Univerzita Pardubice

Fakulta ekonomicko-správní

Analýza kyberkriminality v ČR

Bakalářská práce

2024 Lukáš Volenec

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2023/2024

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Lukáš Volenec**
Osobní číslo:	**E21595**
Studijní program:	**B0688A140004 Informatika a systémové inženýrství**
Specializace:	**Informační a bezpečnostní systémy**
Téma práce:	**Analýza kyberkriminality v ČR**
Zadávající katedra:	**Ústav matematiky a kvantitativních metod**

Zásady pro vypracování

Práce bude zaměřena na popis jednotlivých druhů kyberkriminality, doplněných analýzou dostupných statistických dat souvisejících s kyberkriminalitou.
Osnova:
- Kyberkriminalita.
- Druhy kyberkriminality.
- Zúčastněné subjekty.
- Kyberkriminalita a legislativa v ČR.
- Analýza dostupných dat.

Rozsah pracovní zprávy: **35**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.
KOLOUCH, Jan a Petr VOLEVECKÝ. Trestněprávní ochrana před kybernetickou kriminalitou. Praha: Policejní akademie České republiky v Praze, 2013. ISBN 978-80-7251-402-1.
ZAVRŠNIK, Aleš. Kyberkriminalita. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7552-758-5.

Vedoucí bakalářské práce: **Mgr. David Zapletal, Ph.D.**
Ústav matematiky a kvantitativních metod

Datum zadání bakalářské práce: **1. září 2023**
Termín odevzdání bakalářské práce: **30. dubna 2024**

L.S.

prof. Ing. Jan Stejskal, Ph.D. v.r.
děkan

Ing. et Ing. Martin Lněnička, PhD. v.r.
garant studijního programu

V Pardubicích dne 1. září 2023

Prohlášení

Prohlašuji:

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

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

V Pardubicích dne 30.04.2024

Lukáš Volenec v. r.

Poděkování

Rád bych poděkoval panu Mgr. Davidu Zapletalovi, Ph.D. za cenné rady, věcné připomínky a vstřícnost při konzultacích a vypracování bakalářské práce.

ANOTACE

Práce je věnována analýze kyberkriminality v ČR. Přibližuje samotný pojem kyberkriminalita a čím je tento fenomén moderní doby tak specifický. Vysvětluje jednotlivé formy kybernetických útoků a jejich možnou prevenci. Zabývá se také právní úpravou jak národní, tak i mezinárodní a obsahuje analýzu dostupných dat v této oblasti.

KLÍČOVÁ SLOVA

kyberkriminalita, kyberprostor, počítačové systémy, anonymita, hacking

TITLE

Analysis of Cybercrime in the Czech Republic

ANNOTATION

The bachelor thesis is dedicated to the analysis of cybercrime in the Czech Republic. It introduces the concept of cybercrime itself and explains what makes this modern phenomenon so specific. The thesis also explains the individual forms of cyberattacks and their possible prevention. It also deals with the legal framework at both the national and international levels and includes an analysis of available data in this field.

KEY WORDS

Cybercrime, cyberspace, computer systems, anonymity, hacking

Obsah

Seznam ilustrací

Seznam zkratek

CERT	Computer Emergency Response Team (Tým pro řešení počítačových nouzových situací)
CIA	Confidentiality, Integrity a Access (Důvěrnost, Integrita, Přístup)
CVV	Card Verification Value (Hodnota pro ověření karty)
DDoS	Distributed Denial of Service (Distribuované odepření služby)
DNS	Domaine Name Systém (Systém názvů domén)
DoS	Denial of Service (Odepření služby)
IP	Internet Protocol (Internetový protokol)
LAN	Local Area Network (Lokální síť)
NCKB	Národní centrum kybernetické bezpečnosti
NCTEKK	Národní centrála proti terorismu, extremismu a kybernetické kriminalitě
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PIN	Personal Identification Number (Osobní identifikační číslo)
SKPV	Služba kriminální policie a vyšetřování
VPN	Virtual Private Network (Virtuální privátní síť)
WAN	Wide Area Network (Rozsáhlá síť)

Úvod

V moderní době, digitální éře, ve které nyní žijeme, se kybernetická bezpečnost stala jedním z nejdůležitějších a nejaktuálnějších témat, jak v rámci informačních technologií, tak i ve společnosti jako celku. Riziko kybernetických hrozeb se s rostoucí závislostí na internetu a nových technologiích zvyšuje každým dnem. Tyto hrozby a útoky mají potenciál způsobit značné škody nejen jednotlivcům, ale i organizacím či jednotlivým národům. V této souvislosti je pro všechny jedince užívající digitální platformy důležité rozumět trendům, charakteristikám a dopadům kyberkriminality. I přes technologickou vyspělost zemí světa, je kybernetická kriminalita velkým rizikem.

Cílem této bakalářské práce je prozkoumat a analyzovat fenomén kybernetických hrozeb v České republice, která se řadí mezi technologicky vyspělé státy. Jde také o přispění k diskuzi o možných opatřeních, která by mohla vést k efektivnější prevenci, detekci a potírání kybernetických zločinů v digitálním prostoru.

První část práce se zaměřuje na definici a specifika kyberkriminality. Jsou zde vymezeny základní pojmy důležité k porozumění této problematiky. Zároveň je zdůrazněn význam technologického rozvoje a digitalizace společnosti při formování nových forem kybernetické kriminality. Druhá část práce je věnována jednotlivým druhům kyberkriminality. Vysvětluje různé formy kybernetických zločinů, jako je šíření obsahu, porušování práv duševního vlastnictví anebo klasická kriminalita v kyberprostoru. Diskutováno je o jejich charakteristikách, způsobech provádění, dopadech na oběti a také o prevenci.

Další část práce se zaměřuje na zúčastněné subjekty v oblasti kyberkriminality. Identifikováni jsou zde pachatelé, jež nejsou pouze jednotlivci, ale také skupiny, často až organizované zločinecké sítě a jejich motivace k páchání zločinů. Rovněž je diskutováno o obětech kyberkriminality, včetně jednotlivců, firem a veřejných institucí. Vymezena je zde také národní a mezinárodní právní úprava související s kyberkriminalitou. Je analyzován stávající právní rámec a legislativní opatření, která byla přijata k prevenci kybernetických zločinů. Diskutovány jsou také případné nedostatky. V poslední části práce jsou analyzována dostupná data o kyberkriminalitě v České republice. Tato analýza pak poskytuje pohled na aktuální situaci a vývojové tendence kybernetické kriminality v ČR.

1 Kyberkriminalita

Kriminalita jako taková nás provází již od samotného vzniku lidstva a je nedílnou součástí našich životů. S rozvojem doby se její druhy mění a rozrůstají, a právě vývoj digitálních technologií, které mají obrovské množství uplatnění a bez kterých si již dnešní žití nelze představit, zapříčinil vznik kyberkriminality. Kybernetická kriminalita představuje fenomén moderních časů, který se odehrává v kyberprostoru prostřednictvím internetu, počítačových sítí, mobilních telefonů, a dalších informačních a komunikačních technologií.

1.1 Základní pojmy

Před jakýmkoli zkoumáním nebo analýzou kybernetické kriminality je pro orientaci v této oblasti velmi důležité vymezení klíčových pojmů.

1.1.1 Kyberprostor

Termín „cyberspace“, v překladu tedy kyberprostor, byl použit poprvé v roce 1984 Williamem Gibsonem, který jej definoval spíše literárně a vizionářsky. Pro náš případ a dnešní dobu je ale důležité jeho klasické vymezení. Fyzický svět je svými pravidly či omezeními zcela odlišný od světa kybernetického. Rozhodně nelze předpokládat, že zde platí všechny stejné legislativní úpravy jako ve skutečném světě. Je to nekonečné digitální prostředí, které není omezeno žádnými hranicemi, ale je závislé na moderních technologiích existujících v realitě. Uživatelé tuto globální a všem jedincům dostupnou virtuální realitu mohou nějakým způsobem ovlivňovat. V posledních letech už je na kyberprostor nahlíženo jako na další oblast, a to nejen z hlediska válečných operací, kterou státy a organizace stále více upřednostňují a věnují jí zvýšenou pozornost (Kolouch a Bašta, 2019, s. 36).

1.1.2 Kybernetický útok

Kybernetický útok je snaha o neautorizovaný vstup a poškození počítače, systému, sítě nebo jiné technologie s cílem způsobit škodu. Velmi často jde o různé podvody či vydírání, kdy útočníci požadují výkupné, obvykle v kryptoměně, aby zůstali neidentifikovatelní. Může se jednat i o politicky motivované útoky mezi státy nebo terorismus v kyberprostoru ze strany nestátních subjektů a teroristů. Útoky mohou být realizovány jednotlivci, známými jako hackeři, ale i organizovanými skupinami. Útočníci mohou způsobit různé škody, od deaktivace počítačů, krádeže nebo zničení dat, až po ovládnutí celé infrastruktury nebo zneužití prolomených systémů k dalším útokům. Poslední dobou představuje útok v digitálním prostředí veliké riziko nejen pro jednotlivce, ale i pro bezpečnost celého národa (Legislativa, 2022).

1.1.3 Kybernetická bezpečnost

Kybernetická bezpečnost, též nazývaná digitální ochrana, se zabývá tím, jak ochraňujeme naše digitální informace, zařízení a majetek. U tohoto pojmu je často používána zkratka CIA, která v sobě nese tři slova – Confidentiality, Integrity, Access. Confidentiality neboli důvěrnost znamená udržení tajemství a zajištění přístupu k důvěrným datům pouze autorizovaným subjektům. Integrita symbolizuje platnost našich informací – musíme zajistit, aby je nikdo bez našeho vědomí neměnil a neobsahovaly škodlivé nebo špatné informace. A v neposlední řadě access, tedy přístup, který k naším systémům musíme vždy mít. Důležité je si uvědomit, že zabezpečení je proces, a ne pouhý produkt. Dle světoznámé firmy Microsoft je důležité dodržovat zavedené a správně promyšlené procesy, mezi které patří:

a) Zálohování dat – důležité informace by měly být uchovávány na bezpečném úložišti a měla by existovat spolehlivá, ověřená kopie těchto dat pro případ, že by došlo k poškození nebo ztrátě souboru.

b) Bezpečné chování online – nedůvěryhodné odkazy či přílohy v e-mailech či zprávách by se neměly otevírat, i když působí jako zpráva od známého zdroje.

c) Pravidelná aktualizace softwaru – operační systémy jako Windows, MacOS, iOS nebo Android, stejně jako aplikace a prohlížeče, by měly být pravidelně aktualizovány s nejnovějšími opravami a aktualizacemi od výrobce.

e) Silná a unikátní hesla – bezpečná hesla by měla být dlouhá minimálně 14 znaků, neměla by obsahovat slova z běžného slovníku a neměla by být používána opakovaně na více účtech.

f) Využívání vícefaktorového ověřování – kdekoliv je to možné, by mělo být aktivováno vícefaktorové ověřování, což zvýší bezpečnost účtů (Microsoft, 2021).

1.1.4 Počítač

Pojem počítač je důležité vymezit, i když se definice může zdát jednoduchá, z důvodu trestního zákoníku, kde je používán a jeho vymezení zpravidla není jednoznačné. Jednoduše lze říci, že je to výpočetní jednotka skládající se z hardwarových a softwarových komponent. Často je ale interpretován jako počítačový systém, který je složen z minimálně jednoho počítače a přidruženého softwaru. Dle Úmluvy o počítačové kriminalitě (Zákony pro lidi, 2019) je možné tento systém definovat jako jakýkoli přístroj či skupinu spolupracujících přístrojů, ze kterých alespoň jeden automaticky zpracovává data.

1.1.5 Hardware

Jednoduchá definice hardwaru jako „opak softwaru“, nebo „vše na co si můžeme sáhnout“ používá asi každý laik, ačkoli to takhle jednoduše nelze říci. Slovo hardware lze do češtiny přeložit jako technické vybavení a vyjadřuje souhrn hmotných technických prostředků umožňujících a zároveň rozšiřujících provoz počítačového systému. Řadíme zde veškeré fyzické zařízení, které je nezbytné pro fungování počítačového systému. Jedná se například o procesor, grafickou kartu, základní desku a ostatní vnitřní výbavu nebo na druhou stranu o vnější výbavu, tedy klávesnice, myš, obrazovka a další (Kolouch, 2016, s. 59).

1.1.6 Software

Software, také označovaný jako počítačový program, je souhrnný pojem pro veškerou programovou výbavu PC. Také ho lze označit za spojovací mezičlánek mezi fyzickou výbavou počítače a uživatelem. Veškeré programy jsou uloženy na zvoleném datovém médiu (harddisk, CD, DVD, …) a zároveň jsou jednoduše přenositelné díky různým paměťovým kartám. Software se zpravidla v kontextu jeho užitku dělí na:

a) Aplikační, který jak už název říká představuje veškeré aplikace, jako jsou například hry, prohlížeč nebo antiviry.

b) Systémový, což je operační systém. Pro počítače například Windows nebo Linux, pro mobilní zařízení Android, iOS a další.

Potřeba je uvést také povinnost uživatelů, kteří musí za legitimní licenci k danému softwaru (pokud není nabízen zdarma) zaplatit. Počítačové programy jsou totiž považovány za autorské dílo (Správa sítě, 2022).

