Ing. Josef Bernátek
České vysoké učení technické v Praze
Fakulta biomedicínského inženýrství

Analýza vývoje kriminality související s neoprávněnými přístupy do počítačových systémů v České republice za období 2010–2018

Úvod

Počítačové systémy každým rokem více prostupují do našich každodenních aktivit a ovlivňují nás tak v běžném způsobu života. Mnohdy si dopady jejich výpadku nebo kompromitace ani nedokážeme představit. Nejedná se pouze o neoprávněné přístupy do soukromých e-mailových schránek nebo účtů na sociálních sítích, ale i neoprávněné přístupy do řídících a kontrolních systémů distribuce elektřiny nebo vody. Neoprávněný přístup do internetového bankovnictví a následný neoprávněný příkaz k úhradě ze strany útočníka může mít finanční dopady pro fyzickou i právnickou osobu. Uveřejnění citlivých fotografií z cloudového úložiště dat nebo kompromitující konverzace s milenkou na sociální síti může mít dopad na rodinné vztahy, případně důvěryhodnost u zaměstnavatele. Zveřejnění nebo změna dat v registrech obyvatel může představovat poškození chráněných zájmů a reputace státu v mezinárodním měřítku. Neoprávněný přístup do počítačového systému prvku kritické informační infrastruktury ze strany teroristické organizace může vyústit ve způsobení škod velkého rozsahu, ale i značných ztrát na životech. Uvedeným výčtem několika typů neoprávněných přístupů do počítačových systémů a jejich možných následků je zřejmý nepoměr způsobených dopadů. V každém z těchto příkladů by se však zjednodušeně řečeno mj. jednalo o protiprávní jednání, spočívající v neoprávněném přístupu do počítačového systému.

Z výše uvedených důvodů je patrná nutnost nejen konat preventivní opatření pro předcházení neoprávněných přístupů do počítačových systémů, ale i případná protiprávní jednání objasnit a potrestat jejich pachatele. Vzhledem ke zdánlivé absenci způsobené škody se mnohdy jedná o kriminalitu latentní. Vysokou latenci této trestné činnosti lze předpokládat i s ohledem na nízké právní povědomí o tom, co je v kyberprostoru trestné. Pro kvalifikované hodnocení vývoje kriminality související s neoprávněnými přístupy do počítačových systémů v České republice byl autorem zvolen sběr statistických dat Policie České republiky (dále jen „Policie ČR“) za období 2010-2018. Následně byly pro analýzu relevantních dat o kriminalitě zvoleny vybrané statistické metody, mezi které lze zařadit výpočet elementárních charakteristik časových řad i volbu odpovídající trendové funkce pro predikci očekávaného vývoje. Autorem byla na počátku stanovena hypotéza, předpokládající zvýšení počtu Policií ČR registrovaných trestných činů, v souvislosti s neoprávněnými přístupy do počítačových systémů na konci sledovaného období ve srovnání s jeho počátkem o 300 %.

Teoretická východiska

Kybernetický prostor, představující digitální prostředí, které umožňuje vznik, zpracování a výměnu informací je dostupný téměř každému, nejen k využití, ale i zneužití.[1] Zneužití překračující hranice legality jsou ve zvýšené míře odhalována a kvalifikována jako trestná.[2] Zahraniční legislativa považuje obvykle za trestné, protiprávní jednání se znaky uvedenými v příslušné trestně právní úpravě.[3] Jinak tomu není, ani v českém právním řádu, kdy zákon č. 40/2009 Sb., trestní zákoník (dále jen „trestní zákoník“) považuje za trestné jednání nebo opomenutí, které vykazuje v zákoně uvedené znaky.[4] V případě definice kybernetického trestného činu panují nejen na mezinárodní úrovni značné rozdíly. Lze se setkat s restriktivními přístupy definujícími kybernetickou trestnou činnost, pouze jako technicky sofistikované trestněprávní jednání v kyberprostoru. V České republice je pojem kybernetické kriminality pojat šířeji, kdy zahrnuje mnohdy i skutky z obecné a hospodářské trestné činnosti, u kterých byly jako prostředek k jejich páchání užity informační nebo komunikační technologie. Dle definice Policie ČR trestný čin spáchaný v prostředí informačních nebo komunikačních technologií, včetně počítačových sítí, kdy uvedené prostředí je předmětem útoku nebo je výrazně využito, jako prostředku k jeho spáchání, je kybernetickým trestným činem.[5] Z této definice vyplývá, že za kyber-kriminalitu Policie ČR považuje nejen neoprávněné přístupy do počítačových systémů, ale i šíření dětské pornografie po internetu.

