VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2022 Martina Molnárová

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

KYBERKRIMINALITA V EU

CYBERCRIME IN THE EU

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — Martina Molnárová
AUTHOR

VEDOUCÍ PRÁCE — Mgr. Václav Stupka, Ph.D.
SUPERVISOR

BRNO 2022

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Studentka: Martina Molnárová ***ID:*** 221037

Ročník: 3 ***Akademický rok:*** 2021/22

NÁZEV TÉMATU:

Kyberkriminalita v EU

POKYNY PRO VYPRACOVÁNÍ:

Bakalářská práce se bude věnovat problematice kyberkriminality v Evropské Unii. V práci bude provedena analýza a klasifikace škodlivých jednání páchaných v prostředí informačních a komunikačních technologií a relevantních skutkových podstat trestního práva, prostřednictvím kterých jsou tato škodlivá jednání stíhatelná. Součástí práce bude rovněž analýza vycházející z aktuálních statistik páchání těchto trestných činů zaměřená na identifikaci trendů v této oblasti. V neposlední řadě budou v práci kritické analýze podrobeny současné aktivity a záměry bezpečnostních složek v EU zaměřené na prevenci a vyšetřování kyberkriminality. Součástí práce bude vytvoření webové aplikace v jazyce .NET, která bude sloužit jako rozcestník informací o současných trendech v kyberkriminalitě. Aplikace bude obsahovat strukturované informace o jednotlivých typech kyberkriminality kategorizovaných podle vybrané taxonomie. Aplikace bude umožnovat pokročilé vyhledávání ve strukturovaných datech. Aplikace bude rovněž zpracovávat existující statistické informace vázané na jednotlivé skutky a interpretovat je grafickou formou.

DOPORUČENÁ LITERATURA:

[1] KOLOUCH, Jan. Cybercrime. Praha, CZ.NIC, z.s.p.o. 2016. ISBN 978-80-88168-15-7.

[2] KREMLING, Janine a Amanda M. Sharp PARKER. Cyberspace, cybersecurity and cybercrime. Los Angeles: London. 2018. ISBN 978-1-5063-4725-7.

Termín zadání: 7.2.2022 ***Termín odevzdání:*** 31.5.2022

Vedoucí práce: Mgr. Václav Stupka, Ph.D.

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

Abstrakt

Táto bakalárska práca sa zaoberá kybernetickou kriminalitou v Európskej únii v súčasnosti. Začína popisom najznámejších historických kybernetických zločinov, ktoré dopomohli k vzniku kybernetickej kriminality ako samostatného odvetvia kriminality. Následne sú v práci popísané zmeny ku ktorým došlo pri vývoji kybernetickej kriminality, popisuje praktické problémy pri stíhaní kybernetickej kriminality a jej súčasné trendy. Zároveň načrtá problémy, ktoré vznikajú pri vytváraní adekvátnych štatistických údajov. V praktickej časti práce je následne popísaná základná funkcia aplikácie, ktorá bola vytvorená k práci za účelom podania informácií o kyberkriminalite a prehľadnému sprostredkovaniu dostupných štatistických informácií.

Kľúčové slová

Kybernetická kriminalita (kyberkriminalita), kybernetický incident, kybernetický zločin, skutková podstata, vírus, malware, ransomware, kyberpriestor, webová aplikácia

Abstract

This bachelor thesis deals with cybercrime in the European Union at present time. It begins with a description of the most well-known historical cybercrimes, which has helped to create cybercrime as a separate branch of crime. Subsequently, the work describes the changes that have occurred in the development of cybercrime, describes the practical problems in prosecuting cybercrime and its current trends. At the same time, it outlines the problems that arise in producing adequate statistics. The practical part of the work then describes the basic function of the application, which was created to work for the purpose of providing information on cybercrime and clear mediation of available statistical information.

Keywords

Cybercrime, cyber incident, virus, malware, ransomware, cyberspace, web application

Prehlásenie autora o pôvodnosti diela

Jméno a příjmení studenta:	Martina Molnárová
VUT ID studenta:	221037
Typ práce:	Bakalářská práce
Akademický rok:	2021/22
Téma závěrečné práce:	Kyberkriminalita v EU

Prohlašuji, že svou závěrečnou práci jsem vypracoval samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

.

V Brne dňa: 25.mája 2022 ----------

podpis autora

Bibliografická citácia

Molnárová, M. Kyberkriminalita v EU. Brno: Vysoké učení technické v Brne, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2022. 66 s. Bakalárska práca. Vedúci práce: prof. Mgr. Václav Stupka, Ph.D.

Poďakovanie

Týmto by som chcela poďakovať vedúcemu bakalárskej práce Prof. Mgr. Václavovi Stupkovi, Ph.D. za trpezlivosť, cenné rady a metodickú pomoc, ktoré mi pri písaní práce veľmi pomohli.

V Brne dňa: 25.mája 2022 ----------

podpis autora

Obsah

ZOZNAM OBRÁZKOV

ÚVOD

Cieľom tejto bakalárskej práce je vykonanie zberu dát o kybernetickej kriminalite na základe dostupných zdrojov z tejto oblasti a následná analýza týchto dát (desk research) za účelom definovania problémov pri stíhaní kybernetickej kriminality v Európskej únií. Zároveň táto práca ozrejmuje samotný pojem kyberkriminalita a jeho začlenenie do súčasnej legislatívnej problematiky z pohľadu spolupráce jednotlivých krajín Európskej únie, pri riešení zločinov uskutočnených cez kyberpriestor. Zároveň pojednáva o súčasných trendoch v kyberkriminalite a informuje o súčasnej činnosti (vytváranie medzinárodných zmlúv, snahy o vytvorenie jednotného delenia kybernetických incidentov na základe ich skutkových podstát, efektívnejšie zdieľanie elektronických dôkazných materiálov, atď.) v boji proti kyberkriminalite.

Prvá kapitola teoretickej časti tejto práce predstavuje úvodné vymedzenie pojmu kyberkriminalita, začlenenie tohto pojmu do súvislosti s trestnou činnosťou. Zároveň definuje pojmy kriminalita a kyberpriestor, ktoré tvoria samotný pojem kyberkriminalita. Taktiež prikladá tomuto pojmu historický kontext a popisuje z môjho pohľadu najdôležitejšie udalosti, ktoré najviac dopomohli k definovaniu problému, ktorý kybernetické zločiny predstavujú pomocou najznámejších kybernetických zločinov.

Úmyslom druhej kapitoly je predstavenie v súčasnosti najviac rozšírených druhov kybernetickej kriminality v Európe na základe ich závažnosti. Zároveň je v tejto kapitole načrtnutý základný legislatívny rámec o kybernetickej kriminalite v Európskej únií, ktorý umožňuje jej stíhanie na medzinárodnej úrovni a špecializované organizácie, ktoré boli vytvorené pre zefektívnenie odhaľovania a stíhania kybernetickej kriminality v Európskej únií a v medzinárodnom spoločenstve.

Nasledujúca kapitola tejto práce pojednáva o súčasných trendoch v oblasti kybernetickej kriminality a ozrejmuje problematiku tvorby štatistických údajov. V neposlednom rade uvádza ekonomické dopady kybernetickej kriminality na súčasnú spoločnosť a vplyv pandémie Covid-19 na rozmach a zmeny v súčasnej kybernetickej kriminalite.

Posledná kapitola teoretickej časti tejto práce komplexne definuje požiadavky kladené na efektívne odhaľovanie a stíhanie kybernetickej kriminality, primárne na problémy spojené s vytvorením všeobecne záväznej taxonómie kybernetickej kriminality. Zároveň uvádza príklady v súčasnosti využívaných taxonómií a bližšie vysvetľuje v Európskej únií využívanú taxonómiu ENISA/Europol a alternatívne delenie kybernetických incidentov CIA triádu.

V praktickej časti tejto práce je v prvej jej kapitole načrtnutý popis fungovania webovej aplikácie, prostriedkov, ktoré boli využité za účelom vytvorenia tejto aplikácie, a základný popis problematiky vývoja webovej aplikácie a predstavuje teoretickú rovinu potrebnú na pochopenie problematiky vývoja. V neposlednom rade tiež uvádza základné požiadavky na vytvorenú webovú aplikáciu.

V poslednej kapitole tejto časti práce je riešená praktická implementácia návrhu. Nachádzajú sa tu aj praktické ukážky najzaujímavejších častí kódu, ktoré umožňujú lepšie načrtnutie celkovej funkcie webovej aplikácie.

V závere tejto práce sú následne zhrnuté výsledky vyplývajúce z teoretickej časti tejto práce. V tejto kapitole je taktiež zhrnutie praktickej časti tejto práce, webovej aplikácie, ktorá bola vytvorená za účelom lepšej orientácie v informáciách ohľadom kyberkriminality.

1. ÚVOD DO PROBLEMATIKY KYBERKRIMINALITY

S rastúcim využívaním informačných technológií v globálnom meradle, je možné odsledovať, že využívanie počítačov a Internetu je v súčasnej dobe prakticky všadeprítomné. S rastúcim trendom využívania týchto technológií rastie aj možnosť využívania technológií za účelom ich zneužitia. Je teda možné konštatovať, že informačné technológie vytvárajú novú platformu, ktorá umožňuje širšie rozvinutie, či už existujúcej kriminality, alebo vytvorenia úplne nových typov zločinov.

Kyberkriminalitu, ako ju poznáme dnes, je možné datovať od osemdesiatych rokov minulého storočia, kedy bolo zaznamenané prvé využitie informačných technológií na vykonanie zločinu. V súčasnosti však kyberkriminalita predstavuje omnoho serióznejší problém, pretože sa zvýšila rafinovanosť a sofistikovanosť konania samotných páchateľov, ale aj technológií, ktoré na protiprávne konanie využívajú. Taktiež aj rozmanitosť jednotlivých zločinov je väčšia, a to aj v porovnaní s ostatným desaťročím. Pre lepšie pochopenie termínu kyberkriminalita, je vhodné oboznámiť s pojmami kriminalita (zločinnosť) a kyberpriestor, z ktorých bol pojem kyberkriminalita vytvorený.

Kriminalita je v priamom slova zmysle akákoľvek úmyselná činnosť, ktorá je protiprávna, postihnuteľná a potrestateľná zákonom. Samotná definícia pojmu sa z historického pohľadu menila len mierne, kritériá konania, ktoré sú považované za zločin sa menili zároveň so zmenami sociálnych noriem a územnou lokalitou, čo je rozhodujúce pri tvorbe opatrení zameraných na boj proti kyberkriminalite. Napríklad v Európskej únii je v súčasnosti vďaka vytvoreným medzinárodným organizáciám ako je napr. Europol, možná koordinácia opatrení prijatých proti kybernetickým zločinom, avšak niektoré štáty v iných častiach sveta, ako sú India alebo niektoré africké štáty, ktoré sa stretávajú s narastajúcim množstvom kybernetických zločinov, majú legislatívu značne nedostatočnú alebo v horšom prípade neexistujúcu.

Jedno z prvých využití slova kyberpriestor (cyberspace) bolo zaznamenané v roku 1984 v novele Neuromancer, ktorej autorom je William Gibson (ENISA, 2015). Aj keď táto definícia má len málo spoločného so súčasným významom slova, je možné ju

parafrázovať a definovať kyberpriestor ako abstraktné prostredie slúžiace na reprezentáciu dát, v ktorom priestore počítače fungujú.

Americký národný inštitút pre štandardy a technológie (NIST) v preklade definuje kyberpriestor nasledovne: „Globálna doména v rámci informačného prostredia pozostávajúca zo vzájomne prepojenej siete infraštruktúr, informačných systémov, vrátane internetu, telekomunikačných sietí, počítačových systémov a vstavaných procesorov a kontrolérov.“ Zároveň podľa slovníka Cambridge dictionary je kyberpriestor v preklade definovaný ako elektronický systém, ktorý umožňuje počítačom po celom svete navzájom komunikovať a získavať informácie (Cambridge dictionary, 2022). Z týchto dvoch definícií je zjavné, že v súčasnosti neexistuje presné vymedzenie tohto pojmu, avšak na ich základe je možné definovať kyberpriestor ako abstraktný priestor, primárne prostredie Internetu tvorené počítačovou sieťou, ktoré je oddelené od fyzického sveta.

Po vysvetlení definícií týchto dvoch pojmov je následne možné určiť čo pojem kyberkriminalita znamená v súčasnosti. Európska komisia definuje kyberkriminalitu ako činnosť pozostávajúcu z trestných činov spáchaných online pomocou elektronických komunikačných sietí alebo informačných systémov (Európska komisia). Táto definícia v jednoduchosti zahŕňa všetku kybernetickú kriminalitu.

1.1 Historický kontext

Táto podkapitola popisuje a pojednáva o histórií a vývoji kybernetickej kriminality a v tejto práci je zahrnutá, aby poskytla lepšie pochopenie jednotlivých zločinov, ktoré formovali toto odvetvie kriminality v súčasnosti. Nakoľko je história kyberkriminality, ktorú je možné sledovať len posledných štyridsať rokov veľmi bohatá, sú v tejto kapitole zahrnuté len tie zločiny, ktoré boli svojho druhu prvé, alebo tak významné, že zmenili smer vývoja a samotný pohľad na kybernetickú kriminalitu.

Aj keď je možné povedať, že história kyberkriminality sa začala písať už v 60-tych rokoch minulého storočia, faktom zostáva to, že v tej dobe nebol tento pojem definovaný tak, ako ho poznáme dnes. Z tohto pohľadu sa jej história začala písať až v 80-tych rokoch, keď boli zaznamenané prvé veľké kybernetické incidenty, ktoré zapadajú do súčasného chápania tohto pojmu.

1.2 Počiatky kybernetickej kriminality

V 80-tych rokoch minulého storočia boli počítače využívané už aj bežnými používateľmi. V tomto období bola ochrana dát len málo skúmaná, a ešte menej aplikovaná, čo umožnilo využitie zraniteľností vtedajších systémov. Ich zraniteľnosti boli v tom čase prehliadané z dôvodu, že sa neočakávalo ich využitie na spôsobenie ťažkostí pre vtedajších používateľov. V tejto dobe ešte neboli známe kybernetické útoky, ktoré by zasahovali veľké množstvo koncových používateľov alebo systémov. Ochrana dát používateľov bola výrazne podcenená, čo umožnilo rapídne šírenie prvého škodlivého počítačového programu, ktorý je v súčasnosti známy ako prvý zdokumentovaný počítačový červ.

V novembri roku 1988 bol vytvorený počítačový program nazvaný Morris Worm (Morrisov Červ), pomenovaný podľa jeho tvorcu, Roberta Tappana Morrisa. Rozšírenie tohto škodlivého programu viedlo k zmene vnímania počítačovej bezpečnosti ako u samotných vývojárov, tak aj koncových používateľov. Zdroje uvádzajú množstvo dôvodov pre vytvorenie a rozšírenie tohto programu a nie je možné presne povedať, či účelom tohto programu bolo zahltenie vtedajších zariadení, ktoré využívali OS UNIX alebo, či samotné zahltenie bolo len vedľajším produktom (Boettger, 2000). Samotný program škodlivý nebol, nakoľko jeho jedinou funkciou bola replikácia, ktorá na základe dizajnovej chyby umožňovala viacnásobnú replikáciu na infikovanom zariadení a viedla k spomaleniu infikovaného počítača. Pravdou však zostáva to, že pán Morris vytvoril samoreplikujúci sa program, vďaka ktorému sa stal prvým zdokumentovaným prípadom, a teda človekom, ktorý bol za vytvorenie škodlivého programu aj odsúdený (Kelty, 2011).

Rok 1989 bol rokom, kedy bolo zaznamenané ďalšie prvenstvo v oblasti kybernetických incidentov, ale tentokrát sa vyskytol incident oveľa už škodlivejší ako bol predchádzajúci. V tom roku bol zaznamenaný vznik prvého ransomwaru, ktorý je známy ako AIDS Trojan alebo aj PC Cyborg Ransomware. Samotný vírus bol šírený za pomoci diskiet, ktoré boli rozdávané pacientom, ktorí boli infikovaní AIDS. Samotné fungovanie tohto programu boli založené na tom, že pri vložení diskety do počítača, bol sledovaný počet bootovaní operačného systému (ďalej len OS) a pri dosiahnutí počtu deväťdesiat, boli údaje na zariadení zašifrované. Ransomware následne vyzval obete, ktorých zariadenia boli v danom stave nepoužiteľné, na zaslanie výkupného, po ktorom zaplatení boli dáta

dešifrované. Aj keď samotný design je na súčasné pomery veľmi jednoduchý, tento program predstavil koncepty, ktoré sú využívané dodnes (Gail-Joon Ahn, 2017).

V roku 1999 boli počítačové vírusy a techniky, vďaka ktorým fungovali, ešte relatívne neznáme, ale s rozvojom svetovej počítačovej siete, sa zneužívanie technológií rozvinulo do kyberkriminality, tak ako ju poznáme dnes. Neefektívnosť bezpečnostných techník tej doby dopomohla k rýchlemu šíreniu počítačového vírusu známeho ako Melissa. Tento vírus po infikovaní zariadenia preberal kontrolu nad MS Wordom používateľa a jeho šírenie bolo zabezpečené pomocou emailu. Pri otvorení prílohy priloženej k mailu, ktorá bola pomenovaná tak, aby zaujala, bola podobná správa poslaná prvým päťdesiatim ľuďom v adresnej knihe obete, čo zabezpečilo rýchle šírenie škodlivého programu. Derivácie tejto techniky sú v súčasnosti využívané pri sociálnom inžinierstve a spamových správach (FBI, 2019).

