NSZ ČR

Zpráva o činnosti národního korespondenta pro boj proti kybernetické kriminalitě, pro ochranu práv k nehmotným statkům a kybernetickou bezpečnost za rok 2021

Mgr. Tomáš Foldyna

V Brně dne 9. února 2022
1 SPR 51/2022

I v roce 2021 pokračovaly trendy z předchozích let, navíc umocněné vlivem pandemie onemocnění covid 19, která vedla k rychlému a výraznému přesunutí značné části aktivit z reálného světa do kyberprostoru. Zejména je nutno poukázat na bezprecedentní rozvoj online komunikací v oblastech pracovních, ale zejména vzdělávacích, kdy zásadní část druhého pololetí školního roku 2020/2021 probíhalo vzdělávání na všech úrovních školství v online podobě. Stejně tak i pracovní setkávání a jednání se na jaře a na sklonku r. 2021 odehrávala v převážné míře formou online. Na rozdíl od r. 2020 však již zároveň došlo k návratu jednání probíhající i v prezenční formě. To se týkalo i vzdělávání organizovaného Justiční akademií. Je zjevné, že tento trend bude pokračovat a že kromě jednání, meetingů, seminářů atd. konaných v prezenční podobě bude pokračovat i konání těchto setkání formou hybridní či zcela online.

V souvislosti s uzavřením společnosti, omezenými možnostmi cestovat, provozovat sporty a koníčky došlo také k enormnímu nárůstu volnočasových aktivit provozovaných prostřednictvím sítí, a to ať už se jedná o sociální sítě, hraní her, streamování hudby a filmů atd.

Již tak dřívější dynamický rozvoj informačních technologií a jejich uvádění na trh v neustálých vylepšeních a obměnách (například využití šifrování jako standardu, včetně využití biometrických dat, bezdrátové šifrované přenosy mezi synchronizovanými zařízeními, masivní ukládání dat ve vzdálených úložištích, stále se zjednodušující možnosti využití kryptoměn, nové elektronické platební metody, atd.), byl v r. 2021 ještě výrazně akcelerován jako reakce na omezení způsobená pandemií covid 19.

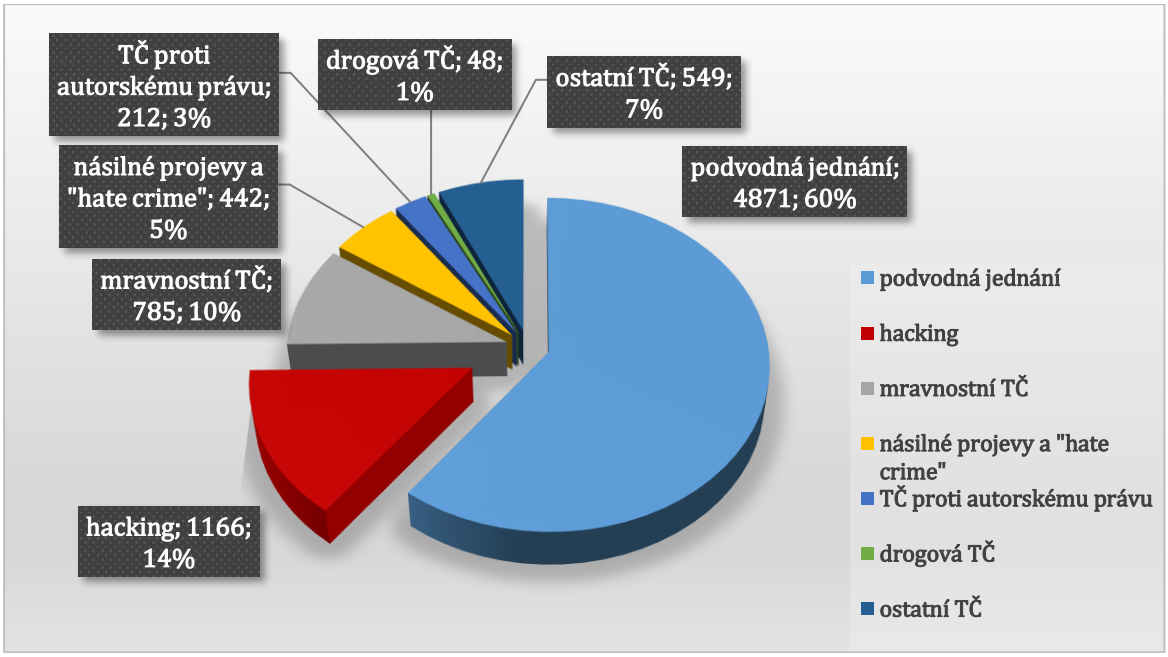
S tím vším pochopitelně souvisel také nárůst a další přesun páchání trestné činnosti z reálného prostoru do kyberprostoru, který ale podle dosavadních statistických údajů ani zdaleka neodpovídal procentuálnímu nárůstu využívání internetu a informačních technologií.

