POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostního managementu

Katedra managementu a informatiky

Boj proti informační kriminalitě v České republice

Bakalářská práce

The fight against information crime in the Czech Republic

Bachelor thesis

VEDOUCÍ PRÁCE

RNDr. Václav HNÍK, CSc.

AUTOR PRÁCE

David ŠACH

PRAHA

2023

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Písku, dne 11. 05. 2023

David Šach

Poděkování

Rád bych touto cestou poděkoval všem, kteří mi pomáhali se zpracováním mé bakalářské práce. Děkuji vedoucímu práce RNDr. Václavu Hníkovi, CSc. za systematické vedení při psaní mé bakalářské práce, jeho náměty a připomínky, které pomohly zdokonalit moji práci. Dále bych chtěl poděkovat celé své rodině za podporu při studiu.

ANOTACE

Práce popisuje a sumarizuje fakta z odborné literatury, z tematických článků a odkazů na internetu týkající se kybernetické kriminality v České republice. Teoretická část se zabývá popisem jednotlivých druhů kyberkriminality, dále aktuálními hrozbami informační kriminality a jejich prevence. Také se zabývá nejnovějšími kyberútoky v České republice v roce 2022.

V praktické části této práce je rozebrána a analyzována případová studie konkrétního vyšetřovaného případu PČR a to od jeho počátku podáním trestního oznámení až po konečný rozsudek. Tento případ byl řešen Policií ČR, Krajského ředitelství policie Jihočeského kraje. Jeho začátek je v roce 2017. Pravomocné skončení tohoto případu bylo již v roce 2018.

KLÍČOVÁ SLOVA

Informační kriminalita * kybernetické hrozby * informační a komunikační technologie * mravnostní trestné činy * oběti.

ANNOTATION

The work describes and summarizes facts from professional literature, from thematic articles and links on the Internet regarding cybercrime in the Czech Republic. In its theoretical part, it mainly deals with the description of individual types of cybercrime, as well as current threats of information crime and their prevention. It also deals with the latest cyberattacks in the Czech Republic in 2022. In the practical part of this work, a case study of a specific case investigated by the Czech Republic is analyzed and analyzed, from its beginning with the filing of a criminal complaint to the verdict.

KEYWORDS

Information crime * cyber threats * information and communication technologies * crimes of indecency * victims.

OBSAH

ÚVOD

Bakalářskou práci na téma „Boj proti informační kriminalitě v ČR“ jsem se rozhodl napsat z několika důvodů. Počítači a kyberprostorem se zabývám i ve svém volném čase a dá se říci, že je to i můj koníček. Toto téma jsem si proto vybral záměrně. V dnešní moderní době prakticky každý člověk denně přímo či nepřímo používá různá elektronická či počítačová zařízení. Toto používání má samozřejmě své kladné, ale i záporné stránky. Proto se v mé bakalářské práci budu hlavně zabývat možnými riziky a nástrahami při používání těchto elektronických zařízení a chováním uživatelů v kyberprostoru. Je všeobecně známo a také studie tak ukazují, že trestných činů a různých podvodných jednání v kyberprostoru a celkově v online prostředí každý rok stoupá a škody rostou do řádů statisíců, v některých případech i do miliónových částek. Oproti minulosti, kdy se jednalo v online prostředí spíše o tzv. přestupkové jednání, se nyní nechá říci, že od ledna 2022 se již jedná především o trestné činy, které zasahují do lidských práv a majetku mnohem více a ve větší formě, a způsobují tak mnohem větší škodu, jak na majetku, tak na finanční újmě uživatele.[1]

V teoretické části své práce popisuji a sumarizuji známá a již publikovaná fakta týkající se obecně informační kriminality, tak boji a prevenci proti ní. Také se zde zaměřuji na práci PČR, SKPV v boji proti kyberkriminalitě. V praktické části práce popisuji konkrétní případ vyšetřovaný PČR, SKPV spadající pod téma informační kriminality v ČR.

Závěrem jsem se pokusil shrnout hlavní bezpečnostní rizika dnešních uživatelů výpočetní techniky jak v České republice, tak ve světě. Zabývám se též otázkou možné obrany proti těmto rizikům a prevenci proti nim. Také jsem se pokusil shrnout celková dnešní a i možná budoucí bezpečnostní rizika v oblasti kybernetické bezpečnosti jak ve světě, tak v České republice.

[1] FIŠER, Miloslav. *Trestných činů v kyberprostoru dramaticky přibylo* [online]. 23. 11. 2022 [cit. 2022-12-10]. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-trestnych-cinu-v-kyberprostoru-dramaticky-pribylo-hlasi-policie-40415280

1. POJEM KYBERNETICKÁ KRIMINALITA

Pod pojmem kybernetický prostor si můžeme představit prostor spojený s virtuálním světem, nebo také můžeme říci prostředí, kde existuje tzv. nekonečno a nikdo neví, kde tento kyber prostor začíná nebo kde končí anebo, jak velký kybernetický prostor všeobecně je. Díky těmto vlastnostem, je toto prostředí velice náchylné k páchání kybernetické kriminality. Pojmem kybernetická neboli počítačová kriminalita Police ČR označuje trestnou činnost páchanou pomocí počítačů, počítačových sítí, různých informačních technologií, ale také čím dál ve větší míře pomocí komunikačních technologií.[2]

V teoretické rovině můžeme kyberkriminalitu nazvat vědou, která se zabývá převážně kriminalitou páchanou v souvislosti s kyberprostorem. Proto v užším pojetí můžeme kyberkriminalitou nazvat trestné činy, jejichž všechna vývojová stádia jsou spáchána v kyberprostoru. Též je možné konstatovat, že v pojetí trestněprávním je kriminalitou rozuměno, platné a účinné trestním právem hmotným upravené skutkové podstaty trestných činů zločinů nebo přečinů.[3]

Pokud se na kyberkriminalitu podíváme v širším pojetí, je možno konstatovat, že je vědou zabývající se kriminalitou, u které však nemusí být dána přímá souvislost s kyberprostorem, ale u které postačuje, aby kterékoli z vývojových stádií spáchaného trestného činu mělo svůj původ právě v kyberprostoru. Nebo alespoň je s tímto kyberprostorem ve větší či menší míře spjata.[4] Proto je možno v širším pojetí kyberkriminality považovat za „cybercrime“ takový trestný čin, u kterého došlo jen k jeho přípravě či pokusu v kyberprostoru, ale k samotnému dokončení a dokonání došlo již v reálném světě. Hned na začátku této práce je také zapotřebí konstatovat, že kyberprostorem se rozumí virtuální počítačový svět. Jedná se vlastně o imaginární prostor tvořený počítačově zpracovanými daty.[5]

---

[2] PREVENCE KRIMINALITY. *Kyberkriminalita* [online]. 20.12.2022 [cit. 2022-12-27]. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/kyberkriminalita/

[3] VÁLKOVÁ, Helena*: Kriminalita*, *D. Hendrych a kol.: Právnický slovník*, 3. vydání, C. H. Beck, Praha 2009**.** [s. 568].

[4] PROVAZNÍK, Jan*.: § 20 [Příprava], in: F. Ščerba a kol.: Trestní zákoník*, 1. vydání, C. H. Beck, Praha 2020. [s. 155].

[5] ŠKOP, Martin. *Hranice práva a kyberprostoru – subversivita kyberprostoru,* Právník č. 10/2005. [s. 1157-1168].

1.1 Jednotlivé druhy kyberkriminality

Výčet jednotlivých různých druhů kyberkriminality není a nikdy nemůže být taxativní a to s ohledem na neustálý technologický pokrok, kterého jsme zejména v poslední době svědci. V následujících kapitolách se proto pokusím nastínit, dle mého názoru, nejpodstatnější druhy kyberkriminality s jejich popisem.

Podvodná jednání

Vzhledem k velmi rostoucímu trendu online prostředí a využívání počítačů v běžném životě, se pro obyčejného uživatele stal zcela běžnou součástí výčet různých hrozeb. Jedno z nejvíce hrozících nebezpečí je přečin podvodu, který následuje s přečinem neoprávněný přístup k počítačovému systému a nosiči. Oba tyto skutky jsou definovány dle ustanovení § 209[6] trestního zákoníku a dle ustanovení § 230[7] trestního zákoníku. Asi nejvíce případů podvodných jednání je provázáno s existencí neustále nově vznikajících e-shopů, kdy pro běžného uživatele se základní znalostí internetu nejde zjistit, zda je nový e-shop podvodný či ne. Velmi často se pak stává, že peníze, které uživatel za zboží v takovém e-shopu zaplatí pomocí kreditní karty nebo bankovního převodu budou zneužity. Dalším problémem u podvodných e-shopů je skutečnost, že zde hrozí následné zneužití platebních údajů. Zadané platební údaje a čísla karet končí dalším prodejem v kyberprostoru, např. na „Darkwebu“. Poslední dobou se tyto případy přenesly do prostředí online inzerce. Začíná se ve velkém využívat tzv. phishing a to především na uživatele, kteří na takových inzertních portálech převážně vystupují jako prodávající.[8]

Hacking

Tato forma počítačové kriminality vychází z toho, že pachatel jedná s úmyslem narušit, získat nadvládu nebo se neoprávněně připojit k přístupu počítačového systému pomocí zneužití zařízení, různého šíření škodlivých kódů, nelegálního software apod. Pokud bychom hledali porušení určitého paragrafu, dá se říci, že

[6] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
[7] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
[8] POLICIE ČESKÉ REPUBLIKY. *Jednotlivé druhy kyberkriminality* [online]. 2022 [cit. 2022-11-23]. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

nejblíže má hacking k porušení dle ustanovení § 230[9] trestního zákoníku. Hackeři ve většině případů a stále více napadají různé e-mailové účty, profily na sociálních sítích a také internetového bankovnictví. Jejich hlavním cílem je získání přístupu do profilů a také zneužití získaných dat k následnému vydírání. Pokud bychom šli dále, tak díky velkému rozmachu WiFi připojení, kdy dnes nenajdeme v každém městě místo, kde se nemůže běžný uživatel připojit k internetu, tak velmi často dochází tzv. sniffingu, které se nechá trestat dle ustanovení § 182[10] trestního zákoníku, kdy pachatelé zaznamenávají veškerý tok informací v dané síti a které následně zneužívají dle jejich potřeb. Celou tuto množinu nelegálního hackingu můžeme přiřadit do tzv. „Black Hat hackingu“, který je určen pro nelegální využití. Existuje také tzv. legální hacking WHITE HACK který slouží k testování a vylepšování zabezpečení počítačových sítí a není zneužíván k nelegální činnosti. Poslední z rodiny hackingu je také tzv. GRAY HACK, který je něco mezi oběma hackingy, kdy jde o to, že hacker bez povolení testuje různé systémy, ale v žádném případě získaná data nebo informace či přístupy, nezneužije k nelegálním účelům. [11]

Blagging

Tento typ podvodu se ve velké míře zneužívá díky tzv. sociálnímu inženýrství, kdy pachatelé mají velmi dobře zmapovanou firmu, ve které chtějí tento podvod využít ke svému prospěchu. Častým případem jsou i osobní vztahy v dané firmě, kdy díky tomu, že pachatel zjistí a poté vyláká důležité informace o ostatních zaměstnancích, jejich funkcích, postech a také možnostech provádění plateb a převodů. Velmi lehce se pak zaměří cíleně na dané oddělení ve firmě (většinou jsou to účtárny), kdy následně pod záštitou majitele, ředitele, budoucího partnera nebo odpovědné osoby, pomocí e-mailu napíše informace k příkazu provedení platby na daný účet (často i fiktivní faktury nebo jiného dokladu). Pověřený pracovník, který ani netuší, že mu tuto zprávu posílá podvodník, platební příkaz provede a peníze odešle. Útočník dokáže takto připravený příkaz (většinou

[9] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
[10] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
[11] POLICIE ČESKÉ REPUBLIKY. *Jednotlivé druhy kyberkriminality* [online]. 2022 [cit. 2022-11-23]. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

e-mailovou zprávu) tak profesionálně zamaskovat, že je pro běžného počítačového uživatele k nerozeznání od pravé informace, se kterou denně pracuje v dané firmě.[12]

Podvodné e-shopy

Stále častěji se vyskytují v online prostředí nové a nové e-shopy, u kterých se většinou díky tomu, že nabízejí velmi atraktivní zboží za někdy až neuvěřitelné ceny, stalo nakupování běžných nic netušících uživatelů denním chlebem. Tato situace je dána tím, že nakupování v e-shopech je velmi moderní a získává na oblibě v jakékoliv věkové kategorii. Podvodní uživatelé, kteří tyto e-shopy s úmyslem podvodu zakládají, se ve většině případů nenacházejí ani v České republice, ale v zahraničí, kdy díky internetu není pro ně problém založit jakýkoliv e-shop kdekoliv a v jakémkoliv státu. Co se týká České republiky, tak scénář je většinou stejný. Na podvodný e-shop umístí pachatel velmi levné a atraktivní zboží a následně jako jediný způsob platby nastaví platbu dopředu, a to zpravidla kreditní kartou. Uživatel pak následně zaplatí, peníze mu odejdou z karty, ale zboží nikdy nepřijde. Jsou také známy případy, kdy se objevují na sociální síti nebo i v inzercích různé nabídky práce. Většinou pro studenty, kdy jejich práce spočívá v přeposílání peněz pachatelům, ze svých bankovních účtů, které sami nabídnou ke spolupráci a následně získávají odměnu za každé přeposlání peněz. Studenti tak ani netuší, že by se dělo cokoliv nelegálního, jelikož zpětnou vazbu od platících zákazníků na e-shopech nemají a často velmi dlouho trvá, než se ukáže, že se jedná o podvod a že svým, byť nedbalostním jednání porušují ustanovení dle § 217[13] trestního zákoníku či podílnictví.[14]

Mravnostní trestné činy

Jedno z nezávažnějších jednáních, které se v kyberprostoru nachází a to velmi aktivně díky neustále se zlepšujícím formám anonymity útočících uživatelů a také rozmachu sociálních sítích a mobilních telefonů s možností přístupu

[12] POLICIE ČESKÉ REPUBLIKY. *Jednotlivé druhy kyberkriminality* [online]. 2022 [cit. 2022-11-23]. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx
[13] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
[14] POLICIE ČESKÉ REPUBLIKY. *Jednotlivé druhy kyberkriminality* [online]. 2022 [cit. 2022-11-23]. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

k internetu u dětí, jsou trestné činy, které patří k opravdu závažným trestným činům porušující ustanovení dle § 201[15] trestního zákoníku ohrožení výchovy dítěte, § 191[16] trestního zákoníku šíření pornografie, § 192[17] trestního zákoníku, výroba a jiné nakládání s dětskou pornografií, § 193[18] trestního zákoníku zneužití dítěte k výrobě pornografie navazující na § 193a[19] trestního zákoníku účast na pornografickém představení a také § 193b[20] trestního zákoníku, navazování nedovolených kontaktů s dítětem. Ve většině případů jde útočníkovi o to, aby konkrétní osobu, kterou chce zneužít, vylákal pod různou záminkou na osobní schůzku anebo k zaslání intimních fotografií. V další fázi, pokud útočník získá požadované fotografie nebo videa, následně tyto šíří pomocí různých služeb v různých komunitních fórech či galeriích. Ne vždy se jedná pouze o tzv. dětské oběti, ale stále častěji se tyto útoky vedou již proti dospělým a zletilým osobám, které jsou pak zneužívání v rámci kuplířství, obchodu s lidmi či různých sexuálních nátlaků.[21]

Trestné činy proti právu autorskému

Ve velkém měřiku jsou na internetu také rozšířena různá online datová úložiště, která většinou fungují v dobré víře, a to k ukládání a možnosti posílání velkých souborů, které dříve klasický e-mail neuměl odeslat, avšak brzy se díky vynalézavosti uživatelů stalo toto prostředí úschoven místem páchání trestného činu dle ustanovení § 270[22] trestního zákoníku, kdy je nelegálně sdíleno dílo autora v rozporu a práv souvisejících s právem autorským.[23]

---

[15] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
[16] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
[17] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
[18] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
[19] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
[20] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
[21] POLICIE ČESKÉ REPUBLIKY. *Jednotlivé druhy kyberkriminality* [online]. 2022 [cit. 2022-11-23]. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx
[22] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
[23] POLICIE ČESKÉ REPUBLIKY. *Jednotlivé druhy kyberkriminality* [online]. 2022 [cit. 2022-11-23]. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

Trestné činy z nenávisti

Díky možnostem moderního přístupu k internetovým službám z jakéhokoli světadílu a také neustále se vylepšujícím anonymním serverům a různých softwarů a VPN, je velice lehké pro různé extremisty projevit své nenávistné názory a založit různá internetová fóra pro stejně smýšlející uživatele a vyvolat tak podměty k nenávisti či výzvu k násilí k určité skupině obyvatel. Často se může jednat také o různé nebezpečné, vyděračské a vyhrožující útoky, které naplňují ustanovení § 175[24] trestního zákoníku, ustanovení § 353[25] trestního zákoníku, ustanovení § 354[26] trestního zákoníku, ustanovení § 357[27] trestního zákoníku a také ustanovení § 355[28] a ustanovení § 356[29] trestního zákoníku.[30]

Cryptomining

Spolu se vstupem kryptoměn do internetového prostředí, kdy hlavním článkem ve světě kryptoměn je považována kryptoměna Bitcoin, která má vysokou hodnotu a jednou z možností jak třeba i část této kryptoměny získat je tzv. těžení pomocí počítačové techniky, došlo k adaptaci útočníků na tzv. cryptojacking systémy, kdy útočník pomocí malware zacílí na počítačový zdroj uživatele, k získání ve stručnosti řečeno větší síly zdroje, který následně využívá k těžení kryptoměny Bitcoin i dalších kryptoměn. Cíl útočníka je jasný, snaží se získat takto nejvíce napadených koncových uživatelů jak v domácím, tak i firemním prostředí. Jednou z šancí, jak oběť může zjistit tento útok je to, že se znatelně sníží výpočetní výkon jeho počítače nebo se velmi značně zvedne teplota počítače, kdy následuje spuštění maximální akcelerace ventilátorů spojený s velkým hlukem.[31]

---

[24] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
[25] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
[26] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
[27] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
[28] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
[29] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
[30] POLICIE ČESKÉ REPUBLIKY. *Jednotlivé druhy kyberkriminality* [online]. 2022 [cit. 2022-11-23]. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx
[31] ESET, Digital Security. *Jak rozpoznat kryptominační útok?* [online]. 2023 [cit. 2023-01-12]. Dostupné z: https://www.eset.com/int/malicious-cryptominers/

Kybergrooming

V dnešní moderní době nesmíme opomenout také tento poměrně nový fenomén páchané trestné činnosti probíhající převážně v kyberprostoru. Jedná se o velmi rizikovou formu komunikace pachatele se svojí potenciální obětí. Cílem těchto útoků je psychická manipulace oběti, převážně se jedná o plánovaný útok na děti. Útočník neboli kybergroomer[32] (dospělý uživatel) se snaží vyvolat ve své oběti falešnou důvěru a tuto potenciální oběť přemlouvá a manipuluje k osobní schůzce. Toto chování má prvky zejména sexuálních trestných činů, nebezpečné vydírání, navazování nedovolených kontaktů s dítětem.[33]

Jak již bylo řečeno, pachatelem této trestné činnosti je většinou dospělá osoba, která se snaží psychicky manipulovat svojí oběť. K jejich seznámení dochází převážně na sociální síti, online hrách, chatovacích místnostech, internetových seznamkách, ale také například na stránkách s nabídkou modelingu. Pachatel se snaží ve své oběti vyvolat falešnou důvěru, chce navázat přátelství, být s obětí kamarád. Pokud se mu toto začne dařit, snaží se z oběti vylákat osobní údaje, telefonní kontakt. Poté může začít tuto oběť uplácet různými dárky. Kupuje kredity do mobilu, platí předplatné online her a podobně.[34]

Oběť poté začne pachateli důvěřovat. Pachatel manipulaci zintenzivňuje a poté může dojít i k osobnímu útoku, pokud oběť podlehne a jde na schůzku s pachatelem. Také zde může mezi pachatelem a obětí docházet k eroticky laděné komunikaci, kdy oběť pošle pachateli své erotické fotografie. Následně nato začne pachatel svojí oběť vydírat, kdy vyhrožuje, že tyto poslané fotografie zveřejní či pošle kamarádům obětí a žádá další zaslané erotické fotografie či požaduje již zmíněnou osobní schůzku. Oběť (dítě) se dostává do začarovaného kruhu a může se stát, že pachateli vyhoví a na sjednanou schůzku s ním jde. Největším problémem při objasňování tohoto trestného činu je jeho obtížné zjišťování, dokazování a skutečnost, že v počátečním stádiu se ve většině případů nejedná o trestný čin, zejména tam, kde není trestná forma jeho přípravy.[35]

---

[32] Kybergroomer je zpravidla sexuální útočník, který k prosazení svého cíle využívá IT prostředí.
[33] VÁLKOVÁ, Helena, KUCHTA, Josef a Jana HULMÁKOVÁ. *Základy kriminologie a trestní politiky*. 3. vydání. Praha: C. H. Beck, 2019. Beckovy mezioborové učebnice. ISBN 9788074007323. [s. 537].
[34] INTERNÍ MEDICÍNA. *Strategie Manipulace dětí v online prostředích* [online]. 2023 [cit.2023-02-21]. Dostupné z: https://www.internimedicina.cz/pdfs/ped/2015/05/09.pdf
[35] VÁLKOVÁ, Helena; KUCHTA Josef a Jana HULMÁKOVÁ. *Základy kriminologie a trestní politiky*.