Statistické metody lze v kriminologii aplikovat pro kvalifikovaný popis kvantitativních dat o kriminalitě.[6] Pro jejich relevantní aplikaci a následnou interpretaci jsou nezbytná zdrojová statistická data o trestné činnosti, která je možno získat primárně z několika následujících kategorií. Počet trestných činů spáchaných na určitém území, za stanovené období, označujeme jako rozsah kriminality. Rozsah kriminality je vyjádřen v absolutních hodnotách. Pro hodnocení kriminality s ohledem na demografické vlivy a případné statistické porovnání území s odlišným počtem obyvatel je vhodnější vycházet z úrovně (indexu) kriminality. Index kriminality vyjadřuje relativní velikost výskytu trestné činnosti na 10 tis. nebo 100 tis. obyvatel. Žádný z výše uvedených ukazatelů neposkytuje ucelené informace o počtu trestné činnosti, spáchané obyvateli s trvalým bydlištěm v hodnocené oblasti, což platí zejména u kyberkriminality, jako mnohdy distančního deliktu.[7] Znalost těchto dat ovšem umožní

[1] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.
[2] ADLER, Freda, Gerhard O. W. MUELLER a William S. LAUFER. Criminology. Eight Edition. New York, NY: McGraw-Hill, [2013]. ISBN 978-0078026423.
[3] HAGAN, Frank E. Introduction to criminology: theories, methods, and criminal behavior. Ninth edition. Los Angeles: SAGE, [2017]. ISBN 978-1483389172
[4] Zákon trestní zákoník. In: Sbírka zákonů. Praha: Tiskárna Ministerstva vnitra, p. o., 2009, ročník 2009, částka 11, číslo 40.
[5] Kyberkriminalita. Policie České republiky [online]. Praha [cit. 2019-03-02]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx.
[6] GAU, Jacinta M. *Statistics for criminology and criminal justice*. Third edition. Los Angeles: SAGE, [2019]. ISBN 978-1506391786.
[7] GŘIVNA, Tomáš; SCHEINOST, Miroslav; ZOUBKOVÁ, Ivana a kol. *Kriminologie*. 4. vyd. Praha: Wolters Kluwer, a. s., 2014. ISBN 978-80-7478-614-3.

nejen lepší představu o počtu spáchaných trestných činů na stanoveném území za hodnocené období, ale i predikci jeho předpokládaného vývoje. Dispozice informacemi o očekávaném vývoji kriminality může zainteresovaným subjektům nejen usnadnit personální plánování, ale i přípravu cílených preventivních opatření. Mezi statistické ukazatele nelze na závěr opomenout strukturu kriminality, jež poskytuje informace o podílu jednotlivých druhů trestné činnosti, věku a pohlaví pachatelů, míře recidivy, objasněnosti apod.[1]

Mezi nejčastěji užívané zdroje informací o registrované kriminalitě lze zařadit kriminální statistiky orgánů činných v trestním řízení. Jedná se o statistiky zpracovávané policejními orgány, státními zastupitelstvími a soudy. Nejúplnější a nejpřesnější obraz o rozsahu kriminality poskytují statistiky Policie ČR, jelikož jsou svým obsahem nejblíže k dokonanému jednání. Obsahují tak informace o veškeré registrované trestné činnosti, bez ohledu na skutečnost, zda byla prověřovaná jednání objasněna. Ani tyto statistiky ovšem neposkytují údaj o celkovém počtu trestné činnosti, jelikož neobsahují kriminalitu latentní. Zkreslení nastává rovněž v důsledku legislativních změn a chyb při statistickém vykazování. Jeden skutek je evidován jako jeden trestný čin i v případě pokračujících trestných činů nebo souběhu trestných činů, u kterých je evidován pouze ten nejzávažnější. Policií ČR jsou evidovány i skutky u nichž je v průběhu trestního řízení zjištěno, že se nejedná o trestná jednání. Jedná se například o trestní řízení ukončená, v souladu s trestním řádem, odložením věci pro neprokázání trestnosti prověřovaného jednání, případně odevzdáním věci k projednání příslušnému orgánu, např. v případě přestupků nebo jiných správních deliktů. Statistiky Policie ČR rovněž obsahují informace o recidivě a počtu objasněných trestných činů, tedy u kterých byl policejním orgánem zjištěn jejich pachatel. Dále obsahují informace o výši způsobené škody, zajištěných výnosů z trestné činnosti, počtu vyšetřovaných osob, jejich pohlaví, věku a státní příslušnosti. V policejních statistikách se užívá pro označení evidované trestné činnosti takticko-statistická klasifikace (dále jen „TSK“). TSK ne vždy koreluje s označením trestných činů uvedených v trestním zákoníku, umožňuje však získat podrobnější informace o struktuře kriminality.[2]

Budapešťská úmluva o kyberkriminalitě[3] z roku 2001 kyberkriminalitu dělí na kriminalitu spojenou s integritou informačních systémů a dat, jako je neoprávněný přístup k počítačovému systému a nosiči informací; obsahem, jako je šíření sexuálního nebo násilného obsahu a porušování autorských práv; počítači, jako nástroje pro páchání tradiční trestné činnosti.[4] Policie ČR eviduje kybernetickou kriminalitu, označovanou v minulosti jako informační kriminalitu, jako samostatnou oblast kriminality od roku 2011. Rozděluje ji na podvodná jednání, hacking, mravnostní

