NSZ ČR

Zpráva o činnosti národního korespondenta pro boj proti kybernetické kriminalitě, pro ochranu práv k nehmotným statkům a kybernetickou bezpečnost za rok 2020

Mgr. Tomáš Foldyna

V Brně dne 11. února 2021
3 SE 101/2021

Úvodem lze v obecné rovině konstatovat, že i v roce 2020 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 podstatnou část roku probíhalo vzdělávání na všech úrovních školství v online podobě. Stejně tak i pracovní setkávání a jednání se od vypuknutí pandemie na jaře 2020 začala odehrávat v převážné míře formou online.

V souvislosti s uzavřením společnosti, nemožností 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. 2020 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. 2020 docházelo 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. 2020 panovala a která vedla k nárůstu oficiálního streamování těchto produktů až o cca 50%. 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 týče kyberkriminality v užším slova smyslu, došlo sice v absolutních číslech k poklesu počtu stíhaných trestných činů neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 trestního zákoníku a opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat podle § 231 trestního zákoníku, když oproti celkem 332 trestným činům v r. 2019 (z toho 15 podle § 231 trestního zákoníku) bylo v r. 2020 stíháno celkově 308 těchto trestných činů (z toho 10 podle § 231 trestního zákoníku). Avšak současně se v r. 2020 rozvíjel nový a poměrně masivní trend kybernetických (ransomwarových) útoků proti zdravotnickým zařízením. Dle předběžných informací NÚKIB řešil GovCERT nejvíce incidentů primárně v oblasti státní správy a zdravotnického sektoru, u něhož počet incidentů meziročně stoupnul o 267 %. Oproti roku 2019 vzrostl i počet incidentů

hlášených jednotlivými obcemi. U kybernetických útoků na nemocnice se jedná zejména o tyto případy:

- **FN Brno** – probíhá prověřování,
- **FN Ostrava** – probíhá prověřování,
- **FN Motol** – věc odložena, jednalo se o neúspěšný pokus o průnik do informačního systému,
- **Krajská nemocnice Karlovy Vary** – věc odložena, nebylo prokázáno, že by došlo k útoku,
- **Psychiatrická léčebna Kosmonosy** – věc odložena, nepodařilo se zjistit pachatele,
- **Nemocnice Benešov** – věc odložena, nepodařilo se zjistit pachatele,
- **Oblastní nemocnice Kladno** – probíhá prověřování.

Nejvýznamnějším a nejzávažnějším incidentem bylo v březnu 2020 zašifrování systémů Fakultní nemocnice Brno ransomwarem, které vyústilo ve významné omezení provozu nemocnice na třech lokalitách a škody v řádu desítek milionů korun.

Závažnost těchto útoků je výrazným způsobem zvyšována tím, že k útokům na zdravotnická zařízení docházelo v době, kdy celý zdravotní systém ČR byl vystaven enormnímu tlaku a jeho kapacity byly maximálně vytíženy.

Z informací NÚKIB rovněž vyplývá, že v roce 2020 byly původcem více než třetiny incidentů škodlivé kódy, přičemž téměř v polovině z nich šlo o ransomware. Další téměř třetina incidentů vyústila v nedostupnost služeb, systémů nebo webových portálů. V polovině z těchto případů šlo o následek DDoS útoků a ve zbytku šlo o pochybení lidského faktoru nebo techniky. Útočníci v roce 2020 využívali v podvodných e-mailech (phishing), cílených spear-phishingových a ransomwarových kampaních tématu pandemie COVID-19, aby zvýšili úspěšnost svých útoků. V posledních dvou letech se zároveň změnil charakter ransomwarových kampaní, kdy sice klesl počet technicky jednodušších plošných útoků, ale přibylo útoků lépe cílených a sofistikovaných.

V souvislosti s ransomwarovými kampaněmi nadále platí, že kybernetické kriminalitě a kriminalitě v kybernetickém prostoru nahrává nízké právní 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 tato 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 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