1.3 Globálne incidenty posledného desaťročia

V závislosti od rastúcej digitalizácie systémov spoločnosti a bežnom využívaní informačných technológií, posledné desaťročie prinieslo veľké zmeny pri aplikovaní škodlivých softwarov. Tieto sa stali sofistikovanejšími a viac vyhľadávanými organizovanými skupinami, jednotlivcami a pravdepodobne aj štátnymi útvarmi. Pozmenené boli aj ciele samotných útokov, nakoľko sa nejedná len o útoky, na jednotlivých používateľov, ale aj o ciele štátneho alebo medzinárodného významu. Súčasne bola zaregistrovaná aj možnosť využitia škodlivých softwarov na presadenie politických alebo štátnych cieľov, a ľudstvo vstúpilo do novej éry v oblasti závažnosti a rozsahu kybernetických incidentov.

V roku 2010 bol zaznamenaný bezpečnostný incident, ktorý umožnil bližšie definovať nový pojem v oblasti kybernetických incidentov, a to: kybernetická zbraň alebo kyberzbraň. Stuxnet je špecifický červ, ktorý bol objavený v Iránskom počítači. Primárna funkcia Stuxnetu je zameraná na systémy, získanie informácií a ovládnutie dohľadových zariadení. Na základe toho, že na vytvorenie takto zložitého programu je potrebná pracovná sila a značné finančné prostriedky, a tiež to, že bol objavený v systéme iránskeho jadrového programu, prevažuje presvedčenie, že pôvod tohto červa je viazaný na Spojené štáty americké v spolupráci s Izraelom. Na základe jeho charakteristík, je

možné ho označiť za kyberzbraň. Objavenie červa viedlo k prehodnoteniu toho, akým spôsobom sú vnímané kybernetické hrozby na úrovni štátneho zabezpečenia (Baezner, 2017).

Rapídne šírenie digitalizácie medzi bežných používateľov síce umožnilo lepší a jednoduchší prístup k informáciám, ale zároveň aj otvorilo cestu pre rafinovanejšie využitie škodlivých softwarov (malware). V období posledného desaťročia sa zmenil profil mnohých malwarov, medzi inými aj ransomwaru a v tomto období bol zaznamenaný aj zatiaľ najhorší útok takéhoto typu (Savita Mohurle, 2017). WannaCry bol prvým známym ransomwarom, ktorý operoval ako červ, tj. pri distribúcií sa sám replikoval, čo umožnilo jeho rapídne šírenie. Samotný software využíval zraniteľnosti na starších OS Windows, ktoré boli v tejto dobe v značnej miere využívané, pričom najväčší problém vznikol v USA, kde bol najviac zasiahnutý sektor zdravotníctva (S. Ghafur, 2019).

Na základe vyššie popísaných incidentov, ich rozsahu a závažnosti, je možné konštatovať, že kyberkriminalita má v súčasnosti stúpajúcu tendenciu aj z pohľadu počtu útokov, ktoré sa zvyšujú s rastúcou mierou digitalizácie, aj závažnosťou kybernetických incidentov.

1.4 Kybernetické incidenty v Európe

S rozvojom technológií umožňujúcich anonymizáciu používateľov a zariadení, ako napríklad virtuálna privátna sieť (VPN), je čím ďalej tým náročnejšie identifikovať nielen autora škodlivého software, ale aj jeho zdroj. Zároveň rastú požiadavky na medzinárodnú spoluprácu pri odhaľovaní kybernetických zločinov. Aj keď je náročné identifikovať autora a zdroj škodlivého softwaru, je možné na základe lokalizácie obete určiť približné miesto kybernetického zločinu. Zároveň na základe počtu obetí jednotlivých útokov je následne možné určiť aj ich počet v krajine, alebo väčšom zoskupení krajín.

Takto zaznamenaný incident sa odohral v roku 2007, kedy bolo cieľom Estónsko. Tento kybernetický zločin sa odohral v rozmedzí troch mesiacov, kedy bol systém serverov Estónska napádaný DDoS útokmi, ktoré ochromili ich činnosť. DDoS je typom útoku, ktorý má za úlohu úplne ochromiť alebo spomaliť atakovanú službu alebo systém. Aj keď sa na základe vtedajšej situácie pripisuje vina Rusku, nie je možné z určitosťou

povedať, kto za týmto útokom stál. Tento útok je popisovaný ako útok kybernetickou zbraňou (Lesk, 2007).

Pri zvyšujúcom sa počte kybernetických zločinov, ich decentralizácií a narastajúcich problémoch spojených so stíhaním a odsúdením ich tvorcov, bolo odpoveďou zo strany Európskej únie vytvorenie koordinačných a bezpečnostných skupín už existujúcich bezpečnostných zložiek. Tieto majú za úlohu sledovať, koordinovať a prípadne pomáhať s riešením kybernetických zločinov členským štátom v Európskej únie. Vytvorením týchto skupín je zaznamenaná lepšia identifikácia kybernetických zločinov a ich obetí.

Príkladom, ktorý demonštruje fungovanie boja proti kyberkriminalite je odhalenie a rozloženie organizovanej skupiny, ktorá vykonávala útoky na bankomaty. Bezpečnostnými zložkami bola táto séria útokov nazvaná ATM Black Box, a je druhom logického útoku prostredníctvom pripojenia neautorizovaného zariadenia (notebooku), ktorý posielal príkazy na výdaj priamo do bankomatu s cieľom vybrať z bankomatu finančnú hotovosť a presvedčiť ho, že s ním komunikuje legitímny používateľ. Páchatelia získavajú prístup k ATM zvyčajne vŕtaním otvorov, alebo roztavením hlavného panelu, aby mohli spomenuté zariadenie fyzicky pripojiť. Zariadenie po pripojení do kabeláže začne posielať príkazy, ktoré spôsobia, že bankomat vydá všetku hotovosť. Jednalo sa o medzinárodnú organizovanú skupinu, z ktorého dôvodu boli realizované príkazy na zatknutie v niekoľkých členských štátoch Európskej únie a páchatelia boli za svoje konanie trestne stíhaní (Europol, 2017).

Jedným z príkladov medzinárodnej spolupráce je eliminácia jednej z najdlhšie fungujúcich rodín škodlivého softwaru s názvom Andromeda. Škodlivý kód tejto skupiny vírusov tvoril širokú sieť botnetov (zariadenia infikované malwarom, ktoré sú pod kontrolou zločinca). Primárnym cieľom Andromedy bola distribúcia malwaru. Na základe možností medzinárodnej spolupráce, ktorú umožňuje spolupráca bezpečnostných zložiek a adekvátna legislatíva, bolo možné koordinovať zásahy na serveroch, ktoré distribuovali Andromedu, čo viedlo k zastaveniu jej činnosti (Europol, 2017).

V Európe bol podľa spoločnosti Europol donedávna považovaný za najväčšiu hrozbu malware Emotet, ktorý bol špecializovaný na bankový systém. Za samotným malwarom stála organizovaná skupina, čo nasvedčuje zmenám v chápaní a vykonávaní

kybernetických útokov. Primárnou funkciou bolo po infikovaní zariadenia, toto zariadenie sprístupniť pre ďalšie malwary. Jeho sekundárnou funkciou bola možnosť spolupráce s inými skupinami a inštalácia ďalších škodlivých softwarov na už infikované zariadenie. Tento malware sa podarilo zastaviť v roku 2021 spoločnou operáciu niekoľkých členských krajín Európskej únie (Nemecko, Holandsko, Litva, Británia, Francúzsko), ako aj USA, Kanady a Ukrajiny (Europol, 2021).

2. KYBERKRIMINALITA SÚČASNOSTI

Z predchádzajúcej kapitoly tejto práce vyplýva, že kyberkriminalita prešla veľkými zmenami, ktoré sú priamo viazané hlavne na rozširovanie a využívanie informačných technológií. Zároveň je možné povedať, že zmenami neprešli len samotné zločiny, ale zmenil sa aj charakter ich vykonávateľov. Zločinci v oblasti kyberkriminality sú v súčasnosti sofistikovanejší a v posledných rokoch sa rozmáha aj trend organizovanej kyberkriminality, tj. vytváranie organizovaných skupín, ktoré dokážu vykonávať kybernetické zločiny efektívnejšie ako jednotlivci. Nakoľko sa zmenil charakter kyberkriminality, zmenili sa aj ciele zločinov. V súčasnosti je hlavným trendom pri rozpínaní kyberkriminality snaha zasiahnuť čo najväčšiu sieťovú štruktúru, alebo veľké množstvo koncových používateľov, prípadne kritickú infraštruktúru nadnárodných podnikov.

Na základe zmien, ktoré nastali pri vykonávaní a rozsahu kybernetických zločinov, museli zmenami prejsť aj legislatívne systémy, ktorých primárnou úlohou je postihovať kriminalitu ako takú, a teda zároveň aj oblasť kybernetickej kriminality. Je možné konštatovať, že zmenami neprešli len vnútroštátne systémy, ale na podklade toho, že tento typ kriminality je silne decentralizovaný, musel zmenami prejsť aj medzinárodný právny systém. Tiež bolo potrebné vytvoriť základy pre lepšiu medzinárodnú spoluprácu pri stíhaní kybernetických zločinov, ktoré presahujú hranice jedného štátneho útvaru a zabezpečiť možnosti získavania a zdieľania elektronických dôkazov za týmto účelom.

Okrem evolúcie, ktorou prešli právne systémy, medzinárodné dohody a nariadenia Európskej únie, boli na základe nutnosti lepšej koordinácie pri odhaľovaní a následne stíhaní tak organizovaných, ako aj izolovaných kybernetických zločinov, vytvorené špeciálne skupiny, ktorých primárnou funkciou je spomenutá činnosť, vo vzťahu ku ktorej im boli udelené rozšírené kompetencie. Tieto skupiny pracujú na základe medzinárodných zmlúv a dohôd, pričom ich fungovanie je podnietené adekvátnym právnym systémom, ktorý umožňuje spoluprácu v potrebnej miere.

Táto kapitola informuje o vytvorenej Európskej legislatíve a vytvorených a podpísaných medzinárodných zmluvách, ktorých úlohou je vytvorenie efektívnejšej spolupráce pri odhaľovaní a stíhaní kybernetickej kriminalite v medzinárodnom spoločenstve aj v rámci

Európskej únie. V neposlednom rade aj popis fungovania organizácie Europol a jej súčastí, ktorých primárnou úlohou je boj proti kybernetickej kriminalite na medzinárodnej úrovni.

2.1 Časté kybernetické zločiny v Európskej únii

V súčasnosti je kyberkriminalita v Európskej únii na vzostupe, čomu napomohol rozmach informačných technológií medzi širokú verejnosť, neprimeraná zručnosť ich používateľov, ktorá ich robí náchylnými voči kybernetickým hrozbám a tiež aj súčasná svetová situácia. Okrem samotného množstva zachytených kybernetických zločinov, ktoré v roku 2020 tvorili až 42% zachytených kriminálnych incidentov v Európskej únii (Interpol, 2020), rástla a stále rastie aj sofistikovanosť útokov a sebaistota tvorcov atakov. Na základe výročných správ medzinárodných organizácií ako sú Europol a Interpol, je zistiteľné, že v súčasnosti je na vzostupe primárne ransomware, malware, či už počítačový alebo telefónny, ktorý má v súčasnosti podľa organizácie Europol najväčšie zastúpenie a útoky na veľké organizácie typu DDoS. Zároveň je z nich možné vyvodiť oprávnený záver, že počas pandémie Covid-19 došlo k nárastu aj iných typov kybernetických zločinov akými sú detská pornografia a zvýšené využívanie informačných technológií na distribúciu zakázaných omamných látok (Interpol, 2020), na ktorom sa zhodujú viaceré organizácie.

Ransomware je vo všeobecnosti software, ktorého úlohou je po infikovaní zariadenia zašifrovať jeho obsah a znemožniť prístup k dátam, ktoré sa na zariadení nachádzajú. Následne je obeti podaná správa o možnosti získania prístupu k dátam po zaplatení výkupného (Richardson, 2017). Tento typ kyberkriminality je v súčasnosti dominantný a to aj medzi útokmi na jednotlivcov, aj na celé organizácie. Zločiny tohto typu predstavujú výzvu, nakoľko pri zasiahnutí organizácie, nie je jedinou obeťou samotná organizácia, ale je postihnuté aj veľké množstvo sekundárnych obetí, ktoré často nemajú vedomosť o zásahu. Z uvedeného možno vyvodiť, že pre zasiahnuté organizácie je schodnejšie akceptovať požiadavku útočníka, nakoľko je pre zasiahnuté organizácie nevýhodné, aby vyšetrovanie prebiehalo, pretože je obvykle veľmi zdĺhavé a náročné (Europol, 2020). Takýto postup postihnutých organizácií nemožno považovať za správny, nakoľko je málo pravdepodobné obnovenie dát v celom ich rozsahu bez správnych údajov, z ktorého pohľadu je postup zasiahnutých organizácií pochopiteľný. Nakoľko ransomware využíva

šifrovanie na vykonanie útoku, tak aj útočník na svoju vlastnú anonymizáciu. Je možné poznamenať, že dostatočná miera anonymity zabezpečuje páchateľom beztrestnosť, nakoľko zistenie ich identity je náročné a často prakticky nemožné.

Malware je vo všeobecnosti škodlivý software, ktorý býva často priložený k podvodnému emailu alebo podvrhnutej stránke. Je súhrnným pomenovaním pre viaceré typy kybernetických útokov, ktoré však pozostávajú z podobných behaviorálnych charakteristík (Konrad Rieck, 2008). Cieľom takéhoto softwaru je zneužiť zariadenie bez vedomia jeho majiteľa, ukradnúť dáta alebo peniaze, či iným spôsobom poškodiť obeť. Najznámejšími typmi sú červ, trójsky kôň, alebo počítačový vírus (Europol). V súčasnosti nie je možné presne povedať, či je využívanie malwaru na ústupe alebo nie, nakoľko rôzne organizácie udávajú nezhodujúce sa údaje. Podľa inštitúcie Europol je malware v súčasnosti na vzostupe, ale organizácie ako Interpol alebo ECS (Európska organizácia kyberbezpečnosti) uvádzajú opačný trend a teda pokles, v rozširovaní malwaru (Interpol, 2020), (Európska organizácia pre kybernetickú bezpečnosť, 2020).

DDoS je distribuovaný útok, ktorý je zameraný na služby a jeho účelom je znemožnenie prístupu k nejakej webovej stránke alebo aplikácií, ktorý často slúži na odvedenie pozornosti od hlavného útoku. V posledných rokoch zaznamenal relatívne veľký návrat, nakoľko sa v dobe pandémie Covid-19 (2020 - 2021) väčšina služieb presunula do kyberpriestoru (Europol, 2020). Primárne je tento typ útokov zameraný na organizácie a nie jednotlivcov. Pri zastavovaní takéhoto zločinu sa problematickým javí to, že takýto útok využíva veľké množstvo zariadení, ktoré sú zneužívané len na samotný útok a nie sú nijakým spôsobom spojené s útočníkmi. Tieto zariadenia sa nazývajú „bot“ a sú to zariadenia, ktoré boli v minulosti infikované malwarom, ktorý umožnil ich využitie na takýto útok. Práve decentralizáciou bolo docielené, že veľké množstvo týchto útokov je náročné v súčasnosti trestne stíhať (Nazario, 2008).

V neposlednom rade je nutné spomenúť aj iné typy kybernetických zločinov, ktoré sú v súčasnosti veľmi populárne a medzi tieto patria najmä šírenie dezinformácií a hanobenie určitých skupín, ktoré zaznamenali značný rozmach (Europol, 2020) (Interpol, 2020). Pri odhaľovaní zločinu šírenia dezinformácií nastáva pri jeho stíhaní problém v tom, že súčasná medzinárodná legislatíva nie je dostatočná na to, aby efektívne dokázala zabrániť jeho šíreniu.

K šíreniu závažnejšej kybernetickej trestnej činnosti vo veľkej miere prispela pandémia Covid-19, počas ktorého obdobia bol napríklad zaznamenaný zvýšený nárast dostupnosti a vyhľadávania detskej pornografie a jej šírenie. Obdobne možno vo vzťahu k zakázaným omamným a psychotropným látkam konštatovať, že bol zaznamenaný výraznejší dopyt a komunikácia ohľadne dostupnosti a distribúcie a teda aj využívanie Dark a Deep webu (Interpol, 2020). V otázke šírenia a distribúcie v spomenutých trestnoprávnych oblastiach sa zastavenie samotného šírenia javí problematickým z dôvodu, že prevažná väčšina obsahu sa voľne šíri na alternatívnych platformách akými sú Deep a Dark web.

2.2 Legislatívny rámec

Charakter kybernetickej kriminality sám o sebe predstavuje niekoľko problémov pre bežné vnímanie trestného práva. Nakoľko je silne decentralizovaný a je do veľkej miery zameraný na informačné technológie, je nutné aby bol právny systém pripravený adekvátne na všetky možnosti, ktoré môžu nastať pri stíhaní kybernetickej kriminality *(Calderoni, 2010)*. Nakoľko je legislatíva každého štátu autonómna, je nutné vytvoriť určité harmonizačné nariadenia v rámci spoločenstiev štátov ako je napríklad Európska únia, ale tiež aj medzinárodné zmluvy, ktoré umožnia stanoviť na ako legislatívnom základe bude kybernetický trestný čin stíhaný, ak tento čin presahuje štátne hranice niekoľkých štátov. V neposlednom rade takéto medzinárodné zmluvy a európske smernice a nariadenia tiež umožňujú aj nadštandardnú spoluprácu pri odhaľovaní a stíhaní kybernetickej kriminality.