[1] VÁLKOVÁ, Helena a Josef KUCHTA. *Základy kriminologie a trestní politiky*. 2. vyd. Praha: C. H. Beck, 2012. Beckovy mezioborové učebnice. ISBN 978-80-7400-429-2.
[2] GŘIVNA, Tomáš; SCHEINOST, Miroslav; ZOUBKOVÁ, Ivana a kol. *Kriminologie.* 4. vyd. Praha: Wolters Kluwer, a. s., 2014. ISBN 978-80-7478-614-3.
[3] Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě. In: Sbírka zákonu. Praha: Tiskárna Ministerstva vnitra, p. o., 2013, ročník 2013, částka 56, číslo 104
[4] ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer ČR, 2017. ISBN 978-80-7552-759-2.

delikty, autorskoprávní delikty, násilné projevy včetně hate crime a ostatní.[1] Veřejnosti však nejsou dostupná kritéria, na základě kterých Policie ČR kyberkriminalitu do těchto kategorií zařazuje. Lze se tedy pouze domnívat, že pod hackingem jsou evidovány i neoprávněné přístupy do počítačových systémů.

Statistická analýza

Policie ČR eviduje neoprávněné přístupy do počítačových systémů kvalifikované dle ust. §§ 230, 231 a 232 tr. zákoníku pod agregovanou kategorií TSK 865 „Poškození a zneužití záznamu na nosiči informací „§§ 230, 231, 232“. Na základě uveřejněných dat uvedených v tabulce č. 1 vyplývá, že v období 2010-2018 bylo v České republice registrováno celkem 4.402 skutků kvalifikovaných v rámci kategorie TSK 865, kdy v průměru se ročně jednalo o 489 skutků s objasněností 27,39 % a způsobenou škodou 101.463.000 Kč.

Tab. 1 Vývoj registrovaných skutků, objasněnosti a výše škod TSK 865

Rok	Registrováno	Objasněno	Index reg. skutků	Škody v tis. Kč
2010	101	29,70 %	0,10	0
2011	134	40,30 %	0,13	0
2012	178	25,28 %	0,17	0
2013	301	25,25 %	0,29	595
2014	669	28,70 %	0,64	15.936
2015	707	20,37 %	0,67	12.463
2016	635	24,72 %	0,60	471.070
2017	784	26,28 %	0,74	394.871
2018	893	25,87 %	0,84	18.231

Zdroj: Statistické přehledy kriminality Policie ČR

V případě dat o celkové kriminalitě za hodnocené období, uvedených v tabulce č. 2, bylo Policií ČR registrováno celkem 2.409.616 skutků, kdy v průměru se ročně jednalo o 267 735 skutků s objasněností 42,89 % a způsobenou škodou 25 558 662 000,- Kč. Při komparaci statistických dat o registrované kriminalitě kategorie TSK 865 se statistickými daty o celkové registrované kriminalitě, se za hodnocené období v případě kategorie TSK 865 jedná o podíl 0,18 % na registrované kriminalitě, 0,11 % na objasněné kriminalitě a 0,40 % na způsobených škodách. V případě kategorie TSK 865, dosahovala průměrná výše škody na skutek 207 443,- Kč, tedy 217 % průměrné výše škody na skutek u celkové kriminality, u které dosahovala „pouhých“ 95 462,- Kč.

Tab. 2 Vývoj registrovaných skutků, objasněnosti a výše škod celkovou kriminalitou

Rok	Registrováno	Objasněno	Index reg. skutků	Škody v tis. Kč
2010	313 387	37,55 %	297,97	24 103 863
2011	317 177	38,54 %	302,17	23 951 057
2012	304 528	39,46 %	289,77	34 214 712

[1] Kyberkriminalita. Policie České republiky [online]. Praha [cit. 2019-03-02]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx.

2013	325 366	39,70 %	309,56	29 054 421
2014	288 660	43,73 %	274,27	28 696 739
2015	24 628	45,29 %	234,88	26 898 577
2016	218 162	46,61 %	206,49	24 790 150
2017	202 303	46,90 %	191,04	20 289 012
2018	192 405	48,23 %	181,69	18 029 429

