dnes již slavný název „hacking“ datuje od doby, kdy se objevily první počítače. Právě v těchto historicky důležitých dobách si tehdejší programátoři museli sami poradit na tehdejších počítačích s programy a jejich chybami, protože neexistovala žádná podpora jako dnes. Takové upravování programů a celkového softwaru, které napomáhalo k tomu, aby lépe fungoval a nevyskytovaly se v něm různé chyby, které si sami programátoři museli spravovat kvůli tomu, aby měli lepší využití, se začalo nazývat „hacks“. Je velice důležité podotknout, že názvy „hacking“ a „hacker“ nebylo vždy označení pro něco nelegálního a společnosti nic nepřinášejícího. Tehdejší programátoři, kteří se nazývali hackeři, byli velice přínosní tím, že se dokázali dostávat do různých programů a poté dokázali opravit různé nedostatky v systému, díky čemu mohly být lépe využívány. Ovšem s odstupem času se tyto názvy začaly využívat pro všechny, kteří stáli za útoky proti počítačům.[16]

Tento negativní pohled veřejnosti na pojem „hacking“ a „hackeři“ přetrval do dnešní doby, je vnímán jako jednání, díky kterému se hackeři dokážou dostat do cizího počítače za účelem nějakého svého, ať už peněžního, nebo jiného obohacení.[17]

Tento zvrat pohledů, co se týče hackingu, začal přicházet na přelomu osmdesátých let. V této době si začínali hackeři mezi sebou vytvářet frakce, ve kterých spolupracovali na prolamování hesel počítačů. Pokoušeli se prolamovat přístup do počítačů, a to trochu odlišně, než je tomu dnes. Využívali spíše svojí hlavu, a to tak, že zkoušeli různé kombinace hesel a svoji představivost, než za pomoci moderních hackerských programů. Poté se prostředí hackingu dále mění ruku v ruce s modernizací informačních technologií a zvětšování prostředí počítačových sítí a jejich dat. Hacking se stává populárním a začíná se jím bavit stále více lidí, i takových, kteří jsou informačními technologiemi skoro nepolíbeni, takoví jedinci jsou označováni jako script- kiddies. Začínají se vytvářet první hackerské programy nazývající se Easy to use, v překladu do českého jazyka „Snadné použití“. Dále se začínají objevovat webové stránky, na kterých hackerské frakce mohou stahovat různé programy využívající díry v systémech za účelem ovládání cizího počítače.[18]

[16] MATĚJKA, M. *Počítačová kriminalita.* Brno: Computer Press, 2002. s. 20.
[17] KOLOUCH, J. *CyberCrime.* Praha: CZ.NIC, 2017. s. 269.
[18] JIROVSKÝ, V. *Kybernetická kriminalita.* Praha: Grada, 2007. s. 48.

3.1 Hackeři

Hacking se na počítači začal rozrůstat, když se objevila celosvětová síť (Word wide web) a kriminální zločinci začali využívat počítač stále více k páchání kriminality. To bylo dáno tím, že se ukázalo, jak moc to ulehčí práci s loupeží peněz nebo něčeho cenného. O dnešních moderních hackerech obecně platí to, že většina z nich jsou velice vzdělaní v oblasti počítačových systémů, programů a počítačových sítí. Podle většiny zdrojů se dá říct, že tito počítačoví experti jsou kategorizováni do několika skupin. Těchto skupin je pět a každá skupina má svůj název, jak už tady bylo řečeno: Script-kiddies, kteří jsou spíše rádoby hackeři. O hackingu a počítačích toho moc nevědí, ale snaží se. Poté jsou tu White-hats hackeři, kteří jsou vnímáni jako pozitivní hackeři a pracují spíše pro větší organizace, ve kterých mají za úkol hledat díry v systému kvůli vylepšování bezpečnosti. Další skupinou jsou Black-hats hackeři, kteří jsou vnímáni jako negativní hackeři, počítačoví zločinci, kteří se chtějí pouze obohatit na druhých. Dalšími jsou Gray-hats hackeři, kteří jsou něco mezi White-hats a Black-hats hackery. Poslední skupinou jsou takzvaní brilantní programátoři, což jsou velice uznávaní hackeři s obrovskými znalostmi. K bližšímu popisu těchto hackerských skupin budou věnovány podkapitoly, které budou následovat.[19]

Hackeři mají o sobě mínění trochu odlišné než veřejnost. Ovšem, jak už bylo řečeno, všichni se nedají házet do jednoho pytle, ale u spousty z nich platí to, že si sami o sobě myslí, že jsou něco jako novodobí rytíři nebo čističi kyberprostoru, kteří si v něm mohou dělat, co se jim zachce. Vždy berou jako výzvu provádění různých triků v počítačových sítích a někteří z nich si dokonce mohou myslet, že dělají službu veřejnosti, když takto bojují se zavedenými systémy. Hackeři jsou silně proti tomu, aby nad nimi někdo držel kontrolu, na oplátku za to by se žádní hackeři neměli vloupávat do počítačů státních organizací. Nikomu nedůvěřují, obecně neuznávají, že by měli být souzení nějakými neznalými kritérii společnosti a drží se svých základních zásad, třeba té, že hackeři by měli být vázáni k tomu, že provádí svou práci, bez toho, aniž by poškozovali jakkoliv počítačový systém. Věří tomu, že přístup ke všemu, co se týká informačních technologií, je dar, který je určen všem lidem na planetě, a mají ulehčovat život. S tímto je spojené to, že vše, co se týče IT, by mělo být zdarma a veřejně přístupné.[20]

[19] PORTERFIELD, J. *White and BlackHat Hackers.* New York: Rosen Publishing, 2016. s. 7-8.
[20] JIROVSKÝ, V. *Kybernetická kriminalita.* Praha: Grada, 2007. s. 53.

3.1.1 Script-kiddies

Do skupiny Script-kiddies podle Jirovského patří lidé, kteří jsou takzvaní „rádoby hackeři“. Většina z nich si dokonce ani neuvědomí, že mohou svou činností páchat trestný čin a berou toto konání spíše jen jako zábavu. Moc toho o hackingu a IT nevědí, žádné útočné programy vytvářet sami neumí. Většinou pouze využívají nějaké základní, lehce ovladatelné programy, které získají od pravých hackerů. K těmto programům se vždy dostávají dřív než zbytek veřejnosti. Většina lidí, kteří se setkali s nějakým hackem na svém soukromém počítači nebo telefonu, se stali obětí právě někoho ze zmiňované skupiny script-kiddies, protože tato skupina má ve svých řadách největší zastoupení ze všech hackerských skupin.[21]Není radno brát tyto útoky skupiny Script-kiddies na lehkou váhu. Většina z těch, kdo si přečtou, něco o této skupině by si nejspíše pomyslela, že jejich útoky nejsou nebezpečné, ovšem opak je pravdou. Útoky, které jsou třeba i neúmyslné, nebo jeho tvůrci s nimi nemají zlé úmysly, dokážou být právě ty nejvíce zničující.[22]

3.1.2 White-hats hackeři

White-hats hackeři jsou pozitivně vnímáni jako počítačoví specialisté s dobrými úmysly. Tito hackeři nevyužívají svůj počítačový um k loupežím či k páchání škod na nějakém softwaru pro své obohacení, ale svoje dovednosti směřují spíše k prospěšným cílům. Dali by se přirovnat k šerifům na Divokém západě, kteří dávají pozor na veřejnost před bandity. Pokoušejí se nanečisto dostávat do systému, což vede k vyhledání různých nedostatků v něm. Díky tomu o této aktivitě může být zjištěno více informací a dá se jí bezpečně předejít. Z tohoto důvodu jsou tito specialisté najímáni a spolupracují s různými firmami a vývojáři softwaru na zjišťování různých děr v počítačové bezpečnosti a prolamování se do systému, což vede k prevenci před hackerskými útoky. Snaží se učit novým věcem v tomto odvětví a zvyšovat své dovednosti, aby mohli být stále před hackery, kteří páchají trestnou činnost v kyberprostoru.[23]

3.1.3 Black-hats hackeři

Black-hats hackeři jsou protikladem White-hats hackerů. Jsou to záporní specialisté v IT, kterým jde pouze o své obohacení a jsou pro to ochotni napadnout

[21] YOUNG, S., AITEL, D. *The Hacker’s Handbook: The Strategy Behind Breaking Into and Defending Networks.* Boca Raton: Auerbach Publications, 2003. s. 32.
[22] JIROVSKÝ, V. *Kybernetická kriminalita.* Praha: Grada, 2007. s. 56
[23] YOUNG, S., AITEL, D. *The Hacker’s Handbook: The Strategy Behind Breaking Into and Defending Networks.* Boca Raton: Auerbach Publications, 2003. s. 34-35.

jakékoli softwary a počítačové sítě, například i nemocnice. I přes tyto hrozné věci, kterých se dopouštějí, a to, že veřejnost na ně pohlíží jako na nějaké lupiče, sami sebe nevidí jako záporné postavy v kyberprostoru. Ovšem, nutno podotknout, většina si uvědomuje, že jejich aktivita není legální a nemají se ani za ty „hodné“ White-hats hackery. Podle jejich mínění jsou ti „zlí“ právě skupiny Skript-kiddies, kteří negativně narušují kyberprostor.[24]

Black-hats hackeři zřídka kdy pracují pouze sami pro sebe. Ve většině případu mají nějakého svého soukromého zaměstnavatele, který se bez využití jejich IT znalostí neobejde a najímá si je na různé nelegální zakázky. Tito zaměstnavatelé často bývají například různé kriminální organizace či dokonce teroristické skupiny, nebo i jiné nebezpečné organizace. Ovšem zaměstnavatelé těchto Black-hats hackerů nebývají pouze jen nějaké nebezpečné organizace, které je potřebují k různým krádežím či jiným nelegálním činnostem. Velice často se s hackery z této skupiny spojují a najímají je i velké firmy nebo menší podnikatelé, kteří potřebují získat patřičné informace o své konkurenci. Takový hacker je nasazen ke zdroji informací v dané firmě, nejčastěji v nějakém oddělení, ve kterém má přístup k počítačovým systémům a softwarům. Z těchto zařízení poté čerpá všechny možné informace, jako například byznys plány, které za poplatek přeposílá svému pravému zaměstnavateli.[25]

Black-hats hackeři jsou si téměř s White-hats hackery svými znalosti v oboru počítačových technologií rovni. Ovšem tyto dvě skupiny v různých odvětvích tohoto oboru jeden druhého převyšují. Co se týče White-hats hackerů, ti mají skvělý přehled v jednotlivých systémových algoritmech. To je nejspíše zapříčiněno tím, že jim jejich zaměstnavatel umožní přístup do všech počítačových sítí a softwarů, tím mají každý jeden proces plně naučený a pod kontrolou. Oproti tomu Black-hats hackeři musí vynaložit velkou vůli k porozumění danému algoritmu softwarů. To, že se toto musí učit a přicházet na algoritmy sami, vede k tomu, že jsou většinou lepší programátoři než White-hats hackeři. Stále se snaží přicházet na nové technologie, které jim ulehčí práci, proto mívají i větší přehled o nových technologiích.[26]

[24] YOUNG, S., AITEL, D. *The Hacker's Handbook: The Strategy Behind Breaking Into and Defending Networks.* Boca Raton: Auerbach Publications, 2003. s. 35
[25] JIROVSKÝ, V. *Kybernetická kriminalita.* Praha: Grada, 2007. s. 55.
[26] YOUNG, S., AITEL, D. *The Hacker's Handbook: The Strategy Behind Breaking Into and Defending Networks.* Boca Raton: Auerbach Publications, 2003. s. 35.

3.1.4 Grey-hats hackeři

Hackerská skupina nazývající se Grey-hats hackeři je skupina, která je na pomezí mezi White-hats hackery a Black-hats hackery. Tudíž tato skupina hackerů není chápána negativně, ale ani úplně pozitivně. Toto by se dalo vysvětlit tak, že Grey-hats hackeři nemají zcela zlé úmysly jako Black-hats, ale také jim není úplně cizí, když se čas od času nabourají do nějaké soukromé počítačové sítě, nebo vyhledají nezákonně díry v softwarech a přiživí se na nich.[27]

3.1.5 Brilantní programátoři

Tato poměrně malá část IT specialistů se neshoduje s žádnou předchozí skupinou. Brilantní programátoři sice nemají nijak zlé úmysly, ale přesto jsou to stále hackeři. Tito hackeři jsou většinou zaměstnáváni nějakou větší technologickou organizací. I přes to, že mají nějakého svého nadřízeného, který jím zadává úkoly, mají vždy hlavně svou hlavu a často mění svůj pohled na zadaný projekt, přičemž může docházet i k tomu, že si nakonec dělají, co chtějí. Jednotlivci ze skupiny brilantních hackerů jsou opravdu„sólovými hráči“. Jen těžko je jejich nadřízení donutí pracovat v týmu a většinou se spoléhají pouze na své schopnosti, které jsou, co se týče informačních technologií, opravdu velké. I přes to, že na projektech pracují zásadně samostatně, svou práci odvedou velice dobře.[28]

3.2 Malware

Kolouch uvádí, že malware je nejvíce využívaný program hackerů, který lze najít. Tento název zahrnuje všechny možné programy, které mají za úkol různými způsoby narušit normální chod počítače nebo ho poškodit. Programem malware se může počítač „nakazit“ například pomocí e-mailových zpráv, který v sobě obsahují různé přílohy a v nich obsažený malware, nebo sítěmi peer-to-peer, které obsahují „nakažené“ data. Program malware je obecný název pro tento škodlivý software, a jak už bylo řečeno, rozděluje se na několik různých druhů, které jsou pojmenovány podle toho, jakou činnost vykonávají. Tyto druhy jsou: ransomware, spyware, adware, trojský kůň, červi, a různé viry.[29]

[27] STEINBERG, J. *Cybersecurity For Dummies.* New Jersey: Wiley. 2019. s. 50.
[28] JIROVSKÝ, V. *Kybernetická kriminalita.* Praha: Grada, 2007. s. 55.
[29] KOLOUCH, J. *CyberCrime.* Praha: CZ.NIC, 2017. s. 204-205.

