NSZ ČR

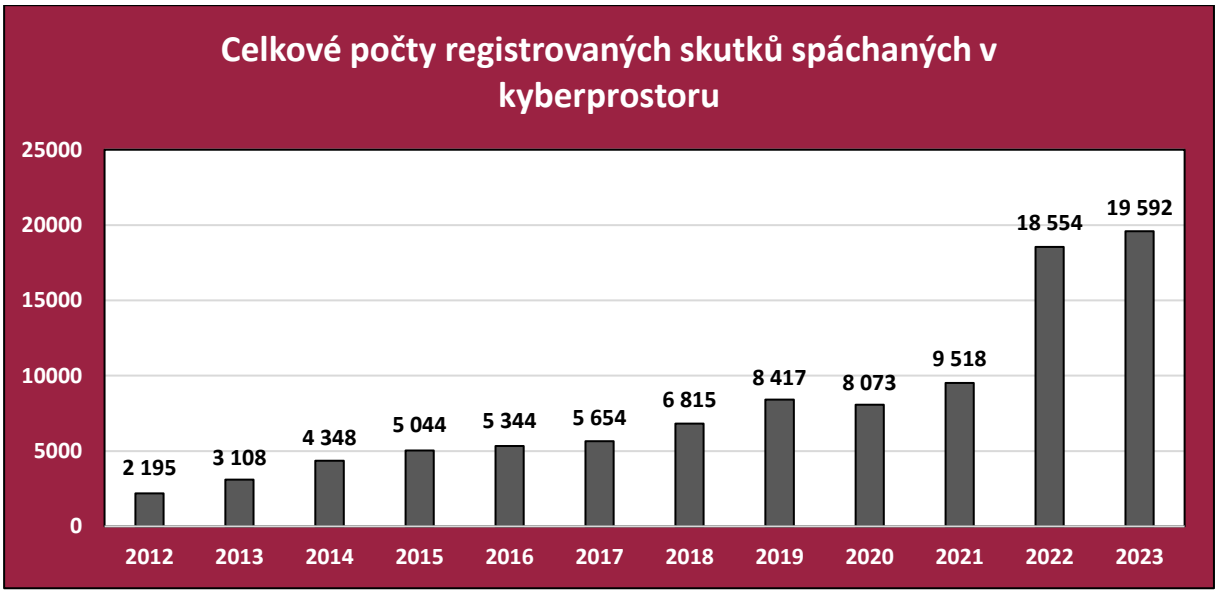
Zpráva o činnosti národního zpravodaje pro boj proti kybernetické kriminalitě, pro ochranu práv k nehmotným statkům a kybernetickou bezpečnost za rok 2023

Mgr. Tomáš Foldyna

V Brně dne 28. února 2024
1 SL 110/2024

Úvodem lze v obecné rovině konstatovat, že po velmi dynamickém růstu nápadu na úseku kybernetické kriminality a kriminality v kyberprostoru v přechozích letech bylo v roce 2023 zaznamenáno zmírnění dynamiky tohoto nárůstu, když v loňském roce došlo ke spáchání 19 592 trestných činů v kyberprostoru oproti 18 554 trestným činům v roce 2022.

Podíl na celkovém nápadu trestné činnosti v roce 2023 tak v případě kybernetické kriminality a kriminality páchané v kybernetickém prostoru překonal 10 %, což je prakticky stejný podíl, jako byl v loňském roce.



Tento výsledek lze přičíst několika zásadním faktorům:

1. V roce 2023 bylo možno poprvé zaznamenat účinnou preventivní kampaň ve veřejné sféře (sociální sítě, televize, rozhlas, tisk, maily atd.) současně realizovanou jak ze strany Policie ČR, bank, korporací, tak i ze strany NÚKIB. Tato kampaň varovala jednak před různými typy internetových podvodů, ale také před útoky na počítačové systémy typu ransomware. Zapojení influencerů pak významně zvýšilo okruh osob, na něž tato kampaň cílila.

2. Realizace několika „velkých“ trestních věcí se zahraničním přesahem, jež byly rovněž s úspěchem medializovány.

3. Efektivní průběh operace „OFENZIVA“ – cílené vyhledávání podvodných inzerátů na internetu a jejich „eliminace“. Tato kampaň necílila na případné oběti, ale je zaměřena přímo proti osobám pokoušejícím se páchat internetové podvody.