Proto také můžeme konstatovat, že kybergrooming není pojmem trestně právním, ale je pojmem kriminologickým. Dle trestního zákona ovšem můžeme kybergrooming přiřadit pod skutkovou podstatu § 193 odst. b[36]. Provedenou novelou trestního zákoníku číslo 141/2014 Sb. se toto podařilo toto napravit. Tato novela vstoupila v platnost dne 22. července 2014 s účinností od 1. srpna 2014. Jedná se o odkazující skutkovou podstatu. Ve svém ustanovení odkazuje na trestné činy svádění k pohlavnímu styku, pohlavní zneužití, zneužití dítěte k výrobě pornografie či výroba a jiné nakládání s dětskou pornografií. Jak již bylo zmíněno, před touto důležitou novelou bylo možné kybergroomingu postihnout převážně v souvislosti s výrobou dětské pornografie, ohrožováním výchovy dítěte v důsledku sexuální komunikace přes IT prostředky a svádění k pohlavnímu styku a zasíláním pornografie dítěti. Co se týkalo samotného jednání, které by vedlo k přímému setkání pachatele a oběti, bylo trestně postižitelné pouze jako příprava znásilnění a proto to také bylo velice obtížné zdokumentovat či dokazovat skutečný úmysl pachatele. Tato nová úprava trestního zákona §193 odst. b[37] rovnou míří na začátek tohoto setkání, tedy už na jeho návrh, ale i zde musí samozřejmě být prokázán úmysl pachatele svojí oběť nějakou formou sexuálně využít.[38]

Touto novelou trestního zákona se hlavně docílila ochrana dětí mladších 15 let před tzv. sexuálním vykořisťováním. Objektivní stránka tohoto strastného činu spočívá v jednání pachatele, který se pokusí nebo navrhne setkat se s dítětem mladším 15 let s úmyslem spáchat nějaký z řad trestných činů, ve kterém § 193 odst. b[39] odkazuje ve svém ustanovení. Pokusem či návrhem setkání je však bráno jako aktivní činnost pachatele, který směřuje k dítěti, které je mladší než 15 let snahu v něm vzbudit a rozhodnout se, aby se zúčastnilo osobnímu setkání, kdy účelem je následně spáchání nějakého výše uvedeného trestného

3. vydání. Praha: C. H. Beck, 2019. Beckovy mezioborové učebnice. ISBN 9788074007323. [s. 537].

[36] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

[37] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

[38] Trestní zákoník, § 193b zákona č. 40/2009 Sb., ve znění pozdějších předpisů

[39] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

činu, který je uveden pod § 193 b[40] nebo spáchání jiného trestného činu se sexuální motivací. V praxi se jedná převážně o navázání kontaktu pomocí IT technologií a kyberprostoru. Tímto pachatelem může být jak fyzická osoba, tak i právnická osoba. V případě pohledu na subjektivní stránku je vyžadováno zavinění formou úmyslu, kdy obligatorním znakem pro spáchání trestného činu je sexuální motiv.[41]

Mezi nejčastější oběti tohoto trestného činu jsou děti a mládež ve věku 10 – 17 let. Pachatelé si tyto oběti cíleně vybírají a tento věk vědí hned od prvního kontaktu s obětí. Dívky jsou vystaveny těmto útokům častěji než chlapci. Oběti kybergroomingu jsou převážně uživatelé internetu a to hlavně děti. Tyto děti tráví, většinu svého volného času v kyberprostoru. Jsou neustále online, mají mnoho účtů na sociálních sítích, dále se věnují hraní online her. Jsou prostě součástí virtuálního prostředí a to bez jakéhokoliv dozoru rodičů či odpovědných osob za jejich výchovu. Zde neustále navazují nové kontakty a to také i s cizími lidmi. Jejich motivem může být buď hledání nových kamarádů či přátel, nebo komunikace se svými vrstevníky.[42] V tomto mladém věku jsou tyto potenciální oběti velmi důvěřivé, hledají pozornost či náklonnost, která jim může v osobním životě chybět. Jsou proto pro útočníka velmi lákavým a mnohdy i snadným cílem.[43]

Nejčastější obětí kybergroomingu jsou:

- Děti a mladiství ve věku od 11 do 17 let převážně ženského pohlaví, osamělé, trávicí mnoho svého volného času v kyberprostoru.
- Většinou se jedná o osoby s nedostatkem kritického myšlení, nepoučené, nevyzrálé, se sníženou sebeúctou.
- Nesmíme také zapomenout na to, že těmito obětmi se také mohou stát senioři.[44]

Pachatel komunikuje se svojí obětí převážně jednostranně. V počátcích této

[40] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
[41] ŠÁMAL, Pavel. *Trestní právo hmotné. 7*., přepracované vydání. Praha: Wolters Kluwer, 2014. ISBN 9788074786167. [s. 627].
[42] KOPECKÝ, Kamil. *Kybergrooming - nebezpečí kyberprostoru*. Olomouc: Net University, 2010. ISBN 978-80-254-7573-7. [s. 4].
[43] INTERNÍ MEDICÍNA. *Strategie Manipulace dětí v online prostředích* [online]. 2023 [cit. 2023-02-21]. Dostupné z: https://www.internimedicina.cz/pdfs/ped/2015/05/09.pdf
[44] KOPECKÝ Kamil. *Moderní trendy v elektronické komunikaci*. Olomouc: Hanex, 2007. ISBN 978-80-85783-78-0. [s. 68]

konverzace je aktivnější. Komunikuje pod falešnou identitou, zároveň se vydává za jinou osobu, než sám je. Pokud se například snaží kontaktovat 12 letou dívku, začne se vydávat za 14 letého chlapce. Po nějaké době začíná tato jednostranná komunikace přecházet v dialog. V této době oběť buď komunikaci ukončí a setkání s tímto predátorem je pouze online, nebo může dojít k plánování a uskutečnění reálné schůzky mezi pachatelem a obětí. Pachatel dokáže ve svém přesvědčování být velmi naléhavý a neodbytný a oběť proto může tomuto nátlaku po nějaké době podlehnout.[45]

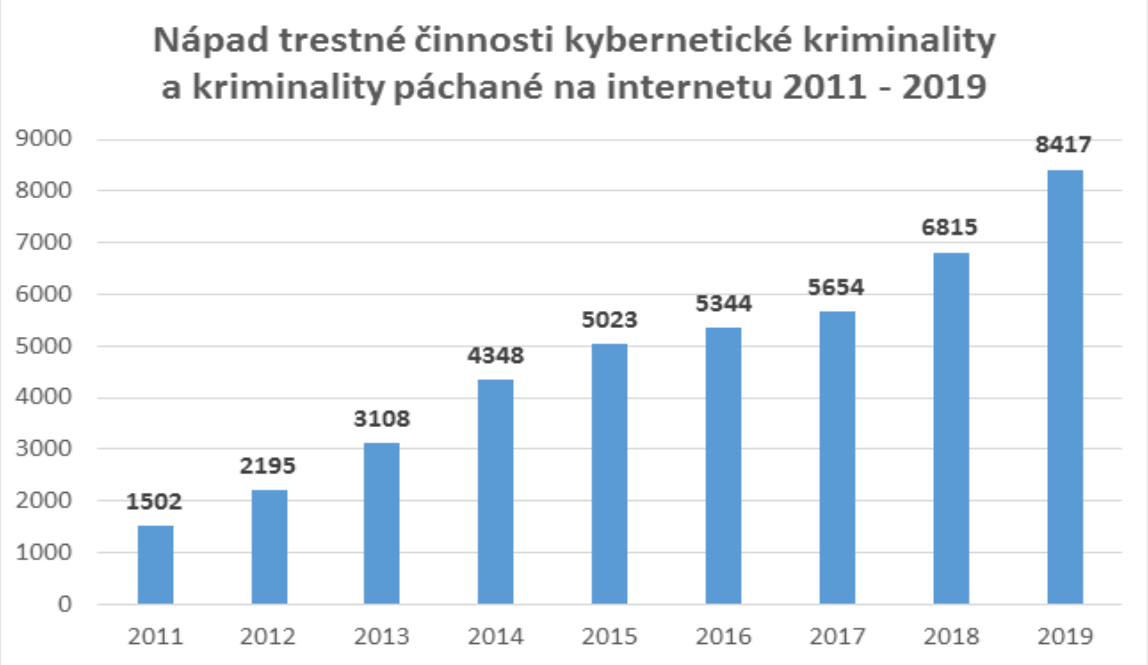
Kdo je pachatelem této trestné činnosti? Na tuto otázku nelze přesně odpovědět. Jedná se o lidi s různým sociálním statutem. Může jít o člověka vysokoškolsky vzdělaného, ale také o osobu se základním vzděláním. Jsou mezi nimi jak prvopachatele, tak recidivisti, kteří byli již za trestný čin stíháni a také odsouzeni. Společnou vlastností těchto pachatelů je patologický zájem o děti a mladistvé. Další povahovou vlastností těchto pachatelů je, že mají v reálném světě problémy se seznamovat, komunikovat či navazovat vztahy s dospělými lidmi. Proto svůj zájem komunikovat přesouvají převážně do kyberprostoru, je to pro ně jednodušší a z jejich pohledu také bezpečnější a anonymní.[46]

Jak jsem již zmínil, pachatele kybergroomingu můžeme zhruba rozdělit na dvě skupiny. První skupinou jsou ti, kteří usilují pouze o sexuální uspokojení a to jen v kyberprostoru a se svojí potenciální obětí se v reálu setkat nechtějí. Druhou skupinou jsou pachatelé, kteří se od prvního kontaktu snaží oběť přemluvit k osobní schůzce s cílem jejího sexuálního zneužití.[47]

Je možná prevence kybergroomingu? Na tuto otázku můžeme kladně odpovědět. Ovšem důležitou roli v tomto sehrává hlavně rodina. Rodiče totiž mohou tomuto úspěšně předejít důslednou a pravidelnou kontrolou činnosti svých dětí a to hlavně v době jejich volného času. Důležité je pravidelně s dětmi komunikovat o tom, s kým se v kyberprostoru setkávají, s kým si píšou či volají. Musí se informovat také o tom, jaké nástrahy na ně mohou v tomto prostředí čekat

[45] KUDRLOVÁ, Kateřina. *Kybergrooming* – 3 roky kriminalizace. Právo, Bezpečnost, Informace. 2017, číslo 4. ISSN 2336-3657. [s. 65]
[46] CHOO, Kim-Kwang Raymond. Online child grooming:a literature review on the misuse of social networking sites for grooming children for sexual offences [online]. 2009 [cit. 2022-10-21]. ISBN 9781921185861. Dostupné z: https://www.aic.gov.au/sites/default/files/2020-05/rpp103.pdf
[47] KOPECKÝ, Kamil a kol. *Rizikové formy chování českých a slovenských dětí v prostředí internetu*. 1. vyd. Olomouc: Univerzita Palackého v Olomouci, 2015. ISBN 978-80244-4868-8. [s. 170]

a jak se jim můžou bránit či je eliminovat.[48] Přiložený obrázek č. 1 graficky znázorňuje nápad trestné činnosti kybernetické kriminality za období od roku 2011 do 2019.



Obrázek č. 1 – Nápad trestné činnosti za roky 2011-2019 [49]

1.2 Kyberkriminální techniky

Počítač, tablet, notebook či chytrý mobilní telefon připojený k internetu má v dnešní době prakticky každý člověk. Proto také každý tento uživatel v kyberprostoru zanechává svojí digitální stopu, digitální otisk ač si je tohoto vědem či ne. Pro potenciální útočníky je proto v kyberprostoru mnoho cílů a rok od roku přibývá mnoho nových případů. Cracker (útočník) pro úspěšné napadení svých cílů používá mnoho různých technik a postupů, které můžeme celkově označit za kybernetické útoky. Mezi nejznámější tyto metody patří:[50]

[48] ZORMANOVÁ, Lucie. *Kybergrooming* [online]. 1.3.2022 [cit. 2023-01-14]. Dostupné z https://clanky.rvp.cz/clanek/22970/KYBERGROOMING.html
[49] E-BEZPEČÍ. *Nápad trestné činnosti kybernetické kriminality*, [online]. 22.1.2020 [cit. 2023-1-18]. Dostupné z: https://www.e-bezpeci.cz/index.php/z-jinych-webu/1749-statistika-kyberneticke-kriminality-za-rok-2019
[50] AIRA. *Co je kyberkriminalita* [online]. 2022 [cit. 2023-01-05]. Dostupné z: https://www.sprava-site.eu/kyberkriminalita/

Brute force

Tento termín lze také popsat jako „brute attack“. V našem prostředí si jej můžeme přeložit jako útok hrubou silou. Jedná se o velice specifický druh kyberútoků se zaměřením na prolamování uživatelských hesel. Je to vlastně pokus o prolomení méně složitých hesel do aplikací a počítačových systémů. K tomuto útoku se používají speciálně navržené programy, které se snaží hrubou silou uživatelovo heslo uhádnout a tím ho prolomit. Pokud se prolomení hesla podaří, útočník se poté snadno dostane k uživatelským datům, e-mailům či bankovním účtům a může tak dojít k nelegální krádeži uživatelských dat či peněz. Princip tohoto útoku si můžeme pospat tak, že prolamovač hesel se snaží uživatelovo heslo uhodnout, zkouší nejprve kombinace ze slovníku hesel a poté náhodné kombinace čísel a písmen. Čím má hacker na toto dost času a čím je výpočetní kapacita počítače hackera lepší, tím je vyšší pravděpodobnost úspěchu prolomení. Ovšem nejlepší ochranou proti tomuto napadení je silné uživatelské heslo, které nejde prolomit anebo jeho prolamování by teoreticky mohlo trvat až několik stovek let, a to je samozřejmě technicky nemožné.[51]

Sniffing

Jedná se o speciální techniku kyberútoků, při které se pachatel snaží odposlouchávat počítače v lokální síti. Slovo „sniff“ je možné přeložit jako čenichat. Princip tohoto útoku je odposlech, ukládání a následné čtení TCP síťových paketů používaných převážně při diagnostice sítě. Nemusí se jednat pouze o speciální programy, ale existuje i hardware, který takto monitoruje provoz počítačové sítě. Pokud se o tento útok pokusí zkušený pachatel, může mít úspěch. Mohl by takto získat používaná uživatelská hesla, či může nerušeně a přitom samozřejmě skrytě sledovat tok příslušné datové komunikace či provoz celé firemní sítě. Tento postup tudíž začne přinášet útočníkovi velice potřebné informace, které pak mohou být použity pro řadu dalších potenciálních útoků, a to formou botnetu, síťového viru či DDoS útoku. Další podpůrný program hackera pro tuto specifickou činnost je i trojský kůň, protože může být primárně upraven na funkci upravenou pro techniku sniffování. Sniffing tudíž vlastně do jisté míry supluje činnost spywaru či

[51] AIRA. *Co je kyberkriminalita* [online]. 2022 [cit. 2023-01-05]. Dostupné z: https://www.sprava-site.eu/kyberkriminalita/

keyloggeru. Celkově tento software umožňující sniffing můžeme pojmenovat sniffer.[52]

Backdoor

V překladu můžeme tento druh útoku nazvat jako zadní vrátka. Útočník pomocí tohoto speciálního programu může velmi snadno a rychle převzít kontrolu nad takto infikovaným počítačem. Backdoor se do napadeného počítače nejčastěji dostane pomocí speciálního trojského koně. Uživatel takto napadeného počítače ve většině případů nic nepozná a ani nemá moc možností si takto vedeného útoku všimnout. Princip tohoto útoku totiž spočívá v obcházení standartních autentizačních a certifikačních mechanismů a protokolů v napadeném zařízení. Pokud se útok podaří, cracker (útočník) si může prohlížet data v napadeném zařízení, může je kopírovat, měnit, mazat, může například i na dálku otevírat a zavírat DVD mechaniku, tisknout na připojené tiskárně a podobně. Tento počítač se pak cracker může pokusit připojit do sítě botnetu. Jedná se o speciální síť takto napadených PC, tyto PC mají společně velmi vysoký výpočetní výkon a mohou tak sloužit jako zhoubný nástroj pro DDoS útoky na internetu či rozesílání spamu nebo těžbu kryptoměn. Jako tyto zadní vrátka do systému můžeme též označit chyby v programových kódech běžících programů na počítačích.[53]

Keylogger

Keylogger může být speciální program nebo také hardwarový prvek připojený k PC. Princip tohoto útoku spočívá v detekci a ukládání veškerých stisknutých kláves, který uživatel v takto napadeném zařízení udělá. Tyto údaje se většinou rovnou ukládají do textového souboru, se kterým pak útočník pracuje a snaží se z něho vyčíst uživatelsky přístupové údaje a hesla. Hardwarový keylogger útočník musí fyzicky připojit k PC a poté si ho musí zase odnést a vyhodnotit jej. Většinou se vkládá mezi klávesnici a počítač, jde o velmi sofistikované a miniaturní zařízení a běžný uživatel si ho nemá šanci vůbec všimnout a není proti němu prakticky obrana. Zatímco proti softwaru může zasáhnout antivirové zabezpečení

[52] AIRA. *Co je kyberkriminalita* [online]. 2022 [cit. 2023-01-05]. Dostupné z: https://www.sprava-site.eu/sniffing/
[53] AIRA. *Co je kyberkriminalita* [online]. 2022 [cit. 2023-01-05]. Dostupné z: https://www.sprava-site.eu/backdoor/

napadaného zařízení v počátku potenciální infekce. Druhou alternativou je software, jedná se hlavně o upravený malware, kterým útočník infikuje napadený počítač a takto tiše, nerušeně, a dálkově ukládá uživatelská data z napadaného PC a ty pak dále vyhodnocuje. Do napadeného počítače se tento červ opět dostane pomocí trojského koně. Útočník se snaží takto ukrást citlivá data, jako jsou důvěrné informace, hesla k internetovému bankovnictví, e-mailové schránce, uživatelským účtům na sociálních sítích a podobně. Pokud je tento útok úspěšný, cracker tyto zcizené informace většinou dostane a ty pak zneužije k dalším kyberútokům.[54]

Hoax

Hoax se šíří většinou prostřednictvím e-mailů či sdílením pomocí odkazů na sociálních sítích. Jedná se o podvrženou, falešnou mystifikující zprávu. Tato zpráva většinou upozorňuje či varuje před neexistujícím či smysleném nebezpečím, nebo se snaží řešit nějaký domnělý problém. Velké riziko spatřuji také v tom, že mnoho lidí, kteří si takto zaslanou zprávu otevřou, jejímu obsahu uvěří a jsou proto vystaveni dezinformacím. Takto upravené zprávy můžeme proto zařadit pod škodlivé programy, které se též označují jako malware. Můžeme proto hoax též označit jako specifickou formu spamu neboli nevyžádané pošty. Principiálně je v této zaslané zprávě uvedena výzva, aby zpráva byla dále šířena co největšímu počtu uživatelů na internetu. Šíření tohoto malwaru tak nevědomky napomáhají samotní uživatelé. Řetězové přeposílání těchto nevyžádaných zpráv má ale i jiná rizika než dezinformace. Výpočetní kapacita poštovních serverů má v důsledku toho velmi vysokou zátěž. Dalším rizikem je to, že uživatel, který tyto zprávy dále přeposílá, tam ponechává všechny dříve vyplněné e-mailové adresy a hacker proto může dále zasílat e-mailové škodlivé červy cíleně. Seznam takto získaných e-mailových adres může být velmi obsáhlý.[55]

Phishing

Tento název se může v principu odvodit z anglického slova fishing, neboli

[54] AIRA. *Co je kyberkriminalita* [online]. 2022 [cit. 2023-01-05]. Dostupné z: https://www.sprava-site.eu/keylogger/
[55] AIRA. *Co je kyberkriminalita* [online]. 2022 [cit. 2023-01-05].]. Dostupné z: https://www.sprava-site.eu/hoax/

rybolov. Jedná se o velmi sofistikovanou a neméně nebezpečnou kriminální techniku, rozesílání podvodných e-mailů. Hlavním účelem je vylákání z potenciální oběti citlivých informací a dat, a ty pak následně zneužít. Cílem toho útoku jsou data typu PIN kód, přihlašovací údaje do internetového bankovnictví, čísla kreditních karet. Tyto nevyžádané zprávy většinou rozesílá spammer a cracker v jedné osobě a to formou spamu. Je to velmi účinná a poměrně jistá forma kyberútoků. Tímto útokem je vždy naráz zasaženo velké množství uživatelů a jeho úspěšnost se uvádí okolo 5 %, což je poměrně vysoké statistické číslo. První tento útok v ČR byl v roce 2006 a byl zaměřen proti CitiBank.[56]

Pharming

Jedná se o profesionální podvodnou kybertechniku, při které se útočník snaží nelegálně dostat k citlivým a důležitým údajům a přihlašovacím heslům jednotlivých uživatelů. Můžeme konstatovat, že Pharming je mladší vylepšená technika phishingu. Pomocí této crackerské metody dochází například k přesměrování jednotlivých oficiálních serverů bankovních institucí či obdobných společností na falešné stránky. Z těchto upravených stránek se do počítače oběti pokusí proniknout podstrčený spyware. Technicky jde o speciální útok na DNS servery a následné přepsání IP adres. Uživatel se pak snaží přihlašovat do svého internetového bankovnictví a vůbec netuší, že se přihlašuje na jiném serveru, který se tváří jako původní domovská stránka banky. Takto získané citlivé údaje hacker ihned začne zneužívat a útočník tak získá plný a kompletní přístup k bankovním účtům svojí oběti. Následně nato ihned začne z takto napadených účtů převádět finanční prostředky na další zahraniční konta či začne nakupovat kryptoměny. Tyto peněžní transakce jsou pak již prakticky nedohledatelné. [57]

1.3 Projevy kybernetické kriminality s odkazem na trestní zákoník

V hlavě V trestního zákoníku, „Trestné činy proti majetku“ se nachází převážně trestné činy proti důvěrnosti, dostupnosti a integritě počítačových dat a systémů. Dále zde máme trestné činy upravené zákonem č 40/2009 Sb[58].,

[56] AIRA. *Co je kyberkriminalita* [online]. 2022 [cit. 2023-01-05]. Dostupné z: https://www.sprava-site.eu/phishing/
[57] AIRA. *Co je kyberkriminalita* [online]. 2022 [cit. 2023-01-05]. Dostupné z: https://www.sprava-site.eu/pharming/
[58] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z:

o trestní zákoník páchané ve vztahu k uloženým informacím. Jedná se zejména o tyto paragrafy:

- Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230[59]).
- Přechovávání a opatření přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231[60]).
- Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232[61]).[62]

Páchané ve vztahu k datům (uloženým informacím), při nichž je počítač prostředkem k jejich páchání:

- Šíření pornografie (§ 191[63]).
- Výroba a jiné nakládání s dětskou pornografií (§ 192[64]).
- Navazování nedovolených kontaktů s dítětem (§ 193b[65]).
- Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi (§ 270[66]).
- Hanobení národa, rasy, etnické nebo jiné skupiny osob (§ 355[67]).
- Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod (§ 356[68]).
- Šíření poplašné zprávy (§ 357[69]).