Je vhodné spomenúť aj to, že pojem kyberkriminalita neoznačuje len jeden typ kriminality, ale hneď niekoľko. Všetky určitým spôsobom využívajú informačné technológie, a to aj keď je miera využitia týchto technológií iná pri každej skupine, ktorú je možné pomocou takéhoto určenia vytvoriť *(Európska komisia)*. V nadväznosti na uvedené, je možné upozorniť, že nie je vhodné vytvoriť len jedno európske všeobecne záväzné nariadenie, ktoré by obsiahlo všetky typy kyberkriminality a umožňovalo by aj jeho priamu implementáciu do právneho systému jednotlivých členských štátov Európskej únie. Totiž takéto nariadenie by muselo byť dostatočne všeobecné, aby zahŕňalo možnosti jurisdikcií všetkých členských štátov Európskej únie, pričom dosiahnutie tohto zámeru sa javí mimoriadne náročné.

Na základe tohto dôvodu a tiež aj nejednoznačnosti pojmu kyberkriminalita bolo pre účely vytvorenia vhodných nariadení na úrovni Európskej únie pri tvorbe dohôd o spolupráci pri stíhaní kybernetickej kriminality, využité delenie kyberkriminality na tri skupiny, ktoré umožňujú bližšie definovať typy týchto zločinov. Takéto všeobecnejšie delenie umožňuje ich premietnutie do potrebnej legislatívy tak, aby bolo možné ju následne aplikovať na väčšie množstvo už konkrétnych skutkových podstát kybernetických zločinov, ktoré spadajú do už definovaných skupín *(Calderoni, 2010)*. Tieto skupiny delia kyberkriminalitu na zločiny špecifické internetu, teda tie ktoré je možné vykonať len prostredníctvom internetu, alebo je ich cieľom nejaká sieťová štruktúra *(Rada Európy, 2001)*. Sem je možné zaradiť všetky zločiny proti CIA triáde, teda zločiny, ktoré priamo zasahujú do bezpečnosti dát *(Calderoni, 2010)*. Ďalšou skupinou sú zločiny, ktoré informačné technológie využívajú, ale samotné technológie nie sú priamym cieľom útoku. Do tejto skupiny boli zaradené online podvody, čo sú podvody, ktoré sú uskutočňované online a pomocou prostriedkov na to určených, ako sú napríklad podvrhnuté webové stránky, škodlivé kódy alebo spamové správy *(Európska komisia)*. Poslednou skupinou sú zločiny, ktoré šíria nejaký škodlivý obsah, či už je to detská pornografia, dehonestujúce komentáre na sociálnych sieťach, alebo iné podnecovanie terorizmu, či rasizmu *(Európska komisia)*. Zároveň je podľa tohto delenia možné do kybernetických zločinov zaradiť aj zločiny, ktoré sú priamo zamerané na porušovanie autorských práv, pokiaľ je toto porušenie limitované na kyberpriestor. Legislatíva, ktorá je využívaná na stíhanie porušení autorských práv mimo online priestoru je aplikovateľná aj na kyberpriestor, nakoľko definícia autorského diela a práv k nemu sa viažucich, sa nemení a teda je aplikovateľná aj pre elektronické diela *(Rada Európy, 2001)*.

Vďaka tomu, že sú nariadenia a dohody vytvorené všeobecnejšie, je možné popísať viac typov kybernetických zločinov oproti stavu, ak by boli vytvárané rovnako ako iné nariadenia, a priamo sa zameriavali na konkrétny typ kyberkriminality *(Calderoni, 2010)*.

Je vhodné poznamenať, že na základe rýchleho tempa rozvíjania informačných technológií a teda nepriamo aj rýchlej evolúcii kyberkriminality, umožňujú takto postavené nariadenia stíhanie aj takých typov kybernetickej kriminality, ktoré sú v súčasnosti len veľmi málo známe. Takto definované nariadenia a dohody tiež môžu byť aplikované pro futurum v prípade ďalšej evolúcie kybernetických zločinov, pokiaľ

svojim charakterom budú tieto zločiny spadať pod jednu z už definovaných skupín. Takto širšie koncipované nariadenia lepšie zabezpečujú zosúladenie stíhania tohto druhu kriminality na území Európskej únie. Podpísané a ratifikované medzinárodné zmluvy umožňujú lepšiu spoluprácu väčších územných celkov na celosvetovej úrovni *(Calderoni, 2010)*.

2.3 Legislatíva Európskej únie o kybernetickej kriminalite

Z dôvodu toho, že kybernetická kriminalita je vykonávaná prostredníctvom kyberpriestoru a je decentralizovaná, môže nastať problém pri definovaní skutkových podstát kybernetických incidentov a ich následnom stíhaní. Pri tomto druhu kyberkriminality je pravdepodobné, že páchateľ trestného činu sa nachádza na inom mieste ako obeť a zároveň, že spadá pod jurisdikciu iného štátu, tj. protiprávnu činnosť vykonáva v inej krajine. Je žiaduce definovať všeobecný rámec, na základe ktorého je možné stíhať aj takýto druh zločinu. Preto majú nariadenia Európskej únie primárne harmonizačný charakter a po ich aplikovaní do právnych systémov členských štátov, je možné stíhanie aj decentralizovaných trestných činov *(Calderoni, 2010)*.

V súčasnosti je v účinnosti niekoľko nariadení a smerníc Európskej únie, ktoré umožňujú spomínanú harmonizáciu a zdieľanie prostriedkov medzi členskými štátmi. Medzi tieto nariadenia a smernice patrí napríklad Smernica ohľadom detskej pornografie (2011/93/EU) a Smernica Rady Európskej únie, ktorá je v súčasnosti najpoužívanejšou (2013/40/EÚ). Spomenuté a smernice vychádzajú z Dohovoru Rady Európy o kyberkriminalite z roku 2001 (s účinnosťou od roku 2004), ktorý je najúspešnejšou medzinárodnou zmluvou, ktorá stavia základy boja proti kyberkriminalite ako druhu kriminality, ktorý je postavený na využívaní informačných technológií, či už priamo, alebo len na sprostredkovanie iného zločinu či škodlivého obsahu. Obsahuje aj navrhované postupy, ktoré by mali byť uskutočnené pri stíhaní kyberkriminality a zdieľania dôkazných materiálov. Tiež stanovuje prvotnú základnú politiku, ktorú by mali členské štáty Európskej únie dodržiavať pri stíhaní kyberkriminality a najmä pri prijímaní vhodnej legislatívy *(Rada Európy, 2001)*.

Za dôležité je potrebné považovať to, že tento Dohovor, ktorý stanovuje základy boja proti kyberkriminalite, bol vytvorený a prijatý pred viac ako dvadsiatimi rokmi, za ktorý

čas sa charakter kybernetickej kriminality podstatným spôsobom zmenil, stal organizovanejším a sofistikovanejším, ale s prihliadnutím na odstup času, nebolo na takúto zmenu v oblasti kybernetickej kriminality reagované prijatím nového Dohovoru, ktorý by adekvátne vystihoval evidovanú zmenu. Preto je nutné spomenúť Smernicu Rady Európskej únie o útokoch na informačné systémy z roku 2013, ktorá nahradila pôvodnú smernicu z roku 2005. Primárnym cieľom tejto smernice je zjednotenie trestného práva v oblasti útokov na informačné systémy a vytvorenie minimálnych pravidiel, ktorých cieľom je vymedziť príslušné skutkové podstaty kybernetickej trestnej činnosti a k nim prislúchajúce sankcie. Táto smernica zaväzuje členské štáty k stíhaniu kybernetickej kriminality na ich území a umožňuje efektívnejšiu spoluprácu justičných orgánov s inými príslušnými orgánmi činnými v trestnom konaní, prípadne civilnými spoločnosťami (hlavne poskytovateľmi informačných služieb) pri odhaľovaní útokov na informačné systémy. Tiež definuje základné pravidlá pre postihovanie takýchto objasnených trestných činov a uloženie primeraných sankcií. V neposlednom rade umožňuje zefektívniť spoluprácu špecializovaných agentúr ako sú napríklad Europol alebo Eurojust s justičnými orgánmi jednotlivých členských štátov Európskej únie *(Európsky parlament a Rada, 2013)*

Faktom zostáva aj to, ako bolo rozvedené v predchádzajúcej kapitole, že v súčasnosti nie je v platnosti všeobecná taxonómia (delenie) a ani všeobecne platná medzinárodná legislatíva na území Európskej únie týkajúca sa kybernetickej kriminality. Vychádzajúc z uvedeného, je možné dospieť k záveru, že niektoré typy kybernetických zločinov, ktorých skutkové podstaty sú na hranici delenia, ktoré bolo využité pri tvorbe všeobecných nariadení Európskej únie, môžu zostať neodhalené a teda aj nepotrestané. Pokiaľ nastal kybernetický incident, ktorý má decentralizovaný charakter a legislatíva krajiny, v ktorej sa nachádza páchateľ definuje kybernetické zločiny na základe iných parametrov, je možné, že zločin nebude odhalený a potrestaný. Inak povedané, ak evidovaný kybernetický incident v tejto krajine nevykazuje znaky kybernetického zločinu, je pravdepodobné, že zostane nepotrestaný. Oproti predchádzajúcemu záveru je možné konštatovať, že vyššie rozvedený uzatvorený Dohovor s predpokladom jeho využívania postavil základy, na ktorých bolo možné vytvoriť organizácie s vyšpecifikovanými právomocami, a tieto dokážu odhaľovať kyberkriminalitu na

medzinárodnej úrovni, a následne potrestať páchateľov týchto zločinov právom tých štátov, ktorých sa kybernetický zločin týka, pokiaľ to dovoľuje legislatíva daného štátu.

2.4 Organizácie

S technickým pokrokom a rozvojom celosvetovej civilizácie sa postupne menil aj charakter kriminality ako takej a začali sa objavovať aj druhy zločinov, ktoré sú v súčasnosti sofistikovanejšie a predstavujú vážnejšie hrozby, ktoré ohrozujú celé národy *(Abransky, 2016)*. Za takýto typ kriminality možno považovať napríklad terorizmus, nadnárodnú organizovanú kriminalitu alebo aj kybernetickú kriminalitu. Nakoľko je možné terorizmus aj určité činnosti organizovanej kriminality, ako je napríklad aj výmena a obchodovanie so súbormi s témou detskej pornografie, do určitej miery presunúť do kyberpriestoru, spadá takáto činnosť aj pod kybernetickú kriminalitu *(Abransky, 2016)*. Je možné dospieť k záveru, že kyberkriminalita je v súčasnosti značným problémom, nakoľko zahŕňa širokú oblasť kriminality, ktorá je vykonávaná pomocou informačných technológií v rámci kyberpriestoru. Zároveň sa v posledných rokoch mení jej charakter na organizovaný typ kriminality a nie je možné ju presne centralizovať na konkrétne územie, čo je pre páchateľov veľkou výhodou. Tieto jej vlastnosti vytvárajú potrebu väčšej spolupráce štátov a väčších štátnych celkov (USA, EU) pri odhaľovaní páchateľov, ktorí vykonávajú takýto typ zločinov. Na základe tejto potreby boli vytvorené organizácie, ktorým boli udelené potrebné právomoci oprávňujúce ich odhaľovať a v určitých prípadoch aj stíhať tento typ kriminality. Jednou z týchto organizácií, ktoré boli vytvorené na základe vyššie rozvedených príkladov medzinárodných zmlúv, ktoré umožňujú stíhanie kybernetickej kriminality, je organizácia Europol.

2.5 Europol

Organizácia Europol sa zameriava na závažnejšie formy kriminality, ktoré svojim charakterom ovplyvňujú celé územie Európskej únie a teda aj na organizovanú kybernetickú kriminalitu. Nakoľko sa charakter kyberkriminality v posledných rokoch zmenil, čo viedlo k tomu, že sa stala závažnejším problémom oproti minulosti, bolo na základe rastúceho počtu zločinov tohto typu vytvorené centrum EC3 a okrem iných vznikli aj skupiny EUCTF a J-CAT, ktoré sa priamo zameriavajú na oblasť kyberkriminality *(Europol, 2022)*

Európske centrum kyberkriminality (EC3) bolo založené v roku 2013, jeho primárnou úlohou je zefektívniť koordináciu zásahov a vyšetrovania kybernetickej kriminality či už na území Európskej únie, alebo zabezpečiť spoluprácu so štátnymi celkami mimo tohto územia. Zároveň na základe vyššie spomenutých zmlúv je jeho úlohou získavať a poskytovať informácie ohľadom kybernetických incidentov a zefektívnenie stíhania kybernetickej kriminality (Buono, 2016). Samotné centrum kybernetické zločiny nevyšetruje, ale na základe medzinárodných zmlúv, nariadení a smerníc Európskej únie, umožňuje efektívnejšiu koordináciu orgánov činných v trestnom konaní členských krajín Európskej únie, ktoré vyšetrujú kybernetické zločiny. Zároveň má toto centrum za úlohu vytvárať analýzy a štatistiky ohľadom kybernetickej kriminality v Európskej únií, táto jeho povinnosť mu vyplýva zo štatútu, podľa ktorého musí poskytovať informácie a súčinnosť pri odhaľovaní a stíhaní kybernetických incidentov v rámci územia Európskej únie, alebo aj tých ktoré prekračujú hranice Európskej únie. V neposlednom rade poskytuje technologické prostriedky, ktoré umožňujú efektívnejšie odkrývanie a stíhanie kybernetickej kriminality *(Europol, 2022)*.

Pracovná skupina Európskej únie pre kybernetickú kriminalitu (EUCTF) bola vytvorená v roku 2010 spoluprácou organizácie Europol, Európskou komisiou a členskými štátmi Európskej únie. Táto skupina je zložená z vedúcich členov jednotiek boja proti kyberkriminalite jednotlivých štátov, ktoré sa podieľajú na jej fungovaní. Jej primárnou funkciu je vytvorenie a propagovanie možností harmonizácie stíhania kriminálneho zneužívania informačných a komunikačných technológií, a teda aj kybernetickej kriminality a aj o úkonoch, ktoré by mohli pomôcť pri zdieľaní dôkazných materiálov a iných prostriedkov *(Rozée, 2013)*. Je teda možné konštatovať, že jej primárnou funkciou je podpora organizácie Europol a jej súčastí alebo orgánov stíhajúcich kybernetickú kriminalitu v členských štátoch Európskej únie. Zároveň táto skupina pracuje v úzkom spojení s pracovnou skupinou J-CAT, ktorá umožňuje spoluprácu príslušných orgánov, ktorých agendou je boj proti kybernetickej bezpečnosti aj mimo územia Európskej únie.

Samotné centrum EC3 a aj pracovná skupina EUCTF však poskytujú len štandardné možnosti zdieľania prostriedkov a informácií a neumožňujú nadštandardné vzťahy pri zdieľaní dôkazných materiálov, čo vedie k veľmi nízkej efektivite pri stíhaní kyberkriminality. Štandardné zdieľanie informácií medzi štátnymi útvarmi pozostáva

z časovo náročného procesu, ktorý spočíva v priamom kontaktovaní jednotlivých organizácií a bezpečnostných zložiek, ktoré sa podieľajú na stíhaní zločinu a aj samotných orgánov, ktoré tieto zločiny vyšetrujú v príslušných štátoch. Takáto komunikácia je teda veľmi časovo náročná a zdĺhavá, nakoľko sú potrebné rozsiahle povolenia na prístup k relevantným dátam a na determináciu, ktoré dáta sú relevantné pre daný prípad *(Reitamo, 2015); (Europol, 2022).* V kontexte s uvedeným je vhodné poznamenať, že tento proces je potrebné absolvovať pri každom vyšetrovanom kybernetickom zločine, čo dokáže pri množstve súčasných zločinov takéhoto typu ešte viac spomaliť spoluprácu a postih páchateľov.

Na základe zjavne neefektívnej spolupráce, ktorá bola uvedená vyššie, bola v roku 2014 v centre EC3 vytvorená skupina J-CAT, ktorá má, ako už bolo spomenuté, právomoci a súčinnosť jednotlivých krajín Európskej únie, ale aj iných štátnych útvarov vo svete, čo umožňuje efektívnejšie stíhanie závažnej kybernetickej kriminality. Je prvou skupinou, ktorá pozostáva so styčných dôstojníkov aj z iných štátov ako sú členské štáty Európskej únie *(Europol, 2022)*. Bola vytvorená ako reakcia orgánov, ktoré vyšetrujú kybernetické zločiny na ťažkosti spolupráce pri zdieľaní prostriedkov a informácií. Nakoľko sa procesy zdieľania dôkazných materiálov môžu natiahnuť na dlhé časové obdobie, čo je veľmi výhodné pre páchateľov kybernetickej kriminality, táto skupina predstavuje možnosti efektívnejšieho zdieľania spomenutých prostriedkov. Zároveň poskytuje možnosti ako sa účinne vysporiadať s právnymi problémami, ktoré vznikajú na základe neefektívnosti prijímania legislatívy a na druhej strane s rýchlym technickým pokrokom informačných technológií, a teda aj možnosťami rýchleho vývoja kybernetickej kriminality. Namiesto tradičnej komunikácie a zdieľania prostriedkov táto skupina sama zhromažďuje informácie, ktoré následne poskytuje všetkým zainteresovaným štátom, ktoré sa podieľajú na stíhaní kybernetického zločinu, čo umožňuje veľkú efektivitu, nakoľko sa proces zdieľania informácií urýchli a doba výmeny informácií sa skráti o minimálne niekoľko mesiacov, ak nie rokov *(Reitamo, 2015).*

Ako bolo v tejto kapitole naznačené, v súčasnosti sú zaznamenané rozsiahle snahy zefektívniť stíhanie kybernetickej kriminality, pričom je možné zdôrazniť, že na vytvorenie skutočne účinných prostriedkov spolupráce a zdieľania dát, vyvstáva potreba

prípravy a následného prijatia ešte ďalších medzinárodných dohôd a zmlúv. Na podklade uvedeného je možné dať do pozornosti, aby súčasné snaženie bolo zamerané na vytvorenie efektívnych medzinárodných záväzných zmlúv, ktoré by presne vymedzovali pojmy ako sú kybernetický incident a zločin, najmä z pohľadu všeobecného definovania ich skutkových podstát. V tomto smere je na mieste poznamenať, že v súčasnosti je veľkým problémom nedostatočná legislatíva v oblasti poskytovania dôkazných materiálov poskytovateľmi informačných služieb, čo tiež značne prispieva k spomaleniu efektívnejšieho stíhania kybernetickej kriminality *(Calderoni, 2010)*. V neposlednom rade za problém možno označiť aj neexistenciu jednotného delenia kybernetickej kriminality, ktoré by sa mohlo stať všeobecne záväzným pre členské krajiny Európskej únie. Vytvorenie takéhoto delenia by jednoznačne umožnilo vytvárať presné štatistiky ohľadom trendov kybernetickej kriminality v súčasnosti, čo by bolo prínosným hlavne pre tvorbu ďalšej analýzy a budúcej prevencie.