3.2.1 Ransomware

Ransomware je druh škodlivého malwaru, který může uživateli daného počítače značně znepříjemnit život. Tento program je u hackerů velice oblíbený. Hackeři ho většinou využívají na přímo vytypované osoby, které svým programem chtějí zasáhnout. Ransomware nebyl vytvořen k tomu, aby díky němu mohla být kradena cenná data a informace z počítače. Jeho využití spočívá v tom, že hacker, který úspěšně napadl počítač, je schopen ho heslem uzamknout do takové míry, kterou není majitel počítače schopen nijak ovlivnit a ztrácí přístup k jeho vlastním počítačovým datům. Hacker poté může požadovat výkupné, nebo něco jiného na oplátku za vrácení přístupu k počítači. Tento velice zákeřný druh malwaru se šíří mnoha způsoby, nejčastěji však bývá ukryt v upraveném souboru s koncovkou zip. a exe., které lze snadno stahovat kdekoliv na internetu. Poté, co je takový napadený soubor stažen do počítače, je pouze otázkou času, kdy se ransomware nahraje do paměti počítače a začne ho heslovat. Další místem, kterým se program šíří, bývá velice často Excel a Word. Pomocí těchto programů většinou znepřístupňují data hackeři firmám. Spoléhají se na to, že v některém oddělení dané firmy se najde někdo, kdo otevře email, ve kterém se v přílohách nachází Word nebo Excel napadený ransomwarem.[30]

3.2.2 Spyware

Program spyware je další druh škodlivého malwaru. Spyware jako špionský malware má za úkol v tichosti slídit a zjišťovat všechna možná soukromá data a informace z cizích počítačů. Tato soukromá data jsou poté přímo posílána do rukou útočníka. Spyware se může šířit jako samostatný škodlivý program pomocí stahování různých souborů do počítače, nebo přes peer-to-peer sítě, nebo může být nainstalován jako součást nějakého jiného bezpečného programu. Ovšem s takovýmto postupem, při kterém dojde k nainstalování spywaru s nějakým jiným bezpečným programem, uživatel zcela souhlasí bez svého vědomí ve smluvních podmínkách. Takovéto programy, jejichž součástí je škodlivý spyware, vytvářejí většinou přímo výrobci těchto programů k tomu, aby mohli sledovat zájmy a činnost uživatele na jeho soukromém počítači a poté mohli shromažďovat všechny tyto informace k vytváření reklamy nebo jiným marketingovým cílům. Uživatel počítače, který napadl spyware, má možnost si všimnout toho, že byl napaden nějakým útočníkem. Všeobecně platí, že pokud byl počítač napaden nějakým malwarem, začne se jeho rychlost značně zpomalovat. Dále napadení spywarem může zaznamenat to, že některé funkce počítače a klávesy vůbec

[30] NEZMAR, L. *GDPR: Praktický průvodce implementací*. Praha: Grada, 2017. s. 228.

nereagují nebo nefungují. Sám Windows může začít hlásit to, že je s počítačem něco v nepořádku, nebo mohou začít vyskakovat různé nechtěné ikony, panely, nebo stále zobrazující se okna.[31]

3.2.3 Adware

Program Adware je nejméně škodlivý malware, který známe. Tento program nemá za cíl nijak vážně poškodit uživatelův počítač nebo mu zcizit jeho osobní data. Jedná se o program, který se naboural do cizího počítače a pouze na něm začne zobrazovat reklamy. Adware opravdu není nijak vážně nebezpečný do té doby, kdy s ním není spojený nějaký jiný malware.[32]Většinu Avaru šíří programátoři, aby se dostala jejich reklama k co nejvíce uživatelům a mohli tak získat peníze na vlastní vytvářené programy. Tyto reklamy se zobrazují prostřednictvím stále vyskakujících oken, zobrazujících se reklam ve spuštěném programu, nebo nastavování prohlížeče a v něm úvodní stránky na jiné reklamní stránky.[33]

3.2.4 Trojský kůň

Škodlivý program Trojský kůň je jeden z nejznámějších druhů malwaru. Trojský kůň je většinou vyslán jako samostatný program, který se nejdřív tváří jako bezpečný, který má být k užitku. Může se například jednat o nějaké počítačové nástroje, počítačové hry, nebo nějaké jiné počítačové programy, které mají vést k užitku uživatele, který si je sám do počítače instaluje bez vědomí, že se v něm skrývá tato hrozba.[34]

Zapnutím nějakého takového programu uživatel na svém počítači dává také nevědomě příkaz k zapnutí Trojského koně, který se sice jako jiné počítačové viry nemůže dál množit, ale dokáže v počítači nadělat velké škody. Nejvíce se využívá hackery pro manipulaci s cizím počítačovým systémem, jako je kopírování a krádež citlivých informací, blokování přístupu do systému, či mazání a přepisování různých souborů a dat. Napadení počítače Trojským koněm může také zapříčinit to, že počítačový systém oslabí svojí ochranu a je tak více náchylný k tomu být napaden

[31] KOLOUCH, J. *CyberCrime.* Praha: CZ.NIC, 2017. s. 207.
[32] KOLOUCH, J. *CyberCrime.* Praha: CZ.NIC, 2017. s. 205.
[33] KRÁL, M. *Bezpečný internet- Chraňte sebe i svůj počítač.* Praha: Grada, 2015. s. 14.
[34] BARVÍŘ, T., MELIŠOVÁ, Š., HAMPL, J., *ECDL – manuál pro začátečníky a příprava ke zkouškám*. Praha: Grada. 2011. s. 200.

jinými škodlivými programy. Tímto také může dojít v počítači k rozšíření druhu Trojského koně s názvem Backdoor, který umožňuje hackerovi řídit počítač na dálku.[35]

3.2.5 Počítačové viry

Počítačové viry jsou velice časté škodlivé programy, jejich účelem je napadávat počítačové programy prostřednictvím počítačových sítí. Tento virus má za úkol škodit počítačovému systému manipulací počítačových dat, jako je mazání či upravování. Viry se často šíří pomocí e-mailových zpráv, a to tak, že se vir skrývá v příloze, o které si uživatel myslí, že je souborem bezpečným jemu adresovaným. Otevřením nakaženého soubor dává uživatel volnost virům napadnout počítač a přidávat své nakažené kopie k bezpečným programům. Asi nejvíce častým způsobem, jak hackeři dostanou své počítačové viry do cizích počítačových systémů, je, že je ukryjí do volně stažitelných souborů, které jsou k mání na internetu nebo do nelegálních programů.[36]

3.2.6 Počítačoví červi

Počítačoví červi jsou velice podobní počítačovým virům, ovšem je mezi nimi rozdíl v tom, že počítačoví červi nedokážou nakazit přímo jednotlivé soubory, ale procházejí do systému pomocí počítačových sítí. Počítačový červ je vytvořen na to, aby se uměl velice rychle množit a šířit, a tak napadávat celé počítačové sítě. Nejdříve napadá jednotlivé soubory v systémech a poté donutí systém k přeposílání jeho napadených kopií k dalším uživatelům, tímto dochází k opravdu velkému zahlcení počítačových sítí tímto programem.[37]

3.3 Phishing

Pojem phishing, neboli v překladu jako „rhybaření“, je odvozeno od názvu klasického rybaření, protože při něm také dochází k „nahazování udic“ a lovení svých obětí. Phishing je podvodná technika, jde o jednu z nejvíce využívaných forem počítačové kriminality využívanou hackery, se kterou se nejspíše setkala většina z uživatelů informačních technologií. Phishing nelze snadno s určitostí definovat. Dal by se popsat jako nelegální postup, během něhož dochází k odcizení soukromých hesel nebo údajů platebních karet. Toto vše se děje za vidinou získání peněz. Nástrojem phishingu bývá nejčastěji e-mail. Funguje to tak, že hacker nejprve vytvoří nějakou

[35] KOLOUCH, J. *CyberCrime.* Praha: CZ.NIC, 2017. s. 208-209.
[36] BARVÍŘ, T., MELIŠOVÁ, Š., HAMPL, J., *ECDL – manuál pro začátečníky a příprava ke zkouškám*. Praha: Grada. 2011. s. 199-200.
[37] KOLOUCH, J. *CyberCrime.* Praha: CZ.NIC, 2017. s. 208.

falešnou stránku, která cílí na nějakou reklamu nebo třeba falešné internetové bankovnictví. Poté zvolí vhodné adresáty nebo rozešle namátkově e-mailové zprávy, ve kterých se nachází adresy těchto falešných stránek, a ty vedou k tomu, aby v nich vyplnil napadený adresát svá hesla a důvěrné informace. Doba pokročila, informační technologie jsou stále více využívány a hackeři jsou si vědomi toho, že e-mailové zprávy bývají nahrazovány sociálními sítěmi. Jako jsou například Facebook, Messenger, Youtube, WhatsApp, nebo třeba Instagram. Tudíž se phishingovými útoky začínají zaměřovat hlavně na tyto sociální sítě.[38]

Phishing má za sebou již značnou historii, jeho začátek sahá až do roku 1995. V této době byly phishingem nejvíce napadány internetové chatové místnosti. Je jisté, že phishing se v dnešní době objevuje násobně mnohem častěji, než tomu bylo dříve. Ovšem tehdy se také objevovaly často účinné metody, které hlavně zneužívaly a těžily z toho, že teprve začínalo období, kdy si lidé pořizovali počítače, které byly připojené k internetu. Tyto metody spočívaly v tom, že hackeři, kteří využívali phishing, předstírali, že jsou administrátoři těchto internetových chatů. Poté svou oběť informovali o tom, že došlo k nějaké chybě a potřebují od nich důvěrné informace a přihlašovací údaje. Autor uvádí, že u phishinguje již od samého začátku nejvíce zajímavé to, že bylo jedno, jakým velkým tempem jdou informační technologie kupředu, nebo jestli má napadená osoba firewall nebo nějaký antivir, protože nic z těchto technologií nemůže ovlivňovat lidský faktor.[39]

Phishing je velice účinná technika, a proto je tak často hackery využíván. Lidé bývají často naivní a otevírají phishingové zprávy bez rozmýšlení na popud různých falešných reklam, falešných nabídek nebo jiných falešných zpráv, které jim něco mohou slibovat či nabízet.[40]

Příznaků phishingu může být mnoho, některé jdou rozpoznat lehce, jiné hůře. Většinou se hackeři při phishingu prostřednictvím zpráv pokoušejí falšovat adresu nějaké organizace, za kterou se vydávají. Tyto zprávy v sobě mívají různé texty, ve kterých se také nachází falešná adresa na webovou stránku organizace, tato adresa ovšem vede na jiné vytvořené stránky, ve kterých stačí, aby dotyčný zadal vyžadované údaje a stává se phishí. Phishing je již poměrně známý, a tak mnozí tuší, jak se proti němu bránit. Největší chyba, kterou může napadená osoba udělat, je klikat na odkazy ve

[38] LANCE, J. *Phishing bez záhad.* Praha: Grada, 2007. s. 28.
[39] LANCE, J. *Phishing bez záhad.* Praha: Grada, 2007. s. 28-29.
[40] LANCE, J. *Phishing bez záhad.* Praha: Grada, 2007. s. 36.

zprávách, které si nejdříve plně neověří. Dále platí to, že by se měl každý vyhnout přihlašování k různým účtům a už vůbec ne k internetovému bankovnictví prostřednictvím odkazu uloženého ve zprávě.[41]

3.4 Dos a DDoS útoky

Hackeři mají v posledních letech stále více v oblibě DoS a DDoS útoky neboli „denial of services attacks“ a „distrubuted denial of services attacks“, které využívají na denním pořádku. Jsou to velice oblíbené metody pro nelegální činnost, protože jsou velice efektivní. Jsou vytvořeny k tomu, aby docházelo k zahlcování počítačů, a tím k přetížení celého počítačového systému, což se hackerům náramně daří. Takovéto zahlcování počítačového systému je možné pro hackery za pomocí nespočetného množství příkazů, které pro vybraný systém mají, s vědomím, že takový objem systém nemůže vydržet a zkolabuje. Útok spočívá v několika krocích. Nejdříve si hacker vyhledá svou oběť, které chce znemožnit přístup k počítačovému systému, poté vyhledá počítačový systém, na který pošle svůj škodlivý program, kterému se také přezdívá „bot“. Tohoto škodlivého bota vyšle přes počítačové sítě do zvoleného počítače, který dále slouží jako takový „přenašeč“. Přes tento již napadený počítač se dále šíří škodlivý program bot a napadá obrovské množství počítačů. Poté co toto hacker úspěšně dokázal, je možné, aby svým škodlivým botem, přes který se mu povedlo úspěšně nakazit velké množství počítačů, tyto počítače přiměl „poslouchat“ jeho rozkazy. Takovouto napadenou síť počítačů, kterou hacker řídí, je schopen využít k tomu, aby z každého jednoho napadeného počítače byl vyslán nějaký objem dat. Ze všech vyslaných objemů dat se vytvoří obrovské množství dat, které koluje do počítačového systému svého cíle a úplně ho zahltí.[42]

Jak už bylo řečeno, DoS a DDoS útoky jsou velice efektivním nástrojem, jak vyřadit z provozu nějaký vybraný počítačový systém. Tyto útoky mají širší využití, protože prostřednictvím nich je možné zahltit a vyřadit z provozu, nebo pouze zpomalit, pro uživatele jakákoliv internetová média nebo třeba webové stránky. DoS útoky a DDoS útoky jsou, dalo by se říct, skoro to samé, ovšem najdou se mezi nimi jisté rozdíly. DoS útok je z této dvojice ten mírnější a o něco bezpečnější. To neznamená, že by jím způsobené škody byly menší, škody zůstávají po jeho dopadu úplně stejné, pouze

[41] NAVARRŮ, M., WALS, N. I. *Nebojte se počítače pro Windows 10 a Android.* Praha: Grada. 2017. s. 78.
[42] JANSA, L., OTEVŘEL, P., ČERMÁK, J., MALIŠ, PETR., MATĚJKA, M. *Internetové právo.* Brno: Computer Press. 2016. s. 398.

jeho úspěšné vykonání je menší, což je zapříčiněno tím, že se dá proti němu lépe bránit. Lepší obrana je zapříčiněna tím, že si stačí dávat pozor a bránit se pouze jenom jednomu zdroji útoku, protože DoS útok je vypouštěn pouze jedním počítačovým systémem, zatímco DDoS útoky jsou pro jejich cíle mnohem náročnější na obranu. DDoS útok, na rozdíl od DoS útoku, je totiž vypouštěn z více zdrojů najednou, které mohou být rozmístěny klidně různě po celém světě, tudíž je těžké se na takovéto útoky připravit a bránit se před nimi.[43]Je zaznamenáno opravdu spoustu případů, kdy byly DoS a DDoS útoky využity na nějaké větší instituce, jako jsou například různá internetová nebo rozhlasová média, televizní kanály, tisková média, velké firmy nebo banky. Jeden z nejznámějších příkladů se uskutečnil, když se proslulá hackerská skupina rozhodla, že vyšle své DDoS útoky proti společnosti MasterCard.[44]

3.5 DNS útoky

DNS útoky, neboli Domain Name Systém attack, také někdy označováno jako pharming, jsou účinným nástrojem počítačových hackerů, které využívají ke sběru informací a dat od jejich obětí. Tyto hackerské triky jsou založeny na útocích, které směřují proti doménovým adresám. Hacker, který tento útok vysílá, má na výběr, buď ho může nasměrovat přímo na vytypovanou doménovou adresu, nebo je schopen ho využít pouze na počítač daného uživatele. Tento útok spočívá v tom, že dojde k přesměrování uživatele nebo zamaskování dané domény na jinou falešnou hackerem vytvořenou doménu. Využití se nachází nejvíce například u internetového bankovnictví či jiných účtů, kde je zapotřebí zadat heslo. Princip je takový, že uživatel, který se snaží dostat na webové stránky svého internetového bankovnictví, se nevědomky přihlásí na falešné, velice uvěřitelné stránky a tím hacker získává přístup k jeho účtu. Tyto DNS útoky jsou velice nebezpečné a také nebezpečnější než phishing. Na rozdíl od phishingu je velice těžké je prokouknout, protože falešné doménové stránky vypadají jako originál a opakovaně nevyskakují žádné žádosti na jejich navštívení.[45]

3.6 Warez

Při provádění počítačové kriminality hrají samozřejmě hlavní roli informační technologie, bez nichž by nic, co zaznělo v této práci, nebylo možné a ani v případě Warezu tomu není jinak. Warez je označován za počítačové pirátství v moderní době.