---

https://www.zakonyprolidi.cz/cs/2009-40

[59] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

[60] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

[61] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

[62] POLICIE ČESKÉ REPUBLIKY. *Jednotlivé druhy kyberkriminality* [online]. 2022 [cit. 2023-01-05]. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

[63] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

[64] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

[65] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

[66] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

[67] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

[68] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

[69] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

Lze konstatovat, že trestní zákoník naplňuje v uvedených ustanoveních závazky z Úmluvy Rady Evropy o kybernetické kriminalitě a to rámci rozhodnutí Rady EU 2005/222/SV o útocích na informační systémy. Pomocí dalších mezinárodních smluv a právních aktů EU se ČR zavazuje k provedení závazků týkajících se veřejně přístupné počítačové sítě. Jedná se například o úmluvu o ochraně dětí před sexuálním vykořisťováním a zneužíváním, dále jde o rámcové rozhodnutí Rady 2000/375/JHA o boji proti dětské pornografii na internetu. Co se týká neoprávněného přístupu ke komunikaci jiného včetně nezákonného odposlechu, toto převážně řeší ustanovení (§182[70]) porušení tajemství dopravovaných zpráv. V jiných případech také můžeme takové jednání kvalifikovat i jako § 230[71] zmíněný výše.[72]

1.4 Dopady globální pandemie koronaviru na kyberkriminalitu

Nemůžeme zde také ovšem opomenout faktor globální pandemie koronaviru. V tomto období trestných činů páchaných v kyberprostoru samozřejmě řádově přibylo. Je to dáno hlavně tím, že firmy a instituce v tomto čase zavedly u svých pracovníků „home office“ a další podobné distanční a online spolupráce. Toto vše samozřejmě přineslo potenciálním útočníkům mnoho příležitostí ke kyberútokům.[73] Statisticky tak můžeme potvrdit, že četnost těchto trestných činů v době pandemie jen rostla. Ušetřeny v tomto směru samozřejmě nejsou ani nemocnice či orgány veřejné správy a v neposlední řadě i na školy.[74]

Proto v tomto období na tento specifický druh trestných činů také zareagoval i Nejvyšší soud ČR a to prostřednictvím judikatorního vývoje. Ze začátku byly trestné činy spáchané v době nouzového stavu hodnoceny jako kvalifikované skutkové podstaty daných trestných činů (např. krádež pečiva v obchodě v době

[70] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
[71] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
[72] POLICIE ČESKÉ REPUBLIKY. *Jednotlivé druhy kyberkriminality* [online]. 2022 [cit. 2023-01-05]. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx
[73] MALÝ, Jan. *Kyberkriminalita v době krize se zaměřením na pachatele* [online]. 10.12.2021 [cit. 2023-01-20]. Dostupné z: https://advokatnidenik.cz/2021/12/10/kyberkriminalita-v-dobe-krize-se-zamerenim-na-pachatele-pravnicke-osoby/#_ftn5
[74] VACOVSKÝ, Marek. *Rok 2020 přinesl více kybernetických útoků* [online]. 1.3.2021 [cit. 2023-02-01]. Dostupné z: https://mobilenet.cz/clanky/rok-2020-prinesl-krome-pandemie-koronaviru-i-vice-kybernetickych-utoku-na-nemocnice-43079

nouzového stavu byla trestána až několika lety odnětí svobody). Naopak později, s důrazem na materiální pojetí trestného činu, se od této aplikace kvalifikovaných skutkových podstat prakticky upouští. V případě kyberkriminality tomu není jinak. V případě materiálního pojetí u například majetkových trestných činů, nelze při kladení tohoto důrazu dojít, a měl by být en bloc využit pro přijetí kteréhokoliv trestného činu, spáchaného v mimořádné době například v době nouzového stavu. Proto toto hodnocení platí i pro trestné činy spáchané v kyberprostoru či s kyberprostorem související.[75]

Jelikož byl v této době také vydán zákaz vycházení v určitou denní dobu či zákaz vstupu do vybraných prostor, docházelo tímto k déle trvajícímu zdržování a pobytu osob v místě jejich bydliště a s tím samozřejmě úzce souvisí i více prostoru pro možné páchání trestné činnosti ať už recidivisty či prvopachateli. Trestné činy spáchané v tomto období je poté možno teoreticky rozdělit do několika kategorií. Jedná se převážně o tyto:

- Jedná se hlavně o trestné činy spáchané ze strachu.
- Dále jde o trestné činy využívající zavedení nouzového stavu v souvislosti s pandemií koronaviru.

Obě tyto kategorie je samozřejmě možné také spáchat i v kyberprostoru.[76]

1.5 RDP protokol a jeho rizika

Jak jsem již v předešlých kapitolách uvedl, v době globální pandemie koronaviru firmy a instituce ve velké míře zavedly využívání HOME OFFICE a dali tak svým zaměstnancům možnost využívat svěřenou výpočetní techniku pro práci z domova a tak se připojovat do firemních sítí dálkovým přístupem.

V této kapitole se budu podrobněji věnovat RDP protokolu. Jedná se o Remote Desktop Protokol a v informatice jde o síťový protokol, pomocí kterého může uživatel využívat či ovládat vzdálený počítač prostřednictvím počítačové sítě. Toto vzdálené připojení pracuje na principu klient-server. Uživatel se prostřednictvím klienta vzdáleně připojí do cíleného počítače. Tyto programy jsou

[75] MALÝ, Jan. *Kyberkriminalita v době krize se zaměřením na pachatele* [online]. 10.12.2021 [cit. 2023-01-20]. Dostupné z: https://advokatnidenik.cz/2021/12/10/kyberkriminalita-v-dobe-krize-se-zamerenim-na-pachatele-pravnicke-osoby/#_ftn5

[76] MALÝ, Jan. *Kyberkriminalita v době krize se zaměřením na pachatele* [online]. 10.12.2021 [cit. 2023-01-20]. Dostupné z: https://advokatnidenik.cz/2021/12/10/kyberkriminalita-v-dobe-krize-se-zamerenim-na-pachatele-pravnicke-osoby/#_ftn5

velmi populární. Existují také verze pro různé operační systémy, i pro mobilní telefony či tablety.[77]

Zmiňovaný protokol vzdálené plochy se v dnešní době stal důležitým nástrojem pro správu podnikových sítí v nové začínající éře hybridních a sdílených pracovišť. Samozřejmě, že z pohledu kyberzločinců se tento protokol stává velmi lákavým cílem k napadení.[78] Hackeři se tak snadněji mohli dostat do podnikových sítí a k citlivým datům pracovníků. Dostupné informace z posledního ESET Threat Reportu[79] nám jasně ukazují, že počet incidentů u koncových zařízení využívajících RDP protokol v posledních dvou letech neustále rostl. Z výsledků měření vyplývá, že za období od ledna do dubna roku 2022 bylo takto zaznamenáno na 121 miliard pokusů o tyto útoky. Princip těchto útoků spočívá v tom, že se útočníci připojují pomocí již zmiňovaného protokolu RDP k Windows serverům z internetu a poté se úspěšně přihlašují jako správci napadených počítačů. K tomuto útoku přitom využívají celou řadu zranitelností atakovaných počítačů. Jakmile se těmto útočníkům podaří proniknout do systému, mohou zjistit jak, kdy a kým je tento serverový systém používán.

Nejpoužívanější útoky prostřednictvím protokolu RDP jsou zejména:

- Instalace škodlivého kódu jako je ransomwaru.
- Instalace speciálního softwarového programu s vybavením, pro vzdálené ovládání počítače, který zajistí přístupy k napadeným serverům a datům, i v případě zjištění pomocí RDP.

Jako prevenci proti a detekci tohoto Tunelování RDP by se proto měly organizace zaměřit na mechanismy a následné detekci založené na hostiteli i na síti. Jako další krok prevence se dále doporučuje zakázání služby vzdálené plochy na všech pracovních stanicích a systémech koncových uživatelů. Dále se doporučuje

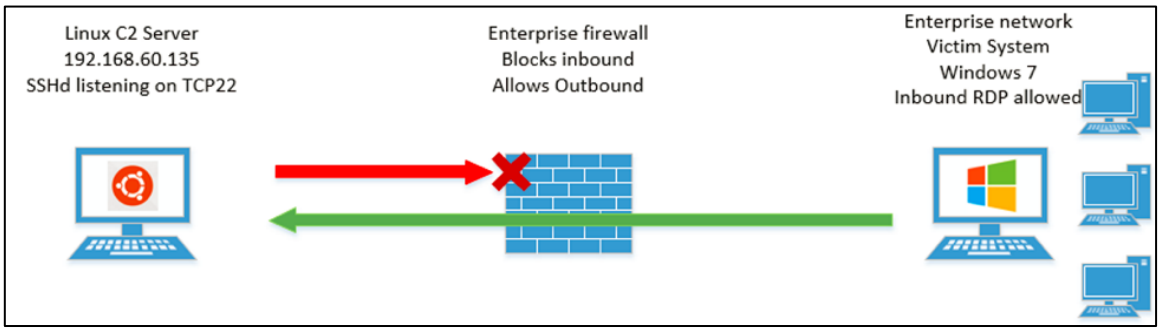
[77] ESET, Digital Security. *Jak chránit firmu před riziky spojenými s RDP,* [online]. 21.7.2022 [cit. 2023-01-20]. Dostupné z: https://digitalsecurityguide.eset.com/cz/jak-ochranit-firmu-pred-riziky-spojenymi-s-rdp

[78] ESET, Digital Security. *Jak chránit firmu před riziky spojenými s RDP,* [online]. 21.7.2022 [cit. 2023-01-20]. Dostupné z: https://digitalsecurityguide.eset.com/cz/jak-ochranit-firmu-pred-riziky-spojenymi-s-rdp

[79] WELIVESECURITY. *THREAT REPORT T1 2022* [online]. 1.5.2022 [cit. 2023-01-20]. Dostupné z: https://www.welivesecurity.com/wp-content/uploads/2022/06/eset_threat_report_t12022.pdf

povolit pravidla firewall brány hostitele, která explicitně odmítají tento příchozí protokol RDP. [80]

Na obrázku č. 2 je detailně vyobrazeno obcházení podnikového firewallu pomocí RDP a síťového tunelování s SSH jako příklad.



Obrázek č. 2 – Obcházení podnikového firewallu [81]

[80] ESET, Digital Security. *Jak chránit firmu před riziky spojenými s RDP,* [online]. 21.7.2022 [cit. 2023-01-20]. Dostupné z: https://digitalsecurityguide.eset.com/cz/jak-ochranit-firmu-pred-riziky-spojenymi-s-rdp

[81] PANY, David a Steve MILLER. *Obcházení síťových omezení prostřednictvím tunelování RDP* [online]. 29.10.2021 [cit. 2023-01-20]. Dostupné z: https://www.mandiant.com/resources/blog/bypassing-network-restrictions-through-rdp-tunneling

2. ZÁVAŽNOST KYBERNETICKÉ KRIMINALITY

Závažnost kybernetické kriminality je různá. Samozřejmě záleží na jejím liniovém přesahu a také druhu. Svá vlastní specifika můžeme také vysledovat v rozdílech pachatelů či poškozených. V těchto skupinách jsou převážně zastoupeny jak kategorie nezletilých mladistvých, tak i mladších dospělých. Co se týká škody, tak u nejzávažnějších deliktů se tato může vyšplhat až do řádů několik milionů korun. Převážně se jedná o trestné činy podvodů, a to hlavně při obchodováním se zahraničím. Jde například o falešné a nastrčené faktury k platbám u firem, kdy tyto firmy převážně obchodují se zahraničím. Tyto nastrčené faktury jsou šířeny prostřednictvím podvodných e-mailových zpráv a falešných pokynů k platbám. Tato vlna útoků byla zacílena převážně na větší firmy s majetkovou a organizační strukturou v zahraničí. Hlavním cílem těchto útoků bylo také získání cenných dat z těchto napadených firem a to především osobních a bankovních údajů jejich majitelů. Takto získané údaje podvodníci pak využijí k podvodným bankovním převodům. [82]

Princip tohoto podvodného jednání spočíval v tom, že si pachatel záměrně vytipuje a vybere konkrétní facebookový profil žádané osoby. Podle tohoto profilu si vytvoří vlastní falešný, ale na první pohled identický profil, který kompletně zkopíruje z původního účtu. Přes tento nový profil se následně pachatel snaží kontaktovat další osoby na sociálních sítích, a to pod nastrčenou identitou. V této komunikaci se pachatel ze začátku snaží nabízet například možnost hraní her na internetu o zajímavé výhry a podobně. Cílem veškeré této komunikace je vylákat ze své potenciální oběti údaje k bankovním účtům, bankovním kartám či telefonní čísla. Po takto získaných datech následně pachatel požaduje zaslání i autorizačních kódů k provedení peněžních bankovních převodů. Pokud se pachateli podaří tyto údaje z oběti vylákat, může poté takovou osobu připravit o velké množství peněz, které okamžitě převádí na různé zahraniční bankovní účty či nakupuje kryptoměny.[83]

[82] Novinyvm.cz: *Výrazný nárůst kriminality v kybernetickém prostředí,* [online]. 29.10.2021 [cit. 2023-01-20]. Dostupné z: https://www.novinyvm.cz/18888-vyrazny-narust-kriminality-v-kybernetickem-prostredi.html

[83] Novinyvm.cz: *Výrazný nárůst kriminality v kybernetickém prostředí,* [online]. 29.10.2021 [cit. 2023-01-20]. Dostupné z:: https://www.novinyvm.cz/18888-vyrazny-narust-kriminality-v-kybernetickem-prostredi.html

Podvodníci takto využívají virtuálního prostředí a daří se jim v mnoha případech vylákat ze svých obětí finanční prostředky. Kontakt mezi pachatelem a obětí je realizován nejčastěji na internetových seznamkách, sociálních sítích či bazarových portálech. Jak již bylo řečeno, pachatelé si zřizují vlastní neexistující identitu a snaží se útočit především na city svých obětí. Ženám se například snaží nabízet seznámení s nezadanými lékaři či americkými vojáky, kteří slouží v zahraničních misích a hledají nový klidný život. [84] Jako příklad druhů a počtů této trestné činnosti může posloužit přiložený obrázek č. 3, který znázorňuje tabulku jednotlivých druhů trestné činnosti páchané v oblasti kybernetické kriminality dokumentované na Krajském ředitelství policie kraje Vysočina v roce 2020.

Typ činnosti	2016	2017	2018	2019	2020
násilná trestná činnost	9	21	14	11	12
mravnost	16	29	38	43	48
majetková trestná činnost	55	59	100	116	185
ostatní a zbývající trestná činnost	16	28	9	12	17
hospodářská trestná činnost	98	122	82	115	172
celkem	**194**	**259**	**243**	**297**	**433**

Obrázek č. 3 – Tabulka jednotlivých druhů trestné činnosti [85]

[84] Novinyvm.cz: *Výrazný nárůst kriminality v kybernetickém prostředí,* [online]. 29.10.2021 [cit. 2023-01-20]. Dostupné z: https://www.novinyvm.cz/18888-vyrazny-narust-kriminality-v-kybernetickem-prostredi.html

[85] Novinyvm.cz: *Výrazný nárůst kriminality v kybernetickém prostředí,* [online]. 29.10.2021 [cit. 2023-01-20]. Dostupné z: https://www.novinyvm.cz/18888-vyrazny-narust-kriminality-v-kybernetickem-prostredi.html

3. PACHATELÉ KYBERNETICKÉ KRIMINALITY

V této kapitole se pokusím charakterizovat vlastnosti pachatelů kybernetické kriminality. Jsou to většinou velmi kvalifikované osoby s hlubokou znalostí dané problematiky, s velmi dobrým přístupem k informačním a komunikačním technologiím. Mají svou dokonalou výpočetní techniku a znají metody jak úspěšně zakrývat svojí nelegální činnost. Tyto metody jsou velice dokonalé a profesionální. Co se týká charakteru osob, může se tak například jednat i studenty vysokých škol, kteří se díky této činnosti velice dobře živí a zároveň mají i dostatečné odborné a technické informace a zkušenosti. V prostředí studentů je i též dostatečná klientela, která má o tyto nelegální prostředky zájem. Další skupina těchto pachatelů se rekrutuje z prostředí podnikatelů. Předmětem jejich podnikání je většinou nákup a prodej výpočetní techniky. Pachatelé této trestné činnosti se v poslední době začínají organizovat do zločineckých skupin, takzvaných gangů. Šéfové těchto gangů se snaží do páchání této trestné činnosti zapojit mladé lidi, které seženou na internetu, zavazují si tak mladé, začínající hackery. Ti pak pod záštitou gangu páchají další zločiny. Většinou však díky nízkému věku nejsou trestně odpovědní.[86]

Každý počítačový hacker je ve svém nitru přesvědčen o své nadřazenosti, o své nepolapitelnosti či nepostižitelnosti. Pokud je opravdu odborník, možnost policie či počítačových expertů a administrátorů sítí je na jeho dopadení mizivá. Většinou se identifikace tohoto pachatele v internetové síti nepodaří. Není ovšem vyloučeno, že i hacker s vysokými znalostmi nemůže udělat chyby a tím umožní i své prozrazení, ustanovení a následné dopadení.[87]

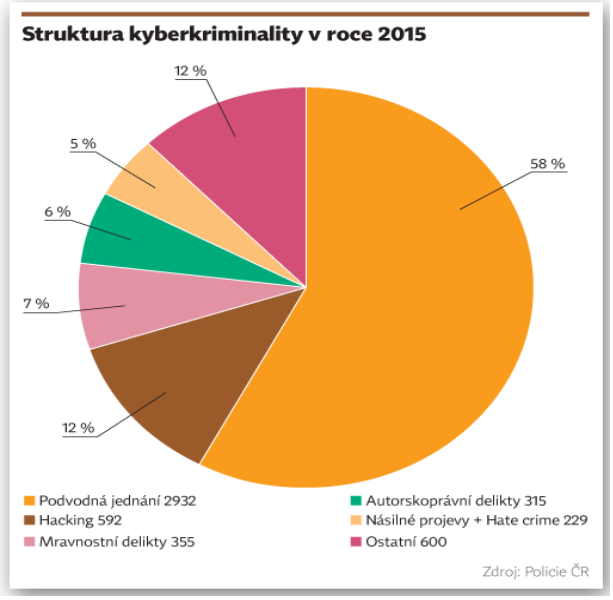
Hackeři mívají podobné povahové vlastnosti. Jsou to většinou osoby s nízkým sociálním postavením, s minimem přátel. Hacker není svým okolím mnohdy uznáván. Bývá též konfliktní, neboť se pohybuje ve velkém rozporu svého postavení, ve svém virtuálním světě a ve světě reálném. S přibývajícím věkem, a především po skončení školního vzdělání mu mohou nastat existenční potíže a také proto v tomto období dochází i ke změně svých životních priorit. Tyto důvody mohou poté vést ke změně jeho životního stylu a to k následnému

[86] POŽÁR, Josef. *Kybernetická kriminalita v organizaci* [online]. 2014 [cit. 2023-01-21]. Dostupné z: https://docplayer.cz/5380892-Kyberneticka-kriminalita-v-organizaci.html
[87] POŽÁR, Josef. *Kybernetická kriminalita v organizaci* [online]. 2014 [cit. 2023-01-21]. Dostupné z: https://docplayer.cz/5380892-Kyberneticka-kriminalita-v-organizaci.html

dobrovolnému ukončení aktivní činnosti hackera. Častým způsobem komunikace mezi hackery je též platforma IRC.[88] Jedná se o komunikaci, která probíhá v reálném čase, a to prostřednictvím počítačů. Není zde výjimkou, kdy tyto rozhovory probíhají nezašifrované, jen identita uživatelů je zastřena.[89]

3.1 Charakteristika pachatelů

Z předchozí kapitoly by se mohlo zdát, že pachatelem kyberkriminality může být pouze hacker či osoba s vysokými znalostmi IT oboru a s velmi sofistikovanou výpočetní technikou. V dnešní době tato teze již samozřejmě neplatí. Jak budu popisovat případ v praktické části své práce, pachatelem se může stát i navenek „obyčejný" člověk (student), který umí a zná použití výpočetní techniky a umí se v tomto prostředí pohybovat. Má znalosti sociálního inženýrství a umí manipulovat s lidmi. Nemusí to být tudíž opravdový IT expert, ale tak jako v našem popisovaném případě to může být student speciální vysoké školy se zaměřením na IT problematiku.[90] Na přiloženém obrázku č. 4 je znázorněná struktura kyberkriminality v ČR v roce 2015.