1.1.7 Data

V oblasti počítačových systémů se termín data tradičně používá k označení čísel, textu, zvukových záznamů, a dalších smyslových vjemů, které jsou vhodné pro zpracování počítačem. Digitální technologie reprezentují data pomocí binárního kódování, kde jsou převedeny na sérii binárních číslic, známých jako bity. Pro praktické použití se obvykle osm bitů spojuje do jednoho bajtu. Formát dat je standardizován, aby umožnil kompatibilitu mezi počítači a programy různých výrobců. Data slouží k zachycení faktů, atributů a událostí a jsou vyjádřením reality v podobě, která umožňuje jejich uchování, zpracování a přenos, se záměrem vytvoření informací. Data jsou tradičně ukládána na nosičích informací, což je pojem velmi důležitý vzhledem k § 230 a § 232 trestního zákoníku (Smejkal, 2018, s. 35-36).

1.1.8 Informace

Informace je definována jako jakákoli sdělitelná poznámka, která získává na hodnotě kontextem. Kontext data transformuje na informaci, která je srozumitelná a použitelná. Hodnota informace je subjektivní, jelikož závisí na procesu transformace dat a jejich užitečnosti pro daného uživatele. Cena dat a hodnota informace nejsou přímo propojeny. Data slouží jako nositelé potenciální hodnoty a můžou být předmětem obchodu. Nicméně, skutečná hodnota dat se projeví až při jejich konkrétním využití. V tomto momentě se zhodnotí jejich přesnost, kompletnost a aktuálnost. Data sama o sobě nepředstavují hodnotu pro příjemce, dokud nejsou úspěšně využita jako informace. Teprve v tomto momentě se stávají užitečnými a relevantními (Sklenák, 2001, s. 2).

1.1.9 Počítačová síť

Počítačová síť je systém propojených počítačů, které sdílí informace a zdroje. Můžeme ji definovat jako souhrn technologií a programového vybavení, které umožňuje tuto komunikaci. Základní rozdělení počítačových sítí je na lokální sítě LAN, které se nacházejí v omezené geografické oblasti, například v budově nebo v kanceláři. Mají kratší vzdálenosti mezi uzly a obvykle vyšší přenosovou rychlost. Jejich časté využití je v domácnostech nebo institucích a umožňují sdílení například tiskáren nebo připojení k internetu. Vzdálené sítě WAN propojují geograficky vzdálené oblasti. Používají se pro komunikaci na velké vzdálenosti a často používají technologie VPN pro zajištění bezpečnosti. Nejznámějším příkladem této sítě je všemi používaný internet (Smejkal, 2018, s. 49-51).

1.1.10 Internet

Internet je rozsáhlá síť propojených počítačů, která umožňuje sdílení informací a komunikaci mezi uživateli z celého světa. Představuje unikátní lidský projekt, který v minulém století radikálně změnil způsob elektronické komunikace. Internet můžeme přirovnat k pavučině, kde vlákna symbolizují spojení a uzly představují jednotlivé uživatele. Tato síť propojuje miliony počítačů a umožňuje jim vzájemně komunikovat a sdílet data. Počítače v kyberprostoru fungují jako servery, které poskytují internetové služby klientům. Tyto servery zajišťují bezproblémový tok informací a dat na základě požadavků klientů (Správa sítě, 2022).

1.2 Pojem kyberkriminalita a jeho definice

Pojem kyberkriminalita, dříve často označována jako informační kriminalita, se skládá ze dvou slov. Kyber, z anglického slova cyber, je předpona, která je spojována s informačními technologiemi, či elektronickou komunikací a kriminalita, latinsky zločin, tedy označuje trestné

nebo zločinné chování. Jednoduše lze tedy říci, že je kyberkriminalita jakákoli trestná činnost páchána prostřednictvím informačních a komunikačních technologií, která obsahuje velké množství nelegálních aktivit. Může zahrnovat například podvody, které jsou v digitálním světě páchány nejčastěji. Bezpečnostní orgány také hojně registrují krádeže, šíření škodlivého softwaru, nepovolený přístup k soukromým informacím, porušení autorských práv nebo také šíření dětské pornografie. (Kolouch, 2016, s. 31)

Odborně je kybernetická kriminalita specializovaným typem trestné činnosti, ve které hraje klíčovou roli počítač či počítačový systém, včetně jeho veškerého vybavení. Tento počítač může být buď hlavním cílem trestného jednání či nástrojem použitým k páchání trestné činnosti (Smejka a kol., 1995, s. 99). Tato definice má ale určité nedostatky a nepřesnosti, i přes snahu vymezit aspekty zločinů tohoto druhu. Je důležité nejprve definovat pojem kriminalita, který je chápán jako soubor činností, které lze zařadit pod skutkovou podstatu trestných činů dle trestního zákona. Kybernetické zločiny jsou však specifické tím, že je obtížné je klasifikovat jako trestné činy, jelikož využívají speciální techniky a postupy. Tyto postupy jsou ale předpokladem pro další jednání, které již obsahuje náplň trestního práva. Skoro každý trestný čin ale lze spáchat pomocí nebo prostřednictvím moderních technologií. Například ublížení na zdraví úderem notebooku do hlavy, přimění jiné osoby prostřednictvím elektronické komunikace ke spáchání zločinu anebo jeho schvalování či podněcování nelze považovat za kybernetickou kriminalitu (Kolouch, 2016, s. 34-36). „*V tomto duchu pak bude možno pod pojmem kybernetická kriminalita zařadit trestné činy tří různých kategorií:*

a) trestné činy, jejichž individuálním objektem charakterizujícím skutkovou podstatu je přímo ochrana počítačového systému, jeho vybavení a součástí před specifickými druhy útoku, resp. oprávněné zájmy osob na nerušené užívání těchto specifických prostředků,

b) trestné činy, kde je způsob spáchání prostřednictvím informační a komunikační techniky jedním ze znaků skutkové podstaty,

c) ostatní v úvahu připadající trestné činy, které nespadají do první ani druhé kategorie, avšak mohou být v konkrétním případě též spáchány prostřednictvím informačních technologií.“ (Kolouch, 2016, s. 37).

1.3 Specifika kyberkriminality

Klasická kriminalita a kyberkriminalita, která je svým charakterem velmi specifická, se liší v mnoha ohledech. Mezi důležité specifikum patří určitě její dostupnost. Rozvoj moderních technologií způsobil potřebu vlastnictví chytrých zařízení, jako jsou počítače, smartphony a další. Pachatelé zločinů si vystačí pouze s potřebnými znalostmi, základní výbavou a připojením k internetu, což je dnes na každém rohu. Mezi nejzásadnější aspekty kyberkriminality pak patří také vysoká latence kyberzločinců, globálnost, anonymita a s ní spojené digitální stopy.

1.3.1 Latence

Kyberkriminalita je jedním z nejutajovanějších typů trestné činnosti, často kvůli nízké pravděpodobnosti odhalení, neochotě obětí tuto aktivitu nahlásit a špatnému zabezpečení. Podle některých studií zůstává až 90 % kyberkriminality skryto. Obecné důvody, jako je obava ztráty důvěry nebo obava z odhalení vlastních nezákonných aktivit, jsou typické pro většinu trestné činnosti, ale v případě kyberkriminality jsou tyto obavy zvláště silné, protože v dnešní době je například nelegální stažení filmu opravdu častá věc. Organizace se obávají ztráty důvěry svých zákazníků, pracovníků nebo akcionářů, což by mohlo způsobit větší škody než samotný kyberútok. Dalším důvodem je strach z přitahování dalšího útoku tím, že by se staly známé jako oběti se slabým zabezpečením. Navíc technická povaha kyberútoků často znamená, že bez specializovaných nástrojů k detekci je těžké je odhalit. Tyto útoky jsou často prováděny na dálku a stopa, kterou pachatelé zanechávají, je obtížně identifikovatelná a vyhodnotitelná (Jelínek, 2021, s. 482-483).

1.3.2 Globálnost

Globální povaha kybernetické kriminality umožňuje pachatelům útočit na oběti prakticky kdekoliv na světě bez nutnosti fyzického kontaktu. To rovněž komplikuje odhalování a stíhání kyberkriminality, jelikož útoky mohou být provedeny daleko přes státní hranice. Většina kybernetické kriminality je sice spojená s internetem, ale i jiné typy sítí, jako jsou privátní firemní sítě nebo sítě řídící průmyslové procesy, mohou být vystaveny riziku. Kyberprostor je otevřený systém bez centrálního řídícího orgánu, přičemž většina činností se odehrává přes několik serverů, což komplikuje určení místa uložení dat a trasování přenosu dat. To často komplikuje postih kyberkriminality prostřednictvím tradičních právních systémů, které jsou založeny na státní suverenitě (Gřivna a kol., 2019, s. 390).

1.3.3 Anonymita

Anonymita v kontextu kyberkriminality představuje schopnost jednotlivců nebo skupin skrýt svou identitu a působit v online prostředí beze stop. Tento aspekt je klíčovým prvkem kyberkriminality a představuje značnou výzvu pro vyšetřovatele a zákonné orgány, kteří se snaží identifikovat a potrestat pachatele. Tento aspekt umožňuje kyberkriminálníkům působit bez obav z odhalení a postihu, což výrazně zvyšuje riziko a škody spojené s jejich činností. To umožňují různé technické nástroje a metody, jako jsou anonymní proxy servery, virtuální privátní sítě (např. VPN), síťové maskování a šifrování dat. Tyto prostředky umožňují kyberkriminálníkům skrýt svou IP adresu a geografickou polohu, což znesnadňuje identifikaci jejich skutečné totožnosti. Kromě toho existují také kryptoměny, které bývají využity k utajení komunikace a transakcí mezi pachatelem a oběťmi. Identifikace a stíhání pachatelů vyžaduje spolupráci mezi různými zeměmi a organizacemi, včetně mezinárodních policejních a bezpečnostních agentur, aby bylo možné překonat překážky spojené s anonymitou a dosáhnout spravedlnosti (Holt a kol., 2015, s. 371-373).

S pojmem anonymita blízce souvisejí také digitální stopy. Všechny softwary totiž získávají veliké množství informací o svých uživatelích, většinou z důvodu modifikace nabízeného softwaru anebo systém poskytují bez poplatků. Informace jsou to především osobní, jako je naše jméno, místo bydliště a kontakt. Dále se jedná o informace citlivé, např. soubory cookies (které lze odmítnout) a lokalizační, jako jsou například naše souřadnice.

Jak už bylo řečeno, některé digitální stopy lze ovlivnit a z toho důvodu se dělí na ovlivnitelné a neovlivnitelné. Ovlivnitelné digitální stopy jsou vytvářeny vědomým využíváním služeb a dobrovolným zveřejněním informací uživateli. To může zahrnovat aktivní používání e-mailu, blogů nebo sociálních sítí, kde uživatelé sdílejí osobní informace, fotografie, příspěvky a další obsah. Neovlivnitelné digitální stopy jsou záznamy vytvářené automaticky v důsledku používání počítačových systémů, jejich připojení k internetu a dalším počítačovým sítím, a také při využívání různých online služeb. Tyto stopy jsou generovány bez přímého zásahu nebo vědomí uživatele a reflektují různé aspekty používání technologie. Patří sem informace, které jsou získávány operačním systémem, a to bez zásahu člověka. Samozřejmě ale nelze říct, že jsou tyto stopy zcela neovlivnitelné, protože existují zkušení uživatelé, kteří si s tím částečně ví rady (Kolouch, 2016, s. 134-145).

2 Druhy kyberkriminality

V digitální době, kdy se naše závislost na moderních technologiích neustále zvyšuje, se kyberkriminalita stává jedním z klíčových bezpečnostních problémů. V této kapitole se tedy zaměříme na její jednotlivé formy, které představují hrozbu pro jednotlivce, podniky i státní instituce po celém světě.

2.1 Kyberkriminalita spojená s integritou informačního systému a dat

Trestněprávní ochrana se vztahuje na počítačové systémy a data, která jsou uložena v těchto systémech nebo k nim mají přístup. Cílem je chránit integritu těchto dat, což zahrnuje ochranu před nepovoleným přístupem, zachování důvěrnosti a zajištění komplexnosti. Tato ochrana brání v přenosu, poškození, vymazání, zhoršení kvality, úpravách nebo blokování počítačových dat a informačních systémů. Zločiny pachatelé typicky provádějí pomocí škodlivých počítačových programů, kterými se mimo jiné v této části práce budeme zabývat (Završnik, 2017, s. 16-18).

2.1.1 Sociotechnika

Sociotechnika, také známá jako sociální inženýrství, i když přímo není považována za kybernetický zločin, často slouží jako základ pro úspěch v již digitálních trestných činech. Tento termín popisuje proces, kdy jsou lidé ovlivňováni, přesvědčováni nebo manipulováni s cílem donutit je vykonat určité akce nebo získat důležité informace, které jsou pro veřejnost utajené. Jeho záměrem je vytvořit dojem, že situace, ve které se oběť nachází, je jiná, než se ve skutečnosti zdá. Jednoduše řečeno, sociální inženýrství můžeme chápat jako "umění klamu". Jelikož každý počítačový systém je závislý na uživateli, stává se tedy nejslabší vrstvou bezpečnostního systému právě člověk, na kterého nemusíme používat žádné technické přístroje čí přístupy (Kolouch, 2016, s. 186-187).