[43] KOLOUCH, J. *CyberCrime.* Praha: CZ.NIC, 2017. s. 296.
[44] JANSA, L., OTEVŘEL, P., ČERMÁK, J., MALIŠ, PETR., MATĚJKA, M. *Internetové právo.* Brno: Computer Press. 2016. s. 398.
[45] JANSA, L., OTEVŘEL, P., ČERMÁK, J., MALIŠ, PETR., MATĚJKA, M. *Internetové právo.* Brno: Computer Press. 2016. s. 396.

Právě internet byl hlavním pilířem, který odstartoval warez ve formě, jak je znám dnes. Warez se dá označit jako takový „spojovatel“ celého počítačové pirátství. Díky němu byly spojeny všechny okruhy, které se týkají počítačového pirátství k sobě. Ještě před warezem bylo normální, že docházelo k pirátství v samostatných jednotlivých okruzích, jako třeba krádež souborů hudby, videí nebo krádeže softwarů. Po nastoupení warezu došlo ke spojení všech těchto okruhů k sobě.[46]

Je pravda, že za počítačové pirátství se dá také označit to, když někdo méně zdatný v odvětví informačních technologií využívá doma pro své účely nějaké takové odcizené soubory nebo nelegálně opatřený software, ovšem za pravým warezem stojí velká skupina hackerů, kteří svou činností chtějí dosáhnout nějaký zisk.[47]

Toto se děje i za předpokladu, že jde o trestný čin, a to dle trestního zákoníku paragrafu 270 o porušení autorských práv a práv souvisejících s právem autorským.[48]

Tyto hackerské skupiny se většinou rozdělují do dvou podskupin, přičemž každá skupina je specializovaná jinak a má na práci odlišnou úlohu. První a důležitější skupina hackerů má na starost nelegální činnost, co se týká prolamování obranných mechanismů a získávání tím daných programů a souborů. Druhá skupina hackerů má za úkol tyto nelegálně získané materiály nějakým způsobem zpeněžit. Hackeři musí zajistit to, aby se o získaných materiálech doslechl co největší počet potencionálních odběratelů. K tomuto co největšímu dosahu jsou nejvíce užitečné WWW stránky a internetové reklamy. Hackeři mají na vybranou, buď získané materiály dají na své WWW stránky zpoplatněné, kde si každý, kdo má k těmto stránkám přístup může pořídit, co se mu zrovna líbí, nebo je na tyto stránky můžou dát úplně zdarma. V tomto případě ale musí vytvořit strategii jiného výdělku. Většinou tato strategie spočívá v reklamách na těchto stránkách, které jsou ovšem také trochu hackery poupraveny. Jakmile si nějaká osoba tyto stránky nabízející warez otevře, začnou se jí objevovat různé odkazy či jí vyskakovat neustále otravující dialogová okna, které jí mají za úkol přimět navštívit jiné stránky, které jsou zpoplatněny. Na těchto stránkách se také může skrývat třeba nějaký

[46] MATĚJKA, M. *Počítačová kriminalita.* Brno: Computer Press, 2002. s. 70.
[47] JANSA, L., OTEVŘEL, P., ČERMÁK, J., MALIŠ, PETR., MATĚJKA, M. *Internetové právo.* Brno: Computer Press. 2016. s. 399-400.
[48] MATĚJKA, M. *Počítačová kriminalita.* Brno: Computer Press, 2002. s. 72.

škodlivý malware, nebo skrytý škodlivý počítačový vir.[49]Tato nelegální činnost byla poměrně zdárně potírána do té doby, než začal být warez využíván v online prostředí. K tomu, aby bylo možné sledovat a odhalit online warez, je nutné přímo sledovat počítačovou síť.[50]

3.7 Příčiny počítačové kriminality

Počítačová kriminalita má více příčin. Jednou ze základních je neustálý vývoj technologií a otevírání tím i novým příležitostem hackingu. Informační technologie jsou stále zdokonalovány takovým tempem, na které by jen stěží šlo dohlížet. Díky neustálým technologickým inovacím získávají také Hackeři do rukou stále nové, vylepšené a často neprozkoumané nástroje pro dopouštění se počítačové kriminality. Z tohoto jasně vyplývá, že jádro příčiny počítačové kriminality je rozmach technologií.[51]

Autor uvádí, že stejně tak jako pro běžnou kriminalitu, tak i pro počítačovou kriminalitu, platí to, že peníze jsou opravdu největším lákadlem, a tudíž i velice častou příčinou k jejímu páchání. Při běžné kriminalitě zřídkakdy dojde k vykradení nějaké velké organizace. Většinou při ní dochází k vyloupení nějakého menšího obchodu nebo domu. Ovšem počítačová kriminalita je velice často soustředěna na online bankovnictví, velké firmy, nebo organizace, při jejichž loupeži si hackeři mohou přijít i k milionovým částkám. Krom peněžního zisku může být důvodem hackera také třeba zisk cenných informací či dat. Dále se také vyskytují hackeři, kteří konají nelegální činnost pouze pro vlastní pobavení nebo získání pocitového obohacení, jako je vykonání msty či dokázání si své výjimečnosti.[52]

Dalším velkým faktorem, který následuje po peněžním zisku a hackery láká pro páchání kriminality přes počítačové systémy, je to, že se při tom cítí více utajení, s pocitem většího bezpečí a nedostižitelnosti. S tímto souvisí i fakt, že zákon pro počítačovou kriminalitu má své nedostatky a potřeboval by rozšířit, tohoto jsou si hackeři vědomi a umí toho využívat. Dále jsou si dobře vědomi toho, že povědomí obyvatelstva o počítačové kriminalitě je stále velmi nízké a staví se k tomuto problému velmi laxně, klasický skoro všemi využívaný antivirový program je lehké obejít.

[49] JANSA, L., OTEVŘEL, P., ČERMÁK, J., MALIŠ, PETR., MATĚJKA, M. *Internetové právo.* Brno: Computer Press. 2016. s. 399-400.
[50] MATĚJKA, M. *Počítačová kriminalita.* Brno: Computer Press, 2002. s. 72.
[51] JYOTSNA. Major causes of cyber crimes you must be aware of. Jigsawacademy.com. [online] 26.6.2020. [cit. 2022-6-3] Dostupné z WWW: <https://www.jigsawacademy.com/major-causes-of-cyber-crimes-you-must-be-aware-of/>
[52]Příčiny počítačové kriminality. cze.digiist.com. [online] 8.4.2020 Copyright © 2022 [cit. 2022-6-3] Dostupné z WWW: <https://cze.digiist.com/chrome/causes-of-cyber-crime-105901.html>

Dokonce i velké firmy tuto hrozbu stále zanedbávají, neuvědomují si rizika a problém řeší, až když je už většinou pozdě.[53]

Další zatím méně běžnou příčinou počítačové kriminality, která se ovšem začíná v dnešní době stále častěji vyskytovat, je příčina z vlastního přesvědčení hackerů, které není vždy pouze sobecké. Jedná se například o jejich nesouhlas s různými organizacemi, s politikou, nebo dokonce s celými vládními nařízeními či různými projevy, cenzurou, nebo s prováděním vojenských akcí. Tyto formy nesouhlasu projevují tím, že všemi způsoby začnou škodit na počítačových sítích a serverech.[54]

[53] DOUPAL, F. Počítačová kriminalita v ČR roste o desítky procent. rmol.cz. [online] 17.19.2015 Copyright © 2009-2022 [cit. 2022-6-3] Dostupné z WWW: <https://www.rmol.cz/novinky/pocitacova-kriminalita-v-cr-roste-o-desitky-procent>

[54] Příčiny počítačové kriminality. cze.digiist.com. [online] 8.4.2020 Copyright © 2022 [cit. 2022-6-3] Dostupné z WWW: <https://cze.digiist.com/chrome/causes-of-cyber-crime-105901.html>

4 Statistická data počítačové kriminality

Tato kapitola se bude zabývat analýzou statistických dat počítačové kriminality. Jak už bylo řečeno v kapitolách předtím, informační technologie zažívají neustálý progres a inovaci, tudíž toto zažívá i kriminalita spojená s informačními technologiemi. Počítačová kriminalita je řádně sledována a zaznamenávána již od roku 2011 až do přítomnosti. Tento zdroj uvádí období let 2011 až 2019 a je v něm uveden opravdu značný nárůst páchání počítačové kriminality. K největšímu počtu spáchaných trestných činů počítačovou kriminalitou jsou podvodné triky na internetu jako například phishing. Co se týká prolamování se do cizího počítačového systému a nosičů informací, během let posílilo a nevypadá to, že by se v následujících letech něco změnilo, spíše naopak. Dokonce začal svou četností výskytu za rok převyšovat i jiné trestné činy. Tento zdroj nabízí náhled růstu počítačové kriminality v rozmezí devíti let, a to za roky 2011 až 2019. Přičemž v roce 2011 bylo zaznamenáno 1502 trestných činů, poté přišel strmý nárůst, a v roce 2019 bylo zaznamenáno 8417 trestných činů spojených s počítačovou kriminalitou.[55]

Dalším analyzovaným zdrojem budou statistiky kriminality vedené Policii ČR, a to tří trestných činů týkajících se počítačové kriminality, konkrétně trestného činu Neoprávněný přístup k počítačovému systému a nosiči informací, trestného činu Opatření a přechování přístupového zařízení a hesla k počítačovému systému a jiných takových dat a trestného činu Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti. Tyto tři trestné činy jsou v uvedené statistice vedeny dohromady.

[55] Statistika kybernetické kriminality za rok 2019. e-bezpeci.cz. [online]. 22.1.2020. [cit. 2022-25-2] Dostupné z WWW: <https://www.e-bezpeci.cz/index.php/z-jinych-webu/1749-statistika-kyberneticke-kriminality-za-rok-2019>.

Tabulka 1: Porovnání nárůstu počítačové kriminality od roku 2012 do roku 2021[56]

Rok	Zjištěné případy	Objasněné případy	Procento objasněnosti
2012	178	45	25,3%
2013	301	76	25,2%
2014	669	192	28,7%
2015	707	144	20,4%
2016	635	157	24,7%
2017	784	206	26,3%
2018	893	231	25,9%
2019	1092	208	19,1%
2020	1287	155	12%
2021	1866	158	8,5%

Tato tabulka představuje nárůst případů trestných činů v jedné skupině, a to jsou: trestný čin Neoprávněný přístup k počítačovému systému a nosiči informací, trestný čin Opatření a přechování přístupového zařízení a hesla k počítačovému systému a jiných takových dat a trestný čin Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti za období od roku 2012 do roku 2021. Z tabulky 1 je jasně vidět velký nárůst případů počítačové kriminality za posledních 10 let. V roce 2012 bylo zjištěno 178 případů, z nichž prokázáno bylo 45, což je 25,3%, zatímco v roce 2021 už znatelně přibylo na 1866 případů a z nich bylo

[56] Kriminalita. Policie České republiky: Úvodní strana. policie.cz. [online]. Copyright © 2021 Policie ČR, všechna práva vyhrazena [cit. 2022-6-3] Dostupné z WWW: <https://www.policie.cz/statistiky-kriminalita.aspx>

objasněno 158. Nutno podotknout, že v rozmezí let 2015 až 2016 se nárůst případu snížil o 72, ovšem od roku 2017 pokračoval růst dále.