Zdroj: Statistické přehledy kriminality Policie ČR

Pro detailnější popis vývoje registrovaných skutků kategorie TSK 865, jak je patrno z tabulky č. 3, byly stanoveny elementární charakteristiky časové řady. V případě indexu registrovaných skutků kategorie TSK 865 ($\mathbf{y_i}$), se jedná o počet registrovaných skutků na 10.000 obyvatel. Pro výpočet indexů byla statistická data o počtu obyvatel převzata z veřejně dostupných ročenek Českého statistického úřadu. V případě roku 2018 byla využita data o počtu obyvatel za rok 2017, z důvodu nedostupnosti dat. První absolutní diference, charakterizující absolutní přírůstek nebo úbytek zkoumaného ukazatele v určitém období, proti období bezprostředně předcházejícímu ($\mathbf{d_{1i}}$), dosáhla nejvyšší hodnoty v roce 2014. V daném roce došlo ke zvýšení indexu registrovaných trestných činů kategorie TSK 865, ve srovnání s rokem 2013 o 35 %. Druhá absolutní diference, charakterizující absolutní zrychlení, resp. zpomalení vývoje ve zkoumané časové řadě ($\mathbf{d_{2i}}$), dosáhla nejsignifikantnější hodnoty v roce 2015. Jednalo se o hodnotu -0,31, z čehož vyplývá největší snížení přírůstku indexu registrované kriminality kategorie TSK 865 za hodnocené období, oproti předchozímu roku o 31 %. Koeficient růstu, charakterizující relativní postupnou rychlost změn hodnot v časové řadě ($\mathbf{k_i}$), dosáhl za sledované období největší hodnoty v roce 2014, kdy došlo ke zvýšení indexu registrované kriminality kategorie TSK 865 na 222 % hodnoty předchozího roku. Relativní přírůstek, charakterizující rovněž postupnou rychlost změn hodnot v časové řadě ($\mathbf{r_i}$), dosáhl nejvyšší hodnoty rovněž v roce 2014 jako koeficient růstu, kdy došlo ke zvýšení indexu registrované kriminality kategorie TSK 865 o 122 % oproti předchozímu roku. Bazický index ($\mathbf{y_i / y_0}$) vyjadřuje celkovou změnu indexu TSK 865 na konci sledovaného období, ve srovnání s jeho počátkem, kdy došlo ke zvýšení o 878 %. Průměrný koeficient růstu dosáhl hodnoty 1,3120, tedy ročně docházelo k nárůstu indexu hodnocené trestné činnosti v průměru o 31,20 %.

Tab. 3 Elementární charakteristiky časové řady registrovaných skutků TSK 865

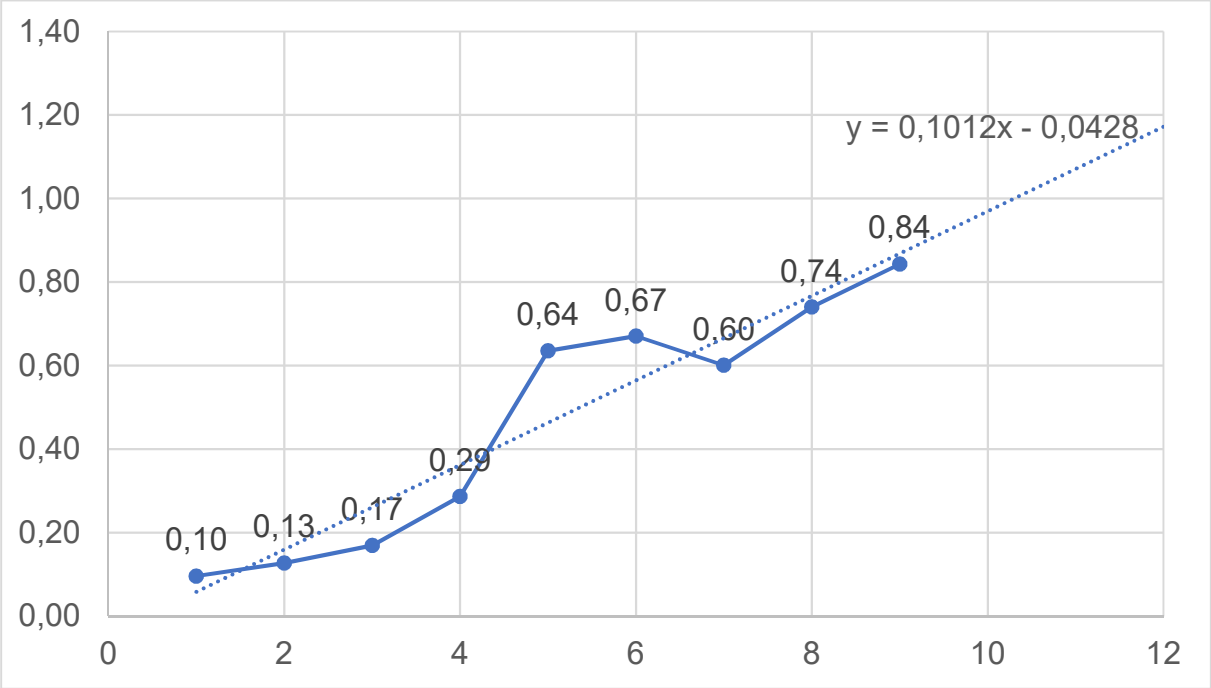
Rok	y_i	d_{1i}	d_{2i}	k_i	r_i	y_i / y_0
2010	0,10	-	-	-	-	-
2011	0,13	0,03	-	1,3293	0,3293	1,3293
2012	0,17	0,04	0,01	1,3268	0,3268	1,7637
2013	0,29	0,12	0,08	1,6908	0,6908	2,9820
2014	0,64	0,35	0,23	2,2196	1,2196	6,6190
2015	0,67	0,03	-0,31	1,0550	0,0550	6,9829
2016	0,60	-0,07	-0,10	0,8963	-0,1037	6,2585
2017	0,74	0,14	0,21	1,2318	0,2318	7,7094
2018	0,84	0,10	-0,04	1,1390	0,1390	8,7812