2.1.2 Hacking

Hacker je označení pro jedince, který má hluboké znalosti o fungování počítačových, a s tím souvisejících operačních systémů a dalších softwarů, včetně principů a mechanismů sítí. Tito jedinci jsou také vynikajícími programátory, kteří jsou schopní vlastní program bleskově vytvořit. Jejich motivací je pochopení fungování informačních technologií a sdílení těchto znalostí s ostatními uživateli. Schopnost hackerů získávat přístup do počítačových systémů pomocí vlastních programů je jedním z mnoha dovedností, přičemž tento přístup nemusí nutně zahrnovat škodlivé úmysly nebo záměr obohacení se. Právě tito hackeři, označovaní jako

skupina White Hats, své schopnosti využívají pro odhalení bezpečnostních nedostatků a k vytvoření schopnějších obranných mechanismů. Druhá skupina Black Hats je pravým opakem. Jejich cílem je napáchat škodu nebo jinou formu újmy a zároveň vlastní majetkový zisk. Tyto nekalé činnosti jsou často spojovány s pojmem cracking (Kolouch, 2016, s. 272-276).

2.1.3 Malware

Malware, což je zkratka pro škodlivý software, je termín označující jakýkoliv software používaný k narušení normálního fungování počítačového systému. Existuje mnoho druhů malwaru, které jsou často pojmenovány podle svých funkcí, které plní. V další části práce si přiblížíme ty nejběžnější, jako je například spyware či počítačový virus (Kolouch, 2016, s. 204-205).

Spyware, vzniklý spojením termínu pro špionáž a software, je typ programu, který může bez vědomí uživatele neoprávněně sledovat a shromažďovat data o aktivitě na počítačovém systému. Získané informace jsou pak předávány pachateli. Spyware se může na počítač dostat samostatně jako škodlivý program, ale často je skrytý v rámci zdánlivě neškodných aplikací, kde oběť potvrdí licenční podmínky bez jakéhokoli přečtení (Kolouch, 2016, s. 207).

Dalším typem malwaru je počítačový virus, což je škodlivý program, který se šíří automaticky bez vědomí uživatele tím, že se kopíruje do jiného spustitelného programu nebo dokumentu. Pokud zapneme software obsahující virus, škodlivý kód skrytý ve zdrojovém kódu nenápadně převezme kontrolu nad počítačem. Virus poté na pozadí provádí škodlivé činnosti a když je hotovo, předá kontrolu zpět původnímu programu. Uživatel si často ani nevšimne, že se něco stalo. Zjištění viru na počítači může být velmi obtížné. Jednou z nejčastějších metod, jak se viry šíří, je prostřednictvím e-mailových příloh. Otevřením a spuštěním nakaženého souboru z e-mailu může virus vniknout do systému a dále se rozšiřovat (Eset, 2020).

Počítačový červ je typ škodlivého softwaru, který obsahuje kód navržený k napadání ostatních počítačů a šíří se dále skrze síťové připojení. Na rozdíl od virů se červi mohou šířit samostatně a primárně využívají elektronickou komunikaci nebo zranitelnosti v síťových aplikacích k rozšiřování. Červi jsou považováni za zvláště nebezpečné, jelikož se mohou rychle šířit po celém světě díky všudypřítomnosti internetu. Po aktivaci může červ způsobit různé škody, včetně mazání souborů, zpomalení systému nebo deaktivaci softwaru, a často slouží k distribuci dalšího škodlivého softwaru. (Eset, 2023).

Trojský kůň je typ softwaru, který obsahuje oběti neznámé funkce, které mohou poškodit systém. Trojské koně se nešíří samostatně a vyžadují k aktivaci uživatelskou interakci. Útočníci

používají trojské koně pro stejné účely jako viry nebo červy, což zahrnuje narušení nebo modifikaci běhu počítačových systémů, jejich zablokování a další (Kolouch, 2016, s. 208-209).

Keylogger je škodlivý software určený k tajnému zaznamenávání stisknutých kláves na počítači, tabletu nebo chytrém telefonu. Tento nebezpečný nástroj představuje vážné hrozby pro osobní bezpečnost a soukromí. Keyloggery mohou existovat jak softwarové, tak i hardwarové. Softwarové jsou nejčastěji distribuovány prostřednictvím zavirovaných souborů, webů nebo elektronické pošty. Jakmile jsou aktivovány, tajně začnou zaznamenávat všechny stisknuté klávesy na klávesnici. Tyto záznamy mohou obsahovat veškeré citlivé a osobní údaje. Hardwarové keyloggery fungují na podobném principu jako softwarové, rozdílné je ale jejich zapojení mezi klávesnicí a počítačem (Software, 2019).

Ransomware je typ škodlivého softwaru, který hrozí uživatelům zničením nebo zablokováním jejich důležitých dat nebo systémů, pokud nezaplatí požadované výkupné. Dříve se ransomware často zaměřoval na jednotlivce, avšak v současné době se objevuje sofistikovanější forma, která je řízena lidmi a míří na organizace. V těchto případech skupina útočníků využívá své schopnosti k získání přístupu do firemních sítí a stanovuje cenu výkupného na základě finančních informací firmy, které se jim podařilo získat. Tento typ ransomwaru představuje závažnější a obtížněji řešitelnou hrozbu pro podniky. (Kolouch, 2016, s. 221-223).

Rootkit je typ softwaru nebo soubor technologií navržený tak, aby se skryl v počítačovém systému a zamaskoval tak přítomnost škodlivých programů. Hlavním cílem rootkitu je získat kontrolu nad počítačem na úrovni administrátora, aniž by o tom uživatel věděl. Existuje několik způsobů, jak může být rootkit nainstalován, často je například maskován jako součást bezpečnostního softwaru nebo jde o zdánlivě neškodná rozšíření aplikací od třetích stran. Ačkoli rootkity nejsou schopné se samostatně šířit z jednoho počítače na druhý, jejich přítomnost v systému představuje seriózní bezpečnostní riziko, protože mohou sloužit jako platforma pro další útoky nebo narušení systému. Antivirové programy totiž mají často problém s detekcí a odstraněním rootkitů, což umožňuje škodlivému softwaru zůstat v systému delší dobu (Kolouch, 2016, s. 209).

2.2 Kyberkriminalita spojena se šířením obsahu

Za kybernetickou kriminalitu nejsou považovány pouze hackerské útoky. Týká se také šíření sexuálního obsahu – především tedy dětské pornografie. Dále mezi ní řadíme i šíření

násilného obsahu nebo obsahu, který porušuje právo duševního vlastnictví. To lze nazývat jako počítačové pirátství (Završnik, 2017, s. 19-20).

2.2.1 Kyberkriminalita spojená se sexuálním obsahem

Do této formy kybernetického zločinu se řadí tzv. extrémní pornografie. To je druh pornografického obsahu, který je velmi urážlivý, odporný nebo jinak obscénní. Obsahuje explicitní a realistické záběry činů, které ohrožují lidský život, nebo mohou vést k vážným zraněním pohlavních orgánů. Tento druh obsahu může zahrnovat i pohlavní aktivity s mrtvými těly nebo zvířaty. K považování tohoto materiálu za pornografický, musí být hlavním účelem vyvolávání sexuálního vzrušení (Završnik, 2017, s. 22-23).

Dětská pornografie šířená nebo dostupná na internetu se obecně dělí na dva typy. Reálná dětská pornografie, což je explicitní záznam skutečného zneužití dítěte, který jasně dokazuje spáchaný trestný čin. Naopak dětská kyberpornografie nezahrnuje skutečné děti, ale počítačově vytvořené obrázky nebo simulace (Završnik, 2017, s. 23). Dle Lanzarotské úmluvy (Zákony pro lidi, 2010) lze dětskou pornografii definovat jako „*široký okruh trestných činů: 1) pohlavní zneužití; 2) trestné činy související s dětskou prostitucí (trestnost protagonistů a objednatelů); 3) trestné činy související s dětskou pornografií (výroba, nabízení, distribuce, držení a prohlížení na webu); 4) trestné činy týkající se účasti dítěte na pornografických představeních; 5) navádění dětí k nemorálním činům (s pasivní přítomností, která není účast); 6) přemlouvání dětí k sexuální činnosti.*“.

2.2.2 Kyberkriminalita spojená s násilným obsahem

Šíření násilného obsahu na internetu se nejčastěji projevuje formou kyberšikany, kyberterorismu anebo nenávistným projevem. Kyberšikana převádí klasické formy šikany do online prostředí, kde může útočník využívat digitální nástroje a technologie, které mají mnohem větší vliv na šikanovaného jedince než běžná šikana. Při využití moderních technologií a možnosti trvalého ukládání dat může docházet k šikanování bez ohledu na fyzickou vzdálenost mezi útočníkem a obětí. Kyberšikana často souvisí i s tradiční šikanou, například tím, že se zaznamenávají fyzické útoky, které jsou poté šířeny online. (Kolouch, 2016, s. 309-310).

Označení kyberterorismus můžeme použít v takovém případě útoku, kde je cílem nebo prostředkem informační či komunikační systém. Pří teroristickém útoku v digitálním prostoru je záměrem útočníků zastrašení obyvatelstva, nucení vlády nebo mezinárodních organizací k určitému jednání anebo destabilizace politických, ústavních, hospodářských a dalších struktur země či mezinárodní organizace. Jednoduše lze kyberterorismus definovat jako používání

počítačových nástrojů k vyřazení důležitých národních infrastruktur, jako jsou energetické systémy a doprava, nebo k přinucení či vystrašení civilistů a vlády. Často bývá označován také jako forma psychologické války (Smejkal, 2018, s. 114-116).

Vznik globálních komunikačních sítí umožnil efektivní prostředek pro šíření rasismu, xenofobie a dalších diskriminačních myšlenek. To je označováno jako nenávistný projev a jedná se především o veřejné urážení skrze počítačové systémy, založené na rasistických a xenofobních motivech, šíření materiálu s těmito motivy anebo popírání, zlehčování či ospravedlňování trestných činů proti lidskosti (Završnik, 2017, s. 29-30).

2.2.3 Kyberkriminalita spojená s porušováním práv duševního vlastnictví

Krádež autorského díla je samozřejmě také považována za kybernetický zločin. Autorské právo vzniká automaticky v okamžiku, kdy je dílo vyjádřeno ve vnímatelné formě. Tímto dílem se rozumí jakékoliv originální písemné, umělecké či odborné výtvory, které mohou být zaznamenány v jakékoliv formě, kterou lze smyslově vnímat, včetně formy elektronické. To zahrnuje i počítačové programy, pokud jsou původním intelektuálním dílem autora. Dále existují také práva průmyslová, která na rozdíl od práv autorských, chrání různé patenty, průmyslové modely, ochranné známky apod. Počítačoví či internetoví piráti jsou právě ti lidé, kteří práva duševního vlastnictví porušují (Kolouch, 2016, s. 277-281).

2.3 Ostatní formy kyberkriminality

Nejrozšířenější formou kyberkriminality jsou různé podvody a klamavá jednání – tedy majetková forma kriminality páchána v digitálním světě. Často se setkáváme s krádeží identity a následného přístupu např. do internetového bankovnictví. Tyto podvody zločinci páchají prostřednictvím mnoha metod, mezi nejznámější paří phishing, vishing nebo pharming.

2.3.1 Phishing

Pojem phishing vznikl od slova fishing – tedy rybaření a jeho průběh je aktivitě rybáře velmi podobný. Útočníci cílí na krádež peněz nebo identity tím, že vás přimějí poskytnout osobní informace, jako můžou být čísla kreditních karet, bankovní údaje nebo hesla prostřednictvím webových stránek, které se tváří jako reálné. Kybernetičtí podvodníci často fingují, že jsou důvěryhodné společnosti, přátelé nebo známí prostřednictvím falešných zpráv, které obsahují odkaz na podvrženou webovou stránku. Tyto e-maily většinou navádějí k okamžité akci nebo něčím hrozí, odkazy na web jsou podezřelé a text zprávy většinou není úplně gramaticky korektní. Důvěryhodné společnosti, jejichž služby využíváme, v e-mailech

většinou oslovují naším jménem – to není případ u phishingových podvodníků. To však ale není jedinou hrozbou, protože phishing má mnoho dalších forem (Microsoft, 2020).

Jednou z nich je spear phishing, který je phishingu zároveň velmi podobný, ovšem s jedním významným rozdílem. Je totiž precizně zaměřen na konkrétní cíl, na rozdíl od phishingu, který je obecnějšího formátu. Útok je zacílen přímo na konkrétní skupinku, organizaci nebo jednotlivce (většinou v organizaci) s cílem získat specifické informace a data, která jsou v této organizaci obsažena. Zločinci se často dozvídají osobní a finanční údaje, různé důvěrné informace anebo obchodní strategie (Kolouch, 2016, s. 264).

Pharming je oproti phishingu zákeřnější a hůře rozeznatelný. Jeho princip spočívá v napadení DNS a následném změnění IP adresy. Když se uživatel pokusí přihlásit do svého bankovního účtu pomocí legitimní webové stránky banky, je okamžitě přesměrován na stránku falešnou, která na první pohled může vypadat jako pravá a na kterou je zvyklý. Následným vyplněním přihlašovacích údajů získá útočník všechny potřebné informace a útok je úspěšný (Správá sítě, 2022).