Obrázek č. 4 – Struktura kyberkriminality v ČR v roce 2015 [91]

[88] IRC- Internet Relay Chat. Přenos psaného hovoru s výměnou informací mezi klienty.
[89] POŽÁR, Josef. *Kybernetická kriminalita v organizaci* [online]. 2014 [cit. 2023-01-21]. Dostupné z: https://docplayer.cz/5380892-Kyberneticka-kriminalita-v-organizaci.html
[90] VEJVODOVÁ, Alžběta. *V boji proti kyberkriminality mají navrch hackeři* [online]. 17.10.2016 [cit. 2023-02-15]. Dostupné z: https://pravniradce.ekonom.cz/c1-65479680-policie-priznava-ze-v-boji-proti-kyberkriminalite-maji-navrch-hackeri
[91] VEJVODOVÁ, Alžběta. *V boji proti kyberkriminality mají navrch hackeři* [online]. 17.10.2016 [cit. 2023-02-15]. Dostupné z: https://pravniradce.ekonom.cz/c1-65479680-policie-priznava-ze-v-

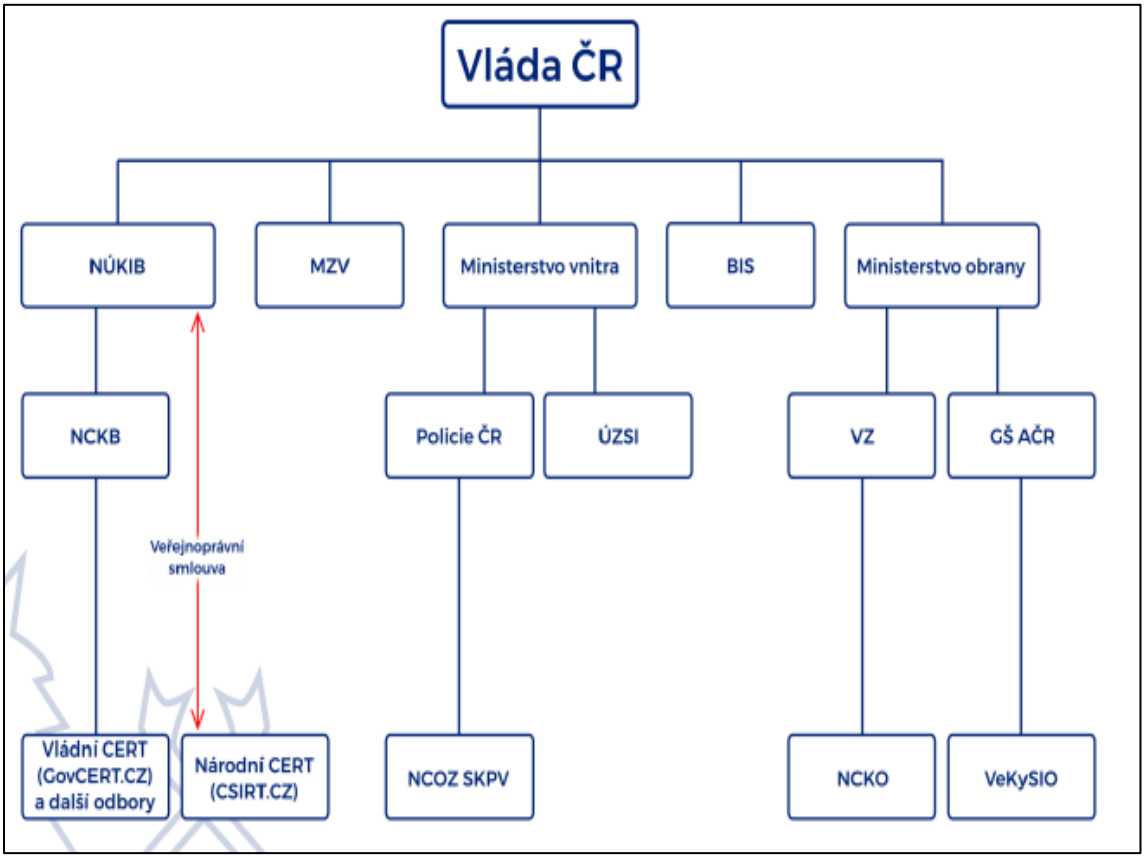
4. KYBERNETICKÁ BEZPEČNOST

Co si představit pod pojmem kybernetická bezpečnost? Jedná se o souhrn různých organizačních, politických, technických, právních a také vzdělávacích opatření a nástrojů. Vše toto směřuje k zajišťování zabezpečeného, odolného a hlavně chráněného kyberprostoru v České republice. Tato opatření jsou žádoucí jak pro subjekty veřejného a soukromého sektoru tak i pro širokou českou veřejnost. Kybernetická bezpečnost musí primárně identifikovat, vyhodnocovat a řešit hrozby v kyberprostoru. Dále musí snižovat možná kybernetická rizika, případně eliminovat dopady kybernetických útoků, informační kriminality, kyberterorismu a kybernetické špionáže. Musí tímto posilovat důvěru, integritu a dostupnost dat, důležitých systémů a dalších klíčových prvků informační a komunikační infrastruktury ČR. Můžeme proto konstatovat, že hlavním smyslem kybernetické bezpečnosti je reálná ochrana prostředí k realizaci informačních práv člověka. Tato celková ochrana již dnes výrazně přesahuje technologickou rovinu, a proto vyžaduje ucelený přístup. Při tomto řešení se proto musí brát v úvahu i specifické politické, kulturní, regionální či ekonomické a mnohé další aspekty a zájmy, které ovlivňují naší velkou závislost na IT technologiích a kyberprostoru. [92] Pro boj s kybernetickými hrozbami jsou dalším nezbytným nástrojem opatření diplomatická, právní, vzdělávací a také netechnická. Jde vlastně zjednodušeně řečeno o budování odolné informační společnosti. Jedním z nejvíce důležitým orgánem státu a státním správy v oblasti kybernetické bezpečnosti je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Přiložený obrázek číslo 5 znázorňuje schéma zajišťování kybernetické bezpečnosti v ČR.[93]

boji-proti-kyberkriminalite-maji-navrch-hackeri

[92] NUKIB. *Národní strategie kybernetické bezpečnosti* [online]. 21.6.2022 [cit. 2023-02-21]. Dostupné z: https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

[93] NUKIB. *Národní strategie kybernetické bezpečnosti* [online]. 21.6.2022 [cit. 2023-02-21]. Dostupné z: https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf



Obrázek č. 5 – Schéma kybernetické bezpečnosti v ČR[94]

4.1 Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)

Jedná se o nejdůležitější orgán kybernetické bezpečnosti a ochrany utajovaných informací v oblastech komunikačních systémů, kryptografické ochrany a také informačních systémů ČR. Tento úřad sídlí v Brně. Dále má na starosti celkovou problematiku v rámci neveřejné služby družicového systému Galileo. Úřad byl zaveden novelou zákona č. 205/2017 Sb. o kybernetické bezpečnosti, tedy zákona č. 181/2014 Sb., ve znění pozdějších předpisů a to ode dne 1. srpna 2017.[95]

[94] NUKIB. *Národní strategie kybernetické bezpečnosti* [online]. 21.6.2022 [cit. 2023-02-21]. Dostupné z: https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

[95] NUKIB. *Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)* [online]. 2023 [cit. 2023-02-21]. Dostupné z: https://www.nukib.cz/cs/o-nukib/

4.2 Výkonná sekce NÚKIB

Další výkonnou sekcí Národního úřadu pro kybernetickou a informační bezpečnosti je sekce NCKB, což je Národní centrum kybernetické bezpečnosti. Tato sekce zejména zajišťuje tyto činnosti:

- má na starost prevence před kyber hrozbami v rámci kritické informační infrastruktury, proti významným informačním systémům, informačním systémům základní služby a také vybraným systémům informatiky ve veřejné správě.
- zajištuje koordinaci v řešení kybernetických událostí v kritické infrastruktuře u provozovatelů se základní službou a orgány veřejné správy.
- má na starosti také osvětovou a vzdělávací činnost v oblasti kybernetické bezpečnosti.
- mimo jiné spolupracuje s národními i mezinárodními organizacemi podílejícími se na zajišťování bezpečnosti kybernetického prostoru.
- provádí a koordinuje výzkum a vývoj v oblasti kybernetické bezpečnosti.
- spolupracuje s kabinetem ředitele při zastupování České republiky v orgánech působících na mezinárodně v rámci oblasti kybernetické bezpečnosti.
- na starosti má také vyhodnocování rizik v oblasti kybernetické bezpečnosti a přijímaní příslušných nápravných a preventivních opatření.
- kontroluje a také plní koordinaci v mezinárodních závazcích při spolupracích na mezinárodních úrovních při realizování platných předpisů, které vyplívají při členství České republiky v EU a NATO a v jiných mezinárodních organizacích. Dále určuje a stanovuje komunikační strategii Úřadu v oblasti kybernetické bezpečnosti ve spolupráci s ostatními organizačními celky Úřadu.[96]

[96] NUKIB. *Národní strategie kybernetické bezpečnosti* [online]. 21.6.2022 [cit. 2023-02-21]. Dostupné z: https://www.govcert.cz/cs/

4.3 Kybernetická kriminalita v roce 2021 v České republice

Tak jako každý rok, tak i v roce 2022 vydalo Nejvyšší státní zastupitelství zprávu o činnosti státního zastupitelství a to za rok 2021. Tato zpráva popisuje aktivity státních zástupců v roce 2021, trendy, statistiky a také shrnuje zajímavé případy. V této zprávě se můžeme dočíst, že v roce 2021 bylo sepsáno okolo 169006 záznamů o zahájení úkonů trestního řízení proti fyzickým osobám a také 939 záznamů proti právnickým osobám, kdy z toho trestních řízení bylo vedeno proti 64364 fyzickým osobám a 326 proti osobám právnickým.[97]. Před soud se pak dostalo 59248 fyzických osob a 286 právnických osob, odsouzeno bylo 49647 osob (čtyři procenta osob bylo zproštěno). V trestních řízeních za celý rok byly zajištěny majetkové hodnoty v celkové výši 7 mld. Kč.[98]

Obrázek č. 6 – Zajištěné majetkové hodnoty v trestním řízení [99]

[97] NEJVYŠŠÍ STÁTNÍ ZATUPITELSTVÍ. *NSZ zpráva o činnosti za rok 2021* [online]. 2021 [cit. 2023-02-22]. Dostupné z: https://verejnazaloba.cz/nsz/cinnost-nejvyssiho-statniho-zastupitelstvi/zpravy-o-cinnosti/zprava-o-cinnosti-za-rok-2021/

[98] NEJVYŠŠÍ STÁTNÍ ZATUPITELSTVÍ. *NSZ zpráva o činnosti za rok 2021* [online]. 2021 [cit. 2023-02-22]. Dostupné z: https://verejnazaloba.cz/nsz/cinnost-nejvyssiho-statniho-zastupitelstvi/zpravy-o-cinnosti/zprava-o-cinnosti-za-rok-2021/

[99] NOVÁK, Jaromír. *Kybernetická kriminalita v roce 2021 očima státního zastupitelství* [online]. 28.7.2022 [cit. 2023-02-22]. Dostupné z: https://blog.nic.cz/2022/07/28/kyberneticka-kriminalita-v-roce-2021-ocima-statniho-zastupitelstvi/

Pokud se podíváme na strukturu kriminality, můžeme zde konstatovat, že stejně jako v minulých letech převažovala zejména majetková trestná činnost, následnou násilnou trestnou činnost charakterizovala stagnace (byť i v roce 2021 pachatelé páchali i agresivní a brutální trestné činy). Alarmující ovšem je, že velká část kriminality se i v roce 2021 přesunula do kyberprostoru, kdy je známo, že za výrazným růstem stojí pandemie COVID-19. Vložený obrázek č. 6 přehledně graficky znázorňuje zajištěné majetkové hodnoty za rok 2021 v trestním řízení. Celkem za rok 2021 státní zastupitelství eviduje 9518 případů kybernetické kriminality. Jedná se o 17,8 % nárůst oproti roku 2020. Mezi nejčastější řadíme podvody mezi soukromými osobami, dále je to neoprávněný přístup a poškození záznamu v počítačovém systému. Také se častěji jedná o nárůst případů o opatření a přechovávání přístupového zařízení a hesla a úvěrových podvodů. Útoků na počítačové systémy s následným vydíráním meziročně přibylo o 45 %. Co se týká investičních podvodů, těch také razantně narostlo oproti předešlému období. Jedná se zejména o podvodná jednání s legendou investice a to především do kryptoměn. Dle závěru Státního zastupitelství můžeme konstatovat, že současné odhalování specifické trestné činnosti v kyberprostoru se jeví jako mimořádně komplikované a velmi těžko dokazovatelné. Pouze výjimečné případy této trestné činnosti se daří jak odhalit tak poté stíhat a případně pravomocně odsoudit. Jsou to ovšem většinou případy českých pachatelů a to převážně pachatelů méně zkušených. Jsou to pachatelé, kteří nevyužívají prostředky k zakrytí své identity a kteří používají běžné bankovní účty či nákupy registrovaných komodit. Můžeme též konstatovat, že tento typ kriminality již zcela zastínil finanční trestnou činnost a projevuje se tak ve všech ostatních druzích páchané trestné činnosti.[100]

4.4 Kybernetická kriminalita v roce 2022 v České republice

V této kapitole se budu podrobněji věnovat kybernetické kriminalitě v České republice a to převážně za období roku 2022. Tato specifická trestná činnost vykazuje i v naší republice vysoký nárůst. Tento problém je však dle statistik již

[100] NOVÁK, Jaromír. *Kybernetická kriminalita v roce 2021 očima státního zastupitelství* [online]. 28.7.2022 [cit. 2023-02-22]. Dostupné z: https://blog.nic.cz/2022/07/28/kyberneticka-kriminalita-v-roce-2021-ocima-statniho-zastupitelstvi/

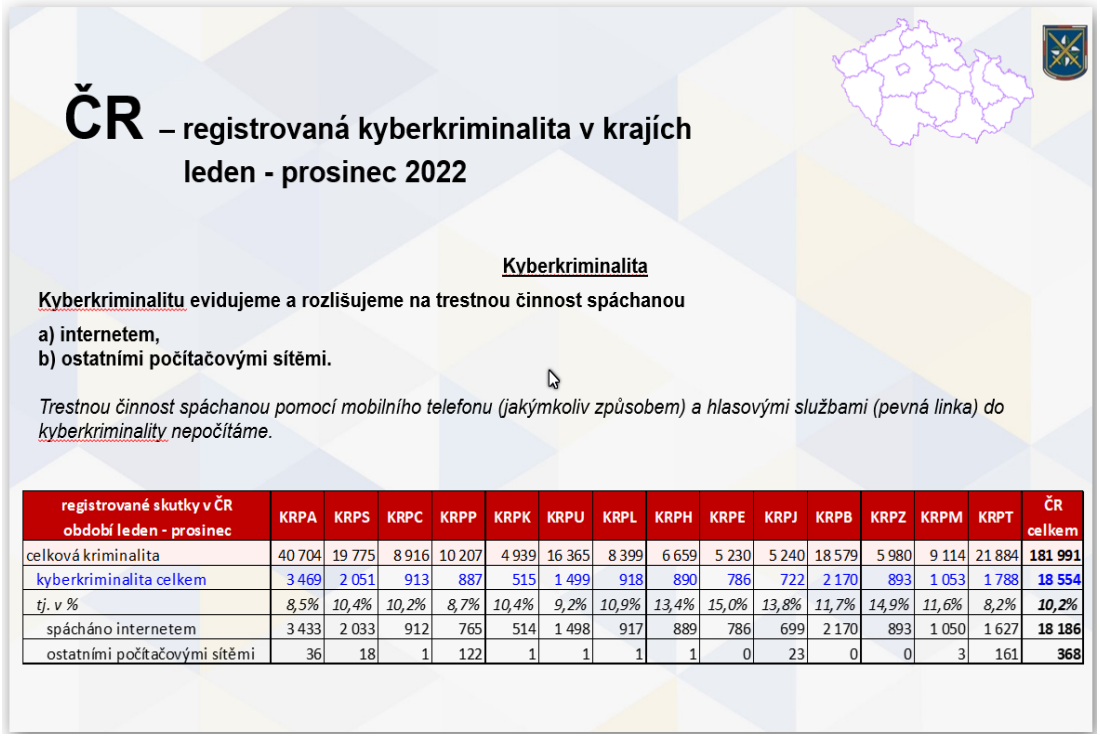
dlouhodobý. Tímto se začíná potvrzovat předpokládaný trend a to je postupný přesun většiny trestné činnosti jako takové do kyberprostoru. Můžeme zde konstatovat, že kriminalitou páchanou v kyberprostoru za období od ledna 2022 do prosince 2022 bylo celkově spácháno 18554 skutků. Tato hodnota tvoří celých 10,2 % celkové registrované kriminality. Dle statistických dat také můžeme konstatovat, že tento trend je stoupající a to meziročně až o 94,9 %.[101]

Jak již bylo řečeno, trend stálého růstu této trestné činnosti je dlouhodobý. Ke konci prosince roku 2022 stoupl meziročně počet skutků hackingu o více jak 53%. O tomto hovoří přesná data, kdy do konce prosince roku 2021 bylo evidováno 1682 těchto skutků, zatímco do konce prosince 2022 to bylo již 2575 skutků. Tato trestná činnost se samozřejmě prolíná. Určitá část těchto skutků probíhá souběhově, kdy se jedná o současné napadení e-mailových a jiných účtů. Zde jde hlavně o napadení jejich přístupových údajů, a to jak těchto e-mailových klientů, tak účtů na sociálních sítích a v neposlední řadě také napadání přístupových údajů do internetového bankovnictví. Jak již bylo několikrát řečeno, pachatelé této rozsáhlé a nebezpečné trestné činnosti využívají velice sofistikované softwarové, ale i hardwarové prostředky, pomocí nichž překonávají většinu zabezpečení a aby obětem této trestné činnosti byly kladeny co nejmenší překážky a mohly okamžitě použít chytré mobilní telefony k autorizaci a tím k dokončení například bankovních převodů. Pachatelé této trestné činnosti velmi často využívají možnost anonymních VPN přístupů do počítačových sítí, dále využívají TOR sítě a to k maximální anonymizaci skutečných svých identifikačních znaků. Pokud porovnáme jednotlivé kraje naší republiky lze konstatovat, že opětovně až dvojnásobný nárůst této trestné činnosti je stále evidován v Karlovarském kraji, a to téměř o 218 %.[102]

Důležitým cílem Policie ČR je proto především koordinace a spojování jednotlivých dílčích skutků do sérií. Tyto série následně spojovat do souvisejících větších celků. Tato praxe totiž povede k vytváření aktuálních metodických doporučení. Pomocí dalšího obrázku č. 7 je znázorněna tabulka údajů

[101] MORAVČÍK, Ondřej. *Vývoj registrované kriminality v roce 2022* [online]. 13.1.2023 [cit. 2023-02-23]. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx
[102] MORAVČÍK, Ondřej. *Vývoj registrované kriminality v roce 2022* [online]. 13.1.2023 [cit. 2023-02-23]. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx

registrované kyberkriminality v jednotlivých krajích v ČR za rok 2022.[103]



ČR – registrovaná kyberkriminalita v krajích
leden - prosinec 2022

Kyberkriminalita

Kyberkriminalitu evidujeme a rozlišujeme na trestnou činnost spáchanou

a) internetem,
b) ostatními počítačovými sítěmi.