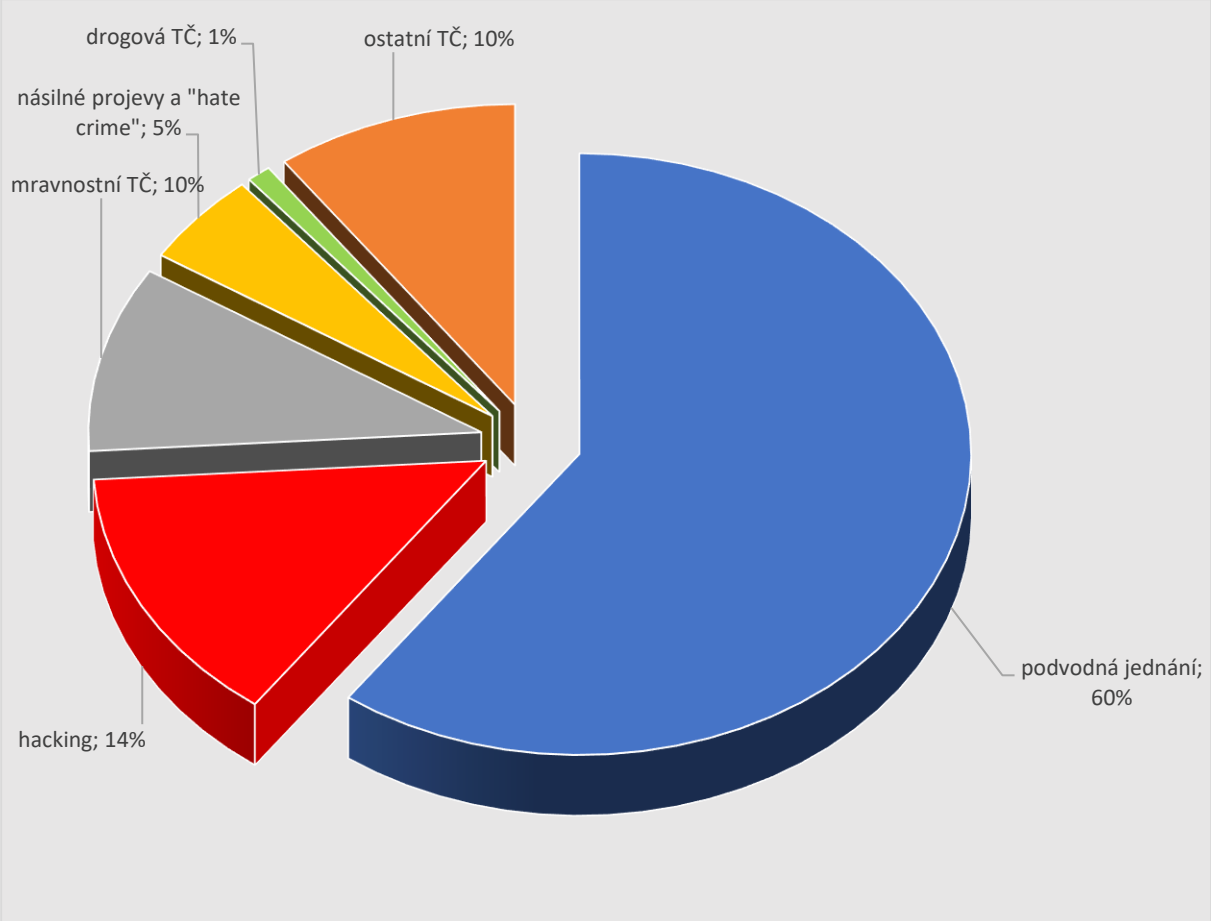
4. Zapojení bankovního sektoru, který se snaží odradit potencionální oběti podvodů od uposlechnutí pokynů pachatele, které vedou k uskutečnění finančních převodů ze svých účtů. Na tomto místě je potřeba vysoce ocenit spolupráci Policie ČR (ÚSKPV) s bankovní asociací a Českou národní bankou.