3. SÚČASNÉ TRENDY V KYBERNETICKEJ KRIMINALITE A JEJ DOPAD NA SÚČASNÚ SPOLOČNOSŤ

Na základe toho, že využívanie informačných technológií sa stalo v súčasnej dobe čoraz väčšou súčasťou každodenného života, a je stále na vzostupe, je možné uviesť, že na základe tejto skutočnosti formy kriminality, ktoré využívajú tieto technológie, sú tiež na vzostupe.

Neúplnosť súčasnej medzinárodnej legislatívy, ktorá sa zameriava na tieto formy kriminality a tiež aj nejednotnosť definícií pri rozlišovaní kybernetického incidentu a zločinu spôsobuje ťažkosti pri spoľahlivých štatistických informácií, ktoré by mohli pomôcť ozrejmiť súčasný stav v trendoch kybernetických zločinov *(Calderoni, 2010)*. Spomenuté nedostatky predstavujú v dnešnej dobe problém, nakoľko ak by nedostatky neboli zaznamenané, bolo by možné na základe týchto informácií spoľahlivejšie určiť, ktoré súčasti informačných infraštruktúr sú najohrozenejšie, tj. či je to technologická stránka, alebo samotní používatelia týchto technológií.

Nakoľko sa kybernetická kriminalita zmenila aj na organizovanejší typ kriminality *(Abransky, 2016)*, ktorý má tendenciu zasahovať väčšie spoločnosti, alebo veľké množstvo jednotlivcov, je možné poznamenať, že sa zmenil aj dopad kybernetickej kriminality na spoločnosť. Zároveň sa zväčšil aj rozsah ekonomických strát, ktoré vznikajú práve prostredníctvom tohto druhu kriminality.

Zároveň je však potrebné dodať, že dopady kybernetickej kriminality nezasahujú len celosvetovú ekonomiku, ale aj každého jednotlivca spoločnosti, či už z pohľadu prijímania nedôveryhodných informácií, alebo rapídnych možností šírenia kybernetických útokov pomocou podvodných stránok alebo emailov.

Pre vysvetlenie tohto problému sú v tejto kapitole spomenuté viaceré štatistické údaje, ktoré sa od seba odlišujú, pretože sú získavané a vedené rôznymi organizáciami. Zároveň sú pre územie Európskej únie veľmi nepresné, nakoľko sa primárna väčšina týchto údajov zameriava na konkrétne štátne útvary alebo globálne celý svet. Tiež je nutné poznamenať, že na základe týchto údajov je obtiažne presne určiť trendy v oblasti kybernetickej

kriminality, nakoľko opätovne vyvstáva problém ich spoľahlivosti a tiež aj toho, že tieto údaje sú vedené rôznymi organizáciami a je veľmi náročné ozrejmiť aké delenie kybernetickej kriminality je využívané. V neposlednom rade táto kapitola podáva príklady ekonomických strát spôsobených kybernetickou kriminalitou na rôzne nadnárodné spoločnosti a tiež aj letmo pojednáva o ekonomických stratách jednotlivcov. Zároveň pojednáva o stave a rozvoji kybernetickej kriminality na začiatku pandémie Covid-19.

3.1 Problémy štatistík kybernetickej kriminality

V súčasnosti je jedným z hlavných problémov pri skúmaní trendov kybernetickej kriminality nedostatok detailných a špecifických štatistických údajov, ktoré by popisovali množstvá zaznamenaných kybernetických incidentov a zločinov na určitom geografickom území. Momentálne na území Európskej únie platí Odporúčanie Rady Európskej únie na vytváranie a vedenie štatistických údajov o kybernetickej kriminalite, avšak tieto už spracované štatistické údaje podľa tohto odporúčania sú zo zdrojov, ktoré sa zaoberajú stíhaním kybernetickej kriminality na území Európskej únie a nie sú verejne dostupné *(Rada Európy, 2020)*. Týmito zdrojmi sú primárne organizácie, ktorých účelom je odhaľovanie a stíhanie kybernetickej kriminality na území Európskej únie a efektívne zbieranie dát o tejto kriminalite, tj. organizácie ako Europol a jeho súčasti zamerané priamo na kybernetickú kriminalitu, Interpol alebo Eurojust.

Časti údajov od týchto organizácií o kybernetickej kriminalite, ktoré sú verejne dostupné, sú hlavne zamerané na kriminalitu celkovo a kybernetickú kriminalitu zmieňujú len okrajovo ako súčasť celkovej kriminality. Tieto štatistiky sú často zamerané primárne na počty otvorených a uzatvorených zločinov *(Rajan, 2017)*, alebo sa zameriavajú skôr na celkový nárast hlásení veľkých organizácií a vynaložených zdrojov, ktoré boli potrebné na vyšetrenie kybernetickej kriminality za určité obdobie *(Europol, 2020)*.

Spomenuté ťažkosti so získavaním informácií v tomto smere sú však spojené aj s charakterom kybernetickej kriminality, na ktorú sa tieto organizácie zameriavajú, tj. organizovaná kybernetická kriminalita, ktorá je zameraná na veľké organizácie alebo veľké množstvo používateľov *(Europol, 2017)*. Z charakteru tohto druhu kriminality vyplýva, že je potrebné ju nahlásiť, avšak ak je kybernetická kriminalita zameraná na

veľké množstvo osôb v rôznych členských štátoch Európskej únie, tieto osoby často tento typ zločinu nenahlasujú, alebo ak ju nahlásia, tak len orgánom v príslušnej krajine, čo spôsobuje problémy pri vytváraní štatistických údajov pre väčšie geografické územie *(Rajan, 2017)*. Je vhodné spomenúť, že v súčasnosti v Európskej únií neexistuje jednotný formulár *(ENISA, 2016)*, ktorý by umožňoval nahlásenie kybernetickej kriminality na jej území, čo vedie k ďalším problémom. Na základe spomenutého je možné vyvodiť, že jedným z problémov pri vytváraní štatistík je nedostatok údajov, nakoľko veľa obetí tento typ kriminality nenahlási, alebo ho nahlási nesprávne, pričom sa takéto hlásenie stáva irelevantným *(ENISA, 2016)*. Je možné k spomenutému prideliť aj nespoľahlivosť delenia kybernetickej kriminality, nakoľko nahlásený kybernetický incident v jednej krajine nemusí byť kategorizovaný ako kybernetický zločin v druhej krajine, z ktorého dôvodu nie je zaradený do štatistických údajov.

Ďalej je vhodné znovu zmieniť, že i keď v súčasnosti neexistuje jednotné delenie kybernetickej kriminality na základe skutkovej podstaty, je pravdepodobné, že následne aj vytvorené a zverejnené štatistické údaje môžu byť v určitých oblastiach kybernetickej kriminality nepresné *(ENISA, 2016)*. V súčasnosti je primárna väčšina spracovaných štatistických údajov k dispozícii z organizácií, ktoré sa zaoberajú výskumom danej témy, alebo sú vývojárom zabezpečení v oblasti kybernetickej bezpečnosti. Tieto spoločnosti môžu využívať vlastné delenia a preto je pravdepodobné, že spracované dáta sa budú mierne odlišovať.

Za problém pri vytváraní spoľahlivých štatistík možno označiť aj decentralizovaný charakter kybernetickej kriminality *(Buono, 2016)*, z ktorého dôvodu je veľké množstvo spracovaných štatistických dát zameraných na celkovú svetovú kybernetickú kriminalitu a nie na zločiny takéhoto charakteru, ktoré sú zamerané na menšie územie *(Rada Európy, 2020)*. Problém vzniká aj pri rôznych prístupoch k spracovávaniu štatistických údajov ohľadom kybernetickej kriminality, kde je možné spracovávať počty nahlásených zločinov alebo tie, ktoré sú aktívne vyšetrované. Pri kybernetickej kriminalite je často veľmi problematické zistiť, ktoré dáta sú relevantné, a teda aj ktoré štatistiky sú prínosom a nie sú zavádzajúcimi *(Rada Európy, 2020)*.

3.2 Aspekty prístupu k štatistikám kyberkriminality

K štatistickým údajom je možné pristupovať z rôznych pohľadov. Ako už bolo naznačené pri kybernetickej kriminalite je potrebné sledovať primárne validitu získaných dát a to hlavne, ak sú predmetom spracovávania hlásenia obetí kybernetických incidentov *(Buono, 2016)*. Zároveň je potrebné prihliadať na to, že kritériá pre zbieranie dát o kybernetickej kriminalite budú odlišné *(ENISA, 2016)* . Menovite je primárnym problémom, čo už bolo naznačené, že kybernetická kriminalita má silne decentralizovaný charakter *(Buono, 2016)*, a teda jej obete a páchatelia často spadajú pod rôzne jurisdikcie. Tiež jedným z problémov je aj samotné využívanie informačných technológií a to z toho pohľadu, že každý zločin zanecháva určitú stopu, ktorú je následne pri stíhaní nutné identifikovať *(Rada Európy, 2020)*. Táto stopa tvorí elektronický dôkaz, ktorý je potrebné adekvátne zdokumentovať a tvorí jeden z aspektov, na základe ktorých je tiež možné vytvárať štatistické údaje *(Rada Európy, 2020)*, nakoľko pri typoch kriminality, ktorá informačné technológie využíva, je na jej základe možné špecifikovať závažnosť kybernetického zločinu.

Z odporúčania Rady Európy z roku 2020 *(Rada Európy, 2020)*, vyplýva, že presné stavy kybernetickej kriminality by mohli byť generované na základe zozbieraných štatistických dát nahlásených zločinov. Na základe týchto údajov, ak by boli delené podľa druhu kybernetického zločinu, by bolo možné presnejšie definovanie trendov v tejto oblasti, čo by umožnilo efektívnejšiu alokáciu zdrojov pre stíhanie kybernetickej kriminality a efektívnejšiu odpoveď na hlásenia o kybernetickej kriminalite na určitom území *(Rada Európy, 2020)*. Toto odporúčanie definuje aj druhý spôsob vytvárania spracovania štatistík, a to na základe otvorených alebo vyriešených nahlásených kybernetických zločinov, aké prostriedky boli vynaložené na uzatvorenie už vyriešených zločinov a aké finančné, alebo iné straty boli zaznamenané obeťami týchto zločinov *(Rada Európy, 2020)*. Vedenie týchto štatistík v oblasti kybernetickej kriminality by logicky mohlo viesť k efektívnejšej legislatíve v tejto oblasti a zároveň by podporilo vytvorenie špecializovaných skupín, ktorých úlohou by bolo kybernetickú kriminalitu postihovať *(Buono, 2016)*.

Okrem samotnej tvorby a spracovania štatistických údajov by bolo vhodné vytvoriť mechanizmy, ktoré by umožňovali nahlásenie kybernetickej kriminality, nakoľko

spomenuté zločiny sú často nahlasované priamo organizáciám v príslušnej krajine obete, však pre efektívne stíhanie kybernetickej kriminality by bolo vhodnejšie aby dané organizácie nahlásili a zdieľali tieto informácie s ostatnými organizáciami, ktoré sú pre zistený a popísaný prípad relevantné *(Rada Európy, 2020)*. Momentálne v Európskej únií nie je zavedený efektívny a jednotný mechanizmus, ktorý by umožňoval takéto zdieľanie informácií, zostáva veľké množstvo kybernetických zločinov nespracované, a teda nie sú zaradené do štatistík *(ENISA, 2016)*.

Ďalším potrebným aspektom štatistík o kybernetickej kriminalite je už spomenutá validita zdrojov, nakoľko v súčasnosti je veľa organizácií, ktoré majú v oblasti špecifické vedomosti, tj. sú to organizácie, ktoré sú civilné a priamo sa zaoberajú informačnou bezpečnosťou, ktorá je priamo spojená s kybernetickou kriminalitou, alebo poskytujú poradenstvo v tejto oblasti *(Rada Európy, 2020)*. Tieto organizácie disponujú určitými dátami ohľadom ich činnosti a je možné vytvárať a bližšie špecifikovať už vytvorené štatistiky na základe týchto dát. Avšak pri takomto spracovaní nastáva problém, pretože mnoho týchto spoločností pracuje na globálnej úrovni a ich dáta sú teda zbierané celosvetovo, preto je potrebné ich adekvátne upraviť *(Rada Európy, 2020)*.

3.3 Dopad rôznych typov kriminality na spoločnosť

V posledných rokoch sa kybernetická kriminalita stala čoraz viac konfliktnou a agresívnejšou voči obetiam a je možné povedať, že v posledných rokoch boli hlavnými cieľmi kybernetickej kriminality primárne veľké organizácie, ktoré sprostredkovávajú služby zamerané na bankové transakcie a obchodovanie, čo spôsobuje veľké straty pre prevádzkovateľov a používateľov týchto služieb *(Riek, 2016)*. Na druhú stranu je možné na základe tohto vývoja doplniť, že kybernetická kriminalita je v súčasnosti jedným z finančne najvýnosnejších druhov kriminality a podľa spoločnosti McAfee bola ekonomická strata v oblasti Európy a centrálnej Ázie k roku 2018 spôsobená týmto druhom kriminality, približne 156 miliárd eur *(Lewis, 2018)*. Na podklade uvedeného je možné opodstatnene konštatovať, že od začiatku pandémie (január 2020) s čím bolo spojené prenesenie ďalších služieb do kyberpriestoru, táto suma vzrástla.

Jedným z možných pohľadov na ekonomické straty spôsobené kybernetickou kriminalitou, je možné pozerať sa na finančné straty samotných obetí *(Riek, 2016)*.

V tomto smere možné označiť za najvýznamnejšie zločiny typu ransomware alebo DDoS útoky. Ransomware, ktorého primárnym cieľom je zašifrovať dáta a ich následné uvoľnenie je podmienené zaplatením výkupného, čo samozrejme spôsobuje signifikantné finančné straty a pre obete je jednoduchšie zaplatiť požadované výkupné, pretože spätné získanie dát je bez kľúča prakticky nemožné *(Richardson, 2017)*. Na základe týchto jeho vlastností, organizácie po celom svete, každá z nich, priemerne vynaloží približne 2 milióny eur na zotavenie sa po takomto útoku *(Scroxton, 2021)*. V prípade útokov typu DDoS sú straty primárne na základe obratu, ktoré majú spoločnosti zo sprostredkovávania služieb, pričom celková ekonomická strata tohto druhu kriminality je len veľmi ťažko determinovateľná, nakoľko veľké spoločnosti môžu v prípade takéhoto útoku stratiť až 50 tisíc eur denne a malé, len pre svetový trh, zanedbateľné čiastky *(Kaspersky, 2014)*.

Ako už bolo spomenuté kybernetická kriminalita sa v súčasnosti zameriava na spôsobenie čo najväčšej škody svojej obeti a na druhej strane ide o vytvorenie zisku nakumulovaním čo najväčších finančných prostriedkov *(Richardson, 2017)*. Pri určitých druhoch kybernetickej kriminality je náročné vymedziť presné škody a rôzne ujmy spôsobené jednotlivým obetiam, pričom sa determinovanie celkovej finančnej straty len odhaduje na základe nahlásených zločinov a je veľmi obtiažne presne definovať straty na určitom geografickom území, nakoľko sa straty obvykle vypočítavajú na základe globálnej ekonomiky *(Lewis, 2018)*. Z uvedeného je možné vyvodiť záver, že štatistické informácie ohľadom ekonomických strát pri kybernetickej kriminalite sú často relatívne nepresné.

3.4 Covid-19

Celosvetová situácia spôsobená pandémiou Covid-19 primäla väčšinu služieb a aj ich zákazníkov na relatívne rýchly presun do kyberpriestoru, často bez adekvátnej bezpečnostnej politiky. Rýchla reakcia na situáciu v podstate umožnila páchateľom kybernetickej kriminality väčší a ľahší dosah na potenciálne obete, čo malo za následok prudký nárast v zaznamenaných kybernetických zločinoch. Na druhej strane spomenutý presun služieb do kyberpriestoru podnietil ich poskytovateľov prehodnotiť bezpečnostnú politiku *(Cosman, 2020)*. Okrem spomenutého k nárastu kybernetickej kriminality prispela aj neistá celosvetová ekonomická situácia, na základe čoho boli zaznamenané viaceré útoky na bankovú infraštruktúru *(Interpol, 2020)*. Zo správy organizácie Interpol za obdobie rokov 2019 – 2020 vyplynulo, že práve počas pandémie došlo

k významnejším posunom cieľov kybernetických zločinov z jednotlivcov na malé, alebo veľké organizácie s tým, že cieľom počas tohto obdobia sa stali aj nadnárodné spoločnosti, poskytovatelia služieb, ale aj vlády viacerých krajín sveta, ktoré zaznamenali zvýšený počet útokov na ich infraštruktúru *(Interpol, 2020) ; (Cosman, 2020)*.