Za nejvýznamnější soudní rozhodnutí je možno v r. 2020 v oblasti kyberkriminality lze označit rozhodnutí Soudního dvora EU ze dne 6. 10. 2020, sp. zn. C 623/17, 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. Soudní dvůr EU zde označuje za nepřípustné zejména to, aby členské státy prostřednictvím vnitrostátní legislativy ignorovaly Směrnici a požadovaly po poskytovatelích služeb elektronické komunikace, zcela všeobecný, časově neomezený, neurčitý a soudně nepřezkoumatelný sběr a předávání provozních a lokalizačních údajů bezpečnostním orgánům členského státu, s odůvodněním, že se jedná o otázku vnitřní bezpečnosti, která právu EU nepodléhá. Soud klade provozní a lokalizační údaje prakticky na roveň obsahu zprávy. Nic z toho však není pro Českou republiku nové a zásadní, neboť se nejedná o právní názor nový, nýbrž pouze zpřesňující dřívější rozhodnutí Soudního dvora EU např. ve věci Tele2 Sverige AB, v souvislosti s nímž již Ústavní soud ve svém nálezu ze dne 14. 5. 2019 sp. zn. Pl. ÚS 45/17 ve věci návrhu na zrušení § 97 odst. 3 a 4 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, § 88a trestního řádu, § 68 odst. 2 a § 71 písm. a) zákona č. 273/2008 Sb., o Policii České republiky, a vyhlášky č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů, konstatoval, že česká právní úprava se evropskému standardu nevymyká. Lze tedy oprávněně a odůvodněně předpokládat, že ani na základě aktuálního rozhodnutí Soudního dvora EU ze dne 6. 10. 2020 nebude nutno domácí legislativu, upravující problematiku data retention, měnit.

Rozhodnutí Nejvyššího soudu sp. zn. 7 Tdo 584/2020
https://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/D716BD2FCB0AE98EC12585C70018854D?openDocument&Highlight=0,null,

Dotčené předpisy

- § 265i odst. 1 písm. e) trestního řádu
- § 353 odst. 1 trestního zákoníku
- § 182 odst. 2 písm. a) trestního zákoníku
- § 230 odst. 2 písm. a), odst. 3 písm. a) trestního zákoníku

Jedná se o rozhodnutí zabývající se trestnou činností spočívající v neoprávněné instalaci sledovacího softwaru do mobilu poškozené. Závěrem je, že takové jednání je trestné.

Rozhodnutí Nejvyššího soudu sp. zn. 7 Tdo 484/2020
https://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/49DE8928E3957290C12585B00019007F?openDocument&Highlight=0,null

Dotčené předpisy
- § 265i odst. 1 písm. b) trestního řádu
- § 209 odst. 1,5 písm. a) trestního zákoníku
- § 230 odst. 2 písm. c), odst. 3 písm. a), odst. 5 písm. a), b) trestního zákoníku

Věc zneužití přístupu do informačního systému krajského úřadu úředníkem a převádění finančních prostředků na soukromý účet.

Rozhodnutí Nejvyššího soudu sp. zn. 7 Tdo 1134/2020
https://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/DE79A4AEC8C6A6C9C1258670001DED27?openDocument&Highlight=0,null

Dotčené předpisy
- § 230 odst. 1 trestního zákoníku

Věc se týká neoprávněné změny hesel k e-mailu a facebookovému účtu poškozené. Nejvyšší soud považuje za přiléhavé přirovnání uvedené státní zástupkyní ve vyjádření k dovolání, že profil na Facebooku je v podstatě virtuální prostor a má podobnou povahu jako „obydlí“, jehož „dveře“ tvoří počítačový systém, či jiný nosič informací, přičemž „klíčem“ k těmto „dveřím“ je bezpečnostní opatření, jimiž je lze odemknout. Trestní zákon při ochraně ústavou zaručeného práva na soukromí sankcionuje jakýkoli neoprávněný vstup do obydlí, a to i za pomoci shodného klíče, aniž by pachatel musel dveře do domu prolamovat násilím. Obdobně je tedy nutno postihovat případy, kdy pachatel prolomí „dveře“ do virtuálního prostoru například za pomoci hesla, které znal z dřívější doby, či za pomoci telefonního čísla, na který jsou tyto soukromé účty navázány. Rozhodující je – obdobně jako u porušování domovní svobody – že v okamžiku, kdy pachatel tohoto způsobu narušení soukromí využívá, ví, že do toho důvěrného prostoru vstupuje neoprávněně, a je s tímto následkem přinejmenším srozuměn. Za překonání „bezpečnostního opatření“ ve smyslu § 230 odst. 1 trestního zákoníku je proto možno považovat i využití duplikátu telefonní SIM karty, na kterou jsou tyto soukromé účty vázány, s jejímž využitím lze do důvěrného prostoru vstupovat přímo, nebo za pomoci nově vygenerovaných hesel.

Rozhodnutí Nejvyššího soudu sp. zn. 8 Tdo 647/2020 a sp. zn. 7 Tdo 865/2020
https://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/809C1E569EC878CCC1258601003A96AC?openDocument&Highlight=0,null

https://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/FE39D131F810A61FC12585FB002F0C54?openDocument&Highlight=0,null,

Dotčené předpisy:

- § 158d odst. 2 trestního řádu
- § 158d odst. 3 trestního řádu
- § 158d odst. 10 trestního řádu

Jedná se o významná rozhodnutí Nejvyššího soudu zabývající se použitelností záznamů ze sledování osob a věcí povoleného ve smyslu § 158d odst. 3 trestního řádu soudcem. Rozhodnutí uzavírají, že záznamy se sledování osob a věcí jsou v těchto případech použitelné za splnění zákonných podmínek i v jiné trestní věci, než v níž byly povoleny a pořízeny.