Trestnou činnost spáchanou pomocí mobilního telefonu (jakýmkoliv způsobem) a hlasovými službami (pevná linka) do kyberkriminality nepočítáme.

registrované skutky v ČR období leden - prosinec	KRPA	KRPS	KRPC	KRPP	KRPK	KRPU	KRPL	KRPH	KRPE	KRPJ	KRPB	KRPZ	KRPM	KRPT	ČR celkem
celková kriminalita	40 704	19 775	8 916	10 207	4 939	16 365	8 399	6 659	5 230	5 240	18 579	5 980	9 114	21 884	**181 991**
kyberkriminalita celkem	3 469	2 051	913	887	515	1 499	918	890	786	722	2 170	893	1 053	1 788	**18 554**
tj. v %	*8,5%*	*10,4%*	*10,2%*	*8,7%*	*10,4%*	*9,2%*	*10,9%*	*13,4%*	*15,0%*	*13,8%*	*11,7%*	*14,9%*	*11,6%*	*8,2%*	***10,2%***
spácháno internetem	3 433	2 033	912	765	514	1 498	917	889	786	699	2 170	893	1 050	1 627	**18 186**
ostatními počítačovými sítěmi	36	18	1	122	1	1	1	1	0	23	0	0	3	161	**368**

Obrázek č. 7 – Registrovaná kriminalita v jednotlivých krajích [104]

4.5 Současná legislativa a zákony v České republice

Celkem 177 ze 193 států OSN k roku 2020 přijalo, či pracuje na specifické legislativě o kybernetické kriminalitě. To ovšem neznamená, že by věcná ustanovení národního trestního práva všech těchto zemí byla na stejné úrovni. Zpráva Rady Evropy[105] uvádí, že 106 států má z velké části hmotněprávní ustanovení trestního práva týkajících se trestných činů proti počítačové kriminalitě a prostřednictvím počítačů implementována převážně v souladu s Budapešťskou úmluvou.[106]

[103] MORAVČÍK, Ondřej. *Vývoj registrované kriminality v roce 2022* [online]. 13.1.2023 [cit. 2023-02-23]. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx
[104] MORAVČÍK, Ondřej. *Vývoj registrované kriminality v roce 2022* [online]. 13.1.2023 [cit. 2023-02-23]. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx
[105] RM. *The global state of cybercrime legislation* [online]. 5.5.2021 [cit. 2023-02-23]. Dostupné z: https://rm.coe.int/3148-1-3-4-cyberleg-global-state-feb2020-v1-public/16809cf9a9
[106] GALUŠKA, Karel. *Kybernetická kriminalita – letem světem* [online]. 20.8.2021 [cit. 2023-02-23]. Dostupné z: https://cz.linkedin.com/pulse/kybernetick%C3%A1-kriminalita-letem-sv%C4%9Btem-na%C5%A1im-pr%C3%A1vem-karel-galu%C5%A1ka

Úmluva Rady Evropy č. 185 o počítačové kriminalitě, označovaná jako Budapešťská úmluva, je první mezinárodní smlouvou o zločinech spáchaných prostřednictvím internetu a jiných počítačových sítí. K podpisu byla otevřena 23. listopadu 2001 a vstoupila v platnost 1. července. 2004. Cílem dohody je sjednocení národních úprav v oblasti kybernetické kriminality prostřednictvím povinnosti smluvních stran implementovat do svých národních právních řádů taková ustanovení, jenž umožní stíhat v Úmluvě definované kybernetické trestné činy. Vytváří se tak jednotný rámec pro společný postup proti pachatelům bez ohledu na místo spáchání trestného činu. Úmluva stanovuje jednak požadavky na opatření, která mají být přijata na národní úrovni a dále pak rámec pro mezinárodní spolupráci. Opatření, kterými se země zavazují implementovat do vnitrostátního práva, se skládají ze třech skupin:

- trestní právo hmotné.
- procesní právo.
- soudní pravomoc.

Česká republika ratifikovala Úmluvu v roce 2013. Jedná se o kompletní formulaci českého právního řádu v tématice počítačové kriminality. V roce 2014 a to konkrétně dne 29. srpna vstoupil v platnost zákon o kybernetické bezpečnosti. Jeho číslo je 181/2014 Sb. Účinnost tohoto zákona byla od 01. ledna 2015. Tento zákon mimo jiné upravuje práva a povinnosti fyzických osob a také působnost a pravomoci orgánů veřejné moci v otázce kybernetické bezpečnosti České republiky. Tento zákon také upravuje a zpracovává příslušné předpisy a zákony Evropské unie. Obecně lze proto konstatovat, že tento zákon upravuje a určuje zajišťování bezpečnosti informačních systémů, elektronických komunikačních prostředků a počítačových sítí.[107]

Nejdůležitějším účelem tohoto zákona je:

- určit a kontrolovat základní úrovně bezpečnostních opatření.
- snaha o zlepšení detekce kybernetických bezpečnostních incidentů.
- generovat a uchovávat hlášení případných bezpečnostních incidentů.
- provádět prevenci a různorodá opatření k reakci na kybernetické bezpečnostní incidenty.

[107] NUKIB.CZ: Legislativa KB, [online]. 4.1.2013 [cit. 2023-02-23]. Dostupné z https:// https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

Ani tento zákon se nevyhnul novelám. Tyto novely jsou účinné od roku 2017 a to prostřednictvím zákona č. 104/2017 Sb. Dále je zde novela z téhož roku pod číslem 183/2017 Sb, a v dalších letech následovaly novely zákonem číslo 35/2018 Sb., zákonem číslo 111/2019 Sb., dále zákonem číslo 261/2021 Sb. a poslední novelizace byla zákonem číslo 226/2022 Sb. a to s účinností k datu od 6. srpna 2022.[108]

4.6 Prevence kybernetické kriminality v České republice

V souvislosti s prevencí proti kybernetické kriminalitě můžeme s uspokojením konstatovat, že Česká republika systémově, aktivně a koordinovaně posiluje tuto prevenci a snaží se poskytovat pomoc a podporu obětem v kyberprostoru. V rámci EU dále činí Česká republika aktivní kroky směřující k plnohodnotné digitalizované společnosti. Proto je také potřebné a nezbytné, aby se prevence kybernetické kriminality, kybernásilí či kyberagrese ve virtuálním prostředí stala hlavním a strategickým cílem do následujícího období. Za poslední období se kybernetická kriminalita dlouhodobě řadí mezi nejstrměji rostoucí trestné činy v České republice. Můžeme to porovnat, kdy v roce 2011 se samostatně eviduje celkem 1500 těchto případů v České republice, zatímco v roce 2019 tato hodnota dosáhla již 8400 případů. Mezi nejčastější trestné činy jsou podvody mezi soukromými osobami či úvěrové podvody, a také ostatní mravnostní trestné činy. Můžeme proto konstatovat, že v této oblasti panuje značná latence. S tak velmi rychlým rozvojem IT technologie lze předpokládat, že tato vysoce specifická trestná činnost bude i nadále postupovat a prolínat se všemi kriminálními problematikami. Kybernetická kriminalita se samozřejmě netýká jen dospělých osob.[109]

Bohužel se nevyhýbá ani těm nejzranitelnějším, a tím myslím dětem. Děti nejsou pouze oběti těchto trestných činů, ale figurují zde často také jako pachatelé kyberkriminality. Jak ve světě, tak i v České republice je stále trvající problém ve stoupajícím počtu kriminálních deliktů, které jsou páchány převážně na sociálních sítích. Toto samozřejmě také úzce souvisí se životním stylem mladší generace.

[108] NUKIB.CZ: Legislativa KB, [online]. 4.1.2013 [cit. 2023-02-23]. Dostupné z https:// https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/
[109] PREVENCE KRIMINALITY. *Strategie prevence kriminality v ČR 2022-2027* [online]. 2022 [cit. 2023-03-01]. Dostupné z: https://prevencekriminality.cz/wp-content/uploads/2021/10/04__spk-2022-2027_strategicka-cast.pdf

Tato věková skupina dětí je totiž příliš důvěřivá, snáze poté sděluje citlivé informace o sobě a o svém okolí i neznámým osobám a nedomýšlí tím možné negativní důsledky. Jednou ze zásadních priorit současnosti by proto měl být boj proti pohlavnímu zneužívání a také pohlavnímu vykořisťování dětí. V dnešní době je již standardem, že děti a mladiství stále více využívají datové služby v mobilních telefonech. Tyto služby již jsou v dnešní době dostupné pro širokou veřejnost a hlavně jsou finančně výhodnější než v minulosti. Přístup na internet tak má tato skupina neustále, mohou proto nerušeně navštěvovat stránky s nevhodným, závadovým či nemorálním obsahem. Chytré telefony těchto dětí většinou nemají aktivovanou žádnou ochranu či rodičovskou kontrolu a to je samozřejmě velké riziko. Děti si toto riziko neuvědomují a podceňují jej a to platí i pro jejich rodiče. Pandemie nemoci covid-19 se do této oblasti samozřejmě také negativně promítla. Běžný život byl v tomto období značně omezen. Proto se také většina aktivit přesunula do virtuálního prostředí. Jednalo se například o distanční výuku žáků ve školách, home office mnohých organizací a státní správy, zvýšený nákup na internetu. Jelikož ani děti nesměly v této době chodit ven, trávily tak svůj volný čas na počítači či mobilním teflonu. Stávaly se tak ve větší míře než v minulém období obětmi kyberšikany, sexuálního nátlaku či narušování soukromí.[110]

Podrobnější poznatky o stavu a vývoji kybernetické kriminality ukazují také samozřejmě různé realizované výzkumy. Jako příklad zde uvádím dokončený výzkum Agentury pro základní práva EU (FRA) „*Zločin, bezpečí a právo obětí*“ [111] publikovaného v roce 2021 či z příspěvku IKSP pro Republikový výbor pro prevenci kriminality pod názvem „*Kybernetická kriminalita v ČR*“.[112]

Dle mého názoru jsou otázky osvěty a prevence v oblasti kyberkriminality naprosto klíčové, zásadní a nepostradatelné. Cílem by mělo být neustále posilovat tato preventivní opatření v kyberprostoru a zabraňovat tak obtěžováním, kyberagrese a kybernásilí.[113] Již zmíněná oblast prevence je velice důležitá

[110] PREVENCE KRIMINALITY. *Strategie prevence kriminality v ČR 2022-2027* [online]. 2022 [cit. 2023-03-01]. Dostupné z: https://prevencekriminality.cz/wp-content/uploads/2021/10/04__spk-2022-2027_strategicka-cast.pdf

[111] 7 FRA-Crime, Safety and Victims‘ Rights (FRA, Fundamental Rights Survey 2019; data collection in cooperation with CBS (NL), CTIE (LU) and Statistics Austria (AT).

[112] MVCR ČESKÉ REPUBLIKY. *Problematika informační kriminality* [online]. Květen 2021 [cit. 2023-03-01]. Dostupné z: https://www.mvcr.cz/clanek/tiskova-zprava-ze-zasedani-republikoveho-vyboru-pro-prevenci-kriminality-713175.aspx

[113] PREVENCE KRIMINALITY. *Strategie prevence kriminality v ČR 2022-2027* [online]. 2022 [cit.

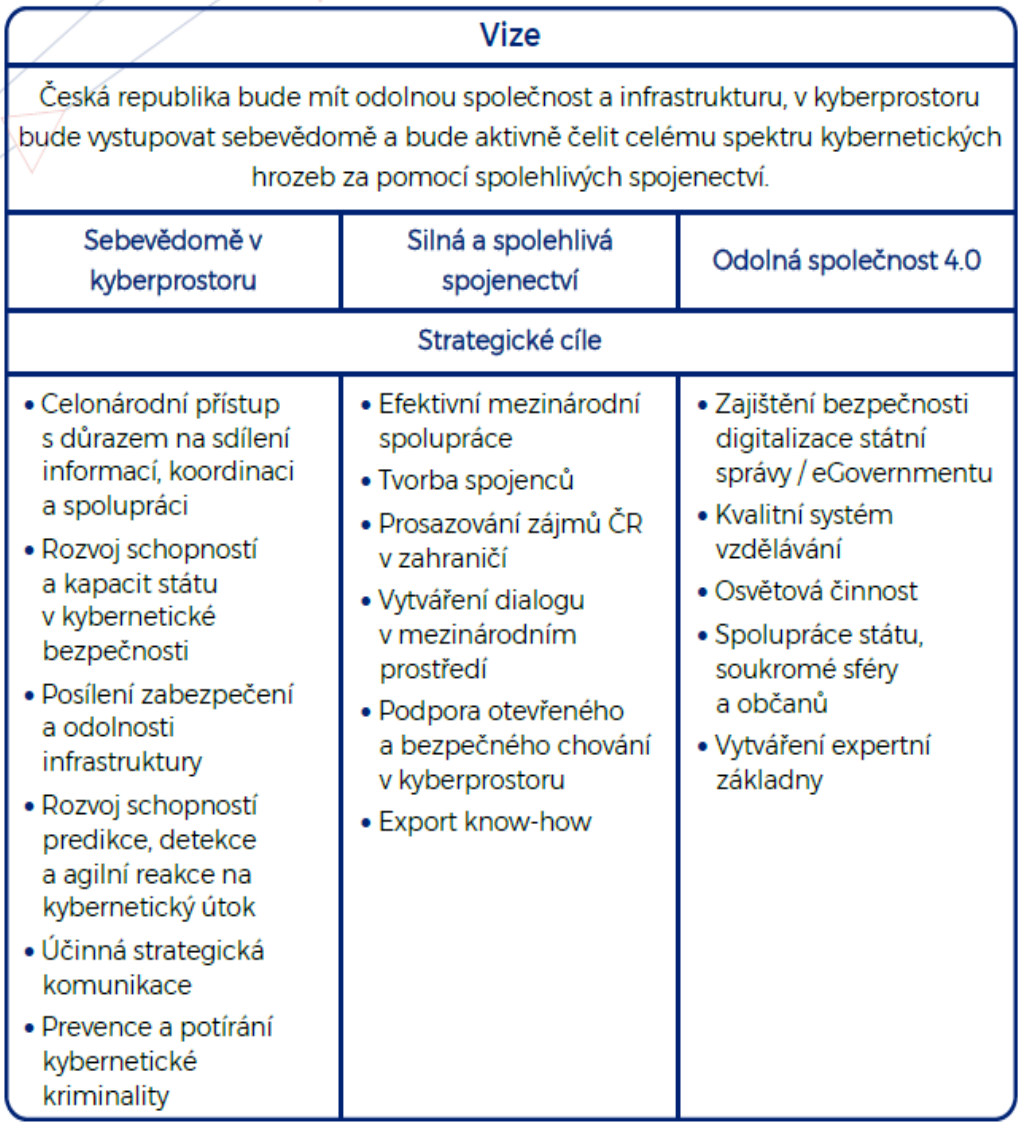
a pomáhá tak řešit celkové posílení kybernetické bezpečnosti naší republiky. Základním stavebním prvkem této prevence je kvalitní centralizované a navzájem provázané zabezpečení IT technologií a informačních systémů. Tyto aktivity poté zaručují velmi spolehlivou ochranu uživatelského prostředí stejně podobně, jako preventivní působení prostřednictvím včasného upozorňování na možná rizika, různé zranitelnosti a další podobné hrozby, které by získanou důvěrnost a integritu digitálního prostředí mohly porušit. V této oblasti prevence je nutné se zaměřovat jak na implementaci moderních bezpečnostních systémových technologií, tak se také nesmí opomenout posilování expertní základny, která pak umí všechny tyto nástroje využívat k potírání či dopadu kybernetické kriminality se zvláštním důrazem na vzdělání a nábor specialistů a IT expertů. Tito pracovníci poté komplexně a koordinovaně zabezpečují i prevenci před Kyberkriminalitou.[114]

Pokud je to jen trochu možné, je v rámci prevence je také zapotřebí nabídnout možnost podílet se na kybernetické bezpečnosti ČR i dalším IT expertům pracujícím jak ve státní správě, tak i v soukromém sektoru. Pokud by v budoucnu nastalo vážné ohrožení ČR, bude možné využít schopnosti těchto našich potenciálních expertů vně státní správy. Tento systém tak pomůže vytvořit časově dostupnou skupinu expertů. Na dalším obrázku č. 8 je znázornění strategických cílů České republiky v oblasti proti boji s Kyberkriminalitou.[115]

2023-03-01]. Dostupné z: https://prevencekriminality.cz/wp-content/uploads/2021/10/04__spk-2022-2027_strategicka-cast.pdf

[114] PREVENCE KRIMINALITY. *Strategie prevence kriminality v ČR 2022-2027* [online]. 2022 [cit. 2023-03-01]. Dostupné z: https://prevencekriminality.cz/wp-content/uploads/2021/10/04__spk-2022-2027_strategicka-cast.pdf

[115] PREVENCE KRIMINALITY. *Strategie prevence kriminality v ČR 2022-2027* [online]. 2022 [cit. 2023-03-01]. Dostupné z: https://prevencekriminality.cz/wp-content/uploads/2021/10/04__spk-2022-2027_strategicka-cast.pdf



Vize		
Česká republika bude mít odolnou společnost a infrastrukturu, v kyberprostoru bude vystupovat sebevědomě a bude aktivně čelit celému spektru kybernetických hrozeb za pomocí spolehlivých spojenectví.		
Sebevědomě v kyberprostoru	**Silná a spolehlivá spojenectví**	**Odolná společnost 4.0**
Strategické cíle		
• Celonárodní přístup s důrazem na sdílení informací, koordinaci a spolupráci • Rozvoj schopností a kapacit státu v kybernetické bezpečnosti • Posílení zabezpečení a odolnosti infrastruktury • Rozvoj schopností predikce, detekce a agilní reakce na kybernetický útok • Účinná strategická komunikace • Prevence a potírání kybernetické kriminality	• Efektivní mezinárodní spolupráce • Tvorba spojenců • Prosazování zájmů ČR v zahraničí • Vytváření dialogu v mezinárodním prostředí • Podpora otevřeného a bezpečného chování v kyberprostoru • Export know-how	• Zajištění bezpečnosti digitalizace státní správy / eGovernmentu • Kvalitní systém vzdělávání • Osvětová činnost • Spolupráce státu, soukromé sféry a občanů • Vytváření expertní základny

Obrázek č. 8 – Strategické cíle ČR v oblasti kyberkriminality[116]

[116] NUKIB. *Národní strategie kybernetické bezpečnosti* [online]. 21.6.2022 [cit. 2023-02-21]. Dostupné z: https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

4.7 Prevence kybernetické kriminality dle vyjádření Policie České republiky

Policejní činnosti v ČR samozřejmě také zahrnují různá preventivní opatření. Jedná se o zcela klíčovou činnost a můžeme konstatovat, že jde o jeden z hlavních pilířů práce policie. Jejím úkolem je tak cíleně reagovat na nové nastupující trendy z oblasti sociopatologických jevů a předcházení jejich rozšiřování. Jak jsem se již několikrát v této práci zmínil, největší poměrný nárůst kriminality je v poslední době v oblasti kyberprostoru. Proto je logické, že i preventivní činnost policie ČR se výrazně na tuto oblast zaměřuje. Jedná se o různé typy přednášek a besed. Statisticky bylo na toto téma v minulém období v rámci 14 krajských ředitelství policie ČR realizováno celkem 2777 přednášek. Během těchto besed se podařilo celkem oslovit 71535 osob. Nesmíme také opomenout další preventivní témata a to jsou hlavně phishingové či podvodné kampaně v online prostředí. Tyto kampaně se rozbíhají v průběhu každého roku v různých obměnách.[117]

V roce 2021 jich bylo vytvořeno více než 20. Témata těchto kampaní byla různá, avšak vždy reagovala na aktuální hrozby v kyberprostoru. Jednalo se například o téma podvodů se složenkami SIPO, kde byly falešné údaje pro platby, dále o podvodné SMS zprávy a e-maily vydávající se za oficiální sdělení Ministerstva práce a sociálních věcí a mnoho podobných. Policie také v oblasti preventivních aktivit realizovala několik celoplošných aktivit s bankovním sektorem. Jako příklad zde uvádím akci s názvem „nepindej“, „volač“, „klikač“ a podobně. Policie ČR se dále zaměřuje také na problematiku témat protidrogové problematice, dopravní problematice a také problematice o péči o obětech a problematice domácího násilí.[118]

Další důležitou součástí prevence jsou pravidla bezpečného chování na internetu. **Můžeme je shrnout do těchto deseti bodů:**

1) Pravidelné aktualizace jak operačního systému počítače, tak jednotlivých programů na něm nainstalovaných. Nainstalování a správná funkce antivirového a bezpečnostního programového vybavení.
2) Namátková kontrola funkčnosti antivirového programu. Některé viry dokáží tento program zablokovat a tak jej znefunkčnit.