Za období roku 2020 bylo zaznamenáno dohromady 1287 případů Neoprávněný přístup k počítačovému systému a nosiči informací, Opatření a přechování přístupového zařízení a hesla k počítačovému systému a jiných takových dat a Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti, ovšem většina těchto případů nebyla vůbec vyřešena. Počet vyřešených případů byl pouze 155, což je jen 12%. Z tohoto počtu objasněných případům se 35 případů dopustila osoba opakovaně trestaná. Dále se objasněných případů dopustilo 13 cizinců. Poté třetí největší skupinou, která stála za poškozením a zneužitím záznamu na nosiči informací, byly děti a to v počtu 11. Po této skupině následovalo 8 mladistvých a 3 nezletilí. Pod vlivem se dopustili 3 lidé a pod vlivem alkoholu pouze 1 člověk. Co se týká roku 2021, tak těchto trestných činů přibylo. Bylo zaznamenáno zmiňovaných 1866 případů, což značí velký nárůst oproti roku 2020. Objasněných případů zůstává podobné množství, a to 158, což je 8,5%. Největší dopadená skupina byla opět, jako minulý rok, složena z opakovaně trestaných osob, a to v počtu 30. Další nejvíce početnou skupinou byla zaznamenána skupina dětí v počtu 18. Dále s rovným počtem 13 osob byli dopadeni nezletilí a cizinci. Pouze v počtu 5 byli dopadeni mladiství, a na rozdíl oproti roku 2020 byla dopadena pouze 1 osoba pod vlivem a žádná pod vlivem alkoholu.[57]

Další zdroje, které budou využity, slouží k analýze počítačové kriminality ze světa. Dle různých výzkumů platí to, že počítačová kriminalita se rok od roku zvyšuje až o 50% a v roce 2021 tomu nebylo jinak. Podle statistik bylo v roce 2021 napadeno prostřednictvím počítače o 50% více firem, než tomu bylo v roce 2020. Je odhadováno, že hackeři napadnou více než 30 000 webových stránek denně.[58]

Jako první počítačový útok bude analyzovaný phishing. Phishingové útoky se také rok od roku zdvojnásobují, a tak tomu bylo i v roce 2021, kdy došlo až k dvojnásobnému růstu v zaznamenaných případech. K nejvíce populárním cestám, jak šířit phishing, bylo použití emailových zpráv, a to až z 96%. Dále se phishing ve 3%

[57] Kriminalita. Policie České republiky: Úvodní strana. policie.cz. [online]. Copyright © 2021 Policie ČR, všechna práva vyhrazena [cit. 2022-25-2] Dostupné z WWW: <https://www.policie.cz/statistiky-kriminalita.aspx>

[58] Cyberattacks 2021: Phishing, Ransomware & Data Breach Statistics. spanning.com [online] 18.1.2022 . [cit. 2022-25-2] Dostupné z WWW: <https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/>.

vyskytoval na falešných webových stránkách. Až 61% firem se přiznalo k tomu, že proti nim byl phishing vyslán prostřednictvím kanálů sociálních médií. Phishing byl z 65% vyslaný přímo na předtím určený cíl, což je více než polovina. V průzkumech bylo zaznamenáno, že až 85% byl phishing řízený pro získání hesel uživatelů.[59]

Další analyzovaná data budou data malwaru. Za rok 2021 byl program malware, stejně tak jako roky předtím, také velice používaný. Data uvádějí, že se jeho využitelnost za tento rok také zdvojnásobila. Malware byl hackery používán k prolamování obrany dat z 10%. Je uvedeno, že až 37% celosvětových organizací se stalo v tomto roce obětí nějakého druhu škodlivého malwaru. Výzkumy dále ukazují, že 95% všech použitých malwarů je vytvořeno pro operační systém Windows.[60]

DoS a DoSS útoky měly za rok 2021 také velké nárůsty v použití. Konkrétní nárůst od minulého roku byl 29% a nárůst mezi čtvrtletími v tomto roce byl až obrovských 175%. Výzkumy ukázaly, že začátkem roku se pohybovaly DDoS útoky kolem 200 Gigabitů za sekundu, zatímco koncem roku se toto číslo zvýšilo na 500 Gigabitů za sekundu. Dále bylo registrováno, že hackeři se nejvíce zaměřovali se svými útoky na průmyslové podniky. Data, která byla zjištěna, ukazují, že kořeny útoků jsou nejčastěji vysílány z oblastí Spojených států amerických, Číny, Brazílie a překvapivě Indie. V tomto roce došlo k největšímu DDoS útoku proti Ruské korporaci, a to až s rozsahem 21,8 milionů žádostí na počítačové servery.[61]

Statistika počítačového warezu se také rok od roku stále zvyšuje. Hackery nelegálně uveřejněný materiál na internetu má zhlednutí ročně až 230 miliard s tím, že až 80% z toho je zapříčiněno nelegálními streamovacími servery. Až 24% šířky pásma je ročně zabíráno nelegálním stahováním autorsky chráněných materiálů. Je statisticky dokázáno, že každý třetí posluchač hudby si daný produkt stáhl nelegálně na internetu.[62]

[59] Phishing statistics for 2021. egress.com. [online]. [cit. 2022-25-2] Dostupné z WWW: <https://www.egress.com/resources/cybersecurity-information/phishing/2021-phishing-statistics>
[60] KERNER, M. S. Ransomware trends, statistics and facts. techtarget.com. [online]. listopad 2021. [cit. 2022-25-2] Dostupné z WWW: <https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts>
[61] TUDOR, D. DDoS attacks have grown stronger in 2021. heimdalsecurity.com. [online]. poslední aktualizace 11.1.2022. [cit. 2022-25-2] Dostupné z WWW: <https://heimdalsecurity.com/blog/ddos-attacks-have-grown-stronger-in-2021/>
[62] SPAJIC, J. D. Piracy statistics. datapro.net. [online] . poslední aktualizace 9.2.2022. [cit.2022-25-2] Dostupné z WWW: <https://dataprot.net/statistics/piracy-statistics/>

4.1 Trestné činy v počítačové kriminalitě

V zákonu č. 40/2009 Sb., trestní zákoník ve znění pozdějších předpisů (dále jen „TZ“) můžeme najít několik trestných činů, co se týče informačních technologií. V ustanovení § 230 TZ je uvedena skutková podstata trestného činu Neoprávněný přístup k počítačovému systému a nosiči informací,[63] jež obsahuje dvě základní skutkové podstaty, které znějí:

„(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.
(2) Kdo získá přístup k počítačovému systému nebo k nosiči informací a
a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,
b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,
c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo
d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat,

bude potrestán odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci.“[64]

Z prvého odstavce tohoto trestného činu vyplývá, že kdo překoná bezpečnostní opatření, a tím získá přístup k počítačovému systému, bude potrestán odnětím svobody až na dvě léta.[65]

Z druhého odstavce vyplývá, že kdo získá přístup do počítačového systému, nebo k nosiči informací a neoprávněně užije v něm uložená data, vymaže, poškodí,

[63] Zákony pro lidi. Zákon č. 40/2009Sb., trestní zákoník [online]. [cit. 2022-25-2] Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2009-40>
[64] Zákony pro lidi. Zákon č. 40/2009Sb., trestní zákoník [online]. [cit. 2022-25-2] Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2009-40>
[65] Zákony pro lidi. Zákon č. 40/2009Sb., trestní zákoník [online]. [cit. 2022-25-2] Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2009-40>

padělá či pozmění, data neoprávněně vloží do počítačového systému, nebo zasáhne do vybavení počítače, bude potrestán odnětím svobody až na tři léta.[66]

Pro třetí a čtvrtý odstavec platí, že jde o „kvalifikované skutkové podstaty“, které obsahují zvlášť přitěžující okolnosti, a proto jsou zde vyšší sazby. Ve třetím odstavci je uvedeno, že kdo spáchá čin uvedený v prvním odstavci v úmyslu způsobit jinému škodu, získat prospěch, nebo v úmyslu omezit funkčnost počítačového systému, bude potrestán na šest měsíců až čtyři léta. Ve čtvrtém odstavci se uvádí, je-li spáchán čin z prvního odstavce členem organizované skupiny, nebo jestliže je činem způsobena značná škoda či způsobena porucha v činnosti orgánu státní správy, územní samosprávy, soudu, jiného orgánu veřejné moci, nebo získá-li tím značný prospěch, způsobí-li poruchu v činnosti právnické a fyzické osoby, bude potrestán odnětím svobody na jeden rok až pět let.[67]

V trestním zákoníku je dále obsažen trestný čin týkající se počítačové kriminality, a to Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle § 231 TZ, jehož první odstavec tvoří základní skutkovou podstatu, jež zní:[68]

„(1) Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává

a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo

b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části,

[66] Zákony pro lidi. Zákon č. 40/2009Sb., trestní zákoník [online]. [cit. 2022-25-2] Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2009-40>

[67] Zákony pro lidi. Zákon č. 40/2009Sb., trestní zákoník [online]. [cit. 2022-25-2] Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2009-40>

[68] Zákony pro lidi. Zákon č. 40/2009Sb., trestní zákoník [online]. [cit. 2022-25-2] Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2009-40>

bude potrestán odnětím svobody až na dvě léta, propadnutím věci nebo zákazem činnosti"[69]

Z prvého odstavce z tohoto trestného činu vyplývá, že kdo v úmyslu spáchat trestný čin porušení tajemství zpráv, nebo přístupu do počítačového systému, vyrobí, nějak zprostředkuje zařízení či jiný prostředek vytvořený k neoprávněnému přístupu do počítačového systému, nebo přístupová hesla, bude potrestán odnětím svobody až na dvě léta.[70]

Pro druhý a třetí odstavec platí, že se jedná o „kvalifikované skutkové podstaty", které obsahují zvlášť přitěžující okolnost, a proto jsou zde vyšší sazby. Ve druhém odstavci je uvedeno, je-li spáchán čin z prvního odstavce členem organizované skupiny či získá-li tímto činem značný prospěch, bude potrestán odnětím svobody až na tři léta. Ve třetím odstavci je psáno, získá-li pachatel činem z prvního odstavce prospěch velkého rozsahu, bude potrestán na šest měsíců až pět let.[71]

Dalším paragrafem zaměřeným na informační technologie je §232 TZ, kdy jde o trestný čin Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti, jehož první odstavec, který představuje základní skutkovou podstatu, zní:[72]

„(1) Kdo z hrubé nedbalosti porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté
a) data uložená v počítačovém systému nebo na nosiči informací zničí, poškodí, pozmění nebo učiní neupotřebitelnými, nebo
b) učiní zásah do technického nebo programového vybavení počítače nebo jiného technického zařízení pro zpracování dat,
a tím způsobí na cizím majetku značnou škodu, bude potrestán odnětím svobody až na šest měsíců, zákazem činnosti nebo propadnutím věci"[73]

[69] Zákony pro lidi. Zákon č. 40/2009Sb., trestní zákoník [online]. [cit. 2022-25-2] Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2009-40>
[70] Zákony pro lidi. Zákon č. 40/2009Sb., trestní zákoník [online]. [cit. 2022-25-2] Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2009-40>
[71] Zákony pro lidi. Zákon č. 40/2009Sb., trestní zákoník [online]. [cit. 2022-25-2] Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2009-40>
[72] Zákony pro lidi. Zákon č. 40/2009Sb., trestní zákoník [online]. [cit. 2022-25-2] Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2009-40>
[73] Zákony pro lidi. Zákon č. 40/2009Sb., trestní zákoník [online]. [cit. 2022-25-2] Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2009-40>

Z tohoto prvého odstavce vyplývá, kdo z hrubé nedbalosti porušením povinnosti ze zaměstnání, funkce, nebo uložené dle zákona. Data, nebo vybavení z počítačového systému zničí, poškodí, nebo učiní zásah do technického či programového vybavení počítače a tím způsobí na majetku škodu, bude potrestán odnětím svobody až na šest měsíců.[74]

Druhý odstavec se týká „kvalifikované skutkové podstaty“, která obsahuje zvlášť přitěžující okolnost, a proto je zde vyšší sazba. Je zde uvedeno, že pokud způsobí činem uvedeným v prvním odstavci škodu velkého rozsahu, bude potrestán odnětím svobody až na dvě léta.[75]

[74] Zákony pro lidi. Zákon č. 40/2009Sb., trestní zákoník [online]. [cit. 2022-25-2] Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2009-40>
[75] Zákony pro lidi. Zákon č. 40/2009Sb., trestní zákoník [online]. [cit. 2022-25-2] Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2009-40>

5 Výzkumná část

5.1 Cíl výzkumu

Cílem výzkumu bylo zjistit povědomí obyvatel a jejich názor na počítačovou kriminalitu a hacking, dále zjistit názory na podmínky a příčiny počítačové kriminality a prozkoumat návrhy na opatření pro omezení počítačové kriminality, které respondenti uvedli.

5.2 Výzkumné otázky

1. Jaké povědomí mají obyvatelé o počítačové kriminalitě se zaměřením na hacking?
2. Jaké jsou podmínky a příčiny počítačové kriminality?
3. Jaká opatření by obyvatelé navrhli, aby se snížila počítačová kriminalita.

5.3 Metodika

5.3.1 Metodika sběru dat

Byla využita kvantitativní strategie, metoda dotazování a technika sběru dat dotazníkem.

5.3.2 Technika sběru dat

Pro sběr dat byl využit dotazník v online systému my.Survio.com. V něm se nacházelo 21 otázek, ve kterých bylo možné zvolit buď jednu nebo více odpovědí a jedna otázka byla pro respondenty otevřená.

5.3.3 Výzkumný soubor

Dotazníkové šetření bylo náhodně určeno obyvatelům prostřednictví internetu za pomoci online systému Survio.com. Zde je přiložen odkaz na dotazník. (https://www.survio.com/survey/d/J4Y1F5J3D2J5L7M5V)

5.3.4 Realizace výzkumu

Realizace výzkumu byla provedena v období 3.3.2022 – 15.3.2022. Pro úspěšné získání informací byla využita kvantitativní strategie, která byla vykonána prostřednictvím anonymního dotazníku.

5.3.5 Analýza dat

Analýza dat byla vykonána na základě odpovědí dotazníkového šetření, do kterého se zapojilo 75 respondentů.

5.3.6 Etika výzkumu

Dotazníkové šetření proběhlo v souladu se zákonem č. 110/2019 Sb., o zpracování osobních údajů ve znění pozdějších předpisů. Osoby zapojené do dotazníkového šetření byly seznámeny s tématem a cílem dotazníku a byly ubezpečeny, že se jedná o anonymní a dobrovolný výzkum, který bude využit pouze jako podklad pro tuto práci.

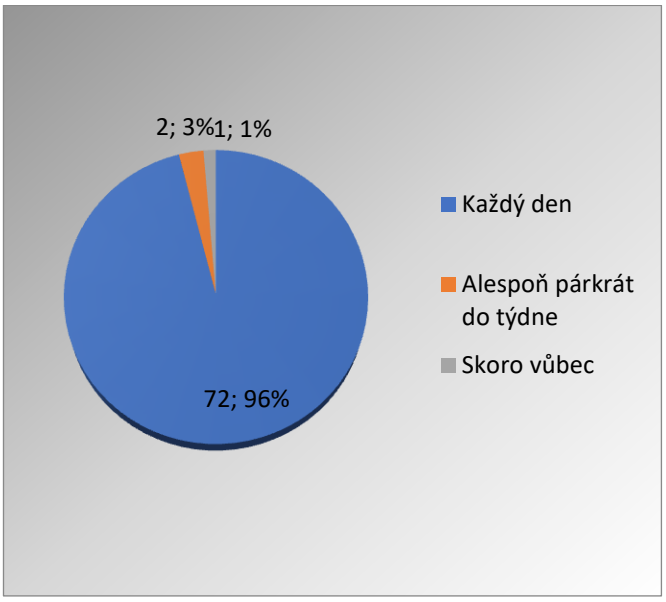
5.4 Výsledky

První otázka dotazníku byla zaměřena na pohlaví respondentů. Bylo zjištěno, že dotazníkového šetření se zúčastnilo 38 mužů (51%) a 37 žen (49%).

Druhá otázka se zaměřovala na věk respondentů. V kategorii 10-20 let bylo 13 respondentů (17%). V další věkové kategorii 21-35 let bylo 29 respondentů (39%). V rozmezí 36-50 let se zúčastnilo 17 respondentů (23%) a ve věku 50+ se zúčastnilo dotazníku 16 respondentů (21%)

Jak často se přihlašujete k internetu?