Události a trendy v oblasti kyberkriminality v roce 2023

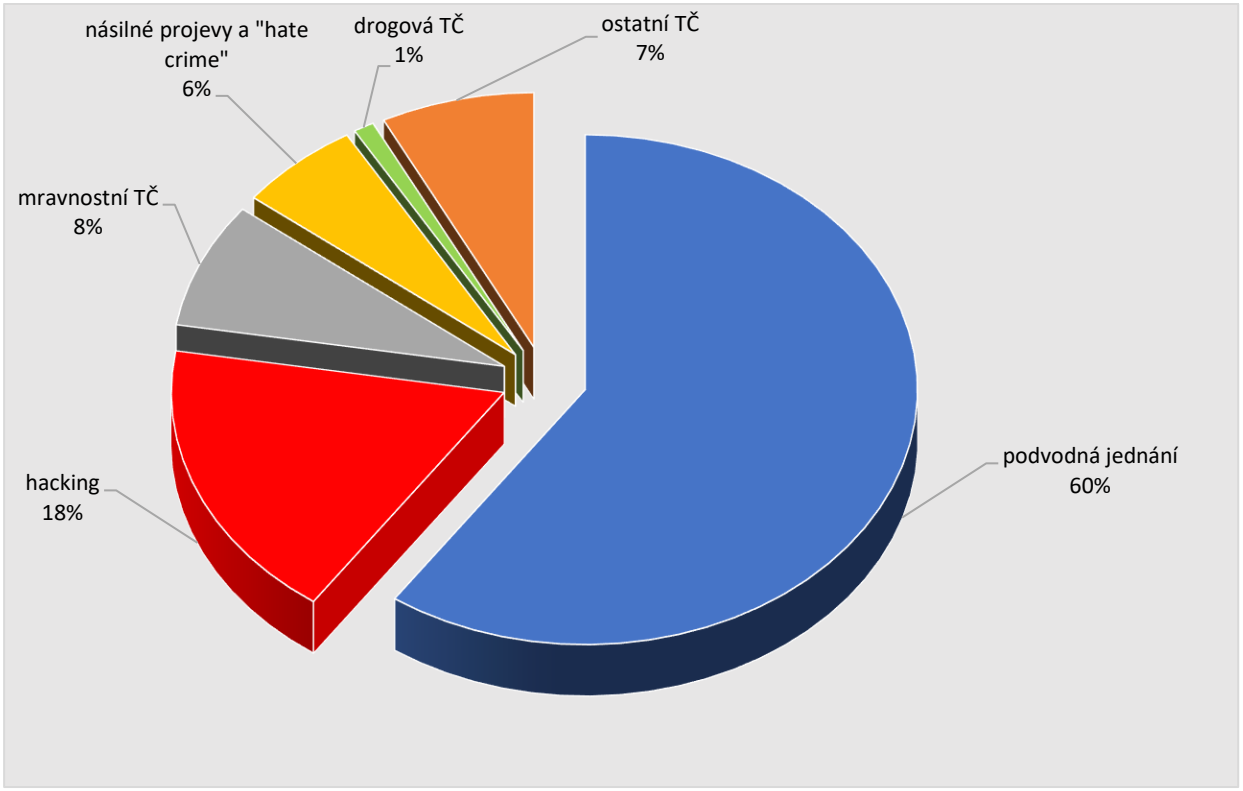
Jak už je výše uvedeno, došlo v roce 2023 ke zvýšení celkové kriminality spáchané v kyberprostoru (kyberkriminalita v širším i v užším slova smyslu) o cca 1 000 případů, což lze přičíst reakci jak orgánů činných v trestním řízení, tak také dalších státních nebo privátních aktérů, kteří dokázali zareagovat na alarmující tempo růstu tohoto typu kriminality v předchozích letech.

Následující grafy převzaté z údajů Policie ČR znázorňují skladbu trestné činnosti páchané v kyberprostoru v letech 2021, 2022 a 2023.