Další formy phishingu jsou sice prováděny výhradně prostřednictvím mobilních telefonů, avšak za zmínku také stojí. Smishing pro rozeslání zpráv zpravidla využívá SMS a hlavním cílem útočníků je přimět uživatele k provedení určité platby nebo ke kliknutí na zavádějící odkazy. Vishing je forma podvodu, která je prováděna pomocí telefonních hovorů. Pachatel při tom obvykle vystupuje pod jinou identitou a snaží se působit jako důvěryhodná osoba nebo zástupce renomované organizace, jako je banka nebo její technická podpora. Cílem je vzbudit důvěru oběti a přimět ji k poskytnutí osobních nebo finančních údajů. Tato metoda je založena na výše zmíněném sociálním inženýrství (Kolouch, 2016, s. 265-266).

2.3.2 Podvodné weby

Na internetu existuje mnoho webových stránek, které lákají uživatele slibem krásných výher nebo nabídkou produktů za nízké ceny. Kybernetičtí zločinci využívají metod sociotechniky a spoléhají se především na naivitu a nedbalost lidí. Jejich činnost může mít obvykle dva hlavní cíle. Pachatel se může snažit získat osobní údaje obvykle pod záminkou registrace či vyplacení fiktivní výhry. Tyto poskytnuté údaje umožňují útočníkovi získat informace, které mohou být následně zneužity pro různé podvody. Mnohem četnější jsou ale finanční podvody, kdy jsou lidé požádání o platbu za zboží, které nikdy nepřijde. Často jsou na těchto webových stránkách za velmi atraktivní ceny nabízeny dopravní prostředky, elektronika a další různé produkty (Kolouch, 2016, s. 266-267).

2.3.3 DoS a DDoS

Pojmy DoS (Denial of Service) a DDoS (Distributed Denial of Service) označují typy kybernetických útoků, jejichž cílem není krádež dat nebo průnik přes bezpečnostní systémy. Oba typy útoků jsou navrženy tak, aby znemožnily běžné využívání webových stránek, služeb nebo infrastruktury, a tím způsobily škody cílové organizaci. Při těchto útocích dochází k přetížení serveru velkým množstvím požadavků, což způsobí, že server nemůže efektivně pracovat a na určitou dobu nedokáže poskytovat své služby. Tyto útoky jsou často prováděny s využitím sítě infikovaných počítačů, označovaných jako Botnet, které zároveň generují obrovský objem požadavků na cílový server (Kolouch a Volevecký, 2013, s. 47-49).

2.3.4 Krádež identity

Krádež identity, známá také jako identity theft, je druh útoku, kdy dojde k odcizení osobních údajů jedince. Útočník tyto údaje využívá často i k trvalému převzetí identity oběti. Ve většině případů bývá motivací útočníka zbohatnutí, ale také může usilovat o získání přístupu k citlivým informacím určité instituce. Dalším motivem může být získání přístupu k informacím o jednotlivcích nebo citlivým datům dané instituce. Charakteristickými projevy pachatele jsou různé nelegální činy, jako je například neoprávněné získání přístupových údajů nebo instalace škodlivého softwaru do počítače napadeného jedince. Po odcizení identity může pachatel zneužít získaných znalostí k útoku na danou osobu anebo k útoku na další oběť, která je většinou osobě s ukradenou identitou blízce známá. Jelikož další oběť o zneužití identity nemá nejmenší tušení, je na ní případný útok obvykle jednodušší (Kolouch, 2016, s. 318-319).

2.3.5 Sniffing

Sniffing je nezákonná metoda odposlechu dat v počítačové síti. Útočník s tzv. snifferem zachycuje a čte data procházející mezi klientem a serverem. Zatímco monitoring sítě prováděný správci sítě pro diagnostiku a údržbu sítě je legální, “monitoring“ bez souhlasu uživatele se stává sniffingem, tedy kyberkriminalitou. Útočníci s daty získanými sniffingem můžou získat citlivé informace jako přihlašovací údaje, e-maily nebo informace o používaných službách. Tito zločinci často počítač infikují i nějakým škodlivým softwarem. Sniffing představuje vážné bezpečnostní riziko. Uživatelé by se měli aktivně chránit a správci sítí zodpovědně používat nástroje pro monitoring. Možnou ochranou před sniffingem může být například firewall nebo použití VPN (Kolouch, 2016, s. 294).

2.3.6 Kybergrooming

Kybergrooming je rafinovaná metoda, kterou sexuální predátoři zneužívají k manipulaci a zneužívání dětí a dospělých online. Pod falešnou identitou si predátor buduje důvěru oběti na sociálních sítích či chatu. Po získání důvěry se snaží vylákat oběť na schůzku, kde může dojít k závažným trestným činům, jako je znásilnění, pohlavní zneužití, okradení nebo vydírání. Predátoři se schovávají za anonymitu online světa a skrývají své skutečné identity a úmysly. Oběti tak těžko ověří, s kým ve skutečnosti komunikují. V případě dětí je už samotné navrhování schůzky za účelem sexuálního zneužití trestné. Pachatelé často předstírají, že jsou mladší, atraktivnější, nebo mají společné zájmy s obětí. Tráví čas s obětí online, sdílí s ní informace a snaží se získat její sympatie. V případě dětských obětí je nejlepší prevencí komunikace s rodiči nebo jinými důvěryhodnými osobami, a především nesdílení osobních informací s lidmi, které neznají (Jelínek, 2021, s. 494-495).

2.3.7 Skimming a zneužívání platebních karet

Skimming je vychytralá metoda podvodu, která se zaměřuje na krádež informací z platebních karet. Dochází k ní v mnoha zemích světa a spočívá v instalaci speciálních zařízení na bankomaty. Tato zařízení na první pohled nejsou rozpoznatelná a slouží ke skenování magnetického proužku platební karty, čímž se získají údaje o kartě jako číslo, jméno držitele, CVV nebo datum platnosti, nebo k natočení PIN kódů zadávaného klientem do klávesnice bankomatu. Získané informace jsou pak zneužity k vytvoření kopie platební karty v zahraničí a následnému výběru hotovosti z bankomatů. Dále také k prodeji na černém trhu s kradenými osobními a finančními údaji. Kromě skimmingu existují i další metody krádeže údajů platebních karet, jako je například již zmiňovaný phishing nebo hacking, za jehož pomocí je možné proniknutí do klientské databáze internetového obchodu a krádež údajů platebních karet (Jelínek, 2021, s. 491).

2.3.8 Nigerijské listy

Další formou kyberkriminality jsou Nigerijské listy, které už jsou v dnešní době poněkud zastaralé, avšak jako fenomén dřívějšího období stojí za zmínku. Nigerijské listy jsou typem podvodu, který zneužívá sociálního inženýrství a cílí na osoby s nízkým povědomím o situaci v rozvojových zemích. Pachatelé lákají oběti na lákavou finanční odměnu za pomoc s převodem peněz z tzv. mrtvých kont. Tyto peníze údajně patří obětem válek, svrženým diktátorům nebo bohatým jedincům nuceným k emigraci. Podvod funguje tak, že oběť je kontaktována prostřednictvím elektronické komunikace s nabídkou a smyšleným příběhem o původu peněz. Pro získání odměny musí investovat peníze do zřízení afrického bankovního

účtu, zaplatit poplatek za založení nové společnosti, a mnoho dalších nesmyslných poplatků. Po zaplacení se pokaždé objeví další komplikace a další požadavky na platby. Čím více peněz oběť investuje, tím je těžší se smířit s nesmyslností celé situace a tím spíše je nakloněna k úhradě dalších poplatků. Dříve nabízená odměna se však nikdy neuskuteční. Nigerijské listy existovaly již před internetem, ale právě ten jim umožnil oslovit mnohem větší počet obětí (Jelínek, 2021, s. 490).

3 Zúčastněné subjekty

Kyberkriminalita je komplexní fenomén zahrnující dva základní subjekty – pachatele a oběť. Specifická je především svou anonymitou a možností pachatelů konat trestné činy po celém technologicky vyspělém světě z pohodlí vlastního domova. Oběti ale nejsou bezbranné, informovanost a prevence u daného jedince je základem ochrany před pachateli.

3.1 Pachatel

Pachatelem trestného činu je osoba, která svým jednáním naplnila znaky trestného činu, pokusu či přípravy, je-li trestná. Mohou to být ti, kdo přímo spáchali trestný čin, nebo ti, kdo využili jinou osobu k jeho provedení (Smejkal, 2018, s. 687). Osoba je považována za účastníka trestného činu, pokud úmyslně plánuje nebo řídí spáchání zločinu, přiměje jiného k rozhodnutí jeho spáchání, nebo mu k tomu pomáhá tím, že zajistí potřebné nástroje, odstraní překážky, podporuje v úmyslu spáchat zločin, slibuje pomoc nebo přiláká oběť na určené místo trestného činu, kde hlídá a poskytuje rady. (Zákony pro lidi, 2023).

3.1.1 Typy pachatelů

V oblasti kyberkriminality existuje mnoho typů pachatelů. Může se jednat o jednotlivce (profesionály či amatéry s omezenými dovednostmi), organizované skupiny s profesionální strukturou, insidery, kteří zneužívají svůj přístup anebo i státní aktéry. Ačkoli existuje určitý archetyp kyberzločince jako mužského jedince ve věku do 30 let, názor na pachatele se mění vzhledem k rostoucí digitalizaci společnosti. Zatímco starší generace může mít tendenci vyhýbat se novým technologiím, mladší generace je s nimi obeznámena od dětství a přijímá je jako součást běžného života.

Když na moment odložíme stranou kyberkriminalitu spojenou se šířením obsahu, jsou digitální zločinci obvykle nadprůměrně inteligentní, s technickými znalostmi a kreativními schopnostmi. Dnes už to ale neplatí úplně stoprocentně – mnoho nástrojů je totiž k dispozici ke koupi nebo jednoduchému získání online, a to i včetně manuálů. V kyberprostoru je jen zřídka zaznamenáno násilné chování, které by ohrožovalo na životech, s výjimkou situací, jako jsou digitální útoky na zdravotnická zařízení nebo kyberterorismus. Počet případů agresivního jednání online je tedy relativně nízký.

Vzhledem k rostoucí úrovni počítačové gramotnosti a dostupnosti internetu není kyberkriminalita omezena na určité sociální skupiny. Pachatelé mohou pocházet z různých socioekonomických vrstev. Zatímco je běžné považovat hackery za osamělé jedince,

kyberkriminalitu mohou páchat i dobře postavení jedinci s motivací získat majetkový prospěch nebo uspokojit jiné potřeby. Z hlediska pohlaví je kyberkriminalita vnímána převážně jako mužská, ale existují i známé případy ženských pachatelek. Jednoduše řečeno – typologie pachatelů se výrazně mění v závislosti na konkrétních formách zločinu prostřednictvím počítačových systémů (Jelínek, 2021, s. 483-485).

3.2 Oběť

Velice různorodé jsou i oběti jednotlivých typů trestných činů v kyberprostoru. Obecně platí, že kyberkriminalita není zaměřena například pouze na peněžní zisk a terčem útoku se může stát takřka kdokoliv. Očividná je situace v případě kyberšikany nebo šíření dětské pornografie, kde jsou zasažené osoby mladší 18 let, tedy děti. Pro většinu forem kriminality v digitálním prostoru však platí, že oběti často trpí nedostatkem znalostí, neopatrností či nadměrnou důvěrou. Často podceňují bezpečnostní opatření jak fyzické, tak softwarové, nejsou opatrní při sdílení osobních informací, nerozvažují rizika otevření příloh v elektronické komunikaci a neaktualizují svá hesla nebo nepoužívají dostatečně silná hesla (Jelínek, 2021, s. 485-486).

V širším slova smyslu lze říci, že obětí může být jednotlivec, který prostřednictvím phishingu, malwaru nebo jiných forem kyberkriminality přijde o peněžní prostředky či důvěrné informace. Terčem útoku často bývají také firemní subjekty, kde nejslabším článkem v zabezpečení je člověk a přes něj většinou vede cesta útočníků – často za použití sociálního inženýrství. Kybernetický útok může být zaměřen také na vládní instituce či celou zemi. Zde už může být řeč o kybernetické válce, ohrožující národní bezpečnost a stabilitu.

4 Kyberkriminalita a legislativa v ČR

Na úvod této kapitoly se sluší začít spíše teoreticky. Působnost práva je na internetu totiž velice složitá, a to hlavně díky jeho charakteristickým znakům. Zajímavý pohled poskytl Radim Polčák (Právo informačních technologií, str. 30-31), dle nějž internet vytvořil bezhraniční prostor, který urychlil globalizaci a změnil náš pohled na svět. Tradiční právní normy, které se opírají o státní hranice a teritoriální principy, mají problém s aplikací na internetové prostředí. Internet umožňuje okamžitý přístup k obrovskému množství dat a jejich šíření po celém světě, což má zásadní dopady na právo a jeho aplikaci. Je takřka nemožné internet jednotně a globálně regulovat, což komplikuje úsilí států a mezinárodních organizací. Za zmínku stojí globální korporace jako Meta, Google apod., které mají v tomto směru velký vliv. Rychlý technologický vývoj převažuje legislativní procesy, což vede k tomu, že právo často nedokáže reagovat na nové technologické výzvy. Existující právní normy by tak měly být častěji nově interpretovány tak, aby se mohly aplikovat na nové situace v online prostředí.