Graf 1: Otázka č. 3[76]

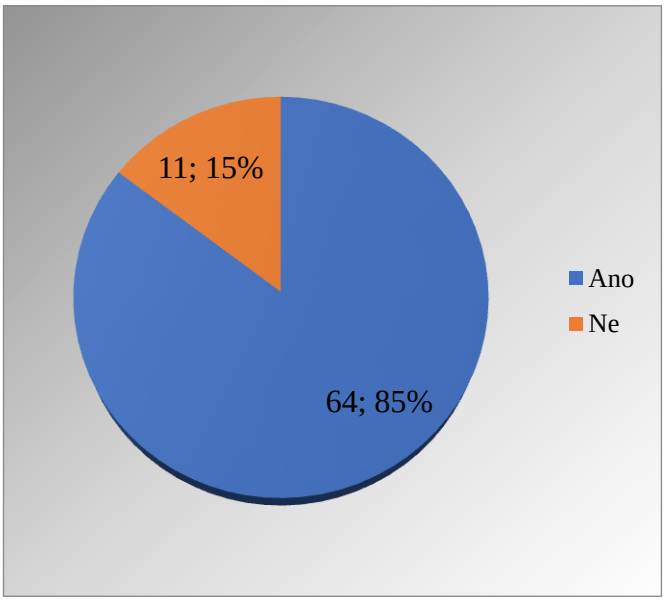


[76] Vlastní zdroj

Třetí otázka se týkala toho, jak často se přihlašují respondenti k internetu. V této otázce, jak se dalo očekávat, respondenti odpověděli skoro jednoznačně z 96%, že se k internetu přihlašují každý den. Pouze dvě osoby se přihlašují alespoň párkrát do týdne a jedna osoba skoro vůbec.

Říká vám něco název počítačová kriminalita?

Graf 2: Otázka č. 4[77]

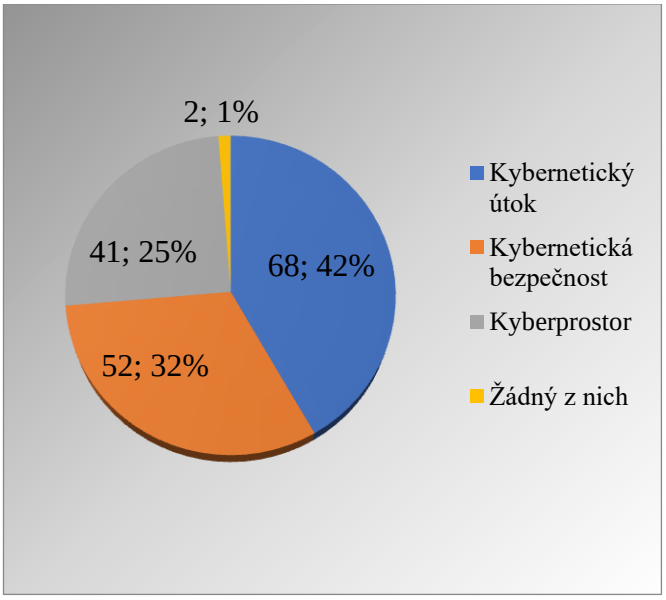


Tato otázka se tázala respondentů, zda jim něco říká název počítačová kriminalita. V převyšujícím počtu 64 respondentů odpovědělo, že ano, a v počtu 11 odpovědělo, že ne.

[77] Vlastní zdroj

Říká vám něco nějaký z následujících názvů?

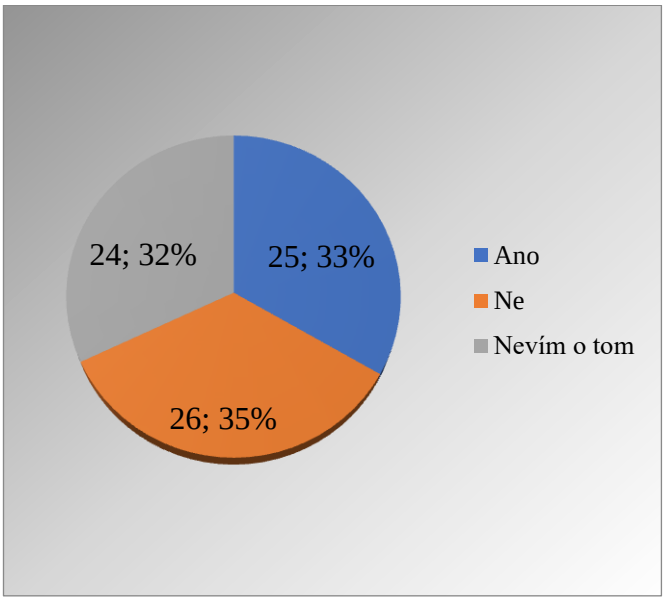
Graf 3: Otázka č. 5[78]



V páté otázce mohli respondenti odpovídat buďto jednou odpovědí či více odpověďmi. Tato otázka zjišťovala, zda respondentům říkají něco pojmy z počítačové kriminality, které jsou uvedeny v grafu. Odpověď kybernetický útok zvolilo 42% respondentů. 32% respondentů zná kybernetickou bezpečnost, a 25% zvolilo, že zná kyberprostor. Pouze 1% zvolilo, že jim nic neříká žádný z uvedených názvů.

Setkali jste se někdy s počítačovou kriminalitou?

Graf 4: Otázka č. 6[79]

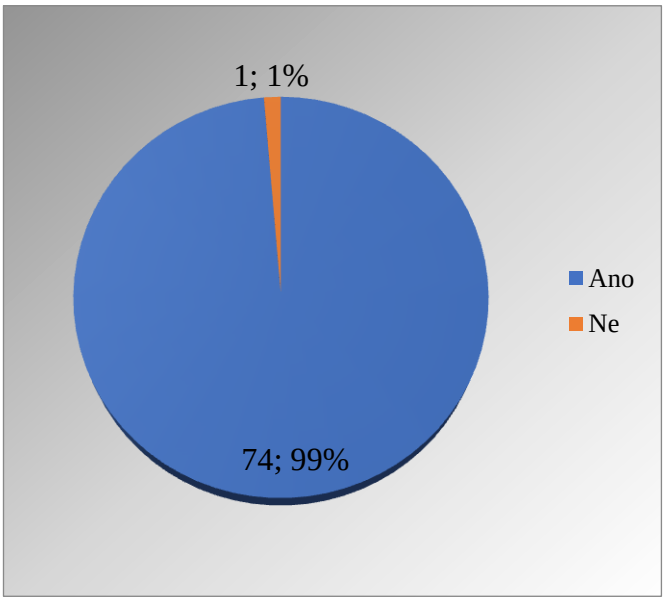


[78] Vlastní zdroj
[79] Vlastní zdroj

Šestá otázka byla zaměřena na setkání respondentů s počítačovou kriminalitou. Z grafu je patrné, že všechny tři otázky dostaly téměř stejný počet odpovědí. Nejvíce respondentů v počtu 26 (35%) odpovědělo ne. Ano odpovědělo 25 (33%) respondentů, a v počtu 24 (32%) odpovědělo, že o setkání s počítačovou kriminalitou neví.

Říká vám něco oslovení hacker?

Graf 5: Otázka č. 7[80]

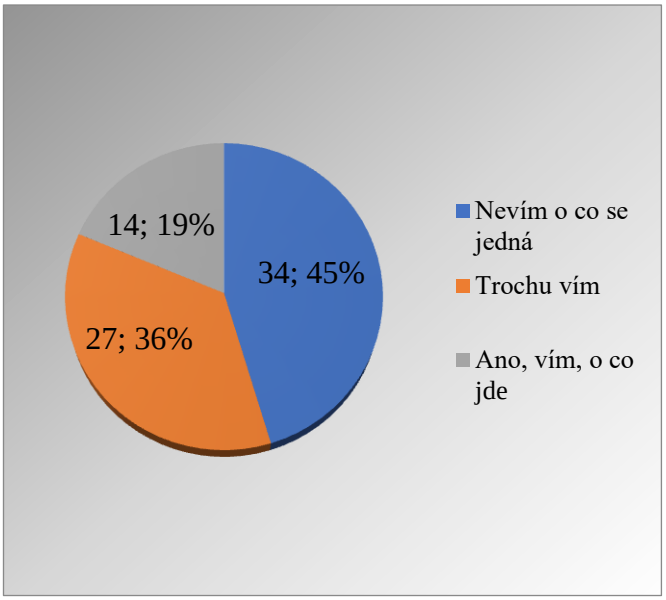


Sedmá otázka se zaměřovala na znalost respondentů názvu „hacker“. V této otázce 99% respondentů odpovědělo, že toto oslovení znají a pouze 1%, což je 1 osoba, oslovení hacker nezná.

[80] Vlastní zdroj

Říkají vám něco názvy White-hats hackeři, Black-hats hackeři, Gray-hats hackeři?

Graf 6: Otázka č. 8[81]

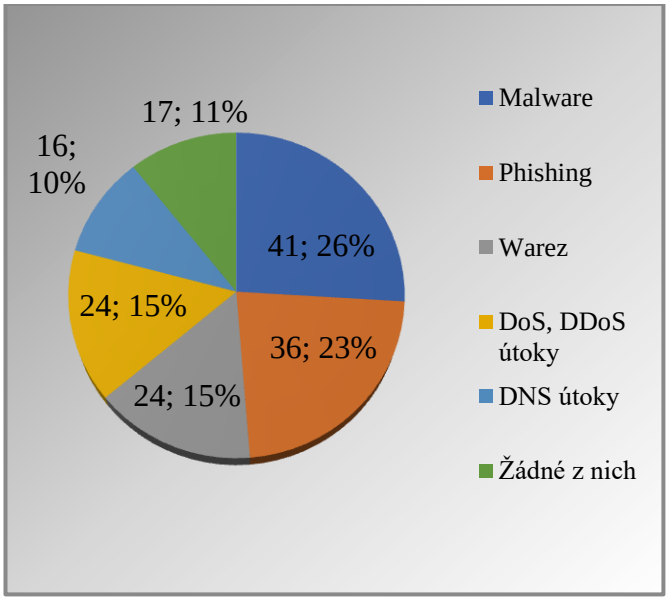


Tato otázka měla za úkol zjistit, jak moc jsou skupiny hackerů známy mezi respondenty. V této otázce nejvíce respondentů uvedlo, že neví, o co se jedná, a to 45%. Druhou nejčastější odpovědí s 36% bylo – trochu vím. Nejmenší skupinou bylo zbylých 19%, kteří odpověděli, že ví, o co se jedná.

[81] Vlastní zdroj

Jaké hrozby vybrané počítačové kriminality znáte?

Graf 7: Otázka č. 9[82]

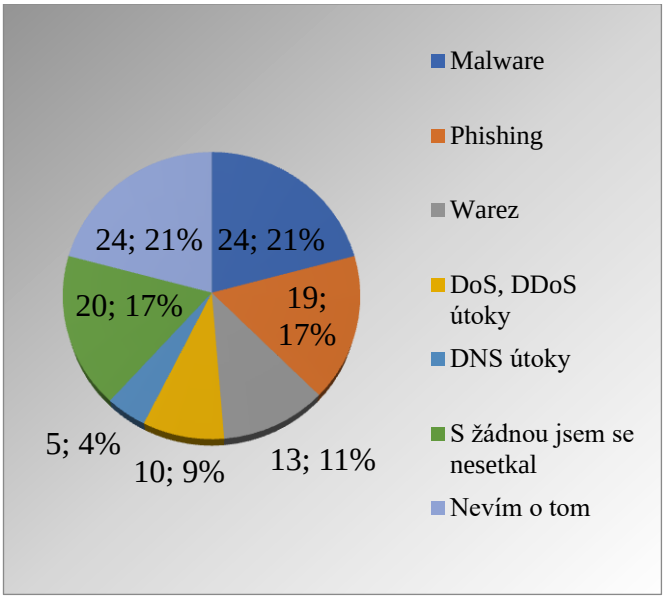


V deváté otázce mohli respondenti odpovědět jednou nebo více odpověďmi. V otázce stálo, jaké hrozby počítačové kriminality znají. Dle grafu největší počet respondentů odpovědělo malware (26%). Druhou nejvíce známo hrozbou byl phishing (23%). Stejný počet respondentů (15%) odpověděl, že znají warez a DoS, DDoS útoky. Nejméně známou hrozbou byla zvolena odpověď DNS útoky s 16 respondenty (10%). Zbylých 11% uvedlo, že žádnou z těchto hrozeb neznají.

[82] Vlastní zdroj

Setkali jste se někdy s nějakou vybranou hrozbou počítačové kriminality?

Graf 8: Otázka č. 10[83]

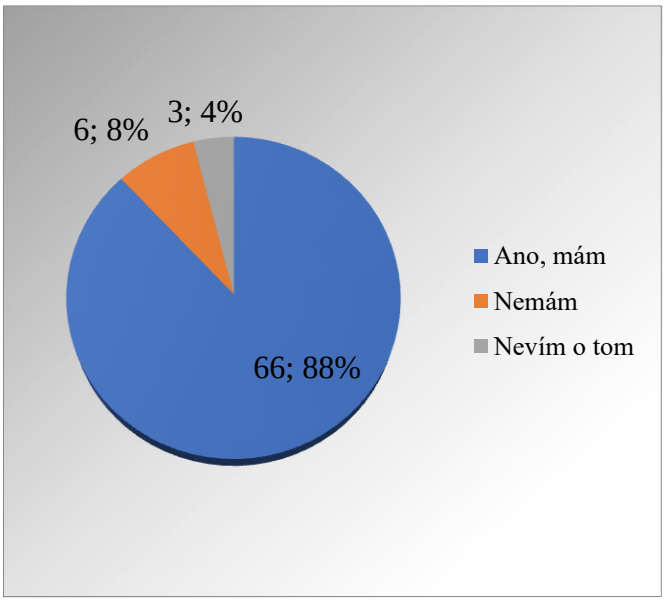


V této otázce s číslem 10 byli respondenti dotazováni, zda se někdy setkali s některou vybranou hrozbou počítačové kriminality, uvedenou v grafu. Respondenti mohli vybrat jednu nebo i více odpovědí. Dle grafu největší počet respondentů (21%) vybralo malware a stejně tak 21% vybralo, že neví, zda se s některou hrozbou setkali. S žádnou z těchto hrozeb se nesetkalo 17% respondentů. Dalších 17% uvedlo, že se setkalo s phishingem. Odpověď warez zvolilo 11% respondentů. Jednou z nejméně volených odpovědí byl DoS a DDoS útok, který zvolilo 9% respondentů a nejméně známou hrozbou byl DNS útok (4%).

[83] Vlastní zdroj

Máte na svém počítači nainstalovaný nějaký ochranný antivir?