Z mezinárodních informací a zkušeností lze také dovodit, že v průběhu r. 2021 docházelo nadále, stejně jako v r. 2020, k masivnímu nárůstu porušování autorských práv na internetu, a to zejména streamováním filmů, hudby a počítačových her, což lze logicky dovodit ze situace, která v r. 2021 panovala a která vedla k nárůstu oficiálního streamování těchto produktů v řádech desítek procent. Tato trestná činnost však zůstává vysoce latentní a velmi těžko odhalitelná a dokladovatelná, takže se neprojevuje v oficiálních statistikách kybernetické kriminality, resp. kriminality páchané v kyberprostoru.

Události a trendy v oblasti kyberkriminality v roce 2020

Co se týká celkové kriminality spáchané v kyberprostoru (kyberkriminalita v širším i v užším slova smyslu) došlo v r. 2021 meziročně k nárůstu tohoto druhu kriminality o 17,9% na 9.518 skutků, což je alarmující fakt s ohledem na skutečnost, že jinak došlo v r. 2021 k výraznému poklesu nápadu celkové trestné činnosti (prakticky o 34.000 věcí).

Následující graf převzatý z prezentace Národní protidrogové centrály znázorňuje skladbu trestné činnosti páchané v kyberprostoru.



Výrazně v loňském roce rostla majetková trestná činnost páchaná prostřednictvím internetu. Výslovně je potřeba zmínit zejména 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 oběti přicestovat a žít s ní. Druhým typem internetových podvodů, který v loňském roce zaznamenal velký nárůst, je podvodná nabídka výhodného obchodování s kryptoměnami, kdy pod záminkou nákupu kryptoměny jsou od oběti vylákány značné finanční prostředky.

Trestné činy proti autorskému právu páchané v kyberprostoru pak činily 3% z celkového objemu, konkrétně pak 212 skutků.

Nadále také pokračovaly již „běžné“ formy podvodného jednání na internetu jako phishing či získávání přístupu k platebním kartám pod záminkou objednání a koupě zboží.

Strmý nárůst zaznamenala v r. 2021 kyberkriminalita v užším slova smyslu, tzv. „hacking“ (§ 230 trestního zákoníku), u níž došlo k nárůstu o 45% na celkovou hodnotu 1.691 skutků.

Naproti tomu v r. 2021 nerostl počet ransomwarových útokům a zejména již nedocházelo k tam masivním ransomwarovým útoků proti zdravotnickým zařízením, jako tomu bylo v r. 2020. Nelze ještě spolehlivě zhodnotit, zda tomu tak bylo v důsledku posílení kybernetické bezpečnosti informačních systému nemocnic, nebo tím, že se pachatelé zaměřili při útocích na jiné objekty. Každopádně však byly cíle

ransomwarových útoků spíše v oblasti veřejné správy (Parlament ČR, magistráty měst, další státní úřady).

V souvislosti s ransomwarovými kampaněmi je nutno zmínit, že touto problematikou se v současné době intenzivně zabývá také Eurojust a Evropská justiční síť proti kyberkriminalitě, která tomuto tématu věnovala podstatnou část svého 11. plenárního zasedání za aktivní účasti zástupce Nejvyššího státního zastupitelství.