4.1 Vývoj právní úpravy kyberkriminality

Již v pozdních 70. letech minulého století začalo být zřejmé, že se vyvíjející digitální technologie stávají prostředím pro nové typy trestných činů, což vyvolalo potřebu zavést speciální právní regulaci. Ve francouzském Štrasburku byla Radou Evropy roku 1977 uskutečněna konference, kde byly vymezeny první formy kyberkriminality. Ve stejném roce byl také navržen Zákon o ochraně počítačových systémů ve Spojených státech amerických, což vyvolalo pocit potřeby nové právní úpravy k řešení tohoto problému. Úmluva o počítačové kriminalitě, vytvořena Radou Evropy spolu se zeměmi jako Japonsko, Kanada, Spojené státy americké a Jihoafrická republika, se stala jedinečným mezinárodně úspěšným právním nástrojem v této oblasti. I přes odmítnutí úmluvy ze strany několika významných zemí, kvůli obavám z narušení nezávislosti například Rusko, ji do současnosti schválilo 56 států, včetně České republiky, která ji podepsala v roce 2005 a schválila o osm let později (Polčák a kol., 2018, s. 543-545).

V českém právním systému se první speciální ustanovení pro oblast kybernetické kriminality realizovalo v roce 1991. Tato úprava se zabývala poškozením a zneužitím záznamu na nosiči informací, s cílem chránit data uložená na těchto nosičích proti neoprávněným změnám a použití. Další významnou úpravou prošel § 152 trestního zákona, který se zaměřoval na porušení autorského práva. Zásadní změnu v oblasti kriminality prostřednictvím informačních a komunikačních technologií představoval Trestní zákoník z roku 2010, který

přinesl řadu nových definic trestných činů v oblasti počítačové kriminality, čímž reagoval na požadavky stanovené v Úmluvě o počítačové kriminalitě. Ačkoli tento zákoník posunul vpřed definici a postih těchto zločinů, v oblasti procesního práva, tedy v pravidlech týkajících se postupů v trestních řízeních, nebyl dosažen podobný pokrok. Trestní řád dosud nebyl dostatečně upraven, což způsobuje určité obtíže při vyšetřování a stíhání kyberkriminality, protože stávající procesní postupy ne vždy odpovídají potřebám moderního světa. Pro boj s kyberkriminalitou už v Česku existují také speciální útvary, jako například Národní centrála proti terorismu, extremismu a kybernetické kriminalitě (NCTEKK), která se specializuje na potírání zločinů v této oblasti či Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) a další (Polčák a kol., 2018, s. 547-548).

4.2 Národní právní úprava

V České republice je mnoho zákonů, které se aspoň některou svou částí mohou týkat kybernetické kriminality a patří mezi ně např. Zákon o ochraně osobních údajů, Zákon o svobodném přístupu k informacím, Zákon o soudnictví ve věcech mládeže a mnoho dalších. Mezi ty nejzásadnější a nejdůležitější ale řadíme:

• Zákon č. 40/2009 Sb., trestní zákoník

• Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim

• Zákon č. 121/2000 Sb., autorský zákon

• Zákon č. 127/2005 Sb., o elektronických komunikacích

• Zákon č. 89/2012 Sb., občanský zákoník

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

(Kolouch, 2016, s. 338).

4.2.1 Zákon o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti byl přijat za účelem ochrany klíčových informačních systémů a infrastruktury, které jsou základem pro správné fungování státu a jeho institucí. Jeho cílem je zajistit odolnost proti kybernetickým útokům a schopnost se rychle zotavit po případných incidentech. Zákon klade důraz na prevenci a připravenost, povinnost hlásit bezpečnostní incidenty příslušným státním orgánům a implementaci efektivních bezpečnostních opatření k ochraně IT systémů. Rovněž stanovuje rámec pro spolupráci mezi

soukromým a veřejným sektorem v oblasti kybernetické bezpečnosti a určuje pravomoci státních úřadů, jako je NÚKIB, který má na starosti dohled nad dodržováním tohoto zákona a koordinaci reakce na kybernetické hrozby a incidenty. (Zákony pro lidi, 2022).

4.2.2 Občanský zákoník

V právním prostředí týkajícím se kybernetické bezpečnosti lze vedle veřejnoprávních norem aplikovat i soukromoprávní ustanovení, tedy občanský zákoník. Ten obsahuje ustanovení chránící soukromí a zakazující zásahy do něj bez zákonného důvodu. Dále stanovuje podmínky pro pořizování a používání obrazových a zvukových záznamů a chrání soukromé písemnosti osobní povahy. Soukromoprávní normy se také vztahují k virtuálnímu majetku, včetně autorských práv, herních či jiných virtuálních účtů. V případě náhrady škody způsobené kybernetickými útoky lze uplatnit institut občanského práva (Zákony pro lidi, 2024).

4.2.3 Kvalifikace zločinů dle Trestního zákoníku

Nový Trestní zákoník, který nabyl účinnosti 1. ledna 2010, přinesl významné změny do legislativy týkající se kyberkriminality. Byly zavedeny skutkové podstaty zaměřené přímo na kybernetickou trestnou činnost a různé typy útoků. Kybernetické zločiny mohou být kategorizovány podle toho, zda je cílem trestného jednání přímo počítač či počítačový systém, nebo zda je počítač použit jako nástroj pro spáchání zločinu. (Kolouch, 2016, s. 338-340) Mezi běžně stíhané kybernetické trestné činy patří ty, které jsou specificky uvedeny v trestním zákoníku, např:

- § 175 vydírání
- § 180 neoprávněné nakládání s osobními údaji
- § 184 pomluva
- § 191 šíření pornografie
- § 192 výroba a jiné nakládání s dětskou pornografií
- § 193 zneužití dítěte k výrobě pornografie
- § 230 neoprávněný přístup k počítačovému systému a nosiči informací
- § 231 opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
- § 232 poškození záznamu v počítačovém systému a na nosiči informací a zásah
- do vybavení počítače z nedbalosti
- § 234 neoprávněné opatření, padělání a pozměnění platebního prostředku
- § 269 porušení chráněných průmyslových práv

- § 270 porušení autorského práva, práv souvisejících s právem autorským a práv k databázi
- § 355 hanobení národa, rasy, etnické nebo jiné skupiny osob
- § 356 podněcování k nenávisti vůči skupině osob nebo k omezování práv a svobod
- § 357 šíření poplašné zprávy
- § 364 a § 365 schvalování či podněcování k trestnému činu
- § 405 popírání, zpochybňování, schvalování a ospravedlňování genocidy (Zákony pro lidi, 2024).

Trestní právo tedy zahrnuje ustanovení, která umožňují efektivní stíhání kyberkriminality, čímž zajišťuje srovnatelnost s ostatními státy a soulad s mezinárodními normami. Nicméně často dochází k tomu, že typické kyberkriminální aktivity jsou posuzovány jako obecnější zločiny. Například některé případy neoprávněného přístupu k počítačovým systémům a údajům, což umožňuje třeba phishing, pharming a mnoho dalších forem kriminality v prostředí komunikačních technologií, jsou stíhány jako podvody, protože s těmito druhy trestných činů mají právní systémy více zkušeností a jsou lépe vybaveny k jejich rozpoznávání a stíhání (Polčák et al., 2018, s. 555).

4.3 Národní úřad pro kybernetickou a informační bezpečnost

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) je česká vládní instituce, která má na starost ochranu kybernetické bezpečnosti státu a jeho kritické infrastruktury. Tento úřad byl zřízen s cílem koordinovat a zlepšovat obranu proti kybernetickým hrozbám a útokům, které mohou ohrozit národní bezpečnost, ekonomiku nebo veřejnou správu. NÚKIB se zaměřuje na vývoj strategie pro zvýšení kybernetické bezpečnosti, monitoruje a hodnotí kybernetické hrozby a incidenty, a poskytuje poradenství a podporu jiným státním institucím, podnikům i veřejnosti v oblasti kybernetické bezpečnosti. Kromě toho úřad spolupracuje s mezinárodními partnery a organizacemi, aby byla zajištěna koordinace na mezinárodní úrovni a aby Česká republika mohla reagovat na globální kybernetické hrozby efektivně a v souladu s mezinárodními standardy (NÚKIB, 2020).

4.3.1 Národní centrum kybernetické bezpečnosti

Národní centrum kybernetické bezpečnosti (NCKB) je specializovaná část Národního úřadu pro kybernetickou a informační bezpečnost, která se primárně zaměřuje na operativní aspekty kybernetické bezpečnosti v České republice. Toto centrum slouží jako hlavní bod pro

monitorování, detekci a reakci na kybernetické incidenty a hrozby. Kromě toho centrum pracuje na zlepšení celkové kybernetické odolnosti země prostřednictvím osvěty, vzdělávání a spolupráce s partnerskými organizacemi jak v tuzemsku, tak v zahraničí. Díky své hlavní roli v systému národní kybernetické bezpečnosti přispívá k rychlé a efektivní koordinaci mezi složkami zajišťujícími bezpečnost (NÚKIB, 2021).

4.3.2 Tým pro řešení počítačových nouzových situací

Vládní tým řešící počítačové nouzové situace, označovaný jako Computer emergency response team (CERT), je specializovaná jednotka zodpovědná za reagování na kybernetické bezpečnostní incidenty a hrozby, které se týkají vládních informačních systémů a sítí. Tento tým pracuje pod správou NCKB a jeho hlavním úkolem je zajistit rychlou a efektivní reakci na bezpečnostní incidenty, jako jsou například útoky DoS, neoprávněné přístupy nebo úniky dat. Jednotka dále podporuje rozvoj a implementaci nejlepších praktik a standardů v kybernetické bezpečnosti a pomáhá s rozvojem politik a strategií, které zlepšují celkovou kybernetickou odolnost vládních institucí. Zároveň slouží také jako hlavní zdroj bezpečnostních informací a poskytují pomoc orgánům státu, organizacím a jednotlivcům. Zároveň mají klíčovou roli při zvyšování povědomí o bezpečnosti na internetu, což je v oblasti kyberkriminality velmi důležité (NÚKIB, 2021).

4.4 Národní centrála proti terorismu, extremismu a kybernetické kriminalitě

Národní centrála proti terorismu, extremismu a kybernetické kriminalitě Služby kriminální policie a vyšetřování (NCTEKK SKPV) byla založena 1. ledna 2023 oddělením těchto tří oblastí z Národní centrály proti organizovanému zločinu a vytvořením nového samostatného celku. Jedná se o výkonný útvar Policie ČR, přičemž potírání kriminality v kyberprostoru je jedním z jeho hlavních úkolů. Terorismus, extremismus a kyberkriminalita jsou oblasti velice specifické a často se vzájemně prolínají, což vyžaduje odbornost ze strany operativců, analytiků a dalších úrovní tohoto útvaru (Policie ČR, 2023).

4.5 Mezinárodní instrumenty

Úmluva Rady Evropy o počítačové kriminalitě je klíčovým mezinárodním nástrojem v boji proti kyberkriminalitě, který byl přijat 56 státy z celého světa. Je považována za nejkompletnější mezinárodní standard v oblasti kyberkriminality. Jejím cílem je harmonizovat přístup k boji s touto problematikou na mezinárodní úrovni a poskytnout efektivní nástroje pro

řešení kyberkriminality ve všech jejích podobách a projevech. Tato Úmluva poskytuje komplexní rámec pro řešení problematiky kyberkriminality a je strukturována do čtyř kapitol (Polčák a kol., 2018, s. 548-550).

První část druhé kapitoly se zaměřuje na vymezení trestných činů, které souvisí s počítačovými daty a systémy. Rovněž pokrývá specifické trestné činy spojené se šířením násilného či sexuálního obsahu nebo s porušováním práv duševního vlastnictví. Druhá část této kapitoly se soustředí na procedurální aspekty, včetně získávání a manipulace s elektronickými důkazy. Třetí se pak věnuje otázkám spolupráce mezi státy v mezinárodním měřítku a vzájemné interakci justičních orgánů. Poslední čtvrtá kapitola pak adresuje procesní záležitosti, jako je stanovení územní působnosti či řešení případných sporů. Dodatek k této Úmluvě dále rozšiřuje katalog trestných činů o rasistické a xenofobní činy spáchané prostřednictvím počítačových systémů (Zákony pro lidi, 2019).

4.6 Evropské právo

Právní úprava kybernetické kriminality v Evropské unii je komplexní a zahrnuje řadu směrnic a nařízení. Na tomto území se zabývá strategií v oblasti kyberkriminality Evropská komise, která má za cíl výrazně snížit kyberkriminalitu prostřednictvím právních předpisů a zlepšením spolupráce mezi orgány zabývajícími se trestním řízením v Evropské unii. Tato snaha je součástí širšího rámce Strategie kybernetické bezpečnosti EU.

Komise navrhla řadu legislativních opatření pro boj proti kyberkriminalitě. V roce 2001 bylo přijato první rámcové rozhodnutí, které se zaměřovalo na podvody a padělání bezhotovostních platebních prostředků a vybízelo členské státy k trestnímu postihu aktivit spojených s manipulací počítačových dat a souvisejících technických prostředků. Vzhledem k tomu, že toto rozhodnutí se časem ukázalo jako nedostatečné, bylo v roce 2019 nahrazeno směrnicí, která má za cíl poskytnout konkrétnější právní rámec pro potírání těchto druhů zločinů a odstranit překážky v prevenci a boji proti nim.