Zdroj: Statistické přehledy kriminality Policie ČR

Pro predikci vývoje registrovaných skutků kategorie TSK 865, na období let 2019–2021, byla autorem zvolena lineární trendová funkce ve tvaru $y = a + bt_i$. Parametry trendové funkce byly odhadnuty metodou nejmenších čtverců následovně, „a=-0,0428“, „b=0,1012“. Aplikací parametrů do rovnice lineárního trendu, byla stanovena prognóza vývoje indexu registrovaných skutků kategorie TSK 865 pro rok 2019 ve výši 0,9696, rok 2020 ve výši 1,0708 a rok 2021 ve výši 1,1721. Pro vyhodnocení vhodnosti zvoleného typu regresní funkce, byly vypočteny indexy determinace, korelace a střední absolutní procentuální chyba odhadu. Index determinace, sloužící k syntetickému popisu stupně shody modelu s empirickými údaji, dosáhl hodnoty 0,907. Index korelace, jako odmocnina indexu determinace, dosáhl hodnoty 0,952. Jelikož se tyto indexy blíží 1, zvolená funkce poměrně dobře popisuje časovou řadu. Střední absolutní procentuální chyba odhadu dosáhla hodnoty 22,78. Pokud by zůstal počet obyvatel České republiky v následujících letech konstantní, došlo by k nárůstu počtu registrovaných skutků kategorie TSK 865 v roce 2019 na 1.027, v roce 2020 na 1.134 a v roce 2021 na 1.241 za rok.

Vhodnost zvolené lineární trendové funkce byla ověřena rovněž aplikací časové řady v modelu polynomického trendu 2. řádu, kdy bylo dosaženo obdobných výsledků u indexu determinace s hodnotou 0,911 a indexu korelace s hodnotou 0,955, avšak vyšší střední absolutní procentuální chyby odhadu 25,89 %. Časová řada byla dále aplikována v modelu exponenciálního trendu, kdy rovněž nebylo dosaženo uspokojivých hodnot pro využití v rámci predikce na následující období. Pro danou časovou řadu byl tedy autorem v případě lineárního trendu zvolen relativně vhodný model, na základě kterého lze očekávat kvalifikovaný odhad budoucího vývoje registrované kriminality kategorie TSK 865 v České republice, jak je patrno z grafu č. 1.

Graf 1 Deskripce indexu registrované kriminality TSK 865 lineárním trendem



Zdroj: Statistické přehledy kriminality Policie ČR

V případě porovnání statistických dat registrované kriminality kategorie TSK 865 jednotlivých územně samosprávných celků za období 2010-2018, jak je uvedeno v tabulce č. 4, jsou zřejmé signifikantní rozdíly mezi jednotlivými kraji. Pro výpočet indexů registrované kriminality byly rovněž jako v případě republikového srovnání využity statistické ročenky Českého statistického úřadu. Pro rok 2018 bylo vycházeno z dat za rok 2017, z důvodu nedostupnosti statistických dat o počtu obyvatel za rok 2018. V případě výše indexu registrované kriminality dominuje hlavní město Praha, ve kterém bylo za sledované období v průměru ročně registrováno 1,58 skutků na 10 000 obyvatel. Následuje Liberecký kraj s průměrnou hodnotou 0,59 skutků, až po Karlovarský kraj, kde bylo registrováno v průměru pouze 0,17 skutků na 10 000 obyvatel. Nejúspěšnější v odhalování pachatelů trestné činnosti kategorie TSK 865 byly policejní orgány Jihočeského kraje, s průměrnou objasněností 40,06 %. Nejméně se policejním orgánům dařilo objasňovat skutky kategorie TSK 865 ve Středočeském kraji, kde byl odhalen pachatel pouze u 15 % registrovaných skutků. Dynamika vývoje počtu registrovaných skutků kategorie TSK 865 byla v téměř všech krajích blízká celorepublikovému průměru, kdy se jednalo v případě koeficientu růstu o interval 1,51 registrovaných trestných činů kategorie TSK 865 v případě Plzeňského kraje až po 1,21 v případě Královéhradeckého kraje.