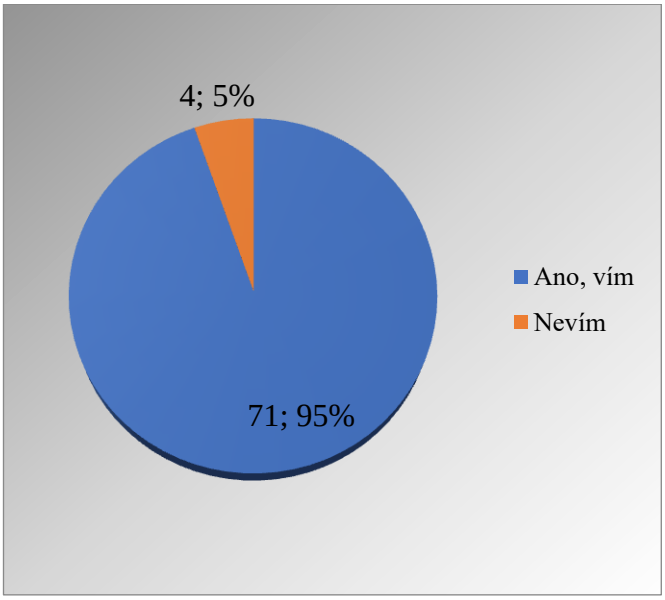
Graf 9: Otázka č. 11[84]



Jedenáctá otázka zjišťovala, zda mají respondenti nainstalovaný antivirový program na svém počítači. Nemalá část respondentů (88%) uvedla, že ho na svém počítači nainstalovaný má. Pouze 8% respondentů antivirový program nemá a 4% dokonce neví, zda mají nějaký antivirový program nainstalovaný.

Myslíte si, že víte, jak se máte chovat bezpečně na internetu?

Graf 10: Otázka č. 12[85]

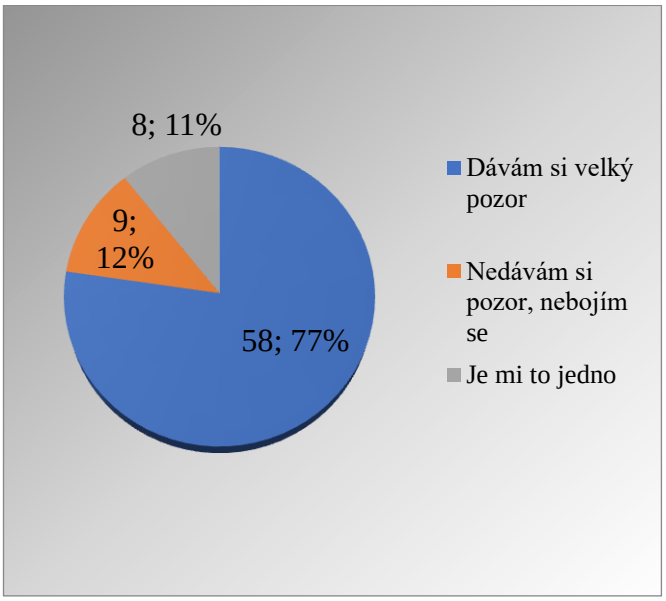


[84] Vlastní zdroj
[85] Vlastní zdroj

Dvanáctá otázka měla za úkol zjistit, jestli si respondenti myslí, že se umí chovat bezpečně na internetu. Z grafu je patrné, že 95% respondentů si myslí, že ví, jak se na internetu bezpečně chovat, a 5% respondentů uvedlo, že neví.

Dáváte si pozor při vstupu na internetu, na jaké stránky a reklamy klikáte, nebo jaké soubory otevíráte?

Graf 11: Otázka č. 13[86]

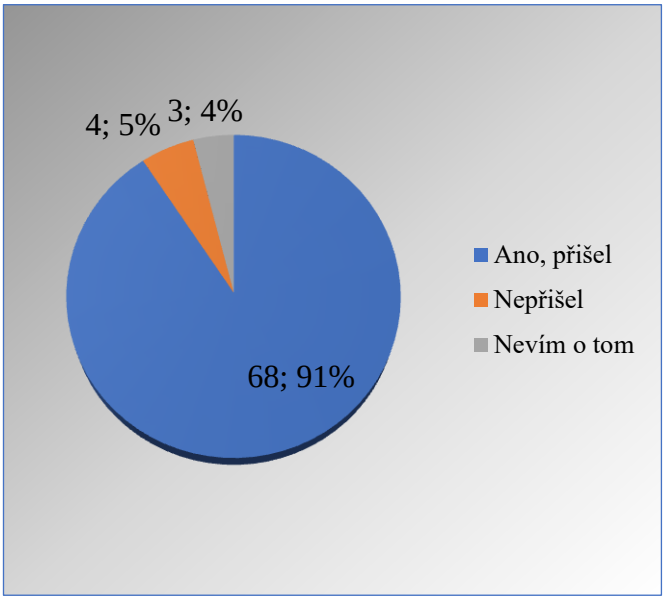


Otázka číslo 13 byla zaměřena na to, jak moc velký pozor si dávají respondenti při vstupu na internet, při vstupu na různé stránky, reklamy či otevírání souborů. V grafu je vidět že 58 respondentů (77%) odpovědělo, že si na toto dávají velký pozor. Dále 9 respondentů (12%) uvedlo, že si nedávají pozor a nebojí se, a pouze 8 respondentů (11 %) uvedlo, že jsou k tomuto riziku lhostejní.

[86] Vlastní zdroj

Přišel vám někdy do emailové schránky neznámý spam s nějakou výhrou, nebo neznámým souborem?

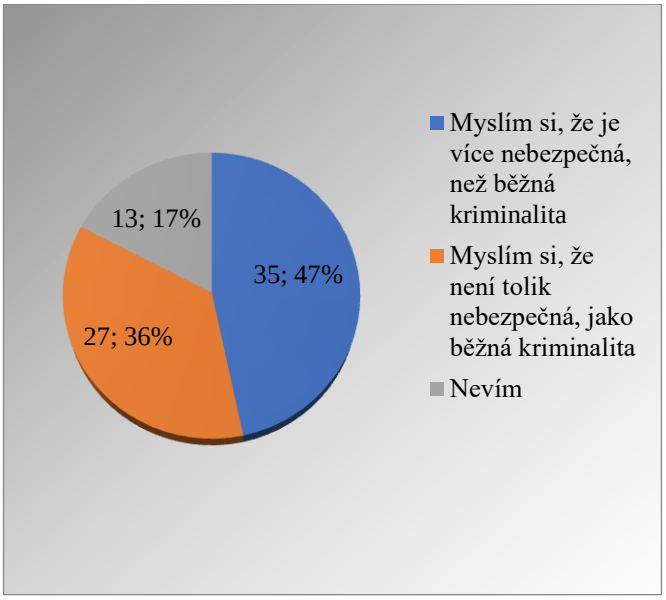
Graf 12: Otázka č. 14[87]



Čtrnáctá otázka zjišťovala, zda byl respondentům někdy doručen spamový email, který jim něco nabízel nebo obsahoval neznámé soubory. Velká část respondentů (91%) odpověděla, že se někdy s takovým emailem setkala. Další skupina byla tvořena respondenty (5%), kterým žádný takový email nepřišel, a zbylá 4% tvořila skupina respondentů, kteří si nejsou vědomi toho, že by dostali někdy nějaký spamový email.

Jak velkou hrozbu podle vás počítačová kriminalita představuje?

Graf 13: Otázka č. 15[88]

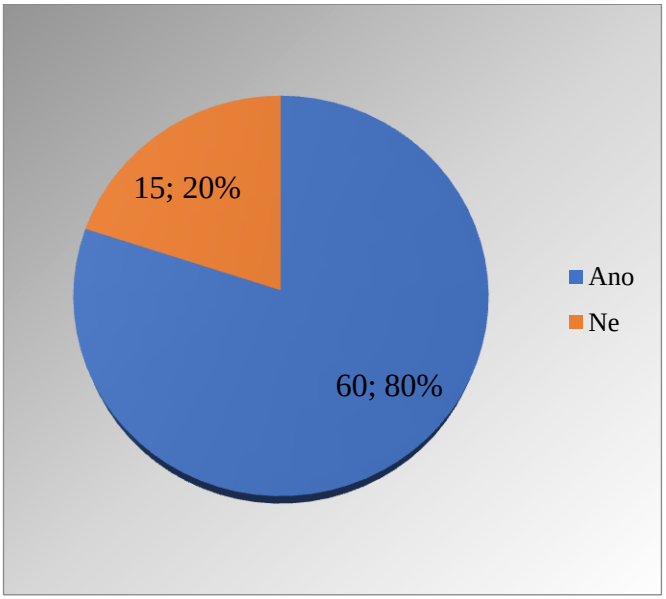


[87] Vlastní zdroj
[88] Vlastní zdroj

Úkolem patnácté otázky bylo zjistit, jak velkou hrozbu dle respondentů tvoří počítačová kriminalita. V této otázce byly názory smíšeny poměrně vyrovnaně. Nejpočetnější skupinu tvořilo 47% respondentů, kteří uvedli, že si myslí o počítačové kriminalitě, že je více nebezpečná než běžná kriminalita. Druhou největší skupinu tvořilo 36% respondentů, kteří považují počítačovou kriminalitu méně nebezpečnou než běžnou kriminalitu. Poslední skupinou bylo 17% respondentů, kteří uvedli, že si nejsou vědomi, jak velkou hrozbu počítačová kriminalita představuje.

Setkali jste se někdy ve svém zaměstnání, škole, nebo v běžném životě se školením, nebo upozorňováním na bezpečný pohyb na internetu, a na počítačovou kriminalitu?

Graf 14: Otázka č. 16[89]

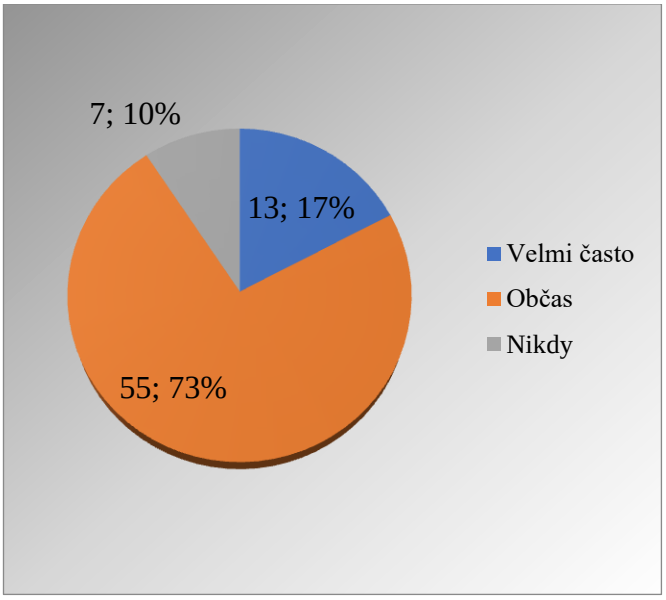


Tato otázka byla zaměřena na to, jestli se respondenti někdy ve svém běžném životě, či zaměstnání a studiu, setkali s upozorňováním nebo školením na bezpečný pohyb na internetu a počítačovou kriminalitu. V grafu je možné vidět, že 80% respondentů odpovědělo kladně a 20% respondentů odpovědělo záporně.

[89] Vlastní zdroj

Jak často k tomuto upozorňování dochází?

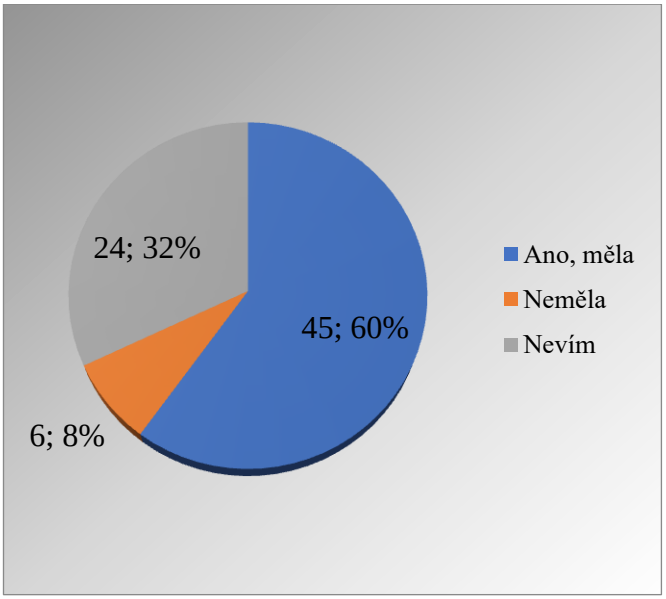
Graf 15: Otázka č. 17[90]



Sedmnáctá otázka měla za úkol zjistit, jak často v životech respondentů k upozorňování na počítačovou kriminalitu dochází. Největší skupina respondentů (73 %) odpověděla, že občas. Druhá skupina (17%) respondentů odpověděla, že k upozorňování dochází velmi často, a 10% respondentů odpovědělo, že k upozorňování na počítačovou kriminalitu nedochází nikdy.

Myslíte si, že Policie ČR by se měla zaměřit více na potírání počítačové kriminality?

Graf 16: Otázka č. 18[91]

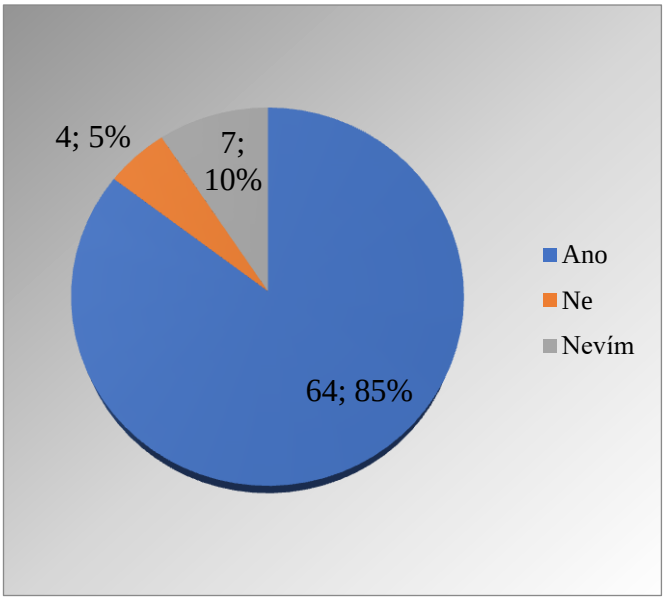


[90] Vlastní zdroj
[91] Vlastní zdroj

Tato otázka byla zaměřena na názor respondentů o rozsáhlejším zaměření Policie ČR na potírání počítačové kriminality. V grafu je vidět, že 60% respondentů uvedlo, že by se Policie ČR měla více na potírání této kriminality zaměřit. Dále vidíme 32% respondentů, kteří uvedli, že neví, a jen malou skupinu respondentů (8%), kteří si myslí, že by se Policie ČR neměla více zaměřovat na potírání počítačové kriminality.