Dalším důležitým krokem byla směrnice z roku 2011 zaměřená na boj proti pohlavnímu zneužívání dětí a dětské pornografii, zejména v kontextu jejich digitálního rozšíření. Z hlediska kyberkriminality je klíčová Směrnice o útocích na informační systémy z roku 2013, která definuje hlavní trestné činy proti informačním systémům a přiblížila se definicím z Úmluvy o počítačové kriminalitě. O rok později pak byla přijata Směrnice o evropském vyšetřovacím příkazu, která zavádí mechanismus evropského vyšetřovacího příkazu pro získání důkazů v

rámci EU. Tento mechanismus umožňuje rychlé a efektivní vyšetřování přeshraničních trestných činů. Tyto právní nástroje spolu s národními zákony členských států tvoří rámec, který má za cíl chránit Evropu před kybernetickými hrozbami a zločiny, zlepšovat prevenci, detekci a reakci na kybernetické incidenty, a poskytovat efektivní nástroje pro přeshraniční spolupráci. (Polčák a kol., 2018, s. 550-553).

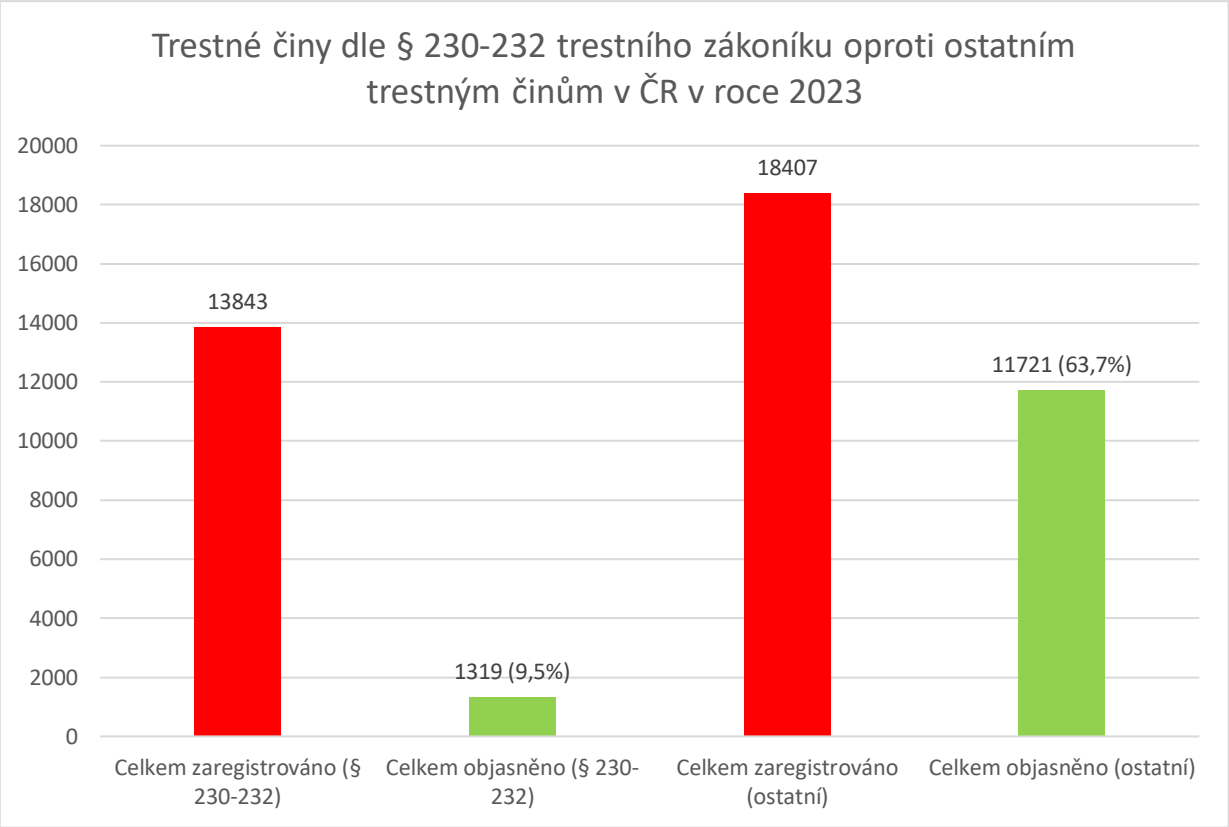
5 Analýza dostupných dat

V prvním desetiletí 21. století byl pro většinu českých občanů pojem kyberkriminalita absolutně nepředstavitelný. Také úřady, poskytující statistické údaje, se tímto tématem nezabývaly. Až v roce 2011 začala Policie ČR do statistik o jednotlivých druzích kriminality zahrnovat právě i tu v digitálním prostředí. Ve finální části práce si ukážeme, jak se v posledních letech kybernetická kriminalita drasticky vyvíjela a porovnání situace v České republice a dalších zemích Evropské unie.

5.1 Problematika statistických údajů o kyberkriminalitě

V České republice není možné přesně určit počet jednotlivých případů, které lze zařadit pod kybernetickou kriminalitu, ani v případě registrovaných skutků. To je způsobeno tím, že v policejních statistikách není kyberkriminalita samostatně vykazována. I když je možné sledovat počet trestných činů souvisejících například s diskriminací nebo porušováním práv, není možné zjistit, zda se tyto trestné činy odehrály v digitálním prostoru.

V současnosti jsou tedy jediné relevantní statistiky ty, tykající se zločinů dle § 230-232 trestního zákoníku, které se obecně mohou zařadit do kyberkriminality, ale zahrnují pouze omezenou část tohoto problému, a to útoky na počítačové systémy, nosiče informací a data. Na obrázku 1 lze vidět graficky znázorněnou trestnou činnost kvalifikovanou v trestním zákoníků právě těmito paragrafy a její objasněnost v porovnání s ostatními zločiny, přesněji tedy s vydíráním – § 175, pomluvou – § 184, šířením pornografie – § 191, výrobou dětské pornografie – § 192, nedovoleným kontaktem s dítětem – § 193b, porušením autorských práv – § 270, hanobením národa, rasy a jiných skupin osob – § 355, podněcováním k nenávisti – § 365 a šířením poplašné zprávy – § 357. Samozřejmě nejde o výčet všech možných trestných činů páchaných v kyberprostoru, avšak těch častějších. Mohu tedy konstatovat, že z 19 592 registrovaných skutků v roce 2023, je 13 843 v souvislosti s útoky na počítačové systémy, nosiče informací a data, a právě kvůli těmto zločinům má kriminalita páchána prostřednictvím informačních a komunikačních systémů tak malou objasněnost.

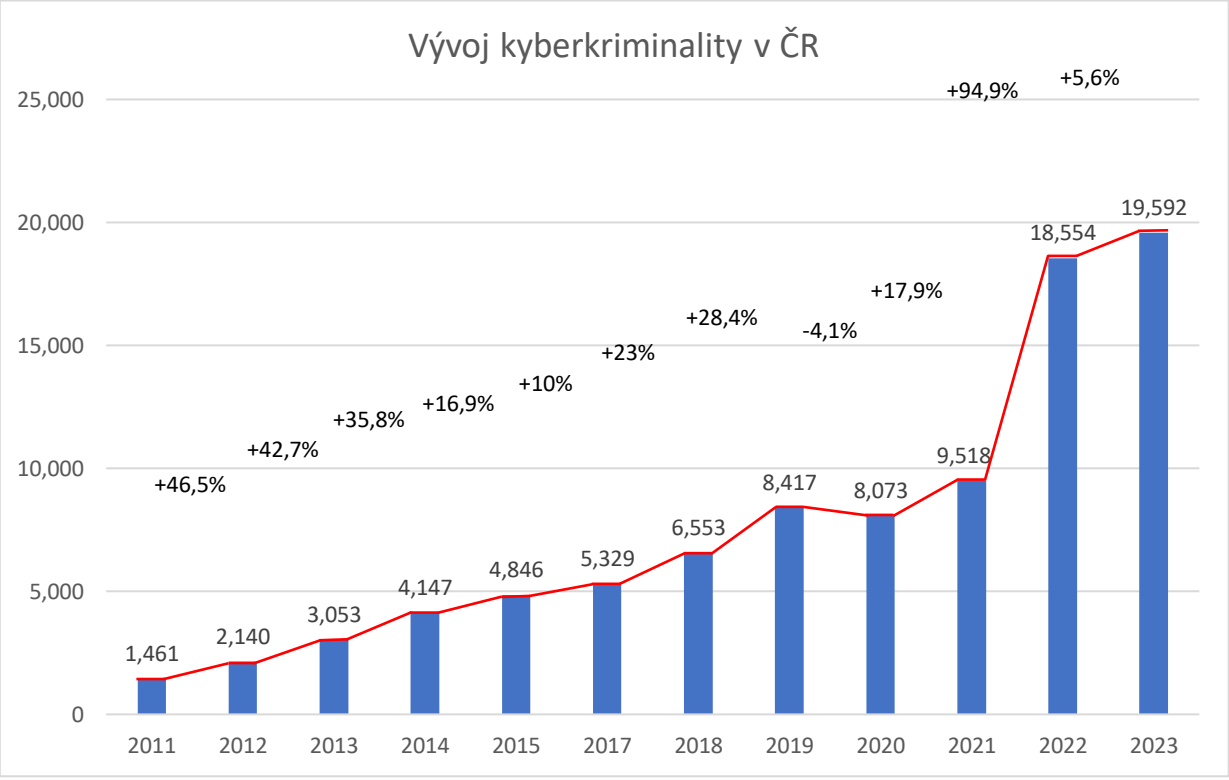


Obrázek 1 - Trestné činy dle § 230-232 trestního zákoníku oproti ostatním zmíněným trestným činům v ČR v roce 2023

Graf podle dat Policie ČR sestavil autor

5.2 Vývoj kyberkriminality v ČR v letech 2011–2023

I přes vysokou latentnost kybernetických zločinů a výše zmíněnou problematiku se statistickými údaji je další analýza kyberkriminality zajisté přínosná. Z dostupných dat sice nelze zjistit, kromě § 230-232, jaké trestné činy byly v kyberprostoru páchány, avšak ve výročních policejních zprávách o vývoji registrované kriminality lze zjistit přesný počet všech kybernetických zločinů. Na obrázku 2 vidíme jak nárust trestných činů v této oblasti, tak i jejich procentuální podíl růstu v Česku v období let 2011-2023. Lze tedy usoudit, že je kriminalita v prostředí internetu a sítí stále na markantním vzestupu. Dle slov Policie ČR tento trend bude i nadále pokračovat a do digitálního prostoru se bude transformovat stále větší množství protiprávního jednání. Z hlediska čísel se kyberkriminalita od roku 2011 až do roku 2023 zvýšila o neuvěřitelných 1 241 %. Nejvyšší nárust byl zaznamenán v roce 2022 o 94,9 %, což podle mnohých expertů zapříčinila epidemie koronaviru a s ním spojené restrikce a zároveň také podpora Ukrajiny po ruské invazi na její území. V ostatních letech byl zjištěn nebezpečný a rychlý růst zločinů až o desítky procent. Pouze v roce 2020 byl v kyberprostoru registrován pokles trestných činů o 4,1 % oproti předchozímu roku.