Tab. 4 Průměr indexu registrovaných skutků, objasněnosti a koeficientů růstu TSK 865 za období 2010-2018

Územní celek	Index reg. skutků	Objasněno	Koeficient růstu
Hl. m. Praha	1,58	22,05 %	1,28
Liberecký	0,59	20,90 %	1,26
Olomoucký	0,55	32,42 %	1,31
Jihomoravský	0,50	33,51 %	1,37
Vysočina	0,48	32,29 %	1,27
Moravskoslezský	0,42	24,42 %	1,23
Zlínský	0,41	25,65 %	1,25
Jihočeský	0,39	40,06 %	1,36
Ústecký	0,38	25,42 %	1,40
Středočeský	0,35	15,83 %	1,44
Plzeňský	0,34	28,64 %	1,51
Královéhradecký	0,31	26,13 %	1,21
Pardubický	0,27	31,01 %	1,50
Karlovarský	0,17	36,08 %	1,22

Zdroj: Statistické přehledy kriminality Policie ČR

V případě statistických dat vyšších územně samosprávných celků, se jednalo o nevýznamné výše hodnot, kdy kupříkladu v Karlovarském kraji nebyl za rok 2010 jako v jediném kraji registrován ani jeden skutek klasifikovaný dle kategorie TSK 865. Vzhledem k nízkému počtu dat, by tudíž podrobnější analýza elementárních charakteristik dílčích časových řad, ani predikce jejich vývoje neměla relevantní vypovídací hodnotu.

Prevence a návrhy na zefektivnění vyšetřování

Komplexní výčet návrhů opatření na prevenci a zefektivnění vyšetřování by mohl být tématem celé publikace. V případě preventivních opatření cílících na potenciální oběť, se bude u fyzických osob jednat o šíření edukačních aktivit a nejlepší praxe v zabezpečení počítačů, mobilních telefonů, domácích síťových prvků a v dnešní době i zařízení internetu věcí, mezi které lze zařadit např. chytré hodinky nebo i internetové kamery, které byly v minulosti útočníky mnohokrát masově zneužívány. Edukační aktivity je vhodné rozšířit výukou kybernetické bezpečnosti, jako povinného předmětu na všech stupních vzdělávání, včetně univerzit třetího věku. Mezi dobré příklady preventivních aktivit směrem k fyzickým osobám lze v České republice zařadit projekt Seznam se bezpečně, který šíří již po několik let pomocí krátkých videí na platformě Stream.cz a osvětových seminářů na školách upozornění před úskalími kybernetického světa[1]. Na zvýšení povědomí o hrozbách v kyberprostoru u studentů cílí Středoškolská soutěž v kybernetické bezpečnosti, organizovaná Českou pobočkou AFCEA, které se v případě loňského druhého ročníku účastnilo více než 3.000 osob z 86 středních škol. [2] Jako vhodné se jeví rozšíření dané soutěže i na studenty základních a vysokých škol.

Preventivní a osvětové aktivity vykonává Česká pobočka AFCEA prostřednictvím kyber-bezpečnostních seminářů pořádaných na Policejní akademii ČR v Praze a činností jí zřízené pracovní skupiny Kybernetická bezpečnost rovněž i pro státní správu a soukromý sektor.[3] Opomenout nelze český slovník pojmů kybernetické bezpečnosti, vydávaný Policejní akademií ČR v Praze a Českou pobočkou AFCEA, pod záštitou Národního úřadu pro kybernetickou a informační bezpečnost. Šíření osvěty a nejlepší praxe je nezbytné nejen pro předcházení páchání trestné činnosti, ale i pro následné vyšetřování, jelikož mnohdy se policejní orgány při vyšetřování setkávají s neexistencí důkazních materiálů pro atribuci pachatele. Je tedy na místě rovněž šířit povědomí o nastavení dostatečného logování aktivit v informačních systémech, včetně procesů pro zajištění důkazních materiálů a hlášení případných kybernetických incidentů policejním orgánům. V případě logování je nutná evidence nejen neúspěšných pokusů o přihlášení do informačních systémů, ale i těch úspěšných, a to s dobou archivace delší než 1 rok. Při zajištění digitálních dat a výpočetní techniky ze strany interních zaměstnanců organizace, musí být dodrženy postupy umožňující uplatnitelnost důkazů i při soudním řízení. Klíčová je dokumentace celého procesu zajištění důkazních materiálů, nejlépe doplněná obrazovým záznamem. Při zajišťování dat z výpočetní techniky je nutné zejména vytvoření bitové kopie pevného disku s využitím blokátoru zápisu a kopie paměti RAM. Jako v případě bezpečnosti práce, se jeví vhodné zavést legislativní požadavky na bezpečnost v kyberprostoru, kdy by zaměstnanci v rámci svých pracovně-právních vztahů, užívající informační a komunikační technologie, museli podstupovat pravidelná