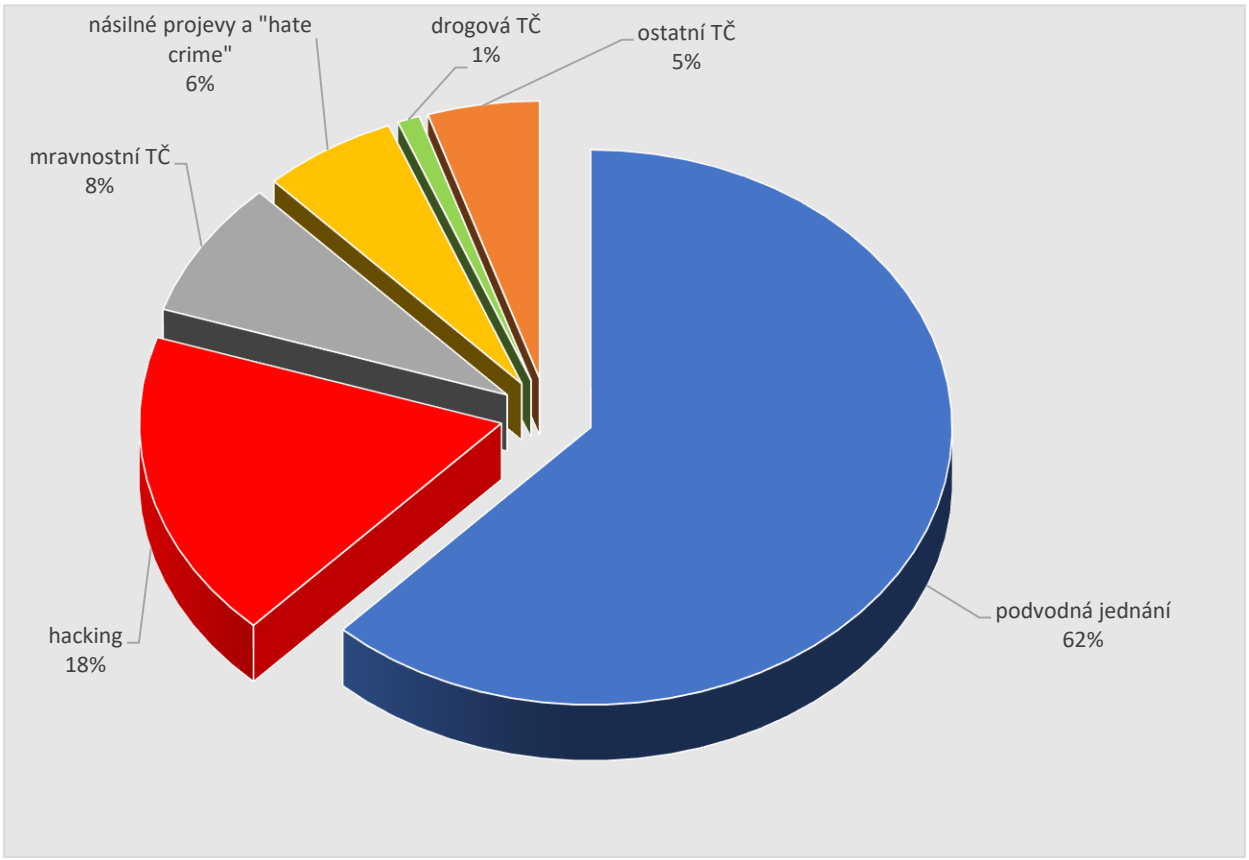
R. 2021



R. 2022


násilné projevy a "hate crime" 6%
drogová TČ 1%
ostatní TČ 7%
mravnostní TČ 8%
hacking 18%
podvodná jednání 60%

R. 2023


násilné projevy a "hate crime" 6%
drogová TČ 1%
ostatní TČ 5%
mravnostní TČ 8%
hacking 18%
podvodná jednání 62%

Jak je patrno z výše uvedených grafů, skladba trestné činnosti v kybernetickém prostoru se v posledních třech letech prakticky nemění či dochází pouze k nepatrným posunům mezi různými typy kriminality, takže nelze vysledovat jakékoli zásadní posuny v trendech v tomto segmentu trestné činnosti.

Nadále pokračovaly v loňském roce podvody typu „americký voják hledá přítelkyni v ČR“, kdy pachatel po navázání bližšího kontaktu a získání důvěry oběti (zpravidla ženy) začne po oběti žádat zasílání dalších a dalších finančních prostředků pod záminkou přestěhování věcí a převodu svých finančních prostředků do ČR, aby mohl za obětí přicestovat a žít s ní.

Druhým typem internetových podvodů, který v loňském roce zaznamenal prudký růst, je podvodná nabídka „výhodného“ obchodování s kryptoměnami, kdy pod záminkou nákupu kryptoměny jsou z oběti vylákány značné finanční prostředky.

Velmi časté jsou také podvodné reakce na inzertní nabídky prodeje zboží, kdy pachatel kontaktuje prodávajícího s nabídkou, že zboží uhradí převodem na účet prodávajícího a zboží poté odveze zásilková služba. Za tímto účelem se pak snaží pachatel vylákat z poškozeného přístupové údaje k jeho platební kartě, kterou následně zneužije a odčerpá finanční prostředky z účtu poškozeného.

Stejně tak v roce 2023 pokračovaly podvody založené na sociálním inženýrství, jejichž podstatou je snaha dostat oběť pod tlak, často pomocí fingovaných telefonátů „bankéře“ upozorňujícího na probíhající „útok“ na účet oběti, která je pak pod hrozbou tohoto nebezpečí přinucena, resp. přesvědčena ke sdělení svých přístupových údajů k účtu nebo k platebním prostředkům (platebním kartám) a následně pak dojde k odcizení veškerých finančních prostředků z účtu oběti.

Naproti tomu v roce 2023 nerostl počet ransomwarových útoků a zejména již nedocházelo k tak masivním ransomwarovým útokům jako v dřívějších letech. Nicméně tento typ kybernetické kriminality nadále ohrožuje počítačové systémy v celé Evropě a působí značné ekonomické škody. Proto je tomuto fenoménu věnována značná pozornost a pod vedením Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) ve spolupráci s Národní centrálou proti terorismu, extremismu a kybernetické kriminalitě (NCTEKK) byla založena pracovní skupina zaměřená na problematiku ransomwaru, jejíž činnosti se účastní rovněž státní zastupitelství.

Nadále platí v rámci ČR i v rámci celé Evropy, že kybernetické kriminalitě a kriminalitě v kybernetickém prostoru nahrává nízké právní i technické povědomí veřejnosti v kombinaci s poměrně omezenými schopnostmi rozpoznat, předcházet a bránit se útokům využívajícím informační technologie, stejně jako nedostatečná regulace, která se jak na národní, tak na celoevropské úrovni značně zpožďuje za dynamickým rozvojem informačních technologií. V tomto ohledu však lze poprvé vysledovat jisté zlepšení, k němuž vedou masivní preventivní kampaně státních orgánů i soukromých subjektů, ať už se jedná o banky nebo poskytovatele internetových služeb.