Počas mesiacov január až apríl 2020 bolo organizácií Interpol nahlásených 907 000 spamových správ, 737 incidentov, ktoré boli priamo spojené s využívaním malwaru a tiež približne 48 000 podvrhnutých webových stránok, pričom všetky tieto incidenty boli priamo spojené s informáciami ohľadom novovzniknutej pandémie, ktorá dopomohla k ich rýchlemu šíreniu *(Interpol, 2020)*. Ako už bolo naznačené je možné skonštatovať, že v tomto období sa dostali do popredia hlavne kybernetické zločiny, ktoré sú vykonávané priamo pomocou informačných technológií a ktoré majú za cieľ sieťovú infraštruktúru, alebo používateľov služieb, ktoré sú poskytované ich pomocou *(Europol, 2020)*. Počas vrcholového obdobia pandémie (2020) boli najviac dominantné kybernetické incidenty typu ransomware, rôzne malwarové útoky, útoky na zahltenie sieťovej infraštruktúry typu DDoS a zločiny zamerané na podvrhovanie webových stránok za účelom získania citlivých informácií a v neposlednom rade aj zločiny zamerané na šírenie dezinformácií *(Interpol, 2020)*.

Počas obdobia pandémie páchatelia kybernetických zločinov využívali hlavne pocit neistoty a prvotný nedostatok informácií. V tomto období bol zaznamenaný aj zvýšený počet kybernetických incidentov, ktoré boli uskutočnené organizovanými zločineckými skupinami, ale aj útoky, ktoré boli zamerané na kritickú infraštruktúru štátov, alebo farmaceutických spoločností *(Cosman, 2020)*. Pred obdobím pandémie boli cieľovými zariadeniami primárne počítače, ktoré následne zbierali informácie zo siete, do ktorej boli pripojené. Počas pandémie bol zaznamenaný nárast malwarových útokov na mobilné zariadenia, nakoľko ich používatelia často nevynakladali rovnaké prostriedky na zabezpečenie ako pri počítačoch *(ENISA, 2020)*.

V nadväznosti na uvedené organizácia ENISA udáva znížený počet kybernetickej kriminality *(ENISA, 2020)*, ktorá je páchaná pomocou informačných technológií ako je fyzická manipulácia so zariadeniami, k čomu nepriamo dopomohla celosvetová pandemická situácia. Oproti konštatovanému, ako je možné vidieť na obrázku nižšie, bol zaznamenaný zvýšený počet už spomenutých ransomwarových útokov, vnútorných

hrozieb od zamestnancov, čo je možné prisúdiť preneseniu pracovného prostredia jednotlivcov zo zabezpečených firemných sietí do domáceho prostredia *(ENISA, 2020)*. V tomto období bol zaznamenaný veľký nárast zločinov zameraných na krádež identity osoby *(ENISA, 2020)*, na ktorom základe je možné predpokladať, že zabezpečenie citlivých informácií širokej verejnosti v kyberpriestore je nedostačujúce.

Top Threats 2019-2020		Assessed Trends	Change in Ranking
1	Malware	—	—
2	Web-based Attacks	—	↗
3	Phishing	↗	↗
4	Web application attacks	—	↙
5	Spam	↙	↗
6	Denial of service	↙	↙
7	Identity theft	↗	↗
8	Data breaches	—	—
9	Insider threat	↗	—
10	Botnets	↙	↙
11	Physical manipulation, damage, theft and loss	—	↙
12	Information leakage	↗	↙
13	Ransomware	↗	↗
14	Cyberespionage	↙	↗
15	Crytojacking	↙	↙

Obrázok 1: Najzávažnejšie hrozby za obdobie 2019-2020

Na základe naznačených spoločenských zmien, ktoré bolo potrebné uskutočniť vzhľadom na pandemickú situáciu a zaznamenané zvýšenie určitých druhov kybernetických zločinov, možno vyvodiť, že spoločnosť nebola na takýto rýchly presun služieb a iných súčastí bežného života do kyberpriestoru pripravená. Nepripravenosť sa následne odzrkadlila na zvýšenej efektivite páchania kybernetických zločinov *(Cosman, 2020)*, ktoré boli zamerané hlavne na krádež a následné využitie citlivých údajov, či už jednotlivca alebo spoločností, čo je možné prisúdiť nepripravenosti a nevedomosti zamestnancov jednotlivých spoločností a ich nedostatočnému zabezpečeniu domácich

sietí, a tiež aj nedostatočným bezpečnostným praktikám pri ochrane citlivých informácií na ich mobilných zariadeniach.

V konečnom dôsledku je možné uviesť, že pandemická situácia síce dopomohla k zvýšeniu kybernetických incidentov, avšak na druhej strane umožnila lokalizovať a identifikovať nedostatky v zabezpečení, či už technického riešenia zabezpečenia, alebo informovanosti širokej verejnosti *(Cosman, 2020)*. Uvedené môže následne viesť k ich náprave a v neposlednom rade aj vytvoreniu efektívnejšej legislatívy vo vzťahu ku kybernetickej kriminalite, či už na úrovni jednotlivých štátov, alebo aj medzinárodných spoločenstiev a tiež aj efektívnejšej spolupráci pri odhaľovaní a stíhaní kybernetickej kriminality.

4. STÍHANIE KYBERNETICKEJ KRIMINALITY V EURÓPSKEJ ÚNII

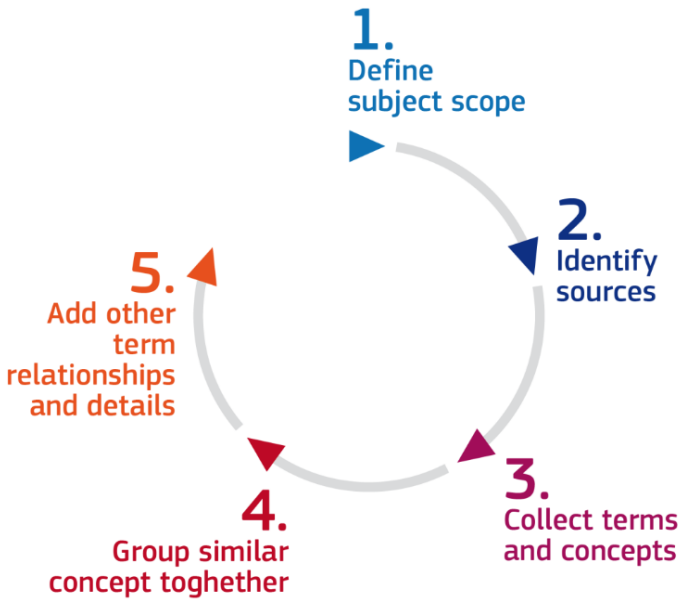
Na základe problému nejednoznačnosti skutkových podstát jednotlivých druhov kybernetickej kriminality a za základe nutnosti presne definovať, ktoré kybernetické incidenty sú považované za zločiny a ktoré nie, vznikli taxonómie (klasifikácie) kybernetických incidentov, ktoré sú uznávané a využívané na medzinárodnej úrovni. V rámci Európskej únie sa v súčasnosti najviac využíva taxonómia vytvorená spoluprácou organizácií ENISA a Europol. Pre vysvetlenie problému, ktorý vzniká pri nejednotnosti klasifikácií kybernetických zločinov je v tejto kapitole uvedené aj delenie a klasifikácia jednotlivých súčastí kybernetickej bezpečnosti na základe CIA triády, ktorá sama o sebe taxonómiou nie je. Taxonómia ENISA/Europol nie je všeobecne záväzná, ale je vo veľkej miere využívaná na prepojenie kybernetických incidentov s ich skutkovými podstatami a platnou legislatívou, na základe ktorej je možné ich postihovať *(Europol, 2017); (Walkowski, 2019)*. Takisto aj CIA triáda využívaná na klasifikáciu oblastí, ktoré je nutné ochraňovať pri zabezpečení dostatočnej miery kybernetickej bezpečnosti nie je štandardizovaná, ale je všeobecne uznávaná a využívaná *(Walkowski, 2019)*.

Táto kapitola obsahuje popisy využívaných taxonómií na úrovni medzinárodnej spolupráce členských štátov Európskej únie, a taktiež popisuje nariadenia Európskej únie, ktoré boli vytvorené za účelom zefektívnenia spolupráce pri odhaľovaní a stíhaní kyberkriminality.

4.1 Metodológia taxonómie

Taxonómiu ako takú je možné definovať ako činnosť, ktorá pozostáva z klasifikácie a vymedzenia určitej veci alebo konceptu. Taxonómia zároveň zahŕňa aj princípy, ktoré tvoria základ pre vytvorenú klasifikáciu, tj. pri taxonómií je definovaná klasifikácia a aj samotný dôvod, pre ktoré ju bolo nutné vytvoriť *(NAI-FOVINO, 2019).* Zároveň je pri taxonómií žiaduce podotknúť, že nie je vždy jednoznačná pre konkrétnu oblasť, ale môže sa približovať a to výraznejšie k určitému kontextu *(Europol, 2017).*

Pre kyberkriminalitu je taxonómia dôležitá, nakoľko umožňuje definovať odlišnosti medzi incidentom a kybernetickým zločinom. Zároveň definuje časti legislatívy, na ktoré je potrebné sa obrátiť v prípade kybernetického zločinu, a tiež aj rozsah samotnej skutkovej podstaty, ktorú je možné trestne stíhať. Pri tvorbe taxonómie je vhodné dodržiavať určité kroky, ktoré umožňujú lepšie definovanie rozsahu, skupín, spísanie legislatívnych a iných zdrojov a určenie termínov *(NAI-FOVINO, 2019).* Z dôvodu lepšieho znázornenia procesu tvorby taxonómie, je k dispozícii nižšie uvedený obrázok, ktorý znázorňuje jednotlivé kroky pri vytváraní taxonómie kyberkriminality. Tieto kroky označujú postupy, ktoré je vhodné použiť pri tvorbe taxonómie *(ENISA, 2016)*. Pri prvej fáze dochádza k definovaniu rozsahu subjektu, ktorý je nutné klasifikovať. V prípade kyberkriminality je vhodné definovať jej základný koncept a vytvoriť základnú sieť kompetencií v rámci prevencie a ochrany voči kybernetickým zločinom. V nasledujúcich dvoch fázach sú definované pojmy, ktoré sú všeobecne uznávanými a označujú kybernetické zločiny a ich všeobecný a stručný popis. V predposlednej fáze sú už vybrané pojmy spájané do skupín, ktoré umožňujú kategorizáciu jednotlivých zločinov tak, aby bolo možné určiť ich skutkové podstaty na základe platnej legislatívy *(ENISA, 2016)*. Následne v poslednej fáze je v prípade taxonómie kyberkriminality priradený vzťah, ktorý majú jednotlivé skupiny k legislatíve, pod ktorú na základe ich skutkovej podstaty spadajú *(NAI-FOVINO, 2019); (Europol, 2016)*.



Obrázok 2: Metodológia taxonómie

Pre zjednodušenie a skompletizovanie je možné povedať, že taxonómia pozostáva z definovania skúmanej oblasti, stanovenia základných pojmov, ktoré je nutné začleniť do skupín, ktoré majú spoločné vlastnosti, na základe ktorých sú následne analyzované *(ENISA, 2016)*.

Ako už bolo spomenuté vytvorená kategorizácia nie je jednotná. V prípade kyberkriminality to znamená, že skupiny vytvorené jedným rozdelením a ich definície sa líšia od inej kategorizácie, ktorá bola vytvorená v rovnakej oblasti *(NAI-FOVINO, 2019)*. V praxi tento problém poukazuje na nejednotnosť a od toho odvodenú nejednoznačnosť pri definovaní skutkových podstát kybernetických zločinov, čo vedie k rozporom na medzinárodnej úrovni *(ENISA, 2016)*. Primárne, ak sa jedná o zločiny, ktoré sú definované na okrajoch jednotlivých skupín, môže dochádzať k ich prelínaniu s inou definovanou skupinou.

Problematickou sa môže javiť nejednotnosť legislatívy z pohľadu jednotlivých členských štátov Európskej únie *(Buono, 2016)*, nakoľko aj keď existujú nariadenia a odporúčania, ktorými sa členské štáty riadia, je potrebné zdôrazniť, že adekvátna legislatíva nie je definovaná rovnako. Z daného dôvodu vznikajú odlišné posúdenia a vyhodnotenia pri odhaľovaní a identifikácií príslušnej skutkovej podstaty kybernetického zločinu.

4.2 Príklady v súčasnosti využívaných taxonómií

V súčasnosti vo svete, vrátane členských štátov Európskej únie, neexistuje jednotná taxonómia kybernetickej kriminality, ktorá by bola štandardizovaná a všeobecne využívaná v medzinárodnom práve a umožnila by efektívnejšie stíhanie kybernetickej kriminality *(ENISA, 2016)*. Z naznačeného je možné vyvodiť, že v súčasnosti existuje veľké množstvo taxonómií, ktoré sú využívané v jednotlivých štátoch, štátnych zoskupeniach (napr. Európska únia), alebo aj v špecializovaných agentúrach a nadnárodných organizáciách, ktoré sa zaoberajú kybernetickou bezpečnosťou.

Podľa špecializovanej agentúry ENISA je evidované veľké množstvo taxonómií, pričom veľa z nich je do určitej miery využívaných *(ENISA, 2016)*. Zároveň agentúra ENISA uskutočnila do roku 2015 výskum v tejto oblasti, ktorého hlavným cieľom bolo vytvoriť návrh možnej spoločnej taxonómie, ktorá by spĺňala podmienky stanovené štátnymi orgánmi, ktoré sa špecializujú na vyšetrovanie a stíhanie kybernetickej kriminality a CSIRT tímov. Pre účely tejto štúdie analyzovala celkovo 12 využívaných taxonómií a ich parametre *(ENISA, 2016)*. Na obrázku nižšie je pre ilustráciu naznačená časť z nich a pre

vysvetlenie problému, ktorý vzniká pri tvorbe a využívaní jednotlivých taxonómií, sú niektoré uvedené nižšie.

NR.	TAXONOMY	PROS	CONS
1.	**CERT NIC.LV taxonomy**	N/A	Outdated.
2.	**The common language**	N/A	Outdated.
3.	**The eCSIRT taxonomy**	N/A	Outdated.
4.	**CERT.PT taxonomy**	Proposed choice of OAP 4.1 working group. Owned by the OAP 4.1 working group. High-level. Already in use in Portugal.	Simplicity of the classification.
5.	**AVOIDIT taxonomy**	N/A	Limited recognition by the business.
6.	**Data Harmonization Ontology**	Created by CSIRTs. Ease of use.	Limited recognition by the business. Simplicity of the classification.
7.	**VERIS**	High level of detail. Significant recognition by the business.	Complexity. (More input and a better technical knowledge from the user required). Owned by a private entity.
8.	**CybOX**	High level of detail. Significant recognition by the business.	Complexity (More input and technical knowledge from the user required). Owned by MITRE[35].
9.	**Hungarian taxonomy**	*N/A due to classification*	*N/A due to classification*
10.	**Phänomene Cybercrime**	Details each element from a high-level point of view.	Crime-specific Draft version, in German
11.	**CSIRT-MU taxonomy**	High-level.	Limited amount of types of events.

Obrázok 3: Taxonómie analyzované organizáciou ENISA

Taxonómia CERT.PT bola navrhnutá už spomenutou súčasťou organizácie Europol, a to skupinou EC3 a bola vytvorená na základe spolupráce niekoľkých CSIRT a portugalskej polície a jej hlavnou výhodou je to, že je možné ju aplikovať na veľké množstvo legislatív členských štátov Európskej únie. Aj keď bola v roku 2015 využívaná veľkým množstvom CSIRT tímov jej hlavnou nevýhodou je vysoký a veľmi široký level klasifikácie jednotlivých druhov kybernetickej kriminality a preto by incident, ktorý je popísaný touto taxonómiou neposkytuje veľa informácií o incidente samotnom. Využitie tejto taxonómie je vhodné pre účely vytvárania štatistických údajov o kybernetickej kriminalite. Táto taxonómia je príkladom medzinárodných snáh o vytvorenie efektívnej klasifikácie

kyberkriminality, ktorú by bolo možné využívať minimálne na efektívnejšiu spoluprácu národných CSIRT tímov *(ENISA, 2016)*.

Príkladmi taxonómií, ktoré boli vytvorené na území jednotlivých štátov môže byť vyššie uvedená taxonómia využívaná na území Maďarska, bola vytvorená maďarskou políciou a slúži na zefektívnenie spolupráce medzi maďarskou políciou a CSRIT tímami (ENISA, 2016), alebo taxonómia kybernetických bezpečnostných incidentov, ktorá bola vytvorená príslušnými orgánmi v Českej republike.

V Európskej únií je v súčasnosti na medzinárodnej úrovni najviac využívaná taxonómia vytvorená spoločnosťou ENISA/Europol *(Europol, 2016)*, ktorej výhodou je to, že prideľuje skutkové podstaty kybernetických incidentov k príslušnej súčasnej medzinárodnej legislatíve. Okrem klasického poňatia taxonómií kybernetickej kriminality je možné pri jej odhaľovaní a stíhaní využiť aj delenie na základe CIA triády, ktorá bola navrhnutá a je využívaná pri zabezpečení kybernetickej bezpečnosti. A je nutné poznamenať, že ani toto delenie nie je vhodné využívať všeobecne, nakoľko sa zameriava len na kybernetické incidenty, ktoré sú mierené na koncové zariadenia alebo sieťovú infraštruktúru a opomína kybernetické zločiny, ktoré informačné technológie len využívajú.