[117] MORAVČÍK, Ondřej. *Vývoj registrované kriminality v roce 2022* [online]. 13.1.2023 [cit. 2023-02-23]. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx
[118] MORAVČÍK, Ondřej. *Vývoj registrované kriminality v roce 2022* [online]. 13.1.2023 [cit. 2023-02-23]. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx

3) Být obezřetný v e-mailové komunikaci. Neotvírat přílohy z nevyžádané pošty pokud neznáme odesílatele této zprávy. Tímto způsobem se velmi často šíří škodlivé programy.
4) Neklikat v obdržených e-mailových zprávách na podvržené odkazy, které uživatele přesměrovávají na podvodné webové stránky.
5) Pokud uživatel zadává svá přístupové hesla do internetových stránek, je dobré si kontrolovat, zda je tento web zabezpečený.
6) Pokud je možná kontrola, tak osobní citlivé informace uživatel zadává jen do ověřených webových stránek.
7) Do své e-mailové komunikace nezadáváme důvěrné informace, jako jsou čísla kreditních karet nebo hesla k bankovním účtům. Tuto elektronickou komunikaci totiž může potenciální útočník zachytit.
8) Rozhodně nevypínat firewall, který je součástí operačního systému a pokud tomu uživatel nerozumí, nechat tento program pracovat v automatickém režimu.
9) Pokud používáme k přístupu na internet cizí počítač například v internetové kavárně, nikdy se zde nesnažíme přihlašovat do svého internetového bankovnictví.
10) Při používání free Wi-Fi připojeních je zapotřebí také obezřetnost. Tato komunikace totiž není šifrovaná a může jí kdokoliv odposlouchávat a tak získat přístup ke všem datům.[119]

4.8 Nejnovější kyberútoky v České republice v roce 2022

Kyberútoky se šíří po celém světě a tak se samozřejmě ani nevyhnuly České republice. Česko se tak v poslední době stalo také terčem těchto útoků. Jejich cílem byl jak veřejný, tak soukromý sektor. Jako příklad zde můžeme uvést útok na vládní web, stránky Českých drah nebo též samotný úřad, který proti těmto rizikům bojuje. Minstr vnitra Vít Rakušan však veřejnost ubezpečil, že tyto kybernetické útoky žádné větší škody nezaznamenaly. Data odcizena nebyla.[120]

[119] FIŠER, Miloslav. *Vědci z Česka a USA spojí síly kvůli kyberbezpečnosti* [online]. 17.1.2023 [cit. 2023-03-17]. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-vedci-z-ceska-a-usa-spoji-sily-kvuli-kyberbezpecnosti-40420204
[120] SEDLÁČKOVÁ, Veronika. *Statisíce počítačů a jediný cíl: Expert pospal nejnovější kyberútoky v Česku* [online]. 26.4.2022 [cit. 2023-04-22]. Dostupné z:

Dle sdělení NÚKIB šlo o specifické DDoS útoky. Tento typ útoků je velmi častý a jeho princip spočívá v tom, že z neznámých IP adres ze zahraničí přijde v jeden okamžik obrovské množství dotazů a připojení na konkrétní webové stránky. Tyto stránky poté přestanou fungovat a stanou se tak nefunkční. Uživatelé se tak na stránky již nemohou připojovat. Fungovat toto připojení na takto napadené stránky může také jít jen například z prohlížeče Microsoft Edge, z ostatních webových prohlížečů jsou stránky nadále nedostupné. Například webové stránky Českých drah tento problém musely řešit. Problém byl hlavně s aplikací „*Můj vlak*“, kdy nebyl možný nákup online jízdenek, problém nastal i s vyhledáváním spojů. Jako další příklad mohu uvést napadení webu „*portal.gov.cz*“. Tento web pouze uváděl, že probíhá technologická odstávka za účelem posílení bezpečnosti webu.[121]

Dalším podobným útokům též čelily i webové stránky karlovarského a pardubického letiště. Na tyto útoky také ihned reagoval ministr vnitra Vít Rakušan. Ve středu 20. dubna 2022 na tiskové konferenci uvedl, že na tyto systémy státních i soukromých institucí kybernetické útoky provedli ruští hackeři. Dále uvedl, že při těchto útocích neunikla žádná data a informace. K těmto útokům se poté přihlásila hackerská skupina Killnet. Tato skupina se také přiznala k útokům na Komerční banku, ta tento útok ovšem nepotvrdila. Úřad NÚKIB na zvyšující se riziko kyberútoků a kyberšpionáže v souvislosti s válkou na Ukrajině upozorňoval již na konci ledna roku 2022. Poté toto upozornění vydal i na konci února 2022. Nabádal organizace, které spadají pod zákon o kybernetické bezpečnosti, k ostražitosti a k provedení aktualizace informačních systémů, aby bylo zabráněno případnému zneužití známých zranitelností v operačních systémech.[122]

Zatím největší DDoS útok za poslední dobu se v naší republice stal dne

---

https://www.seznamzpravy.cz/clanek/audio-podcast-ptam-se-ja-statisice-pocitacu-maji-jediny-cil-expert-popsal-nove-kyberutoky-v-cesku-199778

[121] SEZNAM ZPRÁVY. *Expert pospal nejnovější kyberútoky v Česku,* [online]. 21.4. [cit.2023-04-25]. Dostupné z: https://www.seznamzpravy.cz/clanek/domaci-zivot-v-cesku-masivni-hackerske-utoky-na-ceske-weby-nekonci-napadeny-je-i-web-vlady-199082#utm_content=ribbonnews&utm_term=hacke%C5%99i&utm_medium=hint&utm_source=search.seznam.cz

[122] SEZNAM ZPRÁVY. *Expert pospal nejnovější kyberútoky v Česku,* [online]. 21.4. [cit.2023-04-25]. Dostupné z: https://www.seznamzpravy.cz/clanek/domaci-zivot-v-cesku-masivni-hackerske-utoky-na-ceske-weby-nekonci-napadeny-je-i-web-vlady-199082#utm_content=ribbonnews&utm_term=hacke%C5%99i&utm_medium=hint&utm_source=search.seznam.cz

3. prosince 2022. Tato zpráva se ihned objevila v celém mediálním prostoru. Cílem tohoto útoku byl tuzemský internet a také odstavení jednotlivých služeb firemních zákazníků, firem a státních organizací. Tyto cílené DDoS útoky se hlavně soustředily na infrastrukturu zákazníka nebo operátora. Přicházely tak z ostatních sítí. Jejich cílem bylo okamžité přetížení a celkové zahlcení lokální sítě. Tato síť se tak stává během tohoto útoku zcela nefunkční. Jednotlivé firmy a instituce se tak nemohou dostat ke svým důležitým datům a nemohou proto v tuto dobu pracovat. Časově tyto DDoS útoky začaly v pondělí 24. října 2022 časně ráno. Šlo o velmi rozsáhlý a také poměrně dlouhý útok. Bylo to možné označit za masivní atak. Celkově tento útok trval tři dny v různých cyklech. Obvyklá délka takového útoku do této doby byla v řádu jen několik hodin. Proti těmto útokům existuje jen omezená ochrana či prevence. Důležité proto je, aby se informace o těchto útocích před veřejností netajily. Potýkat se s těmito problémy totiž není žádná ostuda. Přesto je ale potřeba k bezpečnosti proti kyberhrozbám přistupovat komplexně.[123]

Stále více kyberútoků bohužel cílí v naší zemi na nemocnice a zdravotnická zařízení. Nebylo tomu jinak i v roce 2022. Počet těchto útoků na tato zařízení je dle Národního úřadu pro kybernetickou a informační bezpečnost dle statistiky za období roku 2022 přibližně stejný jako tomu bylo v roce 2021. NÚKIB jich v roce 2022 zaznamenal „nižší desítky“, zatímco v roce 2021 jich bylo celkem 26. Tyto velice specifické a nebezpečné útoky NÚKIB eviduje pravidelně v každém měsíci. Většinou převažovaly významné a méně významné incidenty. Jako velmi významný byl klasifikován v tomto roce dosud pouze jeden incident. Šlo o různé techniky napříč celým známým spektrem. Za poslední tři roky, je nevíce kyber útoků vedeno na obor zdravotnictví. Prevenční akce, které se zúčastnili zástupci předních nemocnic, pořádaná NÚKIB v měsíci prosinec roku 2022 v Brně, měla za úkol simulovat napadnutí hackery zdravotní a nemocniční zařízení. Jako hlavní scénář byl zvolen nečekaný výpadek všech provozních systémů. Jednotlivé týmy z jednotlivých zařízení se skládali z řad odborníků pro komunikaci, lékařství a lékařskou péči či kyber bezpečnost. Hlavním a nejdůležitějším cílem tohoto

[123] ŽIVĚ. *Česko zasáhl největší DDoS útok,* [online]. 3.12.2022 [cit.2022-12-03]. Dostupné z: https://www.zive.cz/clanky/cesko-zasahl-nejvetsi-ddos-utok-v-historii-v-cem-byl-specificky-mohl-byt-rizeny-z-ruska-rozhovor-s-tomasem-krestakem-z-o2/sc-3-a-219591/default.aspx

cvičení bylo proškolit přítomné na to, aby byli schopni čelit kybernetickým útokům v reálném světě, pokud by se stali terčem takového sofistikovaného útoku a umět včas reagovat a najít vhodná řešení k obraně. Cvičení se účastnilo 15 zařízení, která neměla možnost účastnit se předchozího ročníku. Šlo o nemocnice, které spadají pod působnost zákona o kybernetické bezpečnosti.[124]

4.9 Nejčastější internetové hrozby v České republice

Tyto hrozby můžeme rozdělit dle závažnosti a rizika napadání. Jako nezávažnější riziko můžeme v Česku označit spyware. Útočníci se takto snaží o krádež přihlašovacích údajů, které uživatel zadává do internetových prohlížečů při přihlašování k různým webovým službám. Schéma tohoto útoku bývá většinou podobný. Tento malware se nejvíce šíří pomocí speciálně infikovaný e-mailových zpráv. Tyto údaje vyplývají ze statistiky, kterou pravidelně vydává antivirová společnost ESET, ve které spyware obsadil první tři příčky. Jako prevenci proti tomuto odborníci doporučují, aby si uživatelé neukládali svá přihlašovací hesla do internetových prohlížečů. Tato hrozba dle expertů ze společnosti ESET zůstane i v roce 2023. Útočníci se snaží tyto podvržené elektronické e-mailové zprávy udělat co nejdůvěryhodnější. Proto je vydávají například za faktury z obchodů, různá shrnutí objednávek nebo návrhy rozpočtů. Nejčastější přílohou těchto podvodných a nebezpečných e-mailů jsou právě spustitelné soubory nebo „*pdf*“ dokumenty s dvojitou koncovkou „*pdf.exe*“. Pokud uživatel tento soubor ve své poště otevře, malware se nainstaluje do jeho počítače. Útočníci se většinou snaží tyto podvodné přílohy neustále měnit a přejmenovávat, aby bylo zabráněno jejich prozrazení. Většinou tyto podvodné zprávy jsou psány v anglickém i českém jazyce.[125]

[124] ČESKÁ TISKOVÁ KANCELÁŘ. *Nemocnice stále čelí kyberútokům,* [online]. 19.12.2022 [cit. 2023-04-25]. Dostupné z: https://www.novinky.cz/clanek/domaci-nemocnice-stale-celi-kyberutokum-40417515

[125] ANTIVIROVÉ CENTRUM. *Internetové hrozby v lednu v České republice* [online]. 15.2.2021 [cit. 2023-04-25]. Dostupné z: https://www.antivirovecentrum.cz/aktuality/internetove-hrozby-v-ceske-republice-leden-2021.aspx

Společnosti ESET, dle uvedených statistik, zaznamenala největší šíření trojského koně „*Spy.Agent.AES*“. Tento se šířil především přílohou s názvem "*PARTS_REQUEST_SO_30005141.exe*". Nejvýraznější hrozbou v lednu byl také trojský kůň „*Spy.Agent.AES a Formbook*“, oba tyto malware se zaměřují na odcizení hesel, která si uživatel uložil do webového prohlížeče. Tyto jednotlivé škodlivé kódy lze zakoupit na darknetu v rámci tzv. "služby". V dnešní moderní době je totiž možné si také pronajmout specifický škodlivý kód. Potenciální útočník jej tedy nemusí sám vytvářet a programovat, ale může si ho na internetu koupit či pronajmout. V tomto druhu obchodů se točí poměrně velké finanční částky a je proto pro mnoho hackerů velmi lukrativní a žádaný. Hackeři považují tyto nákupy služeb jako investice. Přihlašovací údaje k bankovnictví lze prodat až za 1 500 Kč. Databáze hesel mají pro útočníky obrovskou hodnotu.[126]

[126] ANTIVIROVÉ CENTRUM. *Internetové hrozby v lednu v České republice* [online]. 15.2.2021 [cit. 2023-04-25]. Dostupné z: https://www.antivirovecentrum.cz/aktuality/internetove-hrozby-v-ceske-republice-leden-2021.aspx

5. PRAKTICKÁ ČÁST

V této kapitole se budu věnovat případové studii. Tato studie je zpracována na základě skutečného případu řešeného Policií ČR, Krajského ředitelství policie Jihočeského kraje.

Popisovaný případ se začal šetřit v listopadu roku 2017. Popis skutku a informace o probíhajícím prověřování a poté i vyšetřování, jsou autentické, osoby a konkrétní údaje případu jsou anonymizované (smyšlená jména i účty) v souladu s ochranou osobních údajů GDPR.[127]

5.1 Začátek případu

Tento případ začal v polovině října roku 2017 podáním vysvětlení podle §61 odst.1[128] zákona č. 273/2008 Sb., o Policii České republiky na Obvodním oddělení České Budějovice. Studentka Anna Nováková (smyšlené jméno) učinila oznámení o věci, kdy jí neznámá osoba vydírá a zneužívá její profilový účet na Facebook.com nebo e-mail na serveru Seznam.cz. Dále konstatovala, že v současné době nemá přístup do svého e-mailu ani na svůj facebookový profil. Její hesla na e-mail ani na Facebook dle jejího tvrzení, nikdo nezná. Když se náhodou někde u kamarádů nebo ve škole přihlásila na Facebook nebo e-mail tak se vždy odhlásila.

5.2 Věcná příslušnost

Z tohoto obvodního oddělení byl tento spisový materiál postoupen na Územní odbor České Budějovice, 2. oddělení obecné kriminality, Služby kriminální policie a vyšetřování. Na základě věcné příslušnosti dle ZPPP č. 221/2011 byl ihned tento případ dále postoupen na Krajské ředitelství policie Jihočeského kraje, Službu kriminální policie a vyšetřování, Odbor analytiky, Oddělení kybernetické kriminality. Zde byl sepsán s Annou Novákovou protokol o trestním oznámení na neznámého pachatele, který jí dle jejího tvrzení vydíral přes internetový profil na sociální síti Facebook, přičemž vystupoval pod jménem Jiří Smetana (smyšlené

[127] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Obecné nařízení o ochraně osobních údajů)

[128] ZÁKON O POILICII ČR. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2008-273

jméno), požadoval zaslání přihlašovacích údajů k jejímu e-mailovému účtu pod pohrůžkou rozeslání jejích nahých fotek kamarádům, kdy následně získal neoprávněný přístup na její facebookový profil a e-mailový účet anna.novakova@post.cz (smyšlený účet) a tyto zablokoval.

5.3 Zahájení úkonů trestního řízení

Následně vrchní komisař na základě informací z tohoto trestního oznámení podle § 158 odstavce 3[129] trestního řádu zahájil úkony trestního řízení ve věci podezření ze spáchání přečinu vydírání podle § 175 odst. 1[130] tr. zákoníku a přečinu neoprávněný přístup k počítačovému systému a nosiči informací podle § 230 odst. 1, odst. 2 písm. b), odst. 3 písm. a)[131] trestního zákoníku, neboť na podkladě trestního oznámení poškozené Anny Novákové, byl dostatečně odůvodněn závěr, že neznámý pachatel z dosud nezjištěného místa prostřednictvím sociální sítě Facebook kontaktoval z účtu s názvem Jiří Smetana poškozenou Annu Novákovou a pod pohrůžkou zveřejnění jejích intimních fotografií, které předtím nezjištěným způsobem získal po ní požadoval sdělení hesla k její e-mailové schránce u společnosti Seznam.cz, a když toto poškozená odmítla učinit nezjištěným způsobem po překonání hesla pronikl do jejího facebookového účtu a do e-mailové schránky ve kterých změnil přístupová hesla, čímž měla být poškozené způsobena újma.

5.4 Prověřování napadení e-mailové schránky

V rámci prověřování této trestní věci byla opatřena zpráva od společnosti Seznam.cz týkající se napadené e-mailové schránky anna.novakova@post.cz včetně registračních a přístupových údajů k této schránce. Z této zprávy bylo zjištěno, že pachatel do této e-mailové schránky vnikl nejpozději 9. října 2017 v 19.24 hod, kdy z IP adresy 194.112.206.157 (smyšlená adresa) změnil tzv. záchranou e-mailovou adresu pro tuto schránku na rocky123@seznam.cz

[129] TRESTNÍ ŘÁD. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/1961-141
[130] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
[131] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

(smyšlený účet). Následně tento pachatel změnil heslo a nastavení telefonního kontaktu z telefonního čísla poškozené na neznámé číslo.

Dále byla opět společnost Seznam.cz policejním orgánem dotazována na podrobnosti ohledně e-mailové schránky rocky123@seznam.cz. Dle zaslané odpovědi od společnosti Seznam.cz bylo zjištěno, že tato e-mailová schránka má nastavenou záchranou e-mailovou adresu Radek.Novotny@email.cz (smyšlená adresa). Dle doprovodných údajů od společnosti Sezam.cz dále bylo zjištěno, že do e-mailové schránky Radek.Novotny@email.cz bylo nejčastěji přistupováno z IP adres 194.112.206.157 a 177.22.219.21.

5.5 Identifikace IP adres

Pro úspěšné ustanovení pachatele bylo dále klíčové zjistit podrobnosti o IP adresách, ze kterých bylo přistupováno do e-mailové schránky Radek.Novotny@email.cz. K uvedeným IP adresám bylo lustrací ve veřejně dostupné databázi organizace RIPE NCC spravující evropský regionální internetový registr zjištěno, že adresa 194.112.206.157 je veřejná IP adresa Vysoké školy. Vzhledem k tomuto zjištění si policejní orgán vyžádal od této vysoké školy podrobné informace o této IP adrese. Z vyjádření správce počítačové sítě Vysoké školy pak bylo zjištěno, že v příslušných zájmových časech přistupoval z jejich veřejné IP adresy k síti internet prostřednictvím školního WiFi připojení počítač s MAC adresou 44:6 d:57:80: e9:7 b a vnitřní IP adresou 191.167.31.229 a to na základě autorizovaného přihlášení pod účtem studenta školy Radka Novotného. Telefonicky bylo hovořeno se studijním oddělením této vysoké školy. Dle jejich informací student Radek Novotný zde studuje obor aplikovaná informatika. Jako svůj kontaktní e-mail pro komunikaci se školou má tento student nastavenu schránku Radek.Novotny@email.cz.

5.6 Ustanovení podezřelého pachatele

Na základě získaných dat byla provedena lustrace IS PČR a takto byl ustanoven jako Radek Novotný, nar. 1.1.1995 (smyšlená data), trv. bytem, Jindřichův Hradec. Dále bylo zjištěno, že jmenovaný studuje obor aplikovaná informatika a pro komunikaci se školou má nastavený jako kontaktní e-mail výše zmíněnou schránku Radek.Novotny@email.cz. K IP adrese 177.22.219.21 bylo lustrací v databázi organizace RIPE NCC zjištěno, že se jedná o adresu

společnosti Komputer, s.r.o. (smyšlené jméno), což je poskytovatel připojení k internetu v oblasti Jindřichova Hradce, kde má podezřelý trvalé bydliště.

Tato společnost byla proto policejním orgánem vyzvána k zaslání podrobných informací o IP adrese 177.22.219.21. Ze zprávy této společnosti vyplynulo, že uvedená IP adresa je veřejná NAT adresa, přes kterou přistupuje k internetu cca 300 zákazníků společnosti, včetně obyvatel domu v Jindřichově Hradci, což je adresa bydliště podezřelého Radka Novotného. Dalším šetřením policejního orgánu v prostředí internetu bylo dále zjištěno, že pachatel aktivně užíval FB profil Radek R. Novotný (smyšlený profil) a z tohoto profilu komunikoval s poškozenou Annou Novákovou. Dále bylo zjištěno, že e-mailová schránka Radek.Novotny@email.cz je provázána s facebookovým profilem Radek R. Novotný.