Stále více a více se tak ukazuje být problematickým současný nedostatečný právní rámec, který neukládá poskytovatelům povinnost registrovat údaje o využití služeb VPN, šifrování atd., což vede k tomu, že řada pachatelů závažných trestných činů zůstává skryta v anonymním prostředí internetu nebo darknetu.

Významná judikatura

V roce 2023 pokračoval Soudní dvůr Evropské unie (SDEU) ve svém odmítavém postoji ve vztahu k plošnému a nerozlišujícímu uchovávání provozních a lokalizačních údajů s výjimkou případů vážného ohrožení veřejné bezpečnosti (problematika data retention). V návaznosti na svá předchozí rozhodnutí (zejména rozsudek ve spojených věcech C-793/19 SpaceNet a C-794/19 Telekom Deutschland, ze dne 20. září 2022) vydal SDEU například **rozsudek ve věci C-162/22 Lietuvos Respublikos generalinė prokuratūra, ze dne 7. září 2023**, dle kterého musí být článek 15 odst. 1 směrnice o soukromí a elektronických komunikacích (2002/58/ES), ve spojení s články 7, 8 a 11, jakož i čl. 52 odst. 1 Listiny základních práv Evropské unie, vykládán v tom smyslu, že brání tomu, aby osobní údaje z elektronických komunikací, které byly poskytovateli služeb elektronických komunikací uchovávány na základě legislativního opatření přijatého podle tohoto ustanovení a následně na základě tohoto opatření zpřístupněny příslušným orgánům pro účely boje proti závažné trestné činnosti, mohly být použity při vyšetřování kárných provinění v souvislosti s korupcí.

Významným rozhodnutím stran SDEU byl také **rozsudek ve věci C-205/21 Ministerstvo na vatreshnite raboti, ze dne 26. ledna 2023**, dle kterého je systematické shromažďování biometrických a genetických údajů každého obviněného bez dalšího rozlišení za účelem jejich policejní registrace v rozporu s požadavkem na zajištění zvýšené ochrany v souvislosti se zpracováním citlivých osobních údajů.

Upozornit lze také na **rozsudek SDEU ve věci C-349/21 HYA a další, ze dne 16. února 2023**, dle kterého nemusí rozhodnutí povolující odposlech telefonních hovorů obsahovat individualizované odůvodnění. Povinnost odůvodnění totiž není porušena, pokud se rozhodnutí o povolení odposlechu zakládá na podrobné a propracované žádosti příslušného orgánu činného v trestním řízení a důvody povolení mohou být snadno a jednoznačně vyvozeny z přečtení žádosti ve vzájemném spojení s povolením.

Stran problematiky data retention byla významná rovněž rozhodovací činnost Evropského soudu pro lidská práva (ESLP). V rozsudku ve věci **Škoberne proti Slovinsku, č. 19920/20, ze dne 15. února 2024**, se ESLP přiklonil k argumentační linii SDEU ve vztahu k problematice data retention. Případ se týkal trestního řízení proti bývalému soudci, který byl v roce 2013 odsouzen za přijímání úplatků. Jeho odsouzení bylo z podstatné části založeno na provozních a lokalizačních údajích, které orgány činné v trestním řízení získaly pouze díky obligatornímu uchovávání těchto dat příslušnými subjekty. Ačkoli lze nyní ve Slovinsku uchovávat pouze telekomunikační údaje potřebné pro fakturační a obchodní účely, v době odsouzení byli poskytovatelé telekomunikačních služeb povinni uchovávat tyto údaje systematicky a bez rozdílu po dobu 14 měsíců (V České republice momentálně platí doba uchovávání po dobu 6 měsíců). ESLP rozhodl, že v daném případě došlo k porušení čl. 8 Úmluvy (právo na respektování soukromého a rodinného života), neboť takové uchovávání dat nezůstalo v mezích toho, co je v demokratické společnosti nezbytné. Podle soudu lze přisvědčit dosavadnímu názorovému postoji SDEU, že telekomunikační údaje nemohou být předmětem obecného a nerozlišujícího uchovávání za účelem boje proti závažné trestné činnosti.