4.3 CIA triáda

CIA triáda sama o sebe nebola navrhnutá ako taxonómia, ktorá by bola využívaná na delenie kyberkriminality. Samotná skratka odkazuje na prvky bezpečnosti, ktoré sú využívané v bezpečnostných systémoch a je odvodená od anglických slov confidentiality (dôvernosť), integrity (integrita), availability (prístupnosť) a určuje oblasti, ktoré by mali byť chránené pri výbere vhodnej ochrany pred kybernetickým útokom *(Samonas, 2014)*. Tieto tri pojmy slúžia ako ciele, ktoré je nutné zabezpečiť na to, aby bol systém chránený *(Walkowski, 2019)*. Keďže presne vymedzuje oblasti, ktoré je žiaduce chrániť, je vďaka tomu do akej miery bolo do týchto oblastí preniknuté určiť, čo bolo cieľom kybernetického útoku a posúdenie jeho závažnosti. Je možné vyhodnotiť príslušnú skutkovú podstatu a na základe miery narušenia určiť, či sa jedná o kybernetický zločin alebo nie *(Walkowski, 2019)*, aj keď takéto využitie nie je jej primárnym cieľom.

Confidentiality (dôvernosť) vo všeobecnosti označuje snahu zabezpečiť informácie tak, aby neboli bežne dostupné a aby bol k nim obmedzený prístup. V praxi znamená nastavenie bezpečnostnej politiky na takú úroveň, aby zabezpečovala ochranu voči krádeži, alebo nepovolanému nahliadaniu do ochraňovaných dát, čo vo všeobecnosti zahŕňa primárne obmedzenie prístupu. Dôvernosť však môže byť narušená, či už priamo útokom, ako je man-in-the-middle (útok spočívajúci v odchytení komunikácie medzi komunikujúcimi stranami a následné vydávanie sa za jednu komunikujúcu stranu, čo efektívne preruší pôvodnú legitímnu komunikáciu), alebo nedbanlivosťou, kam sa primárne radí ľudská chyba a neadekvátnosť (prílišná jednoduchosť) používaných hesiel *(Walkowski, 2019)*.

Integrity (integrita) z etymologického hľadiska je tento pojem spätý s pojmom nedotknuteľnosť a v oblasti informačnej bezpečnosti znamená zabezpečenie dát voči neoprávnenej manipulácií, a teda zabezpečenie dôvery voči dátam. Jej zabezpečenie zahŕňa hlavne zabezpečenie elektronickej komunikácie a úložiska dát tak, aby bolo možné dokázať, že s dátami nebolo manipulované *(Samonas, 2014)*. Voči integrite je najčastejším bezpečnostným incidentom útok odpočúvaním komunikácie (sniffing, scanning) *(Europol, 2017)*.

Availability (dostupnosť) zabezpečuje dostupnosť dát, ktoré majú byť prístupné či už používateľom, alebo verejnosti a zabezpečuje ochranu tých dát, ku ktorým je prístup zakázaný *(Walkowski, 2019)*. Jednoducho povedané, autorizovaný používatelia majú povolený prístup len k adekvátnym dátam a dáta, ktoré pre nich nie sú podstatné, sú pre nich nedostupné. Pre veľké množstvo online služieb je výmena a prístup k dátam kľúčový pre ich funkciu. Útoky, ktoré proti dostupnosti existujú, sú primárne zamerané na zahltenie služby, aby boli jej dáta nedostupné *(Walkowski, 2019)*. Najčastejším útokom voči dostupnosti dát je DDoS útok, ktorý pracuje na princípe zahltenia siete alebo služby požiadavkami, čím znemožňuje prístup k dátam alebo samotnej službe *(Europol, 2017)*.

Delenie kybernetických incidentov podľa miery narušenia CIA triády má jeden veľký nedostatok, ktorý vyplýva z jej pôvodnej funkcie a na základe ktorého nie je vhodným delením kybernetických zločinov *(Walkowski, 2019)*. Toto delenie sa zameriava na oblasti ochrany v kybernetickej bezpečnosti, tj. bezpečnosť v kyberpriestore, pričom neberie na zreteľ súčasti kybernetickej kriminality, ktoré nie sú primárne zamerané na

kyberpriestor, ale len využívajú informačné technológie. Na podklade uvedeného je možné povedať, že keby bolo využívané len toto delenie, veľká časť kybernetických zločinov by ostala nepovšimnutá, či už z hľadiska trestného stíhania páchateľov alebo spracovávania a vyhodnocovania štatistických údajov ohľadom uskutočnených zločinov *(Walkowski, 2019)*. Preto je nutné využívať delenie, ktoré umožňuje spracovať aj kybernetické zločiny, ktoré sa nezameriavajú priamo na informačné technológie ale využívajú ich len nepriamo, alebo okrajovo.

4.4 ENISA/Europol

V súčasnosti je v Európskej únii využívaná taxonómia vytvorená spoluprácou organizácií ENISA a Europol, ktorej najnovšia verzia pochádza z roku 2017 *(Europol, 2016)*. Bola vytvorená na lepšiu koordináciu spolupráce skupín, ktorých primárnou úlohou je odpoveď na hrozby proti kybernetickej bezpečnosti. Táto taxonómia však nepopisuje len kybernetické zločiny, ktoré priamo využívajú informačné technológie, ale aj tie, ktoré tieto technológie využívajú len okrajovo, pričom je limitovaná na pokusy a vykonanie zločinu *(Europol, 2016)*. Incidenty, ktoré prebehli len náhodou, aj keď pri nich vznikla škoda neeviduje, čo je možné považovať za nevýhodu. Bola vytvorená pre využitie v medzinárodnom spoločenstve krajín Európskej únie a rozdeľuje kybernetické zločiny tak, aby boli postihnuteľné európskym právom.

Samotná taxonómia je primárne využívaná na zjednotenie hlásení incidentov a postupov, ktoré sú realizované na základe právnych predpisov, ktoré k definovaným skupinám kybernetických zločinov prislúchajú *(Europol, 2016)*. Na jej základe je možné prekonať problémy, ktoré vznikajú pri spolupráci koordinačných skupín s organizáciami, ktorých úlohou je vymáhať zákony Európskej únie. Nakoľko zabezpečuje harmonizáciu hlásení o kybernetických zločinoch, je na jej základe možné vytvárať aj štatistiky, ktoré odzrkadľujú situáciu kyberkriminality v Európskej únii *(Europol, 2016)*. Avšak nakoľko táto taxonómia nie je štandardizovaná, je pravdepodobné, že sa štatistiky z rôznych zdrojov nebudú zhodovať. Pričom tento problém nastane v prípade, že tieto zdroje nevyužívajú jednotnú taxonómiu, ale jej variácie, alebo úplne iné delenia.

Ako už bolo okrajovo spomenuté taxonómia mapuje kybernetické incidenty, vytvára z nich skupiny na základe podobností ich skutkových podstát a následne týmto skupinám

pridáva legislatívny základ. Takýmto určením môže byť konkrétny incident jednoducho priradený adekvátnej medzinárodnej legislatíve a následne podradený pod príslušnú legislatívu štátu, v ktorom sa incident odohral *(Europol, 2016)*. Nakoľko nie každý kybernetický incident je aj kybernetickým zločinom, a teda jeho skutková podstata nie je stíhateľná trestným právom, umožňuje táto klasifikácia definovať hranice medzi kybernetickým incidentom a kybernetickým zločinom *(NAI-FOVINO, 2019)*

Tieto skupiny kategorizujú kybernetické incidenty určitého druhu tak, aby mohli byť podradené pod legislatívu, ktorá vo vzťahu k nim bola vytvorená v minulosti. Jedným z príkladov pre takéto delenie je vytvorená skupina kybernetických incidentov, ktorá je v tejto taxonómií označená pojmom availability (dostupnosť), a do určitej miery korešponduje s rovnakým pojmom v CIA triáde *(Walkowski, 2019)*. Do tejto skupiny sú radené všetky kybernetické incidenty, ktoré určitým spôsobom obmedzujú dostupnosť služieb alebo dát, ako sú DDoS a DoS útoky alebo sabotáž *(Europol, 2016)*.

Faktom však zostáva, že toto delenie je všeobecné, jeho primárnou funkciou je zabezpečiť súčinnosť na medzinárodnej úrovni, z čoho možno vyvodiť, že toto delenie nie je celkom vhodné pre aktívne používanie pri stíhaní vnútroštátnych a lokalizovaných kybernetických zločinov.

5. ASP.NET

Asp.net je rozšírením frameworku .net a primárne je využívaný na vytváranie webových aplikácií a taktiež je vytvorený spoločnosťou Microsoft. Asp.net je platforma, ktorá sprostredkováva programovací model, pochopiteľnú infraštruktúru a rôzne ďalšie komponenty, ktoré umožňujú efektívnejšie vytváranie webových aplikácií *(Microsoft, 2021).* Pracuje s protokolom http, ktorý využíva aj na posielanie príkazov. Zároveň využíva aj ďalšie postupy, ktoré zabezpečujú efektívnejšiu komunikáciu a spoluprácu, ktorá je nutná v internetovom prostredí *(Microsoft, 2021)*. Všetky aplikácie, ktoré táto platforma už obsahuje, majú zložky definované tak, aby boli jednoducho použiteľné a aby zjednodušovali vývoj aplikácie.

Primárne je táto platforma určená na vytváranie interaktívnych aplikácií, ktoré sú vo veľkej miere využívané v internetovom priestore. Podporuje viaceré programovacie jazyky, ako sú C#, JavaScript, VisualBasic a iné, ktoré sú využívané na back-end programovanie, tj. na vytvorenie logiky fungovania samotnej aplikácie *(Microsoft, 2021)* (vytvorenie štruktúr a databáz, vytvorenie jednotlivých metód, ktoré sú následne sprostredkované v používateľskom rozhraní...). Nakoľko je rozšírením platformy .net, využíva rovnaký spôsob prekladu jednotlivých programovacích jazykov do natívneho kódu zariadenia.

Asp.net je platforma pracujúca len na strane servera, čo znamená, že pri vytváraní webových aplikácií sú jednotlivé skripty posielané na server, pričom je možné vytvárať aj prispôsobené používateľské rozhranie, aj logiku, ktorá zabezpečuje chod celej aplikácie *(Microsoft, 2021) (Strahl, 2005).* Z tejto definície je zrejmé, že na správne fungovanie webovej aplikácie je nutná komunikácia typu klient-server, čo je zabezpečené protokolom http.

5.1 Komponenty ASP.NET

Primárne komponenty zostávajú rovnaké ako pri platforme .net, nakoľko asp.net je jej rozšírením, avšak na zefektívnenie jej funkcionality a rozšírenie možností boli pridané ďalšie zložky. Tieto zložky definujú primárne autentizačný systém, knižnice, ktoré

indikujú predchádzajúce vzory využité pri modelovaní webových aplikácií, základný framework pre spracovanie webových požiadaviek, kešovanie a iné *(Microsoft, 2021).* Autentizačný systém platformy obsahuje knižnice, databázy a vzorové stránky pre vytvorenie prihlásenia používateľa. Zároveň obsahuje možnosti pre vytvorenie viacvrstvovej ochrany a externú autentizáciu, čo umožňuje vzdialené prihlásenie do už vytvorenej aplikácie. Nakoľko je asp.net platforma, ktorá je serverovo orientovaná, je na zabezpečenie komunikácie klient-server využívaný len základný framework *(Microsoft, 2021)*. Tento framework na strane servera hodnotí kód, ktorý je napísaný v programovacom jazyku a následne na jeho základe generuje html požiadavky, ktoré sú posielané používateľovi *(Microsoft, 2021); (Strahl, 2005)*.

Kešovanie umožňuje dočasné ukladanie webových stránok, využívaných webovou aplikáciu, za účelom zrýchlenia načítania informácií na základe požiadaviek, ktoré klient zadáva. Dočasné ukladanie týchto dát umožňuje rýchlu *(Microsoft, 2021)* odpoveď aplikácie a lepšiu odpoveď na želanie klienta a zobrazenie dát *(Strahl, 2005).*

5.2 Model View Controller (MVC)

MVC je skratkou pre architektonický model využívaný na platforme .net, ktorý umožňuje rozdelenie komponentov aplikácie na tri skupiny, ktoré sú v angličtine pomenované Model, View a Controller *(Microsoft, 2021).* Toto rozdelenie umožňuje lepšie delegovanie jednotlivých akcií, ktoré má aplikácia vykonávať, napríklad požiadavky používateľov sú priamo smerované na riadiacu jednotku, ktorá má na starosti ovládanie všetkých troch komponentov. Ovládač (Controller) vyberie zobrazenie, ktoré sa má používateľovi zobraziť na základe požiadavky prijatej riadiacou jednotkou a následne sú mu zobrazené adekvátne informácie *(Microsoft, 2021)*.

Takýto typ delegácie zodpovednosti umožňuje rýchlejšiu reakciu na požiadavky od koncového používateľa a zároveň umožňuje efektívnejšiu delegáciu zdrojov vo vnútri samotnej aplikácie. Zároveň je takýto druh modelu jednoduchšie programovateľný a udržiavaný, primárne z dôvodu častých aktualizácií aplikácie *(Microsoft, 2021)*.

Model predstavuje logiku a operácie, ktoré má aplikácia vykonávať *(Strahl, 2005)*.. Business logika je v tomto modeli pevne spätá s implementačnou logikou, čo umožňuje zachovanie stavu aplikácie v prípade testovania a aktualizácií softwaru. Zložka View

zodpovedá za reprezentáciu výsledkov používateľovi a obsahuje minimálnu logiku, ktorá je priamo zviazaná so samotným zobrazovaním výsledkov. Ovládač je hlavná zložka celého modelu, ktorá spracováva požiadavky používateľa a na ich základe pracuje s modelom tak, aby výsledkom tejto spolupráce bolo zobrazenie adekvátnej odpovede na komponente View. Primárne zabezpečuje kontrolu nad hlavnými súčasťami aplikácie a ich funkciou a zároveň zabezpečuje interakciu používateľského rozhrania aplikácie s koncovým používateľom *(Microsoft, 2021)*.

5.3 Tvorba webovej aplikácie

Praktickou časťou tejto bakalárskej práce je vytvorenie webovej aplikácie, ktorá umožňuje zobrazovať štatistické a iné informácie ohľadom kyberkriminality. Na tvorbu webovej aplikácie je množstvo rôznych platforiem, avšak v tejto práci bola použitá platforma .net s rozšírením asp.net, ktorý bol navrhnutý za týmto účelom.

Pri tvorbe webovej aplikácie je v prvom kroku nevyhnutné stanoviť základnú predstavu a funkčnosti aplikácie, tj. aké sú požiadavky na sprostredkovanie informácií, používateľské rozhranie, akým typom bude webová aplikácia, atď. Zároveň je nutné definovať požiadavky na jej základný výzor, ako je rozdelenie hlavného menu a umiestnenie využitých objektov na jednotlivých formulároch webových stránok. Následne sa od týchto základných požiadaviek odvíja všetka ďalšia tvorba.

Výhodou platformy .net je to, že pri vytvorení nového projektu (novej formy do ktorej bude vkladaný kód aplikácie) je možné nastavenie, ktoré umožňuje automatické vygenerovanie základných častí, ktoré má webová aplikácia obsahovať, ktoré sú nevyhnutné na spustenie webovej aplikácie. Testovanie webovej aplikácie je možné aj bez pripojenia na internet, nakoľko všetky súbory sú ukladané na hosťujúcom zariadení.

5.4 Základný koncept

V základnom koncepte webovej aplikácie je ako prvé nutné definovať, aké základné funkcie má spĺňať. V prípade webovej aplikácie CCW, je jej základnou funkcionalitou sprostredkovanie štatistických údajov o kyberkriminalite v Európskej únii, pričom používateľovi umožňuje jednoduchú orientáciu v dátach možnosti filtrovania a prívetivého používateľského rozhrania. Sekundárnou funkciou tejto aplikácie je

zobrazovanie základných informácií o jednotlivých zločinoch a spracovávanie štatistických údajov.

Následne je nutné definovať základný výzor aplikácie, ktorý má čo najlepšie zodpovedať požiadavkám, ktoré na definovanú aplikáciu budú kladené. Za týmto účelom bolo vytvorené používateľské rozhranie, ktoré je veľmi jednoduché a pozostáva z hlavného výberu údajov, ktoré majú byť zobrazené a zo sekundárnych položiek, z ktorými je možné následne pracovať.

Ako ďalší krok je vhodné zvoliť platformu, na ktorej bude webová aplikácia vytváraná, čo je ako už bolo spomenuté, platforma .net, vo Visual Studiu, ktorý vytvára kontrolované vývojové prostredie. Platforma .net bola vybraná primárne kvôli rozšíreniam, ktoré vytváranie webovej aplikácie uľahčujú. Ako programovací jazyk bol zvolený C#, nakoľko jeho funkcionalita je obšírnejšia a umožňuje lepšiu variabilitu pri vytváraní jednotlivých komponentov aplikácie.

5.5 Návrh riešenia

Pri návrhu riešenia je potrebné ako prvé zistiť, aké funkcie má aplikácia vykonávať a aké sú požiadavky, ktoré budú kladené na aplikáciu pri jej používaní. Požiadavky budú tvorené hlavne potrebami zo strany používateľov, pre ktorých je aplikácia vytvorená. Nakoľko je aplikácia verejná, nedefinuje nutnosť autorizácie jednotlivých používateľov. Jednotlivé požiadavky na aplikáciu sú nasledovné:

1. Uchovávať a sprostredkovať štatistické a informačné dáta z oblasti kyberkriminality.
2. Filtrácia kybernetických zločinov na základe ich názvov
3. Popis zločinu je uchovaný v databáze a jeho možné zobrazenie na základe kliknutia na príslušný kybernetický zločin v v hlavnom výpise kybernetických zločinov
4. Zobrazenie získaných štatistických údajov (od relevantných zdrojov) v grafickej podobe
5. Uchovávanie ďalších informácií ohľadom bezpečnostných zložiek na ktoré je možné obrátiť sa v prípade podozrenia na páchanú kybernetickú činnosť.