Myslíte si, že by k upozorňování na počítačovou kriminalitu mělo docházet častěji?

Graf 17: Otázka č. 19[92]

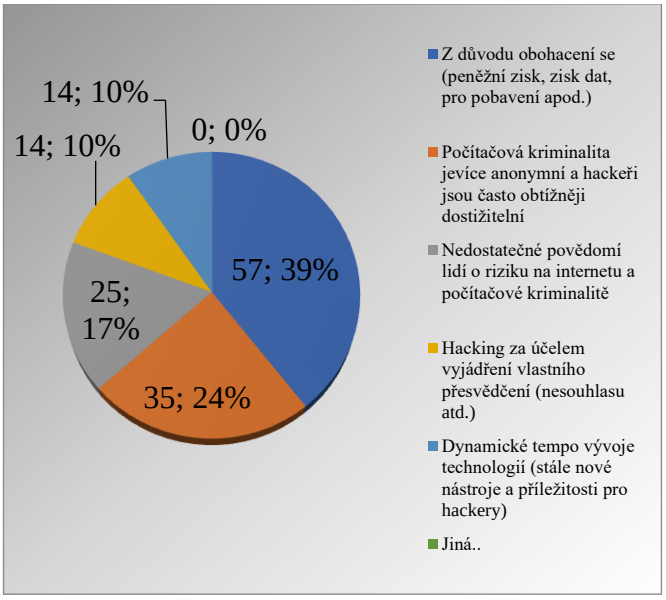


Devatenáctá otázka se ptala respondentů, zda si myslí, že by k upozorňování na počítačovou kriminalitu mělo docházet častěji. V této otázce odpovídalo 85% ano, což je 64 dotázaných. Dále můžeme vidět 10% respondentů, kteří odpověděli, že neví, zda by mělo docházet k upozorňování častěji. Pouze 5% respondentů na tuto otázku odpovědělo, že nemělo.

[92] Vlastní zdroj

jaké si myslíte, že jsou nejčastější příčiny počítačové kriminality?

Graf 18: Otázka č. 20[93]



Pro otázku číslo dvacet mohla být využita buď jedna odpověď nebo i více odpovědí. Otázka měla za úkol zjistit názor respondentů. Respondenti měli vybrat, jaké si myslí, že jsou nejčastější příčiny počítačové kriminality. Nejvíce procent hlasů (39%) získala příčina za účelem nějakého obohacení se. Druhou nejvíce volenou příčinou s 24 % byla počítačová kriminalita z důvodu větší anonymity a obtížnější dostižitelnosti hackerů. Dalších 17% respondentů vybralo, že k počítačové kriminalitě často dochází z důvodu nedostatečného povědomí lidí o riziku na internetu a nedostatečné připravenosti proti počítačové kriminalitě. Poslední dvě příčiny počítavé kriminality dostaly stejné procento hlasů, a to 10%. Z grafu vyplývá, že 14 respondentů zvolilo hacking za účelem vyjádření vlastního přesvědčení, a v tomto případě nečekaně, pouze 14 respondentů vybralo příčinu počítačové kriminality z důvodu neustálého vývoje technologií, zdokonalování hackerských nástrojů a stále větším příležitostem na internetu.

Poslední otázkou byla otevřená otázka, ve které respondenti navrhovali opatření pro snížení počítačové kriminality. Nejčastěji respondenty navrhovaná opatření byla, že by lidé měli být více informováni a upozorňováni na tuto problematiku a o rizicích jejích dopadů, například prostřednictvím médií. Dále to, že by mělo častěji docházet k upozorňování dětí o této problematice, například prostřednictvím různých přednášek ve školách apod., a častějšímu školení lidí ve firmách. Druhým nejčastěji navrhovaným

[93] Vlastní zdroj

opatřením bylo, že by lidé měli více dbát na zabezpečení svých počítačů a telefonů, v lepším případě placeným antivirovým programem. Další nejčastější odpovědí na navrhovaná opatření bylo, že respondenta nic nenapadá nebo se v této problematice nevyzná. Toto jen dokazuje fakt, že tato počítačová kriminalita je stále velice podceňovaná, lidmi přehlížená, a informovanost o ní je velice nízká. Častým návrhem také bylo navyšovat tresty za hacking. Dále padaly návrhy jako: ke každému novému počítači nainstalovaný antivirový program, zavedení státního antivirového programu či zrušení celého internetu.

Diskuse a navrhovaná opatření

Cílem výzkumu bakalářské práce bylo zjistit povědomí obyvatel a jejich názor na počítačovou kriminalitu a hacking, dále zjistit názory na podmínky a příčiny počítačové kriminality, které respondenti uvedli. Konkrétně byly hledány odpovědi na následující výzkumné otázky:

1. Jaké povědomí mají obyvatelé o počítačové kriminalitě?
2. Jaké jsou podmínky a příčiny počítačové kriminality?
3. Jaké opatření by obyvatelé navrhli, aby se snížila počítačová kriminalita?

Do dotazníkového šetření bylo zapojeno 75 respondentů, z nichž bylo 38 respondentů pohlaví mužského a 37 respondentů pohlaví ženského, což je skoro půl na půl. Na dotazník odpovědělo 45 respondentů během pěti minut. Deset minut vyplňovalo dotazník 10 respondentů, 30 minut vyplňovalo dotazník 7 respondentů. Zbylých 13 respondentů strávilo u vyplňování dotazníku více než 30 minut. Ve druhé otázce dotazníku byly uvedeny kategorie rozmezí věku, do kterých se respondenti řadili. Největší počet respondentů byl v rozmezí 21-35 let. Právě u těchto generací se začaly informační technologie využívat nejvíce a oni zažili první sociální sítě. Další skupina s nejvíce respondenty byla do 50let, ovšem ve výzkumné části bylo také důležité to, jak sek této problematice staví mladší lidé pod 20 let nebo starší lidé nad 50 let. Každá tato věková skupina měla své zástupce v podobném počtu. Ve třetí otázce bylo důležité zjistit, jak často se respondenti přihlašují k internetu. V této otázce, i dle teoretické části, bylo očekávané, že internet je nástrojem pro každý den každého z nás, ovšem našla se mezi respondenty jedna osoba, která odpověděla, že internet skoro vůbec nevyužívá.

Další část otázek byla zaměřena na pojmy počítačové kriminality a setkání respondentů s počítačovou kriminalitou. Na otázku, zda respondentům něco říká pojem počítačová kriminalita, odpovědělo ano 64 respondentů. Toto dokazuje, že počítačová kriminalita je stále velice podceňována a informovanost o ní je malá. Dále byly probírány pojmy z počítačové kriminality dle teoretické části. V této otázce respondenti dali nejvíce hlasů pojmu kybernetický útok, druhý pojem byl kybernetická bezpečnost. V šesté otázce byli respondenti dotazováni na setkání s počítačovou kriminalitou, ve které byly odpovědi velice vyrovnané. Největší počet respondentů, kteří dali, že se nesetkali s počítačovou kriminalitou, byl 35%, zatímco 32% respondentů o tom ani neví. Tady je vidět, že lidé se s počítačovou kriminalitou kolikrát setkávají a nejsou si toho vědomi. Dále 33% respondentů uvedlo, že se s počítačovou kriminalitou setkala. Dalšími pojmy byly pojem hacker a hackerské skupiny. Název hacker je v dnešní době poměrně známý a pouze jedna osoba uvedla, že tento pojem nezná. Poměrně velká část respondentů (36%) překvapivě uvedla, že jim něco říkají názvy hackerských skupin, které nejsou v České republice tolik známé. Dokonce 19% respondentů odpovědělo na tuto otázku, že ví, o co jde. Největší skupinou bylo45% respondentů, kteří uvedli, že neví, o co se jedná. Obtížnost dalších dvou otázek byla vyšší a byla zde předpokládaná větší vědomost o této problematice. Byly zde uvedeny vybrané hrozby počítačové kriminality z teoretické části a respondenti měli odpovídat, zda některou z uvedených hrozeb znají či se s některou setkali. Pro obě otázky byla nejvíce hlasovaná hrozba malware, dále nejvíce respondenti znali phishing, toto jsou i dle teoretické práce nejvíce známé hrozby počítačové kriminality. V otázce o setkání s počítačovou kriminalitou nejvíce dotazovaných odpovědělo o malweru, že neví o tom, jestli se s nějakou hrozbou setkali, nebo že se s žádnou nesetkali. Další nejčastěji setkávanou hrozbou byl opět phishing. Tato část odpovědí dotazovaných dokazuje, že povědomí obyvatel o počítačové kriminalitě je stále poměrně nízké a bylo tím tak odpovězeno na výzkumnou otázku číslo 1.

Další skupiny otázek byly zaměřeny na bezpečnost respondentů při využívání informačních technologií. V těch bylo zjišťováno, zda mají respondenti na svém počítači antivirový program a jestli si myslí, že ví, jak se chovat bezpečně na internetu. První otázka se týkala antivirového programu. Tady se opět ukázalo, jak jsou hrozby počítačové kriminality stále ještě podceňovány a lidé si tolik neuvědomují její dopady. Přesto, že 88 % respondentů odpovědělo, že antivirový program má, tak zbylí respondenti uvedli, že žádný antivirový program nemají nebo dokonce o tom ani

nevědí. Toto je trochu zvláštní, protože v další otázce odpovědělo 95% respondentů, že ví, jak se na internetu mají bezpečně chovat a mít antivirový program je první krok k bezpečí. S tímto souvisí i další otázka, ve které respondenti odpovídali, zda si dávají pozor na to, jaké stránky na internetu navštěvují a jaké soubory otevírají. V této otázce 77% respondentů odpovědělo, že si dávají velký pozor. Zbylý podíl respondentů uvedlo, že si nedávají pozor nebo jim je toto riziko úplně jedno. Dále respondenti odpovídali na to, zda jim někdy přišla do emailové schránky neznámá spam zpráva. S touto formou se nejspíše setkala většina uživatelů internetu, a proto 91% respondentů odpovědělo, že přišla, a pouze pár zbylých respondentů uvedlo, že nepřišla nebo si toho nejsou vědomi.

Poslední dvě otázky byly zaměřeny na příčiny počítačové kriminality. V předposlední otázce byly uvedeny příčiny počítačové kriminality, které byly vyzkoumány v teoretické části a respondenti z nich měli vybírat podle svého uvážení ty nejčastější. Nejčastější příčinou podle respondentů, pro kterou hlasovali, byla příčina pro své obohacení, ať už peněžního zisku nebo jiného. Tato respondenty nejčastější příčina se shodovala s teoretickou částí práce, která poukazuje také na to, že peníze jsou největším lákadlem hackerů. Další nejčastěji volenou příčinou, kterou respondenti nejvíce volili, byla vysoká anonymita, která hackery láká a dovádí je k domněnce nedostižitelnosti. Toto tvrzení se shoduje s teoretickou částí, ve které je také tato příčina popsána jako další velice častá příčina po příčině peněžního zisku. Třetí, nejčastěji respondenty volenou odpovědí, byla příčina počítačové kriminality kvůli nedostatečnému povědomí lidí o riziku na internetu a o počítačové kriminalitě. Jak stálo v teoretické části, dle uvedených zdrojů je psáno, že hackeři jsou si dobře vědomi nízkého povědomí lidí o počítačové kriminalitě a jejích rizikách a využívají toho. Tudíž je to také velmi významná příčina této kriminality. Poměrně malou váhu respondenti dali příčině počítačové kriminality za vyjádřením vlastního přesvědčení hackera. O této příčině je v teoretické práci uvedeno, že se jedná zatím o méně běžnou příčinu počítačové kriminality. Tudíž se toto tvrzení shoduje s málo hlasy respondentů na tuto příčinu. Na posledním místě se umístila příčina rychlého tempa vývoje počítačových technologií. V teoretické části bylo zjištěno, že dynamický vývoj počítačových technologií je jádrem příčin počítačové kriminality a díky tomu se stává stále dokonalejší a častější. Respondenti této stěžejní příčině dali i přesto nejmenší počet hlasů s míněním, že tato příčina není tak důležitá. To se neshoduje s teoretickou částí. Tímto bylo odpovězeno na výzkumnou otázku číslo 2.

V poslední otázce vypisovali respondenti své návrhy pro omezení počítačové kriminality. Mezi nejčastějšími návrhy respondentů bylo, že lidé by měli být lépe informováni o rizicích počítačové kriminality. Dále také respondenti odpovídali, že by se o této problematice měly učit děti již na základních školách a také by mělo docházet k upozorňování z řad rodičů. Dalšími častými odpověďmi respondentů bylo, že lidé by měli klást větší důraz na zabezpečení svých informačních zařízení, například si zřídit lepší antivir, a měli by více dbát na bezpečný pohyb na internetu. Dále bylo také často navrhováno, že by se měly zvýšit tresty za konání počítačové kriminality. Také padaly návrhy, že Policie ČR by se na tuto kriminalitu měla více zaměřit, nebo by měl být vytvořen státní antivirus, popřípadě při každém nákupu nového počítače by měl být kvalitní antivirus zdarma. Opatření pro omezení počítačové kriminality, která respondenti navrhli, vedla k odpovědi na výzkumnou otázku číslo 3.

Dále budou navržena opatření, která by mohla být vhodná pro omezení počítačové kriminality. Jako prvním navrhovaným opatřením je, že každý, kdo využívá internet prostřednictvím informačních technologií, by si měl dávat pozor na svůj pohyb na internetu a více dbát na zabezpečení svých informačních zařízení. Při každé návštěvě internetu by si měl každý uživatel zkontrolovat, zda je prohlížečový program, který se chystá využít, aktualizován na aktuální verzi. Potom by si každý měl dostatečně rozmyslet k jaké free Wifi síti se kde připojuje, protože nikdy neví, kdo danou síť sleduje. Poté by si měl každý uživatel dát zvláštní pozor na to, jaké stránky na internetu navštěvuje a jaké reklamy a soubor na stránkách či v emailové adrese otevírá, nebo na jakých stránkách vkládá své přihlašovací a soukromé údaje. Důležité přihlašovací údaje, jako různá hesla, například do internetového bankovnictví, nebo jiných účtů by, by si měl každý uživatel zvolit složité, nepředvídatelné a nastavit si na něm dvoufázové ověřování. V riziku, že se k tomuto heslu již nějakým způsobem hacker dostal, by měl každý uživatel své heslo měnit alespoň jednou do roka. Dále by naprostou samozřejmostí měl být pro uživatele nainstalovaný antivirový program, pokud možno placená verze, která lépe pokrývá hackerské hrozby.