Legislativa

Na počátku roku 2020 došlo ke schválení zákona č. 12/2020 Sb., o právu na digitální služby, jenž stanoví právo fyzických a právnických osob na poskytování digitálních služeb ze strany orgánů veřejné moci a vůči těmto provádět digitální úkony. Tímto zákonem došlo k novelizaci celé řady zákonů veřejného práva, mimo jiné také zákona č. 181/2014 Sb., o kybernetické bezpečnosti, zákona č. 106/1999 Sb., o svobodném přístupu k informacím, a řady jiných zákonů, jimiž je povinna se řídit i soustava státního zastupitelství při výkonu své působnosti.

V reakci na probíhající epidemii covid-19 a na proběhnuvší kybernetické útoky ve zdravotnickém sektoru došlo k úpravě znění vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby ve vztahu k odvětví zdravotnictví. Účelem této úpravy bylo zařazení většího počtu nemocnic mezi provozovatele základní služby. Novela je účinná od 1. ledna 2021.

V srpnu 2020 vstoupila v účinnost novelizace zákona č. 365/2000 Sb., o informačních systémech veřejné správy, která upravuje využívání cloud computingu orgány veřejné správy. Uvedená úprava zavádí pravidla pro ověření poskytovatelů a služeb cloud computingu. V této souvislosti vyvstává určité riziko opatřování digitálních důkazů z cloudových úložišť orgánů veřejné správy umístěných mimo území ČR.

Co se týče interních právních předpisů, tak v roce 2020 došlo na úseku kybernetické kriminality k zásadní změně, a to rozdělení problematiky kybernetické kriminality. Novelizací pokynu policejního prezidenta č.103/2013 došlo k ustanovení pojmu kybernetická kriminalita a ostatní kriminalita páchaná v kyberprostoru a následně došlo ke stanovení úkolů policejních orgánů v nově definovaných problematikách.

V návaznosti na rozhodnutí Soudního dvora EU je nutno znovu připomenout, že i přes potvrzený soulad české právní úpravy problematiky uchovávání provozních a lokalizačních údajů s evropským právem přetrvává vnitrostátní roztříštěnost v interpretační a aplikační praxi tohoto právního institutu, způsobená ustanovením § 136 odst. 20 zákona č. 127/2005 Sb., který stanoví, že interpretační pravidlo, podle něhož, pokud jiný právní předpis hovoří o údajích o telekomunikačním provozu, rozumí se tím provozní a lokalizační údaje podle zákona o elektronických komunikacích. Stále více a více elektronické komunikace v dnešním světě však

probíhá mimo právní rámec tohoto zákona, a proto je nutno postupovat při opatřování údajů o telekomunikačním provozu pomocí analogie, což není šťastné řešení. De lege ferenda tak bude nutno věnovat pozornost i vyřešení této problematiky tak, aby došlo k definování provozních a lokalizačních údajů elektronické komunikace bez ohledu na to, kterým právním předpisem se řídí tzv. „operátor“ služby.

Co se týká připravovaných legislativních změn, tak v průběhu r. 2020 pokračovaly legislativní práce na novém trestním řádu, jehož součástí by měla být i speciální právní úprava opatřování elektronických důkazů, zejména pak právní úprava tzv. online prohlídky či sledování osob a věcí prostřednictvím elektronických systémů. K vyjasnění problematiky opatřování elektronických důkazů pokračovala ve své činnosti také pracovní skupina zřízená Nejvyšším státním zastupitelstvím. Činnost této pracovní skupiny však byla značně zpomalena opatřením souvisejícím s pandemií onemocnění covid-19. Přesto se však podařilo shromáždit veškeré podstatné podkladové materiály, na jejichž základě je možné provést analýzu současného stavu.

Již v současné době je však jisté, že pro účinný boj proti kybernetické kriminalitě, a to zejména proti kyberkriminalitě v užším slova smyslu, bude nezbytné změnit nejen trestní řád, ale zejména zákony upravující prostředí internetu a povinnosti poskytovatelů služeb v této oblasti.

Závěrem je potřeba také upozornit, že v r. 2020 narůstal počet incidentů, které se jeví jako útoky, za nimiž stojí cizí státní moc. Není úkolem státního zastupitelství, aby určovalo, zda a který státní aktér stojí za tím kterým incidentem, nicméně z medializovaných věcí lze upozornit např. na pokračující kybernetický útok na kybernetickou infrastrukturu Ministerstva zahraničních věcí ČR. Vyskytla se však také řada dalších podobných útoků, u nichž je zřejmé, že za nimi s největší pravděpodobností mohou stát cizí státní aktéři.

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.