Dalším významným případem byl **rozsudek ESLP ve věci Yüksel Yalçınkaya proti Turecku, č. 15669/20, ze dne 26. září 2023**, který se týkal odsouzení bývalého učitele za členství v ozbrojené teroristické organizaci, jejíž členové se měly v roce 2016 pokusit o státní převrat. Odsuzující rozsudek byl ze strany vnitrostátního soudu založen primárně na tom, že stěžovatel používal aplikaci pro šifrované zprávy s názvem "ByLock", která měla být podle názoru vnitrostátních soudů určena výhradně pro použití členy předmětné teroristické skupiny. Faktický obsah zpráv přitom nebyl zjištěn, dostačující bylo pouze používání aplikace ByLock. ESLP však takový postup shledal rozporný s čl. 7 Úmluvy, neboť představoval v podstatě automatickou presumpci viny založenou pouze na užití aplikace ByLock, což stěžovateli téměř znemožnilo zprostit se daných obvinění. ESLP rovněž zdůraznil, že z hlediska čl. 6 Úmluvy je důležité zachovat obviněnému možnost zpochybnění jednotlivých předložených důkazů, a to i v případě, kdy se jedná o elektronické důkazy. Důkazní materiál byl totiž v daném případě z velké části získán prostřednictvím činnosti zpravodajské služby, v důsledku čehož byla stěžovateli zamítnuta jeho žádost o předložení nezpracovaných údajů k nezávislému přezkoumání za účelem ověření jejich obsahu a integrity. ESLP proto dospěl k závěru, že neexistovaly dostatečné záruky, které by stěžovateli umožňovaly vést řádnou a účinnou obhajobu.

V rámci vnitrostátní judikatury lze poukázat na **usnesení Nejvyššího soudu ze dne 25. ledna 2023, sp. zn. 8 Tdo 1204/2022**, kde se Nejvyšší soud zabýval typem kybernetické kriminality známým jako „romance scam“. Odsouzený se seznámil s poškozenou prostřednictvím internetové seznamky, přičemž pod smyšlenou historkou, že je původem ze Španělska a v České republice pracuje jako medik a záchranář, vylákal od poškozené postupně přes sto tisíc korun (daný případ je mírně atypický tím, že se poškozená s odsouzeným skutečně potkala, přičemž k předávání peněz docházelo fyzicky). Nejvyšší soud rozhodl, že uvedení v omyl podle § 209 odst. 1 trestního zákoníku nemusí spočívat jen v jednorázovém jednání, kterým pachatel předstírá okolnosti, jež nejsou v souladu se skutečným stavem věci, ale může se skládat z dílčích, na sebe navazujících úkonů (typicky v podobě podání klamavých údajů), jimiž pachatel navodí u poškozeného pocit důvěry, přičemž podáním dalších nepravdivých informací zneužije této důvěry k tomu, aby poškozený provedl transakce ve prospěch obviněného na úkor svého majetku.

Zajímavé je také **usnesení Nejvyššího soudu ze dne 31. 5. 2023, sp. zn. 5 Tdo 1023/2022**, dle kterého nelze za odstranění nebezpečí ve smyslu § 20 odst. 3 písm. a) trestního zákoníku považovat dočasné znepřístupnění internetových stránek, prostřednictvím kterých pachatel uváděl v omyl jiné osoby, aby od nich vylákal peníze na nákup neexistujících dluhopisů v rozsahu způsobení škody velkého rozsahu. Takové jednání není důvodem zániku trestní odpovědnosti za přípravu zločinu podvodu podle § 20 odst. 1 a § 209 odst. 1, odst. 5 písm. a) trestního zákoníku.

Pro účely boje proti kybernetické kriminalitě lze poukázat také na **usnesení Nejvyššího soudu ze dne 24. března 2021, sp. zn. 7 Tdo 219/2021**, které, ač vydáno v roce 2021, bylo v roce 2023 publikováno ve sbírce soudních rozhodnutí [R 56/2022 tr.], a to s následující právní větou: Pokud pachatel s využitím omylu banky odčerpal peněžní prostředky z bankovního účtu, dopustil se tím trestného činu podvodu podle § 209 tr. zákoníku ke škodě banky (viz rozhodnutí pod č. 27/2014-II. Sb. rozh. tr.). To však neplatí bezvýjimečně, zejména nikoli v případě, že pachatel nezaměřil svůj útok (v řadě realizovaných kroků) jen na výběr finančních prostředků z účtu u banky, ale

především na podvodné získání možnosti disponovat s účtem na základě zmocnění vylákaného od majitele účtu. Za takové situace jsou jeho následné úkony (pokyny k převodům či výběrům), byť jsou jinak v rozporu s právem, formálně autorizovány oprávněnou osobou a poškozeným je majitel účtu, nikoli banka, která neměla možnost posoudit neoprávněnost dispozic s účtem.

Usnesení Nejvyššího soudu ze dne 31. ledna 2023, sp. zn. 4 Tdo 1133/2022, kde se Nejvyšší soud zabýval použitelností zvukového záznamu pořízeného a předloženého soukromou osobou, přičemž zde rozsáhle a přehledně rekapituloval dosavadní judikaturní závěry týkající se dané problematiky.