Dalším navrhovaným opatřením je také dle respondentů, že by mělo docházet ke zvyšování prevence proti počítačové kriminalitě. Zvýšení prevence by mohlo být dosaženo lepší informovaností lidí a zvyšováním jejich povědomí o hrozbách počítačové kriminality. K lepšímu informování o počítačové kriminalitě by mělo docházet prostřednictví informačních medií. Firmy by pro své zaměstnance, kteří ke své pracovní činnosti využívají počítač, měly zařídit častější školení o hrozbách počítačové

kriminality, a to klidně jednou do měsíce. Dále by měla prevence cílit již na děti základních škol prostřednictvím výuky nebo různých besed. Také větší důraz na upozorňování dětí o hrozbách počítačové kriminality by měl směřovat od jejich rodičů.

Dalším navrhovaným opatřením je, že by Policie ČR republiky měla vyhledat talentované počítačové profesionály a ty zaměstnat, toto by zajisté vedlo k potlačení počítačové kriminality.

Návrhy vyplývají z analýzy literárních zdrojů a z výsledků dotazníkového šetření.

Závěr

Informační technologie jsou nejvíce rozvíjející se sektor na světě. Neustále dochází k vývoji nových technologických zařízení, která mají usnadňovat lidem jejich život. Ovšem informační technologie mají i své stinné stránky a dají se velice efektivně využívat pro nelegální činnost. Cílem bakalářské práce bylo mimo jiné zjistit formy a četnost počítačové kriminality, zjistit hlavní příčiny, proč k ní dochází, a navrhnout vhodná opatření k jejímu omezení.

Práce je rozdělena na část teoretickou a část empirickou. Teoretická část obsahuje tři hlavní kapitoly a několik podkapitol. V úvodní první kapitole bylo vysvětleno, co je to počítačová kriminalita. Dále byla popsána její historie, jaké první případy počítačové kriminality jsou známy a kdy byly použity první počítačové viry. Dále je kapitola věnována k vysvětlení důležitých pojmů počítačové kriminality, jako je kybernetický útok, kybernetická bezpečnost a kyberprostor. V této kapitole nesměl chybět velice důležitý pojem, který se nazývá Internet, bez kterého by žádný z jiných pojmů neměl význam a počítačová kriminalita by nemohla existovat. Proto mu byl věnován závěr první kapitoly. Druhá kapitola byla věnována pojmu hacking, jeho podmínkám a jeho nejdůležitějším formám. Týkala se forem malwaru, phishingu, warezu, DoS a DDoS útoků a DNS útoků. Každá z těchto forem byla podrobně rozepsána a vysvětlena. V této kapitole také nesmělo chybět vysvětlit název hacker. V dalších podkapitolách bylo vysvětleno, do jakých skupin se tito hackeři zařazují, jak se rozdělují a co je jejich cílem. Na závěr této kapitoly bylo důležitým cílem objasnit příčiny počítačové kriminality. Třetí kapitola obsahuje statistická data počítačové kriminality. Pro lepší znázornění statistických dat byla vyhotovena tabulka, ve které jsou dle statistik Policie ČR znázorněny dohromady tři trestné činy počítačové kriminality a jejich nárůst od roku 2012 do roku 2021. Tyto trestné činy jsou poté podrobněji popsány. Dále byla v této kapitole rozepsána statistická data pro formy hackingu.

Část empirická obsahuje výsledky z dotazníkového šetření a jednotlivé otázky a odpovědi jsou znázorněny v grafech. Tento dotazník měl za cíl zjistit, jak moc je počítačová kriminalita pro respondenty známá a jak se k ní staví. Dále také, jak se staví k prevenci proti počítačové kriminalitě a jaké jsou podle nich její nejčastější příčiny. V poslední otázce dotazníku respondenti navrhovali dle jejich uvážení opatření proti počítačové kriminalitě.

Na závěr výzkumu byla navržena opatření, která by mohla posloužit ke snížení počítačové kriminality.

Jestliže mám shrnout přínos této bakalářské práce, myslím si, že bylo dokázáno to, že počítačová kriminalita je stále ještě velice podceňovaná a znalost této kriminality mezi veřejností je dosti nízká. Toto je dle mého názoru zapříčiněno tím, že se na tuto problematiku a její hrozby mnohdy tolik neupozorňuje jako na jiné. Značná část lidí se již stala nějakým způsobem obětí počítačového zločinu. Jestliže se nezačne na tuto kriminalitu více upozorňovat, myslím si, že je nevyvratitelné, že bude docházet stále častěji k případům počítačové kriminality. Toto souvisí také s tím, že informační technologie a také hrozby na internetu jsou stále častější a stále dokonalejší.

V bakalářské práci se podařilo zjistit formy a četnost počítačové kriminality, její podmínky, příčiny, a navrhnout vhodná opatření k jejímu omezení.

Seznam použitých zdrojů

Literární zdroje

1. BARVÍŘ, T., MELIŠOVÁ, Š., HAMPL, J., *ECDL – manuál pro začátečníky a příprava ke zkouškám.* Praha: Grada. 2011. 240 s. ISBN 978-80-247-3686-0
2. DRMOLA, J. *Protidžihádistický vigilantismus v kyberprostoru.* Brno: Masarykova univerzita. Fakulta sociálních studií, 2018. 176 s. ISBN 978-80-210-8985-3
3. JANSA, L., OTEVŘEL, P., ČERMÁK, J., MALIŠ, PETR., MATĚJKA, M. *Internetové právo.* Brno: Computer Press. 2016. 432 s. ISBN 9788025146644
4. JIROVSKÝ, V. *Kybernetická kriminalita.* Praha: Grada, 2007. 288 s. ISBN 978-80-247-1561-2
5. KOLOUCH, J., BAŠTA, P. *CyberSecurity.* Praha: CZ.NIC, 2019. 560 s. ISBN 978-80-88168-31-7
6. KOLOUCH, J. *CyberCrime.* Praha: CZ.NIC, 2017. 524 s. ISBN 978-80-88168-15-7
7. KRÁL, M. *Bezpečný internet- Chraňte sebe i svůj počítač.* Praha: Grada, 2015. 184 s. ISBN 978-80-247-5453-6
8. LANCE, J. *Phishing bez záhad.* Praha: Grada, 2007. 281 s. ISBN 8024714661
9. MATĚJKA, M. *Počítačová kriminalita.* Brno: Computer Press, 2002. 120 s. ISBN 8072264192
10. MATOUŠKOVÁ, I. *Aplikovaná forenzní psychologie.* Praha: Grada, 2013. 304 s. ISBN 978-80-247-4580-0
11. NAVARRŮ, M., WALS, N. I. *Nebojte se počítače pro Windows 10 a Android.* Praha: Grada. 2017. 176 s. ISBN 978-80-247-5761-2
12. NEZMAR, L. *GDPR: Praktický průvodce implementací*. Praha: Grada, 2017. 304 s. ISBN 978-80-271-0668-4
13. POLČÁK, R., GŘIVNA, T. *Kyberkriminalita a právo.* Praha: Auditorium, 2008. 220 s. ISBN 978-80-903786-7-4
14. PORTERFIELD, J. *White and Black Hat Hackers.* New York: Rosen Publishing, 2016. 64 s. ISBN 978-1-5081-7314-4
15. PROCHÁZKA, D. *První kroky s internetem - 3 vydán.* Praha: Grada. 2010. 112 s. ISBN 978-80-247-3255-8

16. SHAW, J. *Zlo: Věda o temných stránkách lidství*. Přeložil Petra Miketová. Praha: Paseka, 2020. 304 s. ISBN 978-80-7637-047-0
17. STEINBERG, J. *Cybersecurity For Dummies.* New Jersey: Wiley. 2019. 368 s. ISBN 978-1119560326
18. YOUNG, S., AITEL, D. *The Hacker's Handbook: The Strategy Behind Breaking Into and Defending Networks.* Boca Raton: Auerbach Publications, 2003. 896 s. ISBN 978-0849308888

Elektronické zdroje

1. Cyber attacks 2021: Phishing, Ransomware & Data Breach Statistics. spanning.com [online] 18.1.2022 . [cit. 2022-25-2] Dostupné z WWW: <https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/>.
2. DOUPAL, F. Počítačová kriminalita v ČR roste o desítky procent. rmol.cz. [online] 17.19.2015 Copyright © 2009-2022 [cit. 2022-6-3] Dostupné z WWW: <https://www.rmol.cz/novinky/pocitacova-kriminalita-v-cr-roste-o-desitky-procent>
3. JYOTSNA. Major causes of cybercrimes you must be aware of. Jigsawacademy.com. [online] 26.6.2020. [cit. 2022-6-3] Dostupné z WWW: <https://www.jigsawacademy.com/major-causes-of-cyber-crimes-you-must-be-aware-of/>
4. KERNER, M. S. Ransomware trends, statistics and facts. techtarget.com. [online]. listopad 2021. [cit. 2022-25-2] Dostupné z WWW: <https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts>
5. Kriminalita. Policie České republiky: Úvodní strana. policie.cz. [online]. Copyright © 2021 Policie ČR, všechna práva vyhrazena [cit. 2022-6-3] Dostupné z WWW: <https://www.policie.cz/statistiky-kriminalita.aspx>
6. Phishing statistics for 2021. egress.com. [online]. [cit. 2022-25-2] Dostupné z WWW: <https://www.egress.com/resources/cybersecurity-information/phishing/2021-phishing-statistics>
7. Příčiny počítačové kriminality. cze.digiist.com. [online] 8.4.2020 Copyright © 2022 [cit. 2022-6-3] Dostupné z WWW: <https://cze.digiist.com/chrome/causes-of-cyber-crime-105901.html>
8. Statistika kybernetické kriminality za rok 2019. e-bezpeci.cz. [online]. 22.1.2020. [cit. 2022-25-2] Dostupné z WWW: <https://www.e-bezpeci.cz/index.php/z-jinych-webu/1749-statistika-kyberneticke-kriminality-za-rok-2019>.

9. SPAJIC, J. D. Piracy statistics. datapro.net. [online] . poslední aktualizace 9.2.2022. [cit.2022-25-2] Dostupné z WWW: <https://dataprot.net/statistics/piracy-statistics/>
10. TUDOR, D. DDoS attacks have grown stronger in 2021. heimdalsecurity.com. [online]. poslední aktualizace 11.1.2022. [cit. 2022-25-2] Dostupné z WWW: https://heimdalsecurity.com/blog/ddos-attacks-have-grown-stronger-in-2021/

Legislativní dokumenty

1. Zákony pro lidi. Zákon č. 40/2009Sb., trestní zákoník [online]. [cit. 2022-25-2] Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2009-40>

Seznam zkratek

TZ - Trestní zákoník

ICT - Informační a komunikační technologie

IT - Informační technologie

WWW – World Wide Web

Seznam tabulek a grafů

Přílohy

Dotazník:

Výzkumné šetření na téma počítačové kriminality zaměřené na hacking

Dobrý den,

tímto bych Vás chtěl poprosit o vyplnění dotazníku, který slouží jako podklad pro moji Bakalářskou práci, která je zaměřena na počítačovou kriminalitu a hacking.

Dotazník je anonymní, a zabere pouze pár minut.

Předem velmi děkuji za Váš čas.

David Knot

Jaké je vaše pohlaví

a. Muž
b. Žena

Váš věk

a. 10-20 let
b. 21-35 let
c. 36-50 let
d. 50+

Jak často se přihlašujete k internetu?

a. Každý den
b. Alespoň párkrát do týdne
c. Skoro vůbec

Říká vám něco název počítačová kriminalita?

a. Ano
b. Ne

Říká vám něco nějaký z následujících názvů?

a. Kyberprostor
b. Kybernetická bezpečnost
c. Kybernetický útok
d. Žádný z nich

Setkali jste se někdy s počítačovou kriminalitou?

a. Ano
b. Ne
c. Nevím o tom

Říká vám něco oslovení Hacker?

a. Ano
b. Ne
c. Trochu

Říkají Vám něco názvy White-hats hackeři, Black-hats hackeři, Grey-hats hackeři?

a. Ano, vím, o co jde
b. Nevím, o co se jedná
c. Trochu vím

Jaké hrozby vybrané počítačové kriminality znáte?

a. Malware
b. Phishing
c. DoS, DDoS útoky
d. DNS útoky
e. Warez(počítačové pirátství)
f. Žádné z nich

Setkali jste se někdy s nějakou vybranou hrozbou počítačové kriminality?

a. Malware
b. Phishing
c. DoS, DDoS útoky
d. DNS útoky
e. Warez(počítačové pirátství)

f. S žádnou jsem se nesetkal
g. Nevím o tom

Máte na svém počítači nainstalovaný nějaký ochranný antivir?

a. Ano, mám
b. Nemám
c. Nevím o tom

Myslíte si, že víte, jak se máte chovat bezpečně na internetu?

a. Ano, vím
b. Nevím

Dáváte si pozor při vstupu na internet na jaké stránky a reklamy klikáte nebo jaké soubory otevíráte?

a. Dávám si velký pozor
b. Nedávám si pozor, nebojím se
c. Je mi to jedno

Přišel vám někdy do emailové schránky neznámý spam s nějakou výhrou nebo neznámým souborem?

a. Ano, přišel
b. Nepřišel
c. Nevím o tom

Jak velkou hrozbu podle vás počítačová kriminalita představuje?

a. Myslím si, že je více nebezpečná než běžná kriminalita.
b. Myslím si, že není tolik nebezpečná jako běžná kriminalita
c. Nevím

Setkali jste se někdy ve svém zaměstnání, škole, nebo běžném životě se školením nebo upozorňováním na bezpečný pohyb na internetu a o počítačové kriminalitě?

a. Ano
b. Ne

Jak často k tomuto upozorňování dochází?

a. Velmi často
b. Občas
c. Nikdy

Myslíte si, že Policie ČR by se měla zaměřit více na potírání počítačové kriminality?

a. Ano, měla
b. Neměla
c. Nevím

Myslíte si, že by k upozorňování o počítačové kriminalitě mělo docházet častěji?

a. Ano
b. Ne
c. Nevím

Jaké si myslíte, že jsou nejčastější příčiny počítačové kriminality?

a. Z důvodu obohacení se (peněžní zisk, zisk dat, pro pobavení apod.)
b. Dynamické tempo vývoje technologií (stále nové nástroje a příležitosti pro hackery)
c. Hacking za účelem vyjádření vlastního přesvědčení (nesouhlasu atd.)
d. Nedostatečné povědomí lidí o riziku na internetu a počítačové kriminalitě
e. Počítačová kriminalita je více anonymní a hackeři jsou často obtížněji dostižitelní
f. Jiná…

Jaká opatření byste navrhl(a) pro snížení počítačové kriminality?