5.7 Protokoly o ohledání věci

Po úspěšném ustanovení pachatelovo e-mailového účtu a jeho facebookového profilu provedl policejní orgán jejich ohledání. Důvodem tohoto ohledání bylo zadokumentování FB profilu: Radek R. Novotný. Toto zadokumentování bylo provedeno náhledem na veřejně přístupná data z operativního profilu PČR. Tento náhled byl zadokumentován formou printscreenu tohoto náhledu do souboru formátu „pdf“. Tento soubor byl autorizován Hash sumou MD5. Dále bylo zjištěno, že z toho profilu komunikoval doposud neustanovený pachatel s FB profilem poškozené oznamovatelky Anny Novákové. Tento FB profil byl založen v roce 2019 a poslední viditelná aktivita je 27. duben 2014. Dle příspěvků (komentáře k hrám, obrázky, „smajlíky“ atd.) lze důvodně předpokládat, že tento uživatel byl pravděpodobně mladistvý. Na tomto profilu nejsou umístěny žádné fotografie majitele. Dále byla provedena kompletní záloha zájmových e-mailových schránek jak oznamovatelky tak podezřelého.

5.8 Šetření k osobě podezřelého

Osoba Radka Novotného byla lustrována v IS Policie ČR. Dále byla vyžádána zpráva o pověsti z jeho trvalého bydliště. Z této zprávy vyplývá, že podezřelý byl v letech 2013 – 2018 řešen pro jeden přestupek a tento přestupek byl vyřešen

blokovou pokutou. V ostatních systémech PČR byla lustrace jeho osoby negativní, trestán doposud nebyl. Na základě doposud zjištěných informací z probíhajícího šetření bylo přikročeno k předvolání podezřelé osoby k výslechu.

5.9 Úřední záznam o podaném vysvětlení

V půlce prosince roku 2017 se dostavil Radek Novotný k podání vysvětlení podle § 158 odstavce 6[132] trestního řádu. Po řádném poučení policejním orgánem byl seznámen s okolnostmi případu vydírání poškozené Anny Novákové na Facebooku a zablokování jejího FB profilu a e-mailového účtu. K této věci uvedl následující.

Přiznal se k tomu, že to udělal on. Vypověděl: „*Bylo to kvůli počítačový hře Falout. Potřeboval jsem několik e-mailových účtů kvůli tomu, abych mohl vydělávat v té hře herní měnu na více účtech zároveň. Ty účty jsem si nemohl založit sám jako nové, protože oni to mají nějak zabezpečené, aby jeden hráč nemohl účelově založit x herních účtů, takže jsem potřeboval nějaké starší e- mailové účty reálných lidí, co už mají nějakou historii. Chtěl jsem to opravdu na to hraní. Já jsem teda oslovil tu Annu Novákovou víceméně náhodně, přes nějaké společné přátele. Oslovil jsem jí z Facebookového profilu Radek R. Novotný, to je profil, který jsem používal jen párkrát, třikrát, čtyřikrát, měl jsem ho asi půl roku. S tou Annou jsme si psali normálně o škole. Já pak jí požádal, jestli si můžu na její účet u Seznamu zaregistrovat herní účet v té hře Falout. Ona s tím souhlasila a poslala mi odkaz na registraci té hry. No a já přes ten odkaz byl vlastně přihlášenej v její e-mailové schránce anna.novakova@post.cz. No a pak jsem bohužel začal dělat ty blbosti...Zablokoval jsem jí FB profil, e-mailovou schránku a chtěl jsem po ní poslat lechtivé fotky a vyhrožoval jsem jí, jestli mi je nepošle tak fotky které mám od jejího bývalého přítele rozešlu jejím kamarádům na FB.“*

Během tohoto výslechu vyšlo najevo, že se podezřelý připojoval na tyto účty pomocí svého notebooku HP a mobilního telefonu Nokia. K internetu se dotyčný připojoval, dle jeho následného, vyjádření v místě svého bydliště a ve škole pomocí svého školního účtu a hesla. Dále podezřelý uvedl, že se poškozené omlouvá, poskytne Policii plnou součinnost k tomu, aby vše napravil, co udělal.

[132] TRESTNÍ ŘÁD. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/1961-141

Proto Policii vydal facebookový profil poškozené i její e-mailovou schránku.

5.10 Protokol o vydání věci

Po ukončení výslechu o podaném vysvětlení byl Radek Novotný vyzván policejním orgánem k dobrovolnému vydání věci a to jeho notebooku a mobilního telefonu. Podezřelý tedy dobrovolně vydal jak svůj notebook HP včetně nabíjecího kabelu tak svůj mobilní telefon značka Nokia a to pro účely znaleckého zkoumání. Následně na to policejní orgán tyto věci předal specialistovi ke znaleckému zkoumání.

Na začátku února roku 2018 bylo obdrženo odborné vyjádření k těmto dvěma zařízením pracovníkem OKTE. Z tohoto odborného vyjádření se potvrdila výpověď podezřelého. Přistupoval z těchto zařízení do již zmíněných FB profilů a e-mailových účtů. Tyto zařízení se připojovali do internetu v místě jeho bydliště a i ve škole pod jeho přihlašovacími údaji. Na základě těchto informací policejní orgán vydal usnesení podle §160 odstavce 1[133] trestního řádu.

5.11 Sdělení obvinění a výslech obviněného

Na začátku března 2018 vydal policejní orgán usnesení podle § 160 odstavce 1[134] trestního řádu, kdy zahájil trestní stíhání osoby Radek Novotný jako obviněného ze spáchání *„přečinu vydírání podle § 175 odst. 1[135] trestního zákoníku a přečinu neoprávněný přístup k počítačovému systému a nosiči informací podle § 230 odst. 1, odst. 2 písm. b), odst. 3 písm. a)[136] trestního zákoníku".*

Tedy tím, že jiného pohrůžkou jiné těžké újmy nutil, aby něco konal. Překonal bezpečnostní opatření a tím neoprávněně získal přístup k počítačovému systému, získal přístup k počítačovému systému a data uložená v počítačovém systému neoprávněně učinil neupotřebitelnými a takový čin spáchal v úmyslu způsobit jinému jinou újmu.

---

[133] TRESTNÍ ŘÁD. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/1961-141
[134] TRESTNÍ ŘÁD. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/1961-141
[135] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
[136] TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

Po sdělení obviněný bylo policejním orgánem přistoupeno k výslechu obviněného. Po jeho poučení obviněný uvedl, že se v plném rozsahu přiznává k tomu, z čeho je obviněn. Dále uvedl stejné skutečnosti jako při předešlém výslechu.

5.12 Návrh na podmíněné zastavení

Policejní orgán v polovině dubna roku 2018 podal na OSZ Návrh na podmíněné zastavení trestního stíhání podle § 307[137] trestního řádu. Podle § 166 odstavce 3[138] trestního řádu po skončení vyšetřování předložil policejní orgán spis s návrhem na podmíněné zastavení trestního stíhání obviněného. Obviněný se k trestné činnosti v plném rozsahu doznal a s postupem podle § 307 odst. 1, 2[139] trestního řádu vyjádřil souhlas, přičemž vzhledem k osobě obviněného, s přihlédnutím k jeho dosavadnímu životu a všem okolnostem případu, lze rozhodnutí o podmínečném zastavení trestního stíhání považovat za dostačující.

5.13 Podmínečné zastavení

Státní zástupkyně OSZ rozhodla v trestní věci obviněného Radka Novotného podle § 307 odst. 1, odst. 2 písm. b)[140] trestního řádu o podmínečném zastavení trestního stíhání když na účet KSZ složil peněžitou částku ve výši 15 000,- Kč určenou státu na peněžitou pomoc obětem trestné činnosti, a tato částka není zřejmě nepřiměřená závažnosti trestného činu. Podle § 307 odst. 3[141] trestního řádu se obviněnému stanoví zkušební doba na dvanáct měsíců.

Po prostudování spisového materiálu byly OSZ zjištěny následující skutečnosti. Obviněný při výslechu uvedl, že se plně přiznává k tomu, z čeho byl obviněn. Obviněný v průběhu vyšetřování navázal spolupráci s Probační a mediační službou. Kromě doznání je jeho trestná činnost prokazována ve věci dalšími shromážděnými důkazy Následně je z výpisu bankovního účtu KSZ patrné, že obviněný složil částku 15.000 Kč na oběti trestných činů. K osobě

[137] TRESTNÍ ŘÁD. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/1961-141
[138] TRESTNÍ ŘÁD. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/1961-141
[139] TRESTNÍ ŘÁD. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/1961-141
[140] TRESTNÍ ŘÁD. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/1961-141
[141] TRESTNÍ ŘÁD. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/1961-141

obviněného nebyly zjištěny zásadní negativní poznatky, ten do současné doby nebyl soudně trestán.

Z výše uvedených důvodů bylo proto rozhodnuto o podmínečném zastavení trestního stíhání obviněného.

5.14 Jiný pohled na případ

Tento popisovaný případ se díky přiznání obviněného zdá být celkem jednoduchý. Pokud by se ale pachatel k tomuto spáchanému skutku nepřiznal, dle mého názoru by byl stejně obviněn a poté také odsouzen a trest by měl určitě vyšší. Ve prospěch pachatele hrálo hlavní roly jeho plné přiznání, bezúhonnost, spolupráce s PČR a tím také možná domluva se státním zástupcem.

Důkazně si myslím, že vyšetřovatel případu mohl být spokojen a to i bez přiznání pachatele. Měl přesně ustanovený počítač (byla známá jeho MAC adresa) a telefon, ze kterého se přihlašovalo. Věděl i přesné časy tohoto přihlašování. Ustanovení pachatele proto bylo poměrně rychlé a přesné.

Pokud by pachatel počítač a telefon dobrovolně nevydal, mohl policejní orgán poté na základě příkazu k domovní prohlídce toto zajistit. Dle mého názoru tento pachatel udělal řadu chyb, především tím, že se připojoval na internet z připojení doma a ve škole, nějak se nesnažil toto připojení na internet maskovat, například pomocí VPN připojení, anonymních SIM karet, vzdálených přístupů a podobně. Možností je nepřeberné množství. Důležité také bylo, že pachatel pocházel z České republiky. Kdyby byl z ciziny, vyšetřování případu by bylo daleko složitější díky dožádání či by bylo prakticky nemožné.

Velmi dobré pro poškozenou z tohoto případu je, že má opět pod kontrolou svůj e-mailový a facebookový účet, žádné další své soukromé fotky pachateli nedala a tak by ani neměla být do budoucna již nikým vydíratelná.

Myslím si, že tento pachatel se z tohoto poučil a bude si dávat do budoucna dobrý pozor, aby se do takovéto situace již nikdy nedostal. Proto trest, který dostal se mi pro něho zdá dostačující a má i preventivní účinek a tento pachatel by neměl být pro společnost v tomto ohledu již do budoucna nebezpečný.

ZÁVĚR

Téma mé bakalářské práce zní „Boj proti informační kriminalitě v ČR“. Tento boj probíhá neustále a probíhat bude i v budoucnu. Samozřejmě, že se tento problém netýká pouze České republiky, ale jedná se o globální problém všech zemí na celém světě. Kyberkriminality nelze totiž ohraničit státem či kontinentem, je to jev celosvětový. Pachatelé kyberzločinu operují také po celém světě. Kyberkriminalita prostě nezná hranic.

V praktické části své práce se zabývám pouze jednodušším případem kyberkriminality. Je to dáno tím, že pro tuto kazuistiku jsem potřeboval nalézt takový případ, který je již odsouzený (či podmínečně zastavený) a je jej možno hodnotit v plném rozsahu. Jak je ale i v tomto případě patrné i tento trval déle než rok a to nemusel jít k soudu.

Složitější případy jsou totiž rozpracovávány daleko delší časové období, neboť je zde většinou mezinárodní prvek, více pachatelů a sofistikovanější metody při kyberkriminalitě. A v neposlední řadě není možné takové případy do kazuistiky od kolegů získat. Ještě v roce 2022 se touto formou trestných činů zabývala Národní centrála proti organizovanému zločinu, která toto měla v gesci. Policejní prezident Martin Vondrášek ovšem rozhodl o rozdělení NCOZ, přičemž od 1. ledna 2023 vznikl další nový útvar pod policejním prezidiem, který se bude zabývat pouze extremismem, terorismem a kybernetickým zločinem (NCTEKK). Policejní prezident také proto zmínil, že největší rizika pocházejí z kyberprostředí. Konkrétně řekl: „*Jednoznačně jsme došli k závěru, že pandemie a nyní válka to jen potvrzují, že největší riziko pro Českou republiku jsou teroristické a extremistické akce, které jsou zpravidla řízeny ze zahraničí, zpravidla jsou páchány elektronickou formou v on-line prostředí a to považujeme za naprosto zásadní pro vnitřní bezpečnost ČR*,“ uvedl s tím, že okolní státy jdou podobnou cestou.[142]

Ale i na tomto mém prezentovaném případě si můžeme všimnout mnoho důležitých věcí. Především v dnešním přetechnizovaném světě se může obětí kyberkriminality či kyberšikany stát prakticky kdokoliv z nás. Technika jde každým

[142] GRIČOVÁ, Andrea. *Rozdělení NCOZ je správné* [online]. 12.6.2022 [cit. 2023-05-10]. Dostupné z: https://ct24.ceskatelevize.cz/domaci/3504381-rozdeleni-ncoz-je-spravne-rekl-policejni-prezident-kriminalita-s-prichodem-uprchliku

rokem kupředu a dnešní moderní chytré telefony jsou prakticky malé počítače, které nosíme neustále při sobě a ani si pořádně neuvědomujeme, co všechno tyto přístroje umí a jak mohou být na druhou stranu zranitelné. Připojujeme se do svých účtů jak pomocí těchto telefonů tak poté i díky počítačům. Většinou při tomto druhu trestné činnosti je poté pachateli sděleno obvinění z více trestných činů (tak jako v našem prezentovaném případě vydírání a také neoprávněný přístup k počítačovému systému).

Mnoho uživatelů si podvědomě dává více pozor při práci s počítačem či notebookem, ale s telefonem to tak není. Dle různých statistik má antivirový či jiný program naistalováno ve svém počítači více lidí, než v mobilním telefonu. Přitom ale v dnešní době je více informací v mobilních telefonech. Proto se také kyberzločinci často zaměřují na tuto platformu. Jedná se zejména o elektronické bankovnictví, identitu občana a podobné aplikace, které se běžně denně používají a jsou proto zranitelné a je možno pachatelem získat okamžitě zisk (sebrat peníze z cizích účtů).

Jak jsem se již ve své práci zmínil, pachatelé se samozřejmě nezaměřují jen na jednotlivce, ale podnikají také konkrétní útoky na celé organizace, nemocnice a státní správu. Toto se samozřejmě týká i České republiky. Útoky na nemocnice jsou o to nebezpečnější, že ohrožují i životy pacientů a celý chod zdravotnictví.

Dle mého názoru je Česká republika dobře připravena na boj s těmito hrozbami, a to jak po stránce legislativní, technického vybavení tak i IT expertů a v neposlední řadě i odborníky u Policie.

Samozřejmě velice podstatná věc, která se nesmí opomenout je prevence. Protože čím více budou lidé (uživatelé) obezřetní, informovaní a v tomto směru vzdělanější, tím lépe budou čelit hrozbám, které přicházejí a přicházet do budoucna určitě budou. Proto v rámci prevence se musí oslovovat celá populace, počínaje dětmi ve školách a konče seniory, kteří se bohužel v poslední době stávají terčem mnoha kyberútoků a s tím souvisejících podvodů.

SEZNAM POUŽITÉ LITERATURY

MONOGRAFIE:

1. KOPECKÝ, Kamil. *Kybergrooming - nebezpečí kyberprostoru*. Olomouc: Net University, 2010. ISBN 978-80-254-7573-7.

2. KOPECKÝ, Kamil. *Moderní trendy v elektronické komunikaci*. Olomouc: Hanex, 2007. ISBN 978-80-85783-78-0.

3. KOPECKÝ, Kamil a kol. *Rizikové formy chování českých a slovenských dětí v prostředí internetu*. 1. vyd. Olomouc: Univerzita Palackého v Olomouci, 2015. ISBN 978-80244-4868-8.

4. KUDRLOVÁ, Kateřina. *Kybergrooming* – 3 roky kriminalizace. Právo, Bezpečnost, Informace. 2017, číslo 4. ISSN 2336-3657.

5. PROVAZNÍK, Jan: § 20 [Příprava], in: F. Ščerba a kol.: *Trestní zákoník*, 1. vydání, C. H. Beck, Praha 2020. ISBN 978-80-7400-807-8

6. ŠÁMAL, Pavel. *Trestní právo hmotné.* 7., přepracované vydání. Praha: Wolters Kluwer, 2014. ISBN 9788074786167.

7. ŠKOP, Martin. *Hranice práva a kyberprostoru – subversivita kyberprostoru*, Právník č. 10/2005.

8. VÁLKOVÁ, Hana. *Kriminalita*, in: Dušan. HENDRYCH a kol.: *Právnický slovník*, 3. vydání, C. H. Beck, Praha 2009. ISBN 978-80-7400-059-1

9. VÁLKOVÁ, Helena, KUCHTA, Josef a Jana HULMÁKOVÁ. *Základy kriminologie a trestní politiky.* 3. vydání. Praha: C. H. Beck, 2019. Beckovy mezioborové učebnice. ISBN 9788074007323.

POUŽITÉ LEGISLATIVNÍ DOKUMENTY:

1. Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Obecné nařízení o ochraně osobních údajů)

2. Trestní zákoník, § 193b zákona č. 40/2009 Sb., ve znění pozdějších předpisů

POUŽITÉ ELEKTRONICKÉ ZDROJE:

1. AIRA. *Co je kyberkriminalita* [online]. 2022 [cit. 2023-05-01]. Dostupné z: https://www.sprava-site.eu/kyberkriminalita/

2. AIRA. *Co je kyberkriminalita* [online]. 2022 [cit. 2023-05-01]. Dostupné z: https://www.sprava-site.eu/sniffing/

3. AIRA. *Co je kyberkriminalita* [online]. [cit. 2023-05-01]. Dostupné z: https://www.sprava-site.eu/backdoor/

4. AIRA. *Co je kyberkriminalita* [online]. [cit. 2023-05-01]. Dostupné z: https://www.sprava-site.eu/keylogger/

5. AIRA. *Co je kyberkriminalita* [online]. [cit. 2023-05-01]. Dostupné z: https://www.sprava-site.eu/hoax/

6. AIRA. *Co je kyberkriminalita* [online]. [cit. 2023-05-01]. Dostupné z: https://www.sprava-site.eu/phishing/

7. AIRA. *Co je kyberkriminalita* [online]. [cit. 2023-05-01]. Dostupné z: https://www.sprava-site.eu/pharming/

8. ANTIVIROVÉ CENTRUM. *Internetové hrozby v lednu v České republice* [online]. 15.2.2021 [cit. 2023-04-25]. Dostupné z: https://www.antivirovecentrum.cz/aktuality/internetove-hrozby-v-ceske-republice-leden-2021.aspx

9. GALUŠKA, Karel. *Kybernetická kriminalita – letem světem* [online]. 20.8.2021 [cit. 2023-02-23]. Dostupné z: https://cz.linkedin.com/pulse/kybernetick%C3%A1-kriminalita-letem-sv%C4%9Btem-na%C5%A1im-pr%C3%A1vem-karel-galu%C5%A1ka

10. ČESKÁ TISKOVÁ KANCELÁŘ. *Nemocnice stále čelí kyberútokům,* [online]. 19.12.2022 [cit. 2023-04-25]. Dostupné z: https://www.novinky.cz/clanek/domaci-nemocnice-stale-celi-kyberutokum-

40417515

11. ČÍRTKOVÁ, Dana. *Výrazný nárůst kriminality v kybernetickém prostředí* [online]. 21.1.2021 [cit. 2023-01-21]. Dostupné z: https://www.novinyvm.cz/18888-vyrazny-narust-kriminality-v-kybernetickem-prostredi.html

12. Docplayer.cz: Kybernetická kriminalita v organizaci, [online]. 29.10.2021 [cit. 2023-01-20]. Dostupné z: https://docplayer.cz/5380892-Kyberneticka-kriminalita-v-organizaci.html

13. E-BEZPEČÍ. *Nápad trestné činnosti kybernetické kriminality*, [online]. 22.1.2020 [cit. 2023-1-18]. Dostupné z: https://www.e-bezpeci.cz/index.php/z-jinych-webu/1749-statistika-kyberneticke-kriminality-za-rok-2019

14. ESET, Digital Security. *Jak chránit firmu před riziky spojenými s RDP* [online]. 21.7.2022 [cit. 2023-01-20]. Dostupné z: https://digitalsecurityguide.eset.com/cz/jak-ochranit-firmu-pred-riziky-spojenymi-s-rdp

15. ESET, Digital Security. *Jak rozpoznat kryptominační útok?* [online]. 2023 [cit. 2023-01-12]. Dostupné z: https://www.eset.com/int/malicious-cryptominers/

16. FIŠER, Miloslav. *Vědci z Česka a USA spojí síly kvůli kyberbezpečnosti* [online]. 17.1.2023 [cit.2023-03-17]. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-vedci-z-ceska-a-usa-spoji-sily-kvuli-kyberbezpecnosti-40420204