Nejen v rámci ČR, ale v rámci celé Evropy nadále platí, že kybernetické kriminalitě a kriminalitě v kybernetickém prostoru nahrává nízké právní i technické vědomí 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. Zatímco šifrování, využívání kryptoměn, používání biometrie k ověřování přístupů a transakcí je již dnes standardem, stejně jako ukládání dat ve vzdálených úložištích, právní rámce jednotlivých zemí i EU jako celku si neví rady, jak tuto problematiku regulovat, takže orgány činné v trestním řízení narážejí na limity spočívající v nemožnosti opatření některých dat pro účely trestního řízení, neboť nemají právní nástroje, jak tyto data získat. Problémy při nastavení právního rámce regulace této oblasti jsou dány především konfliktem mezi potřebami orgánů činných v trestním řízení pronikat do soukromí uživatelů při objasňování těchto forem trestné činnosti a mírou zajištění ochrany základních práv a svobod těchto uživatelů, zvláště pak mírou ochrany jejich soukromí při užívání informačních technologií.

Stále 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

Za nejvýznamnější soudní rozhodnutí v oblasti kyberkriminality je možno v r. 2021 označit rozhodnutí Soudního dvora EU ze dne 2. března 2021 C-746/18, které se týká výkladu Směrnice Evropského parlamentu a Rady č. 2002/58/ES, o soukromí a elektronických komunikacích, ve znění Směrnice č. 2009/136/EC (dále jen „Směrnice“), a podmínek, za nichž mohou členské státy EU svým vnitrostátním právem upravit sběr a použití provozních a lokalizačních údajů elektronické komunikace. Podstatným z tohoto rozhodnutí je zejména závěr o tom, že provozní a lokalizační údaje soukromých osob nemohou být zpřístupněna orgánům veřejné moci na základě rozhodnutí či povolení státního zástupce, který vykonává ve věci dozor nebo který má zastupovat ve věci obžalobu v řízení před soudem, neboť nesplňuje kritéria nezávislosti. V tomto ohledu je vnitrostátní právní úprava ČR zcela souladná s právem EU, neboť provozní a lokalizační údaje pro účely trestního řízení lze ve smyslu § 88a odst. 1 trestního řádu zpřístupnit pouze na základě příkazu soudu.

Na citované rozhodnutí navazuje další rozhodnutí Soudního dvora EU ze dne 16. prosince 2021 C-724/19, v němž soud dospěl k názoru, že směrnice Evropského parlamentu a Rady 2014/41/EU ze dne 3. dubna 2014 o evropském vyšetřovacím příkazu v trestních věcech musí být vykládán v tom smyslu, že brání tomu, aby měl státní zástupce v přípravné fázi trestního řízení pravomoc k vydání evropského vyšetřovacího příkazu ve smyslu této směrnice, směřujícího k získání provozních a lokalizačních údajů v souvislosti s telekomunikačním provozem, jestliže u obdobného vnitrostátního případu přijetí vyšetřovacího úkonu, jehož účelem je přístup k takovým údajům, spadá do výlučné pravomoci soudce.

Dále v citovaném rozhodnutí soud naznal, že čl. 6 a čl. 9 odst. 1 a 3 směrnice 2014/41 musejí být vykládány v tom smyslu, že uznání evropského vyšetřovacího příkazu vydaného za účelem získání provozních a lokalizačních údajů v souvislosti s telekomunikačním provozem, provedené vykonávajícím orgánem, nemůže nahradit požadavky použitelné ve vydávajícím státě, pokud byl tento příkaz neoprávněně vydán státním zástupcem, zatímco u obdobného vnitrostátního případu přijetí vyšetřovacího úkonu, jehož účelem je získat takové údaje, spadá do výlučné pravomoci soudce.

Toto rozhodnutí Soudního dvora znamená výraznou komplikaci v praxi zajišťování elektronických důkazů v zahraničí, neboť podstatná část těchto důkazů se podle vnitrostátní právní úpravy ČR zajišťuje na základě příkazu soudu, což znamená, že ve všech takových případech by evropský vyšetřovací příkaz měl vydávat i v přípravném řízení soud, přestože zákon o mezinárodní justiční spolupráci takový postup nepředpokládá.

Rozhodnutí Nejvyššího soudu sp. Zn. 6 Tdo 148/2021

Dotčené předpisy

- §12 odst. 2 trestního zákoníku
- § 183 odst. 1 trestního zákoníku
- § 230 odst. 2 písm. a) trestního zákoníku

Jedná se o rozhodnutí zabývající se neoprávněným získáním přístupových údajů do cizí e-mailové schránky a zneužití této schránky zasláním zprávy pod identitou jejího oprávněného uživatele. Závěrem je, že takové jednání je trestné.