Zajímavé rozhodnutí představuje také **rozsudek Městského soudu v Praze ze dne 9. listopadu 2023, sp. zn. 10 A 99/2023**, dle kterého je obecně známou skutečností ve smyslu § 121 o.s.ř., že ChatGPT ve své verzi 3.5 není spolehlivým zdrojem faktických informací, a proto jeho odpověď na dotaz týkající se skutkových otázek není důkazním prostředkem způsobilým k prokázání skutkového stavu.

Legislativa

V loňském roce bylo zaznamenáno několik legislativních změn v oblasti kybernetické kriminality, a to jak na národní, tak i regionální úrovni.

V rámci Evropské unie nadále probíhají některé legislativní procesy, které započaly již v předchozích letech (např. Akt o umělé inteligenci, nařízení ePrivacy, nařízení CSAM apod.). Řada významných legislativních aktů však v roce 2023 byla přijata nebo vstoupila platnost. Patří mezi ně například:

Nařízení o vydávacím a uchovávacím příkazu

Nařízení Evropského parlamentu a Rady (EU) 2023/1543 ze dne 12. července 2023 o evropském vydávacím příkazu a evropském uchovávacím příkazu pro elektronické důkazy v trestním řízení a pro výkon trestu odnětí svobody po skončení trestního řízení přináší výrazné ulehčení přeshraničního přístupu k elektronickým důkazům. Předmětné nařízení umožňuje adresovat příkazy týkající se elektronických důkazů přímo poskytovatelům služeb v jiném členském státě, čímž se snižuje časová náročnost mezinárodní spolupráce a vzájemné právní pomoci.

Směrnice o právních zástupcích za účelem shromažďování elektronických důkazů

Směrnice Evropského parlamentu a Rady (EU) 2023/1544 ze dne 12. července 2023, kterou se stanoví harmonizovaná pravidla pro určování určených provozoven a jmenování zástupců za účelem shromažďování elektronických důkazů v trestním řízení, navazuje na nařízení o předávacích a uchovávacích příkazech. Cílem příslušné směrnice je stanovit povinnost poskytovatelům služeb, kteří nabízejí své služby v Evropské unii, určit alespoň v jednom členském státě právního zástupce příslušného k vyřizování obdržených žádostí podle předmětného nařízení.

Nařízení o digitálních službách (nařízení DSA)

Nařízení Evropského parlamentu a Rady (EU) 2022/2065 ze dne 19. října 2022 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (nařízení o digitálních službách) se vztahuje na zprostředkovatelské služby (srov. čl. 3 písm. g)

nařízení DSA) nabízené příjemcům, kteří mají místo usazení nebo se nacházejí v Evropské unii, a to bez ohledu na sídlo jednotlivých poskytovatelů. Problematickým z pohledu orgánů činných v trestním řízení je především čl. 10 odst. 5 předmětného nařízení, který ukládá poskytovatelům služeb povinnost vyrozumět uživatele služeb o sdělení informací, které se těchto uživatelů týkají, orgánům činným v trestním řízení. Do doby přijetí příslušných prováděcích předpisů bude nutné dbát na řádné plnění poučovací povinnosti vůči povinným subjektům – poskytovatelům zprostředkovatelských služeb tak, aby nedošlo k ohrožení či zmaření účelu trestního řízení jeho předčasným vyzrazením.

Nařízení MiCA

Nařízení Evropského parlamentu a Rady (EU) 2023/1114 ze dne 31. května 2023 o trzích kryptoaktiv a o změně nařízení (EU) č. 1093/2010 a (EU) č. 1095/2010 a směrnic 2013/36/EU a (EU) 2019/1937 zavádí první významnou a zároveň velmi rozsáhlou regulaci v oblasti obchodování s virtuálními měnami.

Směrnice NIS 2

Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2.0) přináší nové požadavky na bezpečnostní opatření a hlášení incidentů v oblasti kybernetické bezpečnosti u vybraných subjektů, dále zpřísnění sankcí za neplnění povinností a prohloubení spolupráce mezi členskými státy v oblasti kybernetické bezpečnosti. Obsah této směrnice musí členské státy implementovat do svých právních řádů nejpozději do 17. října 2024.

Stran národní legislativy je na místě upozornit na přijetí vyhlášky č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu, která společně s dřívějšími vyhláškami č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci a č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu reguluje využívání cloud computingu podle zákona o kybernetické bezpečnosti a podle zákona o informačních systémech veřejné správy. Uvedené vyhlášky mají za cíl zvýšit kybernetickou bezpečnost v souvislosti s využíváním cloudových služeb stran orgánů veřejné moci. Dále lze také v příštím roce očekávat vlivem přijetí směrnice NIS 2 výrazné změny v rámci zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Stejně tak by mělo vlivem nařízení DSA dojít k přijetí vnitrostátní legislativy, která by adaptovala požadavky tohoto nařízení do českého právního řádu, přičemž provedené změny by se měly dotknout též trestního řádu.