[1] Seznam se bezpečně. Stream.cz [online]. Praha: Seznam.cz, 2019 [cit. 2019-04-01]. Dostupné z: https://www.stream.cz/porady/seznam-se-bezpecne

[2] Středoškolská soutěž v kybernetické bezpečnosti. Kybernetická soutěž [online]. Praha: AFCEA, 2019 [cit. 2019-04-01]. Dostupné z: https://www.kybersoutez.cz/

[3] Česká pobočka AFCEA [online]. Praha: AFCEA, 2019 [cit. 2019-04-01]. Dostupné z: https://afcea.cz/

školení a přezkoušení. Nelze opomenout ani vhodnost podpory konceptu Public Private Partnership, mezi policejními orgány a technologickými společnostmi.

U odhalování, prověřování a následného vyšetřování neoprávněných přístupů do počítačových systémů ze strany policejních orgánů jsou rovněž úskalí, která je vhodné překlenout. Policejní orgány se mohou setkat na straně oběti s nedostupností nebo neúplností důkazních materiálů, např. v podobě nedostatečných logů síťového provozu, ale i nedostatečnou spoluprací, způsobenou obavou o ztrátu reputace. Na straně pachatele se lze setkat s užitím anonymizačních internetových služeb, šifrování, virtuálních měn, ale i zneužití veřejně dostupných služeb a sítí, jako nástrojů pro páchání trestné činnosti. Komplikaci může rovněž představovat délka uchování provozních a lokalizačních údajů na straně poskytovatele internetového připojení. V České republice je v současné době, dle zákona č. 127/2005 Sb., o elektronických komunikacích (dále jen „zákon o elektronických komunikacích“) tato doba, tzv. data retention, stanovena na 6 měsíců.[1] Mezinárodní policejní a justiční spolupráce rovněž hraje důležitou roli v odhalování pachatelů kybernetické kriminality, jelikož je mnohdy pro řádné objasnění věci nutné zajištění důkazních materiálů u zahraničních subjektů. S některými státy nemá České republika uzavřeny příslušné mezinárodní smlouvy, tudíž je získání důkazů z těchto zemí mnohdy nemožné. Pokud je příslušná mezinárodní smlouva upravující předávání důkazů pro účely trestního řízení uzavřena, mnohdy se jedná o časově náročný proces trvající několik měsíců. Řešením by mohla být změna příslušných smluvních vztahů, upravujících mezinárodní policejní a justiční spolupráci, pro významnější reflexi dynamiky a přeshraničního rozsahu kybernetické kriminality. Doporučit lze stanovení lhůt na odpověď v délce 30 dnů u mezinárodního dožádání, od data doručení žádosti a elektronizaci celého procesu. Stanovení lhůt pro poskytování informací dle trestního řádu by bylo žádoucí i u českých subjektů poskytujících veřejně dostupnou službu elektronických komunikací nebo zajišťujících veřejnou komunikační síť v České republice. Pro tyto české subjekty, působící na českém trhu, by mohla být dostačující lhůta na poskytnutí informací v délce 10 dnů od doručení žádosti, kdy se lze inspirovat např. lhůtou pro přenesení telefonního čísla, stanovenou v zákoně o elektronických komunikacích.

Vhodně nastavená personální politika u policejních orgánů má rovněž dopady na boj s kyberkriminalitou. Úskalím může být finanční ohodnocení expertů pro vyšetřování kybernetické kriminality, kteří dají přednost mnohdy lépe placeným pozicím v komerčním sektoru, ale i nevhodné personální rozložení vyšetřovatelů v rámci jednotlivých útvarů. Pro udržení stávajících policejních expertů a motivaci nových uchazečů o tuto profesi, nejen v oblasti vyšetřování kybernetické kriminality, lze doporučit zavedení příplatku za odbornost pro vybraná služební místa, ve výši až 100 % základního tarifu, jako složky služebního příjmu nezávislé na výši osobního příplatku. Klíčové je také zdokonalování technických schopností a získávání dalších znalostí u policistů na všech úrovních organizační struktury, přicházejících do kontaktu s kybernetickou kriminalitou. Kybernetické technologie mají odlišnou dynamiku vývoje od klasických nástrojů pro páchání obecné trestné činnosti. V případě policistů služebně zařazených u základních útvarů a služby kriminální policie a vyšetřování, lze doporučit implementaci každoročních vzdělávacích seminářů, zaměřených na ochranu

[1] Zákon o elektronických komunikacích. In: Sbírka zákonů. Praha: Tiskárna Ministerstva vnitra, p. o., 2005, ročník 2005, částka 43, číslo 127.