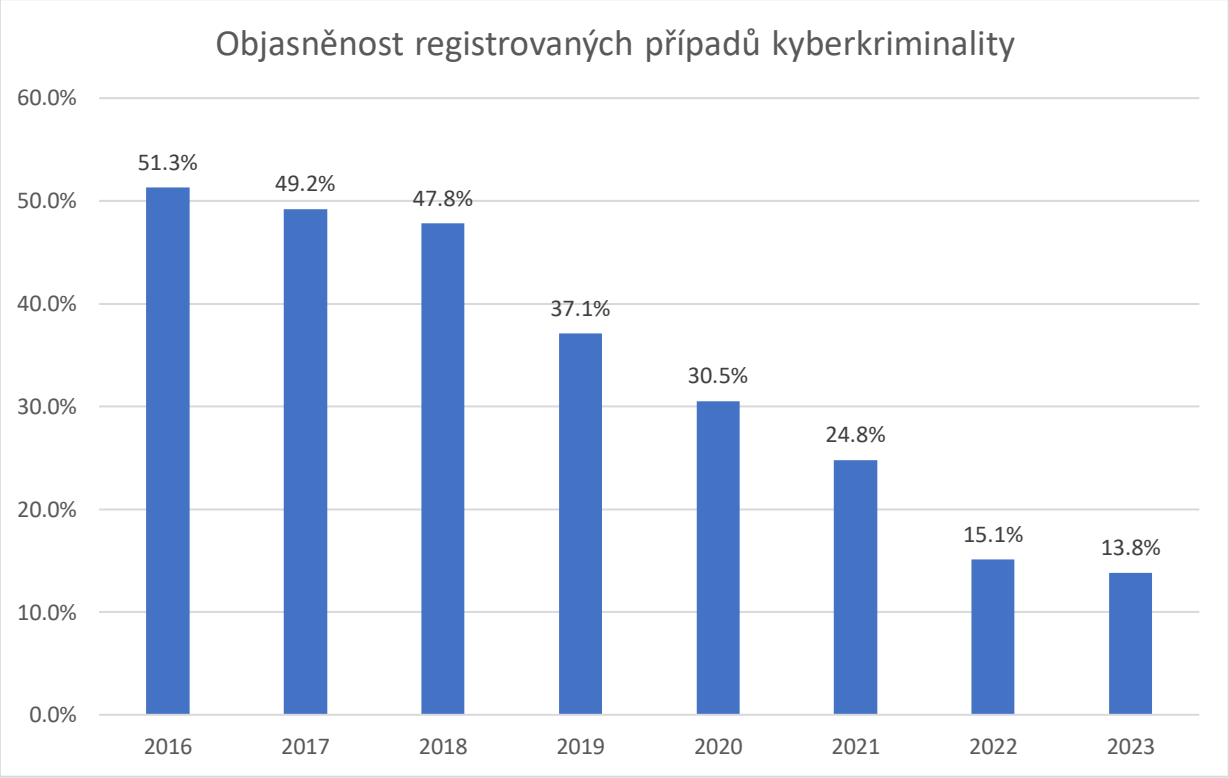


Obrázek 2 - Vývoj kyberkriminality v ČR

Graf podle dat Policie ČR sestavil autor

5.3 Objasněné případy kyberkriminality v průběhu let

V posledních letech se kybernetická kriminalita v České republice mnohonásobně zvýšila a v roce 2023 dosáhla svého maxima. Činy páchané prostřednictvím internetu a sítě mají totiž svá specifika. Jsou nízkonákladové a dostupné pro všechny lidi s určitou znalostí v oblasti digitálních technologií. Pachatelé se mohou vydávat za kohokoliv a jejich činy v kyberprostoru mají vysokou míru latence. Oběti totiž často o daném útoku nebo podvodu nemají nejmenší tušení. Moderní technologie se neustále vyvíjí a lidé si je více a více osvojují. To ale platí i pro zločince, a proto je pro policii čím dál složitější zločin ve světě počítačů odhalit. Na obrázku 3 vidíme graficky vyjádřenou procentuální úspěšnost objasněných případu v posledních osmi letech. Od roku 2016, kdy bylo objasněno 2 558 z 4 990 skutků, se úspěšnost Policie ČR v tomto oboru průběžně výrazně zhoršovala. V roce 2023 už se povedlo objasnit pouze 2 703 z 19 592 registrovaných skutků, což je těžko uvěřitelných 13,8 %.

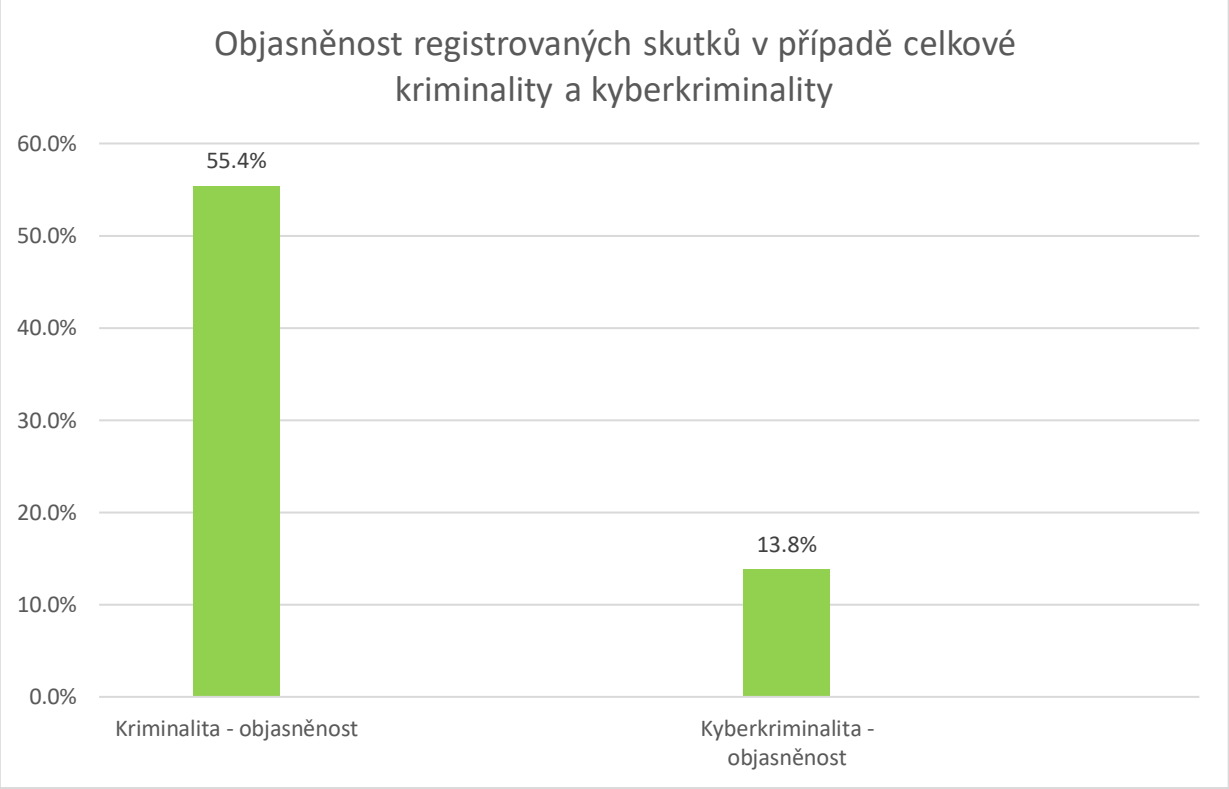


Obrázek 3 - Objasněnost registrovaných případů kyberkriminality

Graf podle dat Policie ČR sestavil autor

5.4 Objasněné skutky v případě kyberkriminality a celkové kriminality v roce 2023

S vývojem techniky a kriminalistických postupů zaznamenaly orgány působící v boji proti kriminalitě v rámci 21. století enormní zlepšení. Za posledních 10 let dosáhla kriminalita svého stropu v roce 2013, kdy bylo registrováno 325 366 skutků, z čehož objasněno jich bylo pouze 142 207 neboli 43,7 %. S průběhem dalších let zjištěné činy zpravidla klesaly a jejich objasněnost stoupala. V roce 2023 už se čeští policisté mohou pyšnit s 55,4 procenty vyřešených případů, z celkových 181 417 zaznamenaných. Naproti tomu kyberkriminalita má opačný trend. Jak už bylo dříve zmiňováno, registrované skutky rostou a jejich objasněnost klesá, jak můžeme vidět na situaci v roce 2023 znázorněné na obrázku 4.

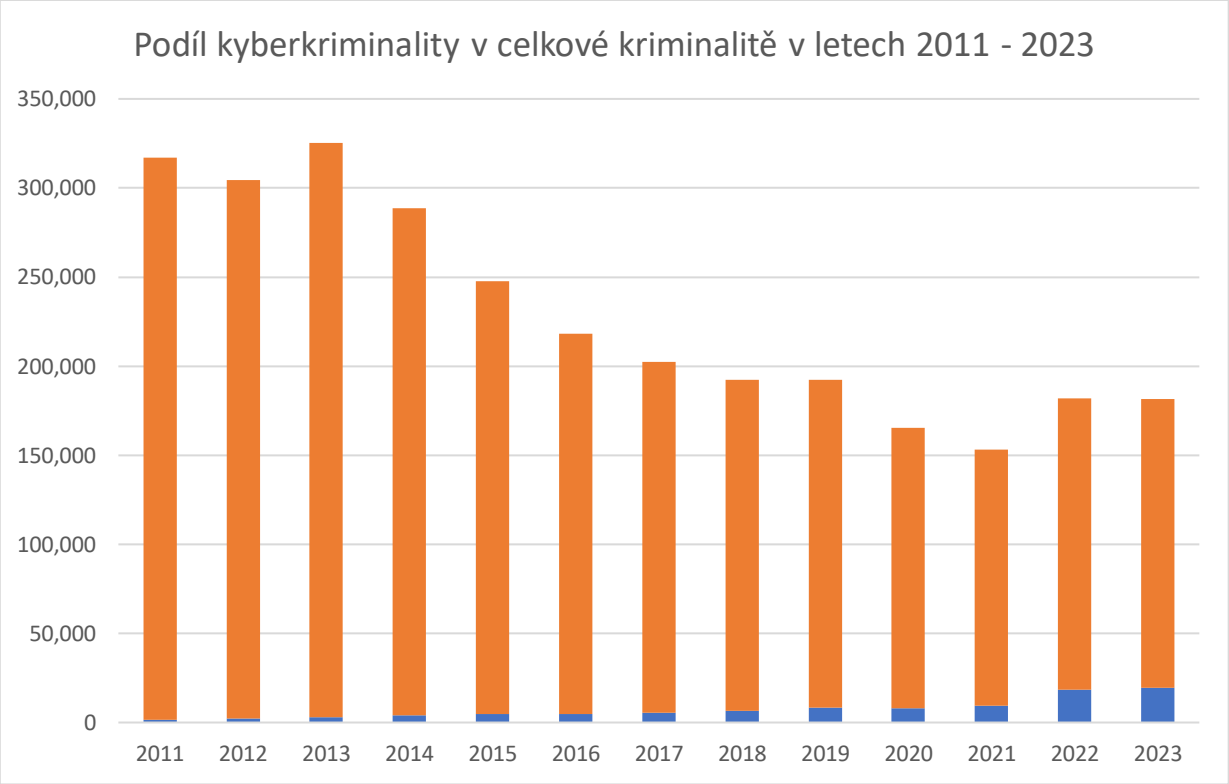


Obrázek 4 - Porovnání objasněnosti trestných činů v případě kyberkriminality a celkové kriminality v roce 2023

Graf podle dat Policie ČR sestavil autor

5.5 Kyberkriminalitika a její podíl v celkové kriminalitě

V České republice je registrováno hned několik druhů kriminality, jako je majetková, násilná, drogová, mravnostní nebo také hospodářská a mnoho dalších. To vše znázorňuje oranžová část sloupce na obrázku 5. Na druhou stranu modrá část znázorňuje zločin v digitálním prostředí. Z grafického znázornění na tomto obrázku lze vyčíst, že celková kriminalita v průběhu 13 let razantně klesla a to o 42,8 procent. Přesněji tedy tento pokles začal v roce 2014 a svého minima dosáhl v roce 2021, pravděpodobně z důvodu epidemie koronaviru a s tím spojenými omezeními. V roce 2022 znovu sledujeme nárust celkové kriminality o 28 678 případů, ve kterém má velký podíl kriminalita kybernetická. V internetovém světě totiž trestné činy v tomto období vzrostly o 9 036 případů, což je skoro třetina celkového růstu. To samé lze říci i o roce 2023, ve kterém je tento podíl ještě o trochu větší.

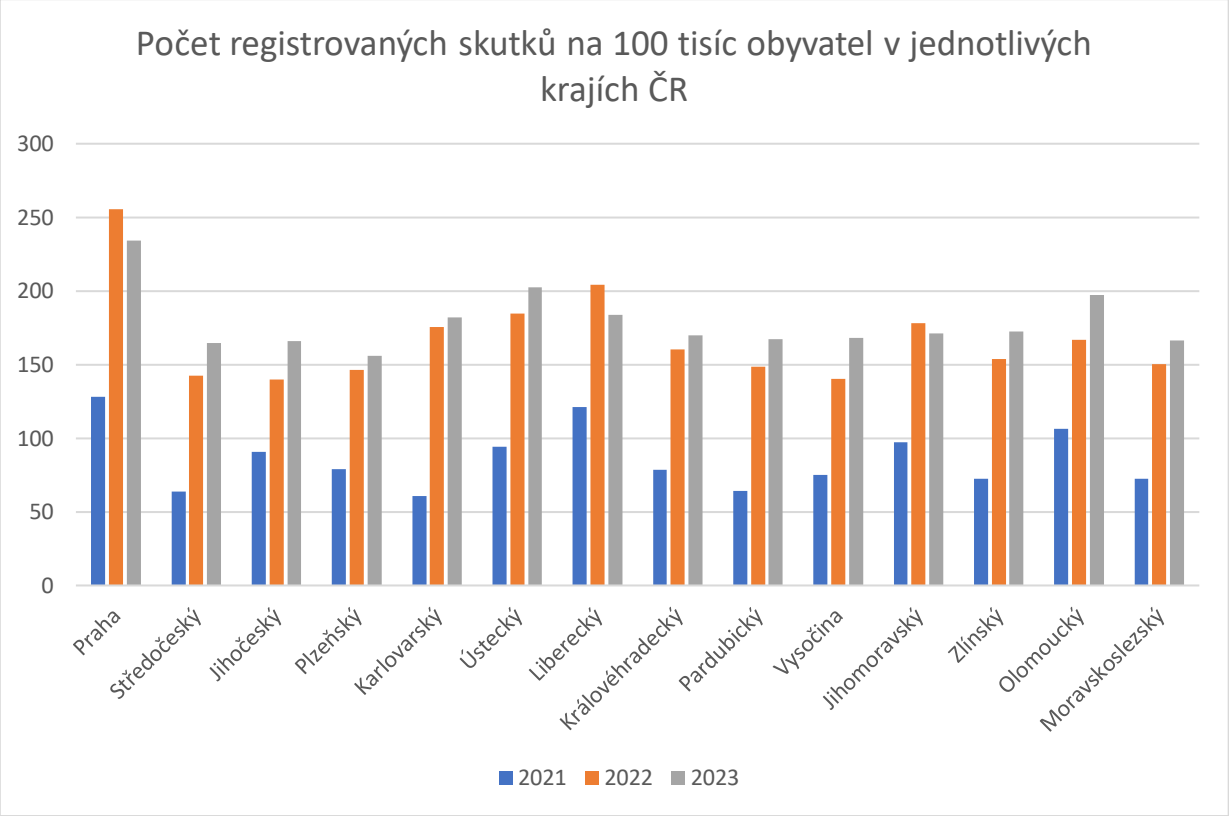


Obrázek 5 - Podíl kyberkriminality v celkové kriminalitě

Graf podle dat Policie ČR sestavil autor

5.6 Kyberkriminalita v jednotlivých krajích ČR

K analýze kybernetické kriminality v České republice samozřejmě patří i porovnání situace ve všech třinácti krajích České republiky a v hlavním městě Praha pro roky 2021-2023, znázorněné na obrázku 6. Největším „epicentrem“ kriminality v digitálním prostředím je samozřejmě právě Praha. Nejvíce registrovaných skutků v přepočtu na 100 tisíc obyvatel zde bylo v roce 2022 a to 256. V ostatních krajích už je situace poměrně podobná, avšak když vezmeme v úvahu všechny tři roky, nejmenší čísla vykazuje kraj Středočeský (v průměru 124 případů za rok na 100 tisíc obyvatel). Skoro stejná je situace v Plzeňském, Pardubickém, Moravskoslezském kraji a na Vysočině. Naopak více případů v průměru registruje kraj Ústecký, Olomoucký a Liberecký. Poslední zmiňovaný zaznamenal za poslední tři roky v průměru 170 kybernetických trestných činů na 100 tisíc obyvatel, takže se nejvíce přibližuje hlavnímu městu Praze (206 případů).