Na celosvětové úrovni pokračovala vyjednávání ve vztahu k připravované úmluvě OSN proti kybernetické kriminalitě, nicméně z důvodu přetrvávajících neshod dosud nedošlo k předložení finálního návrhu Valnému shromáždění OSN.

Vnitrostátní aktivity na úseku kybernetické kriminality

V roce 2023 pokračovalo státní zastupitelství v naplňování koncepce rozvoje schopností státního zastupitelství na úseku boje proti kybernetické kriminalitě a kriminalitě v kybernetickém prostoru, kterou schválil nejvyšší státní zástupce v roce 2022.

Zejména se plně realizuje specializace státních zástupců od okresní úrovně až po Nejvyšší státní zastupitelství na tento typ kriminality. Stejně tak pokračovaly aktivity směřující k znovuobnovení činnosti sítě specialistů státního zastupitelství v oblasti kybernetické kriminality, která uskutečnila celostátní setkání na podzim loňského roku.

Rovněž pokračovaly aktivity směřující ke zkvalitnění vzdělávání státních zástupců na úseku kybernetické kriminality. Ve spolupráci s Policií ČR se podařilo všem státním zástupcům, kteří mají přístup do ETŘ, zajistit přístup i do metodického webu ÚSKPV Policie ČR. Dále se podařilo, rovněž ve spolupráci s Policií ČR, sestavit katalog elektronických důkazů a procesních postupů jejich opatřování, který bude v nejbližší době publikován. Mimo to také probíhají práce na přípravě uceleného vzdělávacího programu pro státní zástupce a příslušníky Policie ČR.

V této souvislosti nelze pominout významný podíl státních zástupců na vzdělávacích akcích Justiční akademie ČR, ale také jejich účast na vzdělávacích akcích Justiční akademie SR. Vyzdvihnout je třeba rovněž spolupráci s Českou advokátní komorou na jejích vzdělávacích akcích. Již nyní se však státní zástupci coby lektoři aktivně podílejí na organizaci vzdělávacích akcí na téma kyberkriminality pořádaných Justiční akademií ČR.

V souvislosti s výše zmíněnými vzdělávacími akcemi je na místě výslovně vyzdvihnout sérii seminářů pořádaných ve spolupráci s americkou ambasádou v Praze, kdy byly státním zástupcům, soudcům a příslušníkům policie představeny prostřednictvím amerických kolegů cenné a praktické poznatky z praxe US orgánů při vyšetřování kybernetické a počítačové kriminality.

Za významnou rovněž považujeme soustavnou a úzkou spolupráci státního zastupitelství a Národního úřadu pro kybernetickou a informační bezpečnost, a to jak v rovině konzultací, tak v rovině účasti na vzdělávacích nebo popularizačních akcích pro odbornou, ale i laickou veřejnost.

Zahraniční aktivity na úseku kybernetické kriminality

Státní zastupitelství se spolu s Ministerstvem spravedlnosti ČR a Policií ČR v uplynulém roce výrazně podílelo na zajištění rozvojové spolupráce organizované Ministerstvem zahraničních věcí, když státní zástupci spolu s dalšími specialisty předávali zkušenosti z boje proti kybernetické kriminalitě svým kolegům ze Senegalu a z Thajska.

Státní zástupci se rovněž účastní dalších aktivit na mezinárodní úrovni, z nichž mezi nejvýznamnější v současné době patří vyjednávání zcela nové úmluvy proti kybernetické kriminalitě na půdě OSN.

Další významnou nadnárodní aktivitou, na níž se státní zástupci podílejí, je činnost Evropské sítě proti kybernetické kriminalitě, která funguje v rámci Eurojustu a která přispívá ke sdílení zkušeností z boje proti tomuto druhu kriminality nejen mezi jednotlivými státy EU, ale také mezi dalšími přidruženými státy.

Hlavní výzvy pro r. 2024

1) Za hlavní výzvu v roce 2024 považuji zlepšování stávajícího nedostatečného právního rámce pro boj s kyberkriminalitou.

2) Dále pokračovat ve vzdělávacích aktivitách pro policejní orgány a státní zástupce.

3) Udržení a další rozvoj aktivit na mezinárodní úrovni, které výrazně ovlivňují pozici ČR při vyjednávání o nadnárodních instrumentech boje proti kybernetické kriminalitě.

4) Postupně se připravovat na nástup nových technologií v oblasti kyberkriminality související s rozvojem umělé inteligence a deepfake.

5) Posílení lidských zdrojů v oblasti boje proti kybernetické kriminalitě.

Závěrem lze konstatovat, že rok 2023 je možné označit za rok, v němž byla problematice kybernetické kriminality věnována skutečně adekvátní pozornost ze strany státní moci i soukromého sektoru, což se projevilo zmírněním dynamiky růstu počtu nově zaznamenaných trestných činů. To je možno považovat za dobrou zprávu, která opravňuje k mírnému optimismu.