Najdôležitejšími požiadavkami, ktoré boli spomenuté sú body 1., 3. a 4., nakoľko základnou myšlienkou aplikácie je zrozumiteľné sprostredkovanie zozbieraných štatistických údajov dát a priehľadné sprostredkovanie základných informácií o jednotlivých kybernetických zločinoch podľa taxonómie ENISA/Europol. Na tieto požiadavky následne priamo nadväzujú požiadavky v bodoch 2., 5. nakoľko tieto určujú rozširujúce možnosti pri narábaní s aplikáciou ako je vyhľadávanie konkrétneho kybernetického zločinu a popis špecializovaných skupín, na ktoré je možné sa obrátiť v prípade podozrenia na páchaný kybernetický zločin. Funkcia aplikácie popísaná v bode 5. je sekundárna, nakoľko umožňuje len jednoduchšie získanie potrebných informácií a neumožňuje samotné nahlásenie kybernetického zločinu.

Ďalším krokom pri vývoji webovej aplikácie je vytvorenie návrhu schémy, ktorý bude implementovaný a ktorý zodpovedá definovaným požiadavkám. Schéma webovej aplikácie definuje tri hlavné stránky aplikácie, ktoré sa nachádzajú v hlavnom výbere CYBER CRIME WEB, a to: Štatistické informácie, Kybernetické zločiny a Organizácie, ktoré ukazujú na jednotlivé podstránky, ktoré sprostredkovávajú požadované informácie v podobe databáz alebo v prípade štatistických údajov grafického zobrazenia.

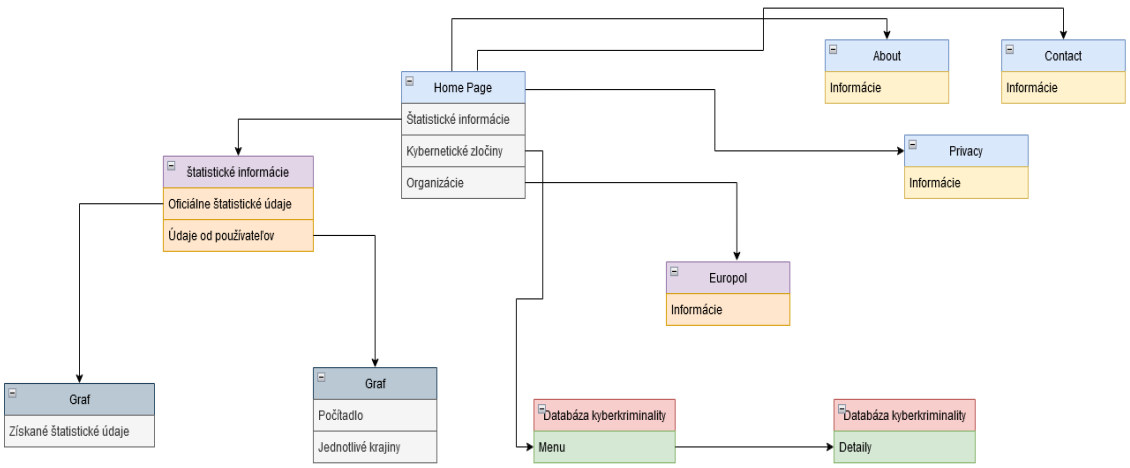
CYBER CRIME WEB je hlavnou záložkou aplikácie, na ktorej je zobrazený základný výber stránok, ktoré aplikácia zobrazuje a na základe tohto výberu je následne možné pristupovať k ďalším funkciám, ktoré aplikácia umožňuje. V záložke, ktorá je nazvaná ako Štatistické informácie sú definované podstránky, v ktorých sú graficky zobrazené získané štatistické informácie ohľadom kybernetickej kriminality, ktoré umožňujú zreteľnejší prehľad o stavoch a trendoch kybernetickej kriminality pre používateľa. V tejto časti webovej aplikácie sú preto definované jednotlivé podstránky, ktoré po vstupe do nich (kliknutie na príslušnú ikonu) umožňujú zobrazenie vybraných dát. Dáta uchované týmto spôsobom sú staticky vytvorené a nie je možné ich meniť na základe požiadaviek používateľa.

V záložke: Kybernetické zločiny je následne vytvorená a zobrazovaná databáza kybernetických zločinov na základe taxonómie ENISA/Europol v ktorej je možná filtrácia relevantných kybernetických zločinov na základe ich mien. Zároveň je v tomto vytvorenom liste po kliknutí na príslušný obrázok, nachádzajúci sa vedľa názvu zločinu,

možné pristúpiť k podrobnejšiemu popisu kybernetického zločinu, čo je umožnené previazaním databáz, ktoré tieto informácie ukladajú.

V okne, ktoré bolo nazvané ako Organizácie sú následne definované jednotlivé podstránky, ktoré ukladajú informácie o bezpečnostných zložkách na území Európskej únie, ktorých primárnou úlohou je odhaľovať a vyšetrovať kybernetické zločiny. V tejto podstránke nie je možné nahlasovať kybernetické zločiny, ale v jednotlivých stránkach sú uložené informácie ukazuje informácie o tom akým spôsobom fungujú organizácie Europol, primárne funkcia skupín EC3 a EUCTF, Interpol a iné.

V neposlednom rade webová aplikácia obsahuje záložky About a Contact, ktoré poskytujú základné informácie o webovej aplikácií a možnosti kontaktovania.



Obrázok 4: Schéma webovej aplikácie

6. IMPLEMENTÁCIA

Táto kapitola poníma o implementácií webovej aplikácie z programovacieho hľadiska, tj. popisuje zaujímavé časti zdrojového kódu aplikácie. Z hľadiska technickej implementácie webovej aplikácie je nutné definovať dva rôzne pohľady – backend (funkčná strana aplikácie, ktorá sa stará o všetku logiku aplikácie a jej jednotlivé funkcie) a používateľské rozhranie, ktoré sprostredkováva prostredie na zobrazovanie informácií používateľovi aplikácie.

Na vytvorenie serverovej strany aplikácie bol využitý jazyk C# a na vytvorenie používateľského rozhrania bola využitá technológia HTML. Pri tvorbe webovej aplikácie bol v platforme .net využitý model MVC, ktorý umožňuje vytvorenie interaktívnych systémov na základe definovania kontrolérov, zobrazenia samotnej stránky a modelu, na základe, ktorého sú jednotlivé súčasti definované. V následných kapitolách sú popísané a vysvetlené ukážky kódov, ktoré boli esenciálne pre vytvorenie aplikácie.

6.1 HomePage

V ponímaní platformy .net je HomePage, jej kontrolér a model základným nastavením a zobrazením, odkiaľ sú ďalej smerovaní vyššie spomenuté zobrazenia About, Privacy, a Contact. Zároveň zobrazuje základné nastavenia, ktoré sú vopred definované pri vytvorení nového projektu, ako je grafika a implementácia a webové rozhranie. Táto stránka je pri vytvorení nového projektu vo Visual studiu vygenerovaná automaticky. Samotná grafika je definovaná v súbore **style.css**, ktorý je implementovaný v hlavnom súbore aplikácie, ktorý definuje hlavné zobrazenie a funkcionalitu, tj. Layout.cshtml, ktorý je zobrazením hlavného výzoru aplikácie. Všetky ďalšie stránky, ktoré sú v aplikácií definované implementujú túto grafiku automaticky, a teda nie je potrebné vytváranie novej grafiky pre každú stránku.

Okrem základnej grafiky definuje aj rozhranie pre navigáciu v rôznych ďalších stránkach webovej aplikácie. Pre účely tejto aplikácie tento panel ukazuje len na doplnkové stránky aplikácie, ktoré nemajú v aplikácií žiadnu ďalšiu väčšiu funkciu. Samotné súčasti

aplikácie, ktoré priamo zobrazujú potrebné informácie sú bližšie určené v hlavnej časti stránky HomePage a nie v kontrolnom paneli.

Toto grafické rozhranie je však nutné definovať pomocou programovacieho jazyka. Na základe novo vytvoreného štýlu aplikácie, ktorý bol vytvorený na základe voľne dostupného projektu, ktorý je dostupný ako na youtube tak aj na githube *(Doyle, 2021)* a bol vybraný pre lepšiu a jednoduchú orientáciu boli v tele hlavnej stránky vytvorené „okná“. Tieto „okná“ umožňujú jednoduché ovládanie súčastí aplikácie.

Obrázok 5: Grafické znázornenie "okien" hlavného menu

Vyššie uvedený obrázok tvorí ukážku zobrazenia „okien“, ktoré sú ďalej používané na zobrazenie definovaných súčastí a tvoria grafickú stránku aplikácie, pričom na vstup do stránok, ktoré sú naviazané na grafické ikony, je možný po kliknutí na príslušný obrázok. Nižšie uvedený obrázok naopak znázorňuje programovaciu alebo technickú stranu aplikácie a bližšie vysvetľuje akým spôsobom bolo takéto zobrazenie dosiahnuté.

Nižšie uvedený obrázok znázorňuje ukážku implementácie jednoduchého skriptu, ktorý len definuje parametre zobrazenia, do primárnej stránky webovej aplikácie. Kód je členený do jednotlivých tried (class), ktoré umožňujú definovať jednotlivé komponenty a ich umiestnenie na výslednej stránke. Tieto komponenty boli vopred definované v už spomenutom predpise zobrazenia a v tomto kóde sú už priamo implementované. V tomto prípade je v kóde definované zobrazenie jednej možnosti výberu na hlavnej stránke, a to **Statistics**.

Na grafickom zobrazení je možné vidieť, že obe okná majú obrázky, ktoré sú rovnakej veľkosti. Na nižšie uvedenom obrázku je možné vidieť, že v kóde je definované len umiestnenie daného obrázka v pamäti zariadenia. Samotné zarovnanie a veľkosť je definovaná v už spomenutom predpise štýlu aplikácie, a to konkrétne v príkazom **card-img-top**, ktorý má vo svojom predpise uvedené potrebné parametre.

```
@{
    ViewData["Title"] = "Home Page";
}
<div class="jumbotron" style="background-color: cornsilk; margin-block-end:2.5em; margin-top: 2.5em">
    <h3 style="text-align:center;"> CybercrimeWeb </h3>
</div>
<div class="action-menu">
    <div class="container">
        <div class="row row-cols-1 row-cols-sm-2 row-cols-md-3 g-3">
            <div class="col">
                <div class="card h-100">
                    <a asp-controller="Statistics" asp-action="Statistics">
                        <img src="@Url.Content("~/images/chart.png")"
                             class="card-img-top">
                    </a>
                    <div class="card-body">
                        <h5 class="card-title">
                            Statistics
                        </h5>
                        <p class="card-text">
                            Zobrazenie jednotlivych statistik
                        </p>
                    </div>
                </div>
            </div>
```

Obrázok 6: Ukážka HTML kódu hlavnej stránky aplikácie

6.2 Databázový systém

Pri tvorbe webovej aplikácie je možné využiť niekoľko rôznych riešení ukladania dát, ako je napríklad ukladanie do súborov na serveri, avšak najčastejšie využívaným riešením je databázový systém na strane servera, ktorý ukladá požadované dáta. Táto webová aplikácia využíva databázy typu SQL, nakoľko sú priamo podporované a bežne využívané v praxi. V prípade webovej aplikácie CCW je využitých hneď niekoľko takýchto databáz, ktoré zhromažďujú či už dáta zadané používateľom, alebo sú pripravené na ukladanie štatistických dáta, ktoré do nich budú priradené z bakalárskej práce.

V súčasnej štruktúre webovej aplikácie je priamo využívaná 1 databáza – CrimeApp_Data, ktorá však obsahuje pre jej potreby aj abstraktnú databázu CrimeData. Crimes databáza je hlavná databáza využívaná na ukladanie informácií ohľadom kybernetickej kriminality a v aplikácií je zobrazená 2x. Prvé zobrazenie je ako zoznam jednotlivých druhov kybernetickej kriminality a ich pomenovaní. Druhé zobrazenie je

viditeľné po kliknutí na niektorý zločin v hlavnom zozname a po vstupe po kliknutí na obrázok priradený ku konkrétnemu konkrétneho zločinu sú viditeľné ďalšie dáta, ktoré prislúchajú každému zločinu v hlavnom zozname. Pre tieto potreby bola vytvorená aj abstraktná databáza, nakoľko bolo potrebné rozlíšiť dáta s ktorými je potrebné pracovať v hlavnom zozname a v konkrétnych vstupoch. Nakoľko MVC model a SQL databáza neumožňuje duálne definovanie rovnakých dát, je v abstraktnej databáze definovaný názov zločinu zobrazený v hlavnom zozname a v databáze CrimeApp_Data všetky ostatné informácie.

Zároveň na základe obmedzení súčasnej verzie MVC modelu ASP.NET bolo potrené vytvoriť vlastný projekt pre databázový systém a pre prácu s týmto systémom a následne bolo potrebné vykonať migráciu databázy tak, aby s ňou mohol hlavný projekt pracovať.

6.3 Filtračný systém

Jedna zo základných požiadaviek kladená na túto webovú aplikáciu bola prehľadnosť zozbieraných štatistických dát. Na dosiahnutie požadovanej prehľadnosti je využívaný filtračný systém, ktorý v súčasnosti zobrazuje jednotlivé položky v databázach na základe zobrazovania príslušného kybernetického zločinu na základe jeho názvu. V prípade zobrazovania štatistických údajov je ich filtrácia uskutočnená vo vytvorenom prehľadnom rozdelení spracovaných štatistických údajov do jednotlivých stránok v ktorých sú zobrazené príslušné grafy.

Na vytvorenie filtrácie bol využitý prvok **SearchBar**, ktorý po zviazaní s databázou umožňuje výpis jednotlivých položiek v nej na základe ich názvu. Tento prvok pracuje ako jednoduché vyhľadávanie, ktoré na základe napísaného názvu vyhľadá v spárovanej databáze príslušný prvok podľa jeho mena a následne zobrazí všetky informácie, ktoré sú priradené k ID, ku ktorému je priradený názov každého prvku v databáze. Na základe tohto ID je následne možné vypísať aj ďalšiu podstránku, každého prvku v hlavnej databáze, kde sú zobrazené podrobnejšie informácie.

Výzor vyhľadávania je na základe požiadaviek a prístupu modelu MVC vytvorený vo View, ako html prvok, ktorý neplní samotnú funkciu vyhľadávania, ale len výzor príslušného komponentu. Je definovaný ako prvok **TextBox**, čo umožňuje používateľom zadávať názvy kybernetických zločinov, ktoré majú byť vyhľadané v príslušnej databáze.

Typ tohto vstupu je definovaný ako **submit**, čo umožňuje posunúť informáciu ďalej a hodnota **Search** definuje, že daný používateľský vstup bude ďalej spracovávaný na vyhľadávanie.

```
@using (Html.BeginForm()) {
    <p>
        Find by name: @Html.TextBox("SearchString")
        <input type="submit" value="Search"/>
    </p>
}
```

Obrázok 7: Zápis SearchBar komponenty vo View

Vytvorenie funkcie vyhľadávania a spárovanie vytvoreného prvku je uskutočnené v kontrolére, ktorý definuje riadenie funkcií, ktoré majú byť vykonané pri využívaní prvku. Kontrolér využíva metódu **GetAllCrimes**, ktorý bola definovaná pri práci s databázou, a umožňuje vypísanie všetkých prvkov databázy na základe ID, ktoré prislúcha každému prvku. Kontrolér vyhľadávania pracuje na princípe toho, že vezme parameter databázy **Name** a používateľský vstup a vyhľadáva v databáze príslušné prvky na základe tohto vstupu. Pri nájdení zhody je požadovaný prvok, ktorý je zhodný so zadaním používateľa vypísaný. V prípade, že používateľ zadá vstup, ktorý sa v databáze nenachádza sa nevypíše žiaden prvok a stránka zostane prázdna.

```
var crimeAssetModels = _crimeAsset.GetAllCrimes();

if (!string.IsNullOrEmpty(searchString))
{
    crimeAssetModels = crimeAssetModels.Where(m => m.Name.Contains(searchString));
}
```

Obrázok 8: Ukážka zápisu kontroléra vyhľadávania

6.4 Grafické zobrazenie štatistických dát

Štatistické dáta je najvhodnejšie a najprehľadnejšie zobrazovať v grafickej podobe – v podobe grafu. Asp.net umožňuje vytvárať grafy v samotnej komponente staticky, avšak pre potreby tejto práce boli využité grafy Json, ktoré sú dynamicky načítavané. Json je všeobecne využívaný na načítavanie dát zo servera a ich následné zobrazenie vo webovej

aplikácií alebo stránke. V tomto prípade sú načítavanými dátami modely grafov, ktoré sú vytvorené ako objekty, ktoré je možné na základe parametrov zo servera a dát, ktoré sú definované v aplikácií načítať. Json ktorý obsahuje databázu rôznych typov grafov, ktoré je možné použiť. Tieto grafy je následne možné zviazať s databázou, čo je využité primárne v prípade vytvárania a spracovávania dynamických dát. Pre účely tejto aplikácie boli vytvorené statické dáta, ktoré nie sú definované v databáze, ale ako set dát, ktoré sú určené priamo v samotnej aplikácií.