Rozhodnutí Nejvyššího soudu sp.zn. 7 Tdo 482/2021

Dotčené předpisy

- § 230 odst. 2 písm. a), odst. 3 písm. a) trestního zákoníku
- § 329 odst. 1 písm. a) trestního zákoníku

Věc zneužití přístupu do informačního systému Policie ČR a neoprávněných lustrací v tomto systému k soukromým účelům.

Rozhodnutí Nejvyššího soudu sp.zn. 7 Tdo 483/2021

Dotčené předpisy

- § 24 odst. 1 písm. b) trestního zákoníku
- § 230 odst. 2 písm. a), odst. 3 písm. a) trestního zákoníku
- § 329 odst. 1 písm. a) trestního zákoníku

Věc účastenství na předchozí trestní věci zneužití přístupu do informačního systému Policie ČR a neoprávněných lustrací v tomto systému k soukromým účelům, ve formě návodu ke spáchání tohoto trestného činu.

Legislativa

V průběhu r. 2021 nadále pokračovaly rekodifikační práce na novém trestním řádu, které se ve značné míře zabývaly právě přípravou části týkající se operativně pátracích prostředků a zajišťovacích institutů, které se dotýkají právě i zajišťování elektronických důkazů. Tyto práce byly ve 2. polovině r. 2021 ukončeny a materiál byl předložen k projednání rekodifikační komisi.

Zákonem č. 150/2021 Sb. byl novelizován zákon č. 289/2005 Sb., o Vojenském zpravodajství, v tom směru, že Vojenskému zpravodajství je svěřeno zajišťování cílené detekce kybernetických útků a hrozeb majících původ v zahraničí a směřujících proti důležitým zájmům státu, identifikace a vyhodnocování takových útoků a hrozeb, jakož i přijímání opatření k jejich odvracení.

Nadále také pokračovaly legislativní práce na evropské úrovni týkající se zejména nové směrnice k data retention.

Rovněž tak bylo zahájeno vyjednávání na půdě OSN ohledně zcela nové úmluvy proti kybernetické kriminalitě, které však nijak výrazně nepokročily v důsledku pandemie onemocnění covid 19.

Hlavní výzvy pro r. 2022

1) Za hlavní výzvu v roce 2022 považuji co možná nejúčinnější využití stávajícího, nedostatečného, právního rámce pro boj s kyberkriminalitou.
2) S ohledem na setrvalý růst trestné činnosti páchané v kyberprostoru se jako vhodné jeví vybudování samostatného centrálního pracoviště na úrovni celorepublikového útvaru Policie České republiky, který by zastřešoval objasňování kyberkriminality na území republiky a nahradil současnou sekci kyberkriminality Národní centrály proti organizovanému zločinu. Jako nezbytné se jeví investice do materiálního vybavení i lidských zdrojů, které by měly tomuto narůstajícímu nebezpečí čelit.

3) Stejně tak je nutno zaměřit pozornost na vybudování moderního právního rámce, který umožní účinně se s riziky kyberkriminality vypořádat za současného zajištění ochrany základních práv a svobod.
4) Posílení lidských zdrojů v oblasti boje proti kybernetické kriminalitě zejména v rovině soustavného vzdělávání.

Závěrem je potřeba také upozornit, že v r. 2021 narůstal počet incidentů, které se jeví jako útoky, za nimiž stojí cizí státní moc.

Z výše uvedeného je zřejmé, že obraně před kybernetickými útoky jak jednotlivců, tak i státních aktérů je nutno do budoucna věnovat stále větší pozornost a investovat jak do materiálového vybavení, tak hlavně do lidských zdrojů, které by měly tomuto narůstajícímu nebezpečí čelit. K tomu je také nezbytné, aby v následujícím období obnovila co nejrychleji po uklidnění současné pandemické situace činnost síť specializovaných státních zástupců na tuto problematiku. Stejně tak je nutno zaměřit pozornost na vybudování moderního právního rámce, který umožní účinně se s těmito riziky vypořádat za současného zajištění ochrany základních práv a svobod v míře obvyklé v demokratickém právním státě.