Obrázek 6 - Kyberkriminalita v jednotlivých krajích ČR

Graf podle dat Policie ČR sestavil autor

5.7 Kyberkriminalita v ČR a v zemích Evropské unie

Porovnání s ostatními zeměmi Evropské unie je nejlepší způsob pro nastínění závažnosti situace v Česku. V rámci kriminality obecně je podle posledních výzkumů společnosti World Population Review Česká republika osmou nejbezpečnější zemí na světě. Když vezmeme v potaz pouze Evropskou Unii, nacházíme se za Irskem, Dánskem, Rakouskem, Portugalskem a Slovinskem na místě šestém. V kriminalitě kybernetické už to takhle lehce říci nelze, protože statistiky o tomto stále poměrně nově rostoucím fenoménu nemusí být úplně nejpřesnější. Je obtížné zjistit, jakým způsobem je vedou ostatní země EU (zejména ty, které do unie vstoupily později), anebo jaké trestné činy do této oblasti zaznamenávají. Jak už bylo výše zmíněno, i u nás je toto problémem.

Pro toto porovnání bylo z běžně dostupných zdrojů možné shromáždit data o kybernetických trestných činech v roce 2023 pouze u dalších čtrnácti zemí EU. Z těchto vybraných státu se nejlepšími čísly může chlubit Maďarsko, které zaznamenalo 105,57 zločinů v přepočtu na sto tisíc obyvatel. Podobná situace je i v Řecku, které zaregistrovalo 111,07 případů. Zdaleka nejhorší je v tomto ohledu Estonsko se 497,04 skutky. Situace v České republice by se dala porovnat s Německem (187,46 trestných činů), které je na tom dle statistik lépe o pouhých 2,49 registrovaných případů v přepočtu na sto tisíc obyvatel. Na obrázku 7 tedy vidíme situaci v České republice v porovnání s některými zeměmi Evropské unie.

Obrázek 7 - Registrované skutky v ČR v porovnání s ostatními zeměmi Evropské unie

Graf podle dat statista.com sestavil autor

Závěr

Cílem bakalářské práce bylo prozkoumat a analyzovat fenomén kybernetických hrozeb v České republice, která se řadí mezi technologicky vyspělé státy. Na začátek byly definovány pojmy jako kyberprostor, kybernetický útok a bezpečnost, informace, počítačová síť, software a další, které jsou k porozumění této problematiky významné. Následně bylo třeba samotný pojem kyberkriminalita vysvětlit a vymezit. K tomu navazovala anonymita, globálnost, vysoká latence a další aspekty, které toto téma činí tak specifickým a odlišným od kriminality tradiční. Dále jsem se věnoval jednotlivým formám kyberkriminality, a to od činů spojených s integritou informačních systému a dat, přes skutky v souvislosti s šířením obsahu, až po ostatní nejčastější a nejznámější formy kybernetických útoků, včetně jejich charakteristiky a příkladů. Při každém trestném činu v této oblasti figuruje oběť a samozřejmě i pachatel, jež byly analyzovány v další kapitole práce. Dále se práce zabývá rozborem národní a mezinárodní legislativní úpravy spojené s kyberkriminalitou a shrnutí relevantních právních norem. V závěrečné části práce se nachází analýza dostupných dat o kyberkriminalitě v ČR, která shrnuje statistické údaje v dané oblasti.

Na začátku analýzy je zmíněná problematika se získáváním a vykazováním statistických údajů v České republice a v kombinaci s vysokou latencí kyberkriminality jsou tyto údaje nejspíše pouhým zlomkem skutečných trestných činů v této oblasti. Z dostupných dat Policie ČR byl zjištěn vývoj kriminality prostřednictvím informačních a komunikačních technologií v letech 2011–2023. Na tyto informace následně navazuje objasněnost registrovaných skutků, což je především díky zmíněným specifikám této formy kriminality, další kámen úrazu. Procento objasněnosti případů bylo dále porovnáno s objasněností trestných činů v případě tradiční kriminality. V další části analýzy je zobrazený podíl kybernetické kriminality v kriminalitě celkové. Následně bylo v porovnání jednotlivých krajů ČR zjištěno, že je dle očekávání nejvíce trestných činů páchaných v této oblasti v hlavním městě, kterému se svými čísly nejvíce přibližuje Liberecký kraj. Uvedeno je také porovnání situace v České republice s některými ostatními zeměmi Evropské unie.

Na základě provedené analýzy lze shrnout, že kyberkriminalita představuje významný a rostoucí problém v České republice. Její specifika, jako je anonymita pachatelů a obtížná dokazatelnost, kladou vysoké nároky na orgány činné v trestním řízení. Zároveň se stále vyvíjí a mění, takže je nutné neustále aktualizovat legislativu. Jak již bylo výše zmíněno, tento trend bude i nadále pokračovat a s vývojem umělé inteligence budou kybernetické útoky pouze nabírat na síle. Jednotlivci či organizace tedy musí být připraveny i na nově se formující hrozby.

Mnoho firem, především těch menších, po kybernetickém útoku často zkrachuje. Dnes už je tedy nutností zavedení oddělení pro kybernetickou bezpečnost, které bude obeznámeno se všemi známými riziky a schopné rychlé reakce v případě útoku. Práce zároveň zdůrazňuje důležitost prevence kyberkriminality a doporučuje zaměřit se na osvětu široké veřejnosti.

Použitá literatura

Gřivna, Tomáš, Scheinost, Miroslav a Zoubková, Ivana. 2019. *Kriminologie.* 5. aktualizované vydání. Praha : Wolters Kluwer, 2019. ISBN 978-80-7598-554-5.

Holt, Thomas J., Bossler, Adam M. a Seigfried-Spellar, Kathryn C. 2015. *Cybercrime and digital forensics: an introduction.* London : Routledge, 2015. ISBN 978-1-138-02130-3.

Jelínek, Jiří. 2021. *Kriminologie.* Teoretik. Praha : Leges, 2021. ISBN 978-80-7502-499-2.

Kolouch, Jan a Bašta, Pavel. 2019. *CyberSecurity.* Praha : CZ. NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.

Kolouch, Jan a Volevecký, Petr. 2013. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha : Policejní akademie České republiky v Praze, 2013. ISBN 978-80-7251-402-1.

Kolouch, Jan. 2016. *CyberCrime.* Praha : CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7.

Polčák, Radim a kolektiv. 2018. *Právo informačních technologií.* Praha : Wolters Kluwer, 2018. ISBN 978-80-7598-045-8.

Sklenák, Vilém. 2001. *Data, informace, znalosti a Internet.* Praha : C.H. Beck, 2001. ISBN 80-7179-409-0.

Smejkal, Vladimír. 2018. *Kybernetická kriminalita.* 2. rozšířené a aktualizované vydání. Plzeň : Vydavatelství a nakladadtelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7.

Smejkal, Vladimír, Sokol Tomáš a Vlček Martin. 1995. *Počítačové právo.* Beckova edice právo a hospodářství. Praha : C.H. Beck, 1995. ISBN 80-7179-009-5.

Završnik, Aleš. 2017. *Kyberkriminalita.* Právní monografie (Wolters Kluwer ČR). Praha : Wolters Kluwer, 2017. ISBN 978-80-7552-758-5.

Použité online zdroje

Eset. Co je počítačový virus + druhy virů. *Eset.com.* [Online] 2020. [cit. 2024-03-05]. Dostupné z: https://www.eset.com/cz/virus/.

Eset. Slovník pojmů Eset - červ. *Eset.com.* [Online] 2023. [cit. 2024-03-05]. Dostupné z: https://help.eset.com/glossary/cs-CZ/worms.html.

Legislativa. Kybernetický útok (kyberútok). Definice, typy, následky a prevence. *Legislativa.cz.* [Online] 2022. [cit. 2024-03-04]. Dostupné z: https://legislativa.cz/zdroje/kyberneticka-bezpecnost/kyberneticky-utok.

Microsoft. Co je to kybernetická bezpečnost? *Microsoft.com.* [Online] 2021. [cit. 2024-03-04]. Dostupné z: https://support.microsoft.com/cs-cz/topic/co-je-to-kybernetick%C3%A1-bezpe%C4%8Dnost-8b6efd59-41ff-4743-87c8-0850a352a390.

Microsoft. Ochrana před útoky phishing. *Microsoft.com.* [Online] 2020. [cit. 2024-03-12]. Dostupné z: https://support.microsoft.com/cs-cz/windows/ochrana-p%C5%99ed-%C3%BAtoky-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44.

NÚKIB. Kybernetická bezpečnost. *Nukib.cz.* [Online] 2021. [cit. 2024-04-02]. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/.

NÚKIB. O NÚKIB. *Nukib.cz.* [Online] 2020. [cit. 2024-04-02]. Dostupné z: https://nukib.gov.cz/cs/o-nukib/.

NÚKIB. Vládní CERT. *Nukib.cz.* [Online] 2021. [cit. 2024-04-02]. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vladni-cert/.

Policie ČR. Kriminalita. *Policie.cz.* [Online] 2024 [cit. 2024-04-02]. Dostupné z: https://www.policie.cz/statistiky-kriminalita.aspx.

Policie ČR. Národní centrála proti terorismu, extremismu a kybernetické kriminalitě SKPV. *Policie.cz.* [Online] 2023. [cit. 2024-04-02]. Dostupné z: https://www.policie.cz/clanek/narodni-centrala-proti-terorismu-extremismu-a-kyberneticke-kriminalite.aspx.

Software. Co je to Keylogger? *Software.cz.* [Online] 2019. [cit. 2024-03-05]. Dostupné z: https://www.software.cz/co-je-to-keylogger.

Správa sítě. Co je internet. *Sprava-site.eu.* [Online] 2022. [cit. 2024-04-02]. Dostupné z: https://www.sprava-site.eu/internet/.

Správá sítě. Pharming. *Sprava-site.eu.* [Online] 2022. [cit. 2024-03-12]. Dostupné z: https://www.sprava-site.eu/pharming/.

Správa sítě. Software. *Sprava-site.eu.* [Online] 2022. [cit. 2024-03-04]. Dostupné z: https://www.sprava-site.eu/software/.

Statista. Cybercrime. *Statista.com.* [Online] 2024. [cit. 2024-04-02]. Dostupné z: https://www.statista.com/search/?q=cybercrime&Search=&p=1

Zákony pro lidi. Sdělení č. 104/2013 Sb. m. s. *Zakonyprolidi.cz.* [Online] 2019. [cit. 2024-04-02]. Dostupné z: https://www.zakonyprolidi.cz/ms/2013-104.

Zákony pro lidi. Sdělení č. 59/2016 Sb. m. s. *Zakonyprolidi.cz.* [Online] 2010. [cit. 2024-04-02]. Dostupné z: https://www.zakonyprolidi.cz/ms/2016-59.

Zákony pro lidi. Zákon č. 181/2014 Sb. *Zakonyprolidi.cz.* [Online] 2022. [cit. 2024-04-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181.

Zákony pro lidi. Zákon č. 218/2003 Sb. *Zakonyprolidi.cz.* [Online] 2023. [cit. 2024-04-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2003-218.

Zákony pro lidi. Zákon č. 40/2009 Sb. *Zakonyprolidi.cz.* [Online] 2024. [cit. 2024-04-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40.

Zákony pro lidi. Zákon č. 89/2012 Sb. *Zakonyprolidi.cz.* [Online] 2024. [cit. 2024-04-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2012-89.