V aplikácií sú spracovávané štatistické dáta z rôznych zdrojov, ktoré umožňujú sledovanie trendov kybernetickej kriminality za posledné roky, zobrazenie členských štátov Európskej únie na základe toho, do akej miery sú ohrozované z pohľadu uskutočnených kybernetických zločinov a iné relevantné informácie, ktoré umožňujú lepší prehľad v danej problematike.

Aj napriek tomu, že sú dáta statické, tj. nemenia sa dynamicky v čase, nakoľko použité dáta nie sú pre tento účel tvorené, umožňujú grafy Json určitú interaktivitu pri zobrazovaní grafov. Táto interaktivita spočíva primárne vo vypisovaní hodnôt, ktoré prislúchajú prvkom v grafe. Grafy sú v modely MVC vytvorené z príslušných komponentov zobrazenia grafu vo webovej aplikácií, komponenty Model, ktorá je použitá na nastavenie mien a kontroléru, ktorý zabezpečuje spárovanie grafického zobrazenia a definovaných setov dát.

V komponente View sa ako už bolo spomenuté nachádza definícia výzoru a popisu samotného grafu, ktorá je definovaná pomocou javascriptu. Zároveň je v tejto komponente určené aj dynamické načítavanie zobrazenia grafu zo serverového úložiska Json. Samotné dáta sú načítavané z komponenty Controller, kde sú aj definované. Na spárovanie setov dát z tejto komponenty je využité dynamické dátové úložisko **ViewBag**, ktoré umožňuje práve dynamické presúvanie dát medzi komponentami.

Pri definovaní grafov je použitý aj komponent Model, ktorý umožňuje definovať predpis celého grafického zobrazenia definovaním triedy **DataPoint**, ktorá je následne využívaná pre definovanie už konkrétnych statických dát v komponente Controller. Na základe tejto funkcie je možné poznamenať, že pri tvorbe grafov pracuje komponent Model podobne ako abstraktná trieda, nakoľko je určený na vytvorenie predpisu, ktorý je následne použitý pre ďalšie fungovanie.

```
99+ references
public class DataPoint
{
        96 references
        public DataPoint(string label, double y)
        {
            this.Label = label;
            this.Y = y;
        }

        [DataMember(Name = "label")]
        public string Label = "";

        [DataMember(Name = "y")]
        public Nullable<double> Y = null;
}
```

Obrázok 9: Ukážka komponentu model

Na nasledujúce ukážke je možné vidieť definovanie grafu, ktorý obsahuje jednu hodnotu na osi X a jednu os Y. Tento typ grafu je využívaný pre výhodnejšie sledovanie trendov kybernetickej kriminality za posledných niekoľko rokov v komponente Controller, kde je možné vidieť definovanie jednotlivých dátových setov (**DataPoint**), ktoré sú následne presúvané ako list do komponenty **ViewBag**, ktorá ich následne, ako už bolo spomenuté, sprostredkováva komponente View, ktorá ich následne zobrazí používateľovi vo webovej aplikácií.

```
},
data: [{
    type: "stackedBar",
    name: "Phishing",
    showInLegend: true,
    color: "#4978B1",
    yValueFormatString: "$#,##0M",
    dataPoints: @Html.Raw(ViewBag.DataPoints1)
},
{
    type: "stackedBar",
    name: "Finančná strata",
    showInLegend: true,
    color: "#7E9BC8",
    yValueFormatString: "$#,##0M",
    dataPoints: @Html.Raw(ViewBag.DataPoints2)
},
```

Obrázok 10: Definovanie grafu v komponente View

Okrem grafického zobrazenie jednej X-ovej osi a jednej osi Y bolo pre možnosti porovnávania jednotlivých dát využité aj zobrazenie dvoch osí Y k jednej osi X. Tento typ grafu je podobne definovaný ako už predchádzajúci spomenutý avšak pre definovanie jednotlivých dát využíva niekoľko dátových setov na základe dát, ktoré sú porovnávané.

7. ZÁVER

Problémy, ktoré vznikajú pri odhaľovaní kybernetickej kriminality už boli popísané viacerými zdrojmi a je možné povedať, že každý zdroj odhalil nový nedostatok. Cieľom tejto práce bolo vykonať prieskum v oblasti kybernetickej kriminality a naznačiť kritické problémy pri stíhaní tohto druhu kriminality.

Pri spätnom pohľade na históriu je možné vidieť, že kriminalita ako taká bola súčasťou spoločnosti už od veľmi dávnej doby a menil sa len jej rozsah, zameranie, spôsob páchania, alebo len samotná definícia toho, čo bolo považované za protiprávne. Dnes je situácia približne obdobná. Kriminalita je rozšírená aj v súčasnej globalizovanej spoločnosti a zmenil sa len jej rozsah a na základe technologických vymožeností boli vytvorené nové možnosti páchania protiprávneho konania, ako sú napríklad zločiny špecifické pre kybernetickú kriminalitu. Z morálneho hľadiska konanie v oblasti kybernetickej kriminality nemožno považovať za správne, ale z čisto praktického hľadiska je páchanie tohto druhu kriminality veľmi výhodné z dôvodu, že značné množstvo páchateľov tejto kriminality zostane nepotrestaných, a práve nedostatky odhaľovania a stíhania kyberkriminality sú hlavnou príčinou. Jedným z problémov je práve neexistencia spoločného a jednotného delenia kybernetických zločinov, pričom práve vytvorenie takéhoto delenia, ktoré by bolo všeobecne záväzné a aktualizované, odzrkadľujúce súčasné trendy v kybernetickej kriminalite, by vyriešilo najzávažnejšie problémy pri stíhaní kybernetickej kriminality akými sú napr. nedostatky jednotlivých právnych systémov, alebo nedostatočná medzinárodná spolupráca.

Teoretická časť práce pojednávala o kyberkriminalite ako súčasti kriminality, popisovala jej rozvoj a zmeny, ktoré reagovali na rozvoj technológií a snažila sa popísať nedostatky pri jej odhaľovaní, stíhaní a potrestaní. Cieľom praktickej časti bolo vytvoriť webovú aplikáciu, ktorá zobrazuje informácie o kybernetických zločinoch a štatistické údaje.

Okrem spomenutého existujú aj mnohé ďalšie aspekty kybernetickej kriminality, či už z pohľadu zložiek, ktoré ju majú odhaľovať a stíhať, alebo z pohľadu páchateľov, ktorých vynaliezavosť v súčasnom svete už nemá zábran. Pre rapídny rozvoj informačných technológií a teda aj kyberkriminality môžeme len predpokladať a obozretne odhadovať čo budúcnosť v tejto oblasti môže priniesť.

LITERATÚRA

[1] Microsoft [online], 2021 [cit. 2021-11-6]. Dostuné z: https://docs.microsoft.com/en-gb/aspnet/core/mvc/. *Overview of ASP.NET Core MVC*

[2] Microsoft, [online], 2021 [cit. 2021-11-6]. Dostuné z: https://dotnet.microsoft.com/learn/aspnet/what-is-aspnet. *What is ASP.NET?*

[3] Strahl, Rick., [online], 2005 [cit. 2021-11-6]. Dostupné z: https://www.codemag.com/article/0511061/A-Low-Level-Look-at-ASP.NET-Architecture. *A Low Level Look at ASP.NET Architecture*. CODE Magazine 6(6).

[4] ENISA, [online], 2015 [cit. 15.02.2022]. Dostuné z: https://www.enisa.europa.eu/publications/definition-of-cybersecurity. *Definitions of Cybersecurity*

[5] Cambridge dictionary, [online], 2022 [cit. 15.02.2022]. Dostuné z: https://dictionary.cambridge.org/dictionary/english/cyberspace. *Meaning of cyberspace in English*

[6] European Comission, [online], 2022 [cit. 15.02.2022]. Dostuné z: https://ec.europa.eu/home-affairs/cybercrime_en. *Cybercrime*

[7] Boettger L., [online], 2000 [cit. 16.02.2022]. Dostuné z: https://www.giac.org/paper/gsec/405/morris-worm-affected-computer-security-lessons-learned/100954. *The Morris Worm: How it Affected Computer Security and Lessons Learned by it*

[8] Kelty, C. [online], 2011 [cit. 16.02.2022]. Dostupné z: https://escholarship.org/uc/item/8t12q5bj. *The Morris Worm*, Limn, 1.

[9] Holt Thoma J., [online], 2017 [cit. 16.02.2022]. Dostuné z: https://books.google.sk/books?hl=en&lr=&id=0T8lDwAAQBAJ&oi=fnd&pg=PA105&dq=AIDS+Trojan+or+PC+Cyborg+Ransomware&ots=cYkehsTdJH&sig=tLZlQ63MpXMqWoBdIfAgR4sl6-Q&redir_esc=y#v=onepage&q=AIDS%20Trojan%20or%20PC%20Cyborg%20Ransomware&f=true. *Cybercrime Through an Interdisciplinary Lens*

[10] FBI, [online], 2022 [cit. 16.02.2022]. Dostuné z: https://www.fbi.gov/news/stories/melissa-virus-20th-anniversary-032519. *The Melissa Virus*

[11] Mohurle S., Patil M., [online], 2017 [cit. 17.02.2022]. Dostuné z: https://sbgsmedia.in/2018/05/10/2261f190e292ad93d6887198d7050dec.pdf. *A brief study of Wannacry Threat: Ransomware Attack 2017*, International Journal of Advanced Research in Computer Science Volume 8, No. 5, May-June 2017, ISSN No. 0976-5697

[12] Ghafur S., Kristensen S., Honeyford K., Martin G., Darzi A., Aylin P., [online], 2017 [cit. 25.02.2022]. Dostuné z: https://www.nature.com/articles/s41746-019-0161-6. *A retrospective impact analysis of the WannaCry cyberattack on the NHS*, npj Digital Magazine 2(98)

[13] Lesk M., [online], 2007 [cit. 30.02.2022]. Dostuné z: https://ieeexplore.ieee.org/abstract/document/4288051. *The New Front Line: Estonia under Cyberassault*, IEEE Security & Privacy 5(4) 76-79, ISSN: 9692366

[14] Europol, [online], 2020 [cit. 25.02.2022]. Dostuné z: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020.*Internet Organised Crime Threat Assessment (IOCTA) 2020*

[15] Europol, [online], 2017 [cit. 18.02.2022]. Dostuné z: https://www.europol.europa.eu/media-press/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation. *Andromeda botnet dismantled in international cyber operation*

[16] Europol, [online], 2021 [cit. 18.02.2022]. Dostuné z: https://www.europol.europa.eu/media-press/newsroom/news/27-arrested-in-successful-hit-against-atm-black-box-attacks. *27 arrested in successful hit against ATM Black Box attacks*

[17] Interpol, [online], 2020 [cit. 25.02.2022]. Dostuné z: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19. *INTERPOL report shows alarming rate of cyberattacks during COVID-19*

[18] Richardson R., North Max M., [online], 2017 [cit. 25.02.2022]. Dostuné z: https://digitalcommons.kennesaw.edu/facpubs/4276/. *Ransomware: Evolution, Mitigation and Prevention*, International Management Review, 13(1) 10-21

[19] Európska organizácia pre kybernetickú bezpečnosť, [online], 2020 [cit. 01.03.2022]. Dostuné z: https://ecs-org.eu/documents/publications/602a76674b32a.pdf. *Ecso barometer 2020:"cybersecurity in light of covid-19"*

[20] Rieck, K., Holz, T., Willems, C., Düssel, P., Laskov, P., [online], 2008 [cit. 18.03.2022]. Dostuné z: https://doi.org/10.1007/978-3-540-70542-0_6 *Learning and Classification of Malware Behavior*, Lecture Notes in Computer Science, vol 5137. Springer, Berlin, Heidelberg.

[21] Nazario J., [online], 2008 [cit. 05.03.2022]. Dostuné z: https://www.sciencedirect.com/science/article/abs/pii/S1353485808700862. *DDoS attack evolution*, Network Security, 2008(7) 7-10

[22] Walkowski D., [online], 2019 [cit. 05.03.2022]. Dostuné z: https://www.f5.com/labs/articles/education/what-is-the-cia-triad. *What Is the CIA Triad?*

[23] Samonas S., Coss D., [online], 2014 [cit. 05.03.2022]. Dostuné z: https://www.proso.com/dl/Samonas.pdf. *The cia strikes back: redefining confidentiality, integrity and availability in security*, Journal of Information Security, 10(3), ISSN: 1551-0123

[24] Europol, [online], 2016 [cit. 15.03.2022]. Dostuné z: https://www.europol.europa.eu/publications-events/publications/common-taxonomy-for-law-enforcement-and-csirts.*Common Taxonomy for Law Enforcement and CSIRTs*

[25] Europol, [online], 2020 [cit. 15.03.2022]. Dostuné z: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2017. *Internet Organised Crime Threat Assessment (IOCTA) 2017*

[26] NAI-FOVINO, I., NEISSE, R., HERNANDEZ-RAMOS, J. L., POLEMI, N., RUZZANTE, G.,FIGWER, M., LAZARI, A., [online], 2021 [cit. 15.03.2022]. Dostuné z: https://www.researchgate.net/profile/Jose-Hernandez-Ramos-2/publication/337784794_A_Proposal_for_a_European_Cybersecurity_Taxonomy/links/5dea3b404585159aa4661236/A-Proposal-for-a-European-Cybersecurity-Taxonomy.pdf. *A Proposal for a European Cybersecurity Taxonomy*, Publications Officeof the European Union, Luxembourg, ISBN: 978-92-76-11603-5

[27] ENISA, [online], 2016 [cit. 11.05.2022]. Dostuné z: https://www.enisa.europa.eu/publications/information-sharing-and-common-taxonomies-between-csirts-and-law-enforcement. *Information sharing and common taxonomies between CSIRTs and Law Enforcement*

[28] Calderoni F., [online], 2016 [cit. 11.05.2022]. Dostuné z: https://link.springer.com/article/10.1007/s10611-010-9261-6. *The European legal framework on cybercrime: striving for an effective implementation,* Crime, Law and Social Change 54

[29] Rada Európy, [online], 2001 [cit. 09.04.2022]. Dostuné z: https://rm.coe.int/1680081561. *Convention on Cybercrime*

[30] Európsky parlament, [online], 2013 [cit. 09.04.2022]. Dostuné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013L0040. *Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA*

[31] Abransky H., *Organized Crime*, Boston: Cengage Learning, 2016, 440 s. ISBN-10: 1305633717
[32] Buono L., [online], 2016 [cit. 17.03.2022]. Dostuné z: https://link.springer.com/article/10.1007/s12027-016-0432-5. *Fighting cybercrime between legal challenges and practical difficulties: EU and national approache*, ERA Forum, 17 343-353
[33] Europol, [online], 2022 [cit. 09.04.2022]. Dostuné z: https://www.europol.europa.eu/about-europol. *About Europol*
[34] Rozéen S., Kaunert C., Léonard S., [online], 2001 [cit. 09.04.2022]. Dostuné z: https://www.tandfonline.com/doi/abs/10.1080/15705854.2013.817808. *Is Europol a Comprehensive Policing Actor?* Perspectives on European Politics and Society 14(3), 372-287
[35] Europol, [online], 2021 [cit. 20.04.2022]. Dostuné z: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/euctf. *EUCTF*
[36] Europol, [online], 2022 [cit. 18.04.2022]. Dostuné z: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3. *European Cybercrime Centre - EC3*
[37] Reitamo T., Oerting T., Hunter M., [online], 2015 [cit. 15.04.2022]. Dostuné z:https://scholar.google.sk/scholar?q=reitano+2015+cybercrime&hl=sk&as_sdt=0&as_vis=1&oi=scholart. *Innovations in International Cooperation to Counter Cybercrime: The Joint Cybercrime Action Taskforce (J-CAT)* The European Review of Organised Crime 2(2), 142-154, ISSN: 2312-1653
[38] Cosman I., Mihai Cosmi-I., [online], 2020 [cit. 10.04.2022]. Dostuné z: https://bulletin.cepol.europa.eu/index.php/bulletin/article/view/489/357. *The Impact of COVID-19 on Cybercrime and Cyberthreats*
[39] Lewis J., [online], 2018 [cit. 12.04.2022]. Dostuné z: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf. *Economic Impact of Cybercrime-No Slowing Down*
[40] Kaspersky, [online], 2014 [cit. 15.04.2022]. Dostuné z: https://www.kaspersky.com/about/press-releases/2014_reality-of-rising-ddos-attacks-sees-european-businesses-take-action-to-reduce-financial-and-reputational-impact. *Reality of Rising DDoS Attacks Sees European Businesses Take Action to Reduce Financial and Reputational Impact*
[41] Riek M. a spol., [online], 2016 [cit. 12.04.2022]. Dostuné z: https://pure.tudelft.nl/ws/portalfiles/portal/28985021/WEIS_2016_paper_54_2.pdf. *Estimating the costs of consumer-facing cybercrime: A tailored instrument and representative data for six EU countries*
[42] Scroxton A., [online], 2021 [cit. 15.04.2022]. Dostuné z: https://www.computerweekly.com/news/252506646/Cost-of-ransomware-

attack-in-financial-sector-exceeds-2m. *Cost of ransomware attack in financial sector exceeds $2m*

[43] Doyle W., [online], 2021 [cit. 10.02.2022]. Dostuné z: https://github.com/wesdoyle/lightlib-lms. *Library management system*

ZOZNAM SKRATIEK

Skratky:

VPN	Virtuálna privátna sieť
OS	Operačný systém
ECS	Európska organizácia pre kyberbezpečnosť
EU	Európska únia
USA	Spojené štáty americké
NIST	Americký národný inštitút pre štandardy a technológie