17. FIŠER, Miloslav. *Trestných činů v kyberprostoru dramaticky přibylo* [online]. 23. 11. 2022 [cit. 2022-12-10]. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-trestnych-cinu-v-kyberprostoru-dramaticky-pribylo-hlasi-policie-40415280

18. GRIČOVÁ, Andrea. *Rozdělení NCOZ je správné* [online]. 12.6.2022 [cit.2023-05-10]. Dostupné z: https://ct24.ceskatelevize.cz/domaci/3504381-rozdeleni-ncoz-je-spravne-rekl-policejni-prezident-kriminalita-s-prichodem-uprchliku

19. HUDEČEK, Tomáš. *Úmluva o počítačové kriminalitě* [online]. 4.1.2013 [cit. 2023-02-23]. Dostupné z:https://rm.coe.int/16804931c0

20. CHOO, Kim-Kwang Raymond. *Online child grooming:a literature review on the misuse of social networking sites for grooming children for sexual offences* [online]. 2009 [cit. 2022-10-21]. ISBN 9781921185861. Dostupné z: https://www.aic.gov.au/sites/default/files/2020-05/rpp103.pdf

21. INTERNÍ MEDICÍNA. *Strategie Manipulace dětí v online prostředích* [online]. 2023 [cit. 2023-02-21]. Dostupné z:

22. https://www.internimedicina.cz/pdfs/ped/2015/05/09.pdf

23. MALÝ, Jan. *Kyberkriminalita v době krize se zaměřením na pachatele* [online]. 10.12.2021 [cit. 2023-01-20]. Dostupné z: https://advokatnidenik.cz/2021/12/10/kyberkriminalita-v-dobe-krize-se-zamerenim-na-pachatele-pravnicke-osoby/#_ftn5

24. MORAVČÍK, Ondřej. *Vývoj registrované kriminality v roce 2022* [online]. 13.1.2023 [cit. 2023-02-23]. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx

25. MVCR ČESKÉ REPUBLIKY. *Problematika informační kriminality* [online]. Květen 2021 [cit. 2023-03-01]. Dostupné z: https://www.mvcr.cz/clanek/tiskova-zprava-ze-zasedani-republikoveho-vyboru-pro-prevenci-kriminality-713175.aspx

26. NEJVYŠŠÍ STÁTNÍ ZATUPITELSTVÍ. *NSZ zpráva o činnosti za rok 2021* [online]. 2021 [cit. 2023-02-22]. Dostupné z: https://verejnazaloba.cz/nsz/cinnost-nejvyssiho-statniho-zastupitelstvi/zpravy-o-cinnosti/zprava-o-cinnosti-za-rok-2021/

27. NOVÁK, Jaromír. *Kybernetická kriminalita v roce 2021 očima státního zastupitelství* [online]. 28.7.2022 [cit. 2023-02-22]. Dostupné z: https://blog.nic.cz/2022/07/28/kyberneticka-kriminalita-v-roce-2021-ocima-statniho-zastupitelstvi/

28. Novinyvm.cz: Výrazný nárůst kriminality v kybernetickém prostředí, [online]. 29.10.2021 [cit. 2023-01-20]. Dostupné z:: https://www.novinyvm.cz/18888-vyrazny-narust-kriminality-v-kybernetickem-prostredi.html

29. NUKIB. *Národní strategie kybernetické bezpečnosti* [online]. 21.6.2022 [cit. 2023-02-21]. Dostupné z: https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

30. NUKIB. *Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)* [online]. 2023 [cit. 2023-02-21]. Dostupné z: https://www.nukib.cz/cs/o-nukib/

31. PANY, David a Steve MILLER. *Obcházení síťových omezení prostřednictvím tunelování RDP* [online]. 29.10.2021 [cit. 2023-01-20]. Dostupné z: https://www.mandiant.com/resources/blog/bypassing-network-restrictions-through-rdp-tunneling

32. POLICIE ČESKÉ REPUBLIKY. *Jednotlivé druhy kyberkriminality* [online]. 2022 [cit. 2023-01-05]. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

33. POLICIE ČEKÉ REPUBLIKY. *Statistický přehled kyberkriminality za rok 2020,* [online]. 8.7.2020 [cit. 2022-04-26]. Dostupné z: https://www.policie.cz/clanek/statisticke-prehledy-kriminality-za-rok-2020.aspx

34. POŽÁR, Josef. *Kybernetická kriminalita v organizaci* [online]. 2014 [cit. 2023-01-21]. Dostupné z: https://docplayer.cz/5380892-Kyberneticka-kriminalita-v-organizaci.html

35. PREVENCE KRIMINALITY. *Kyberkriminalita* [online]. 20.12.2022 [cit. 2022-12-27]. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/kyberkriminalita/

36. PREVENCE KRIMINALITY. *Strategie prevence kriminality v ČR 2022-2027* [online]. 2022 [cit. 2023-03-01]. Dostupné z: https://prevencekriminality.cz/wp-content/uploads/2021/10/04__spk-2022-2027_strategicka-cast.pdf

37. RM. *The global state of cybercrime legislation* [online]. 5.5.2021 [cit. 2023-02-23]. Dostupné z: https://rm.coe.int/3148-1-3-4-cyberleg-global-state-feb2020-v1-public/16809cf9a9

38. SEDLÁČKOVÁ, Veronika. *Statisíce počítačů a jediný cíl: Expert pospal nejnovější kyberútoky v Česku* [online]. 26.4.2022 [cit. 2023-04-22]. Dostupné z: https://www.seznamzpravy.cz/clanek/audio-podcast-ptam-se-ja-statisice-pocitacu-maji-jediny-cil-expert-popsal-nove-kyberutoky-v-cesku-199778

39. SEZNAM ZPRÁVY. *Expert pospal nejnovější kyberútoky v Česku,* [online]. 21.4.2022 [cit. 2023-04-25]. Dostupné z: https://www.seznamzpravy.cz/clanek/domaci-zivot-v-cesku-masivni-hackerske-utoky-na-ceske-weby-nekonci-napadeny-je-i-web-vlady-199082#utm_content=ribbonnews&utm_term=hacke%C5%99i&utm_medium=hint&utm_source=search.seznam.cz

40. TRESTNÍ ŘÁD. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/1961-141

41. TRESTNÍ ZÁKONÍK. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

42. VACOVSKÝ, Marek. *Rok 2020 přinesl více kybernetických útoků* [online]. 1.3.2021 [cit. 2023-02-01]. Dostupné z: https://mobilenet.cz/clanky/rok-2020-prinesl-krome-pandemie-koronaviru-i-vice-kybernetickych-utoku-na-nemocnice-43079

43. VEJVODOVÁ, Alžběta. *V boji proti kyberkriminality mají navrch hackeři* [online]. 17.10.2016 [cit. 2023-02-15]. Dostupné z: https://pravniradce.ekonom.cz/c1-65479680-policie-priznava-ze-v-boji-proti-kyberkriminalite-maji-navrch-hackeri

44. WELIVESECURITY. *THREAT REPORT T1 2022* [online]. 1.5.2022 [cit. 2023-01-20]. Dostupné z: https://www.welivesecurity.com/wp-content/uploads/2022/06/eset_threat_report_t12022.pdf

45. ZÁKON O POILICII ČR. *Zákony pro lidi* [online]. 2023 [cit. 2023-06-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2008-273

46. ZORMANOVÁ, Lucie. *Kybergrooming* [online]. 1.3.2022 [cit. 2023-01-14]. Dostupné z https://clanky.rvp.cz/clanek/22970/KYBERGROOMING.html

47. ŽIVĚ. *Česko zasáhl největší DDoS útok,* [online]. 3.12.2022 [cit. 2023-04-25]. Dostupné z: https://www.zive.cz/clanky/cesko-zasahl-nejvetsi-ddos-utok-v-historii-v-cem-byl-specificky-mohl-byt-rizeny-z-ruska-rozhovor-s-tomasem-krestakem-z-o2/sc-3-a-219591/default.aspx

SEZNAM POUŽITÝCH OBRÁZKŮ

SEZNAM POUŽITÝCH ZKRATEK

CERT - činnost Vládního CERT České republiky

DDoS útoky -Denial-of-service je typ útoku na internetové služby nebo stránky

ESET – Firma ze slovenska, která má specializaci na online bezpečnost a antivir

FRA - European Union Agency for Fundamental Rights

GDPR - Obecné nařízení o ochraně osobních údajů

IKSP - Institut pro kriminologii a sociální prevenci

IS PČR - lustrační systém PČR

NAT adresa - Network Address Translation

NCKB - Národní centrum kybernetické bezpečnosti

NCTEKK - Národní centrála proti terorismu, extremismu a kybernetické kriminalitě

NIS - Network Information Security

NÚKIB - Národní úřad pro kybernetickou a informační bezpečnost

OKTE - Odbor kriminalistické techniky a expertiz

OSZ - Okresní státní zastupitelství

RDP - Remote desktop protokol

RIPE NCC - Mezinárodní organizace, nezávislá, podporující infrastruktury internetu pomocí technických koordinací v regionech, kde působí

SSH - Secure shell protokol

SEZNAM PŘÍLOH

Příloha č. 1 : Vzor žádosti policejního orgánu o poskytnutí informací podle § 8/1 trestního řádu

Příloha č. 2: Vzor protokolu o vydání věci

Příloha č. 3: Zákon číslo 226/2022 Sb., kterým se mění zákon číslo 181/2014 Sb., o kybernetické bezpečnosti – strana první

Příloha č. 3: Zákon číslo 226/2022 Sb., kterým se mění zákon číslo 181/2014 Sb., o kybernetické bezpečnosti – strana druhá

Příloha č. 3: Zákon číslo 226/2022 Sb., kterým se mění zákon číslo 181/2014 Sb., o kybernetické bezpečnosti – strana třetí

PŘÍLOHY PRÁCE

Příloha č. 1 : Vzor žádosti policejního orgánu o poskytnutí informací podle § 8/1 trestního řádu

POLICIE ČESKÉ REPUBLIKY
Krajské ředitelství policie Jihočeského kraje
Služba kriminální policie a vyšetřování
Odbor analytiky
Oddělení kybernetické kriminality

Č. j. KRPC

České Budějovice 5. prosince 2017
Počet stran: 1

Seznam. cz, a.s.
Radlická 3294/10
150 00 PRAHA 5
IČ: 26168685

Žádost o poskytnutí informací podle § 8/1 trestního řádu

V souladu s ustanovením **§ 8/1 trestního řádu** žádám o sdělení informací k ustanovení uživatele níže uvedené emailové adresy:

Radek.Novotny@email.cz

1. Aktuální registrační údaje včetně autentizačního tel. čísla

2. Přístupové záznamy k výše uvedenému účtu

3. Uveďte všechny vámi evidované žádosti o vydání hesla k účtu (změna hesla, ověření uživatele jiným způsobem nežli heslem - kontrolní otázky, zaslání hesla na autentizační email, telefon atd.)

Požadované informace zašlete prosím v **elektronické podobě** ke shora uvedenému číslu jednacímu datovou schránkou na adresu Policie České republiky, Krajské ředitelství policie Jihočeského kraje,

kpt. Mgr. Jan Neznámý
vrchní komisař

VZOR

Příloha č. 2: Vzor protokolu o vydání věci

POLICIE ČESKÉ REPUBLIKY
Krajské ředitelství policie Jihočeského kraje
Služba kriminální policie a vyšetřování
Odbor analytiky
Oddělení kybernetické kriminality
Lannova 26, 370 74 České Budějovice

VZOR

Č. j. KRPC-

České Budějovice 1. prosince 2017
Počet stran: 1

Protokol o vydání věcí

Dne **11.12.2017** v **15:02** hodin byl(a) podle § 78 odst. 1 trestního řádu vyzván(a):**Radek Novotný,**

k vydání:

- notebook zn. HP, výr. č. NXM2E, používaný, poškozený pravý horní pant, včetně napájecího kabelu (zapečetěno do plastového sáčku)

- mobilní telefon zn. Nokia, bez SIM a paměťové karty, IMEI1: 866952764374987978, včetně nabíječky a plastového krytu (zapečetěno č. pečeti 0069)

jako věcí, které mohou sloužit pro důkazní účely.
Poučení:
Podle § 78 odst. 1 trestního řádu, kdo má u sebe věc důležitou pro trestní řízení, je povinen ji na vyzvání vydat, nevyhoví-li výzvě, může mu být věc odňata (§ 79 trestního řádu).
Podle § 78 odst. 2 trestního řádu, povinnost podle odstavce 1 se nevztahuje na listinu nebo na jiný hmotný nosič obsahující obrazový, zvukový nebo datový záznam, jejichž obsah se týká okolnosti, o které platí zákaz výslechu, ledaže došlo k zproštění povinnosti zachovat věc v tajnosti nebo k zproštění povinnosti mlčenlivosti.
Podle § 78 odst. 3 trestního řádu, nikoho nelze nutit, aby předložil nebo vydal věc, jež v době, kdy je požádáno o její předložení nebo vydání, může sloužit jako důkaz proti němu nebo proti jeho osobě blízké; tím nejsou dotčena ustanovení o odnětí věci, domovní prohlídce, prohlídce jiných prostor a pozemků a osobní prohlídce.
Podle § 78 odst. 4 trestního řádu, je-li to potřebné pro účely zabránění zmaření propadnutí nebo zabrání věci, orgán činný v trestním řízení uvedený v odstavci 1 vydá příkaz, že osoba, jíž byla věc zajištěna, nesmí po dobu zajištění takovou věc převést na jinou osobu nebo ji zatížit. Právní jednání učiněné v rozporu s tímto zákazem je neplatné; soud k neplatnosti přihlédne i bez návrhu.
Podle § 78 odst. 7 trestního řádu, osoba, které byla věc zajištěna, má právo kdykoli žádat o vrácení takové věci. Byla-li žádost zamítnuta, může ji tato osoba, neuvede-li v ní nové důvody, opakovat až po uplynutí 30 dnů od právní moci rozhodnutí.

Po poučení vyzvaná osoba uvádí:

Dobrovolně vydávám svůj mobilní telefon a notebook včetně nabíječek pro účely znaleckého zkoumání.

Po přečtení prohlašuji, že protokol souhlasí, nežádám oprav ani doplnění a jako správný a úplný podepisuji dne 1.12.2017 v 10:05 hodin.

Osoba, která věci převzala:	Přítomen:	Osoba, která věci vydala:
kpt. Mgr. Jan Neznámý vrchní komisař	kpt. Ivan Neznámý	Radek Novotný

Současně potvrzuji, že jsem převzal(a) kopii tohoto protokolu jako potvrzení o vydání věci

Příloha č. 3: Zákon číslo 226/2022 Sb., kterým se mění zákon číslo 181/2014 Sb., o kybernetické bezpečnosti – strana první

226/2022 Sb.

ZÁKON

ze dne 20. července 2022,

kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů

Parlament se usnesl na tomto zákoně České republiky:

ČI.I

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., zákona č. 183/2017 Sb., zákona č. 205/2017 Sb., zákona č. 35/2018 Sb., zákona č. 111/2019 Sb., zákona č. 12/2020 Sb. a zákona č. 261/2021 Sb., se mění takto:

1. V § 1 odstavec 2 včetně poznámek pod čarou č. 6 a 17 zní:

"(2) Tento zákon zapracovává příslušný předpis Evropské unie[6], zároveň navazuje na přímo použitelný předpis Evropské unie[17] a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů.

6) Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

17) Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA ("Agentuře Evropské unie pro kybernetickou bezpečnost"), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 ("akt o kybernetické bezpečnosti").".

2. V § 22 se na konci písmene x) tečka nahrazuje čárkou a doplňuje se písmeno y), které zní:

"y) je orgánem certifikace kybernetické bezpečnosti podle čl. 58 aktu o kybernetické bezpečnosti[17].".

3. Za § 22a se vkládá nový § 22b, který včetně nadpisu zní:

"§ 22b

Autorizace subjektů posuzování shody podle aktu o kybernetické bezpečnosti

(1) Stanoví-li přímo použitelný předpis Evropské unie vydaný na základě aktu o kybernetické bezpečnosti konkrétní nebo dodatečné požadavky na subjekty posuzování shody s cílem zajistit jejich technickou způsobilost k hodnocení

Příloha č. 3: Zákon číslo 226/2022 Sb., kterým se mění zákon číslo 181/2014

požadavků na kybernetickou bezpečnost, Úřad v souladu s čl. 58 odst. 7 písm. e) aktu o kybernetické bezpečnosti [17] rozhoduje o žádostech o autorizaci subjektu posuzování shody, a pokud autorizovaný subjekt posuzování shody porušuje požadavky aktu o kybernetické bezpečnosti[17] nebo přímo použitelného předpisu Evropské unie vydaného na základě aktu o kybernetické bezpečnosti, o pozastavení vykonatelnosti, o změně nebo o zrušení rozhodnutí o autorizaci.

(2) Subjekt posuzování shody v žádosti o autorizaci podle odstavce 1 doloží plnění konkrétních nebo dodatečných požadavků stanovených přímo použitelným předpisem Evropské unie vydaným na základě aktu o kybernetické bezpečnosti.

(3) V rozhodnutí o pozastavení vykonatelnosti rozhodnutí o autorizaci podle odstavce 1 stanoví Úřad lhůtu pro zjednání nápravy. Zjedná-li subjekt posuzování shody nápravu, sdělí tuto skutečnost bez zbytečného odkladu Úřadu. Shledá-li Úřad zjednání nápravy za dostačující, zruší rozhodnutí o pozastavení vykonatelnosti rozhodnutí o autorizaci. Jestliže autorizovaný subjekt posuzování shody ve stanovené lhůtě nezjedná nápravu, rozhodne Úřad o změně či zrušení rozhodnutí o autorizaci.

(4) Úřad rozhodne v řízení o žádosti o autorizaci podle odstavce 1 nejdéle do 120 dnů od zahájení řízení, v mimořádných případech do 180 dnů.".

4. V § 25 se za odstavec 10 vkládají nové odstavce 11 až 13, které znějí:

"(11) Výrobce nebo poskytovatel produktů, služeb nebo procesů vydávající EU prohlášení o shodě se dopustí přestupku tím, že

a) vydá EU prohlášení o shodě, ač pro jeho vydání nejsou splněny podmínky stanovené aktem o kybernetické bezpečnosti[17],

b) neuchovává dokumenty a informace podle čl. 53 odst. 3 aktu o kybernetické bezpečnosti[17],

c) nepředloží vyhotovení EU prohlášení o shodě Úřadu a agentuře ENISA podle čl. 53 odst. 3 aktu o kybernetické bezpečnosti[17], nebo

d) neposkytuje informace o kybernetické bezpečnosti v rozsahu a způsobem uvedeným v čl. 55 aktu o kybernetické bezpečnosti[17].

(12) Držitel evropského certifikátu kybernetické bezpečnosti se dopustí přestupku tím, že neinformuje příslušné subjekty posuzování shody o veškerých později zjištěných zranitelnostech nebo nesrovnalostech.

(13) Právnická nebo podnikající fyzická osoba se dopustí přestupku tím, že

a) zneužije známku nebo označení evropského systému certifikace kybernetické bezpečnosti, evropský certifikát kybernetické bezpečnosti, EU prohlášení o shodě anebo jiný dokument podle aktu o kybernetické bezpečnosti[17],

b) padělá nebo pozmění evropský certifikát kybernetické bezpečnosti, EU prohlášení

Příloha č. 3: Zákon číslo 226/2022 Sb., kterým se mění zákon číslo 181/2014 Sb., o kybernetické bezpečnosti – strana třetí

o shodě anebo jiný dokument podle aktu o kybernetické bezpečnosti[17],

c) provede činnost posouzení shody podle aktu o kybernetické bezpečnosti[17] na úroveň záruky "vysoká", přestože k tomu není oprávněna podle čl. 56 odst. 6 aktu o kybernetické bezpečnosti[17],

d) jako subjekt posuzování shody autorizovaný podle čl. 60 odst. 3 aktu o kybernetické bezpečnosti[17] vydá evropský certifikát kybernetické bezpečnosti k produktu, procesu nebo službě, které nesplňují kritéria obsažená v přímo použitelném předpise Evropské unie vydaném na základě aktu o kybernetické bezpečnosti,

e) provede činnost posouzení shody, vyhrazenou přímo použitelným předpisem Evropské unie vydaným na základě aktu o kybernetické bezpečnosti autorizovanému subjektu posuzování shody, bez autorizace, nebo

f) vystupuje jako akreditovaný subjekt posuzování shody bez akreditace podle čl. 60 odst. 1 aktu o kybernetické bezpečnosti[17] nebo mimo rozsah této akreditace.".

Dosavadní odstavec 11 se označuje jako odstavec 14.

5. V § 25 odst. 14 písm. a) se slovo "nebo" nahrazuje čárkou a na konci textu písmene se doplňují slova "anebo odstavce 12 nebo 13".

6. V § 25 odst. 14 písm. b) se slova "písm. f) nebo" nahrazují textem "písm. f)," a na konci textu písmene se doplňují slova "nebo odstavce 11".

Čl.II

Účinnost

Tento zákon nabývá účinnosti dnem následujícím po dni jeho vyhlášení.

Pekarová Adamová v. r.

Zeman v. r.

Fiala v. r.