a základní zajištění digitálních stop nevyžadujících specializované metody. Na těchto seminářích by měly být rovněž školeny postupy základního šetření na internetu s využitím logických operátorů při vyhledávání informací ve vztahu k trestné činnosti. Pro policisty zařazené na specializovaných pracovištích vyšetřování kybernetické kriminality, by měly být sestaveny rovněž každoroční vzdělávací semináře, avšak s hlubší úrovní výstupních znalostí. Tato specializovaná školení by měla obsahovat metody zajišťování nestandardní výpočetní techniky a dat, práci s analytickými nástroji pro digitální forenzní analýzu, ale i trasování kryptoměn. Opomenout nelze potřebu moderního technického vybavení pro zajišťování výpočetní techniky a dat, a vhodných nástrojů pro digitální forenzní analýzu. Aplikace výše uvedených opatření může umožnit zefektivnění celého procesu šetření, prověřování a vyšetřování, nejen neoprávněných přístupů do počítačových systémů, ale obecně celé kybernetické trestné činnosti.

Závěr

Počet skutků spáchaných v souvislosti s neoprávněnými přístupy do počítačových systémů, kvalifikovaných Policií ČR jako trestných dle ust. §§ 230, 231, 232 tr. zákoníku, se v období 2010-2018 zvýšil o 878 %, což potvrdilo autorem stanovenou hypotézu v úvodní části článku. Ve srovnání s celkovou registrovanou kriminalitou se však jednalo za hodnocené období o poměrně nízké zastoupení podílem 0,18 % na registrované kriminalitě a 0,11 % na objasněné kriminalitě. Průměrná výše škody na skutek u kategorie TSK 865 dosahovala 217 % průměrné výše škody na skutek u celkové registrované kriminality. Ačkoliv se v případě počtu registrovaných skutků, klasifikovaných v rámci kategorie neoprávněných přístupů do počítačových systémů, jedná o zanedbatelný podíl celkové kriminality, za sledované období docházelo k jeho průměrnému ročnímu nárůstu o 31,20 %. Význam nárůstu je o to vyšší s přihlédnutím ke klesající tendenci počtu registrovaných skutků celkové kriminality, kdy došlo k jejímu snížení na konci sledovaného období ve srovnání s počátečním obdobím o 37 %.

Vyhodnocení registrované kriminality, související s neoprávněnými přístupy do počítačových systémů, bylo provedeno rovněž na úrovni vyšších územně samosprávných celků, u kterých byly hodnoceny průměrné indexy registrovaných skutků, míra objasněnosti a koeficienty růstu. Nejvíce bylo sledovaných skutků registrováno na území hlavního města Prahy, kdy se ročně jednalo v průměru o 1,58 skutků na 10.000 obyvatel. Nejméně bylo registrováno skutků v Karlovarském kraji, kde se jednalo za sledované období o podíl 11 % registrovaných skutků na 10 000 obyvatel území hlavního města Prahy. V objasněnosti byly rovněž zaznamenány značné rozdíly, kdy nejvíce se dařilo objasňovat hodnocenou trestnou činnost v Jihočeském kraji a to v průměru ve 40 % případů, nejméně poté na území Středočeského kraje, ve kterém byl zjištěn pachatel pouze v 16 % případů. Dynamika nárůstu hodnocené trestné činnosti dosahovala na jednotlivých územích hodnot v intervalu 1,21 – 1,51, tedy ve všech krajích docházelo ke konstantnímu nárůstu hodnocené trestné činnosti.

Pro predikci vývoje kriminality, související s neoprávněnými přístupy do počítačových systémů, byl na časovou řadu 2010-2018 autorem zvolen a aplikován model lineárního trendu. Po odhadnutí parametrů trendové funkce, metodou nejmenších čtverců, byl predikován vývoj indexu registrovaných skutků pro rok 2019

ve výši 0,9696, rok 2020 ve výši 1,0708 a rok 2021 ve výši 1,1721. Lze tedy očekávat signifikantní nárůst zkoumané trestné činnosti i v následujících letech. Vzhledem k dynamice jejího vývoje, nízké míře objasněnosti a možným dopadům na zdraví a životy obyvatel, v případě neoprávněného přístupu do informačních systémů prvků kritické informační infrastruktury, je vhodné učinit všechna dostupná opatření, pro lepší prevenci, snížení počtu spáchaných skutků, i efektivnější vyšetřování již dokonaných skutků. V otázkách prevence je vhodné se zaměřit zejména na edukaci koncových uživatelů počítačových systémů, jak v otázkách zabezpečení užívaných technologií, tak jejich bezpečného užívání. Edukační aktivity je vhodné cílit na studenty všech stupňů školní soustavy. Pro efektivnější vyšetřování hodnocené trestné činnosti, lze provést na straně policejních orgánů aktivity směřující k zefektivnění personální politiky, zvýšení finančního ohodnocení, ale i modernizaci technického vybavení a absolvování pravidelných školení pro vybrané policisty. Na legislativní úrovni, by mohlo zefektivnit vyšetřování stanovení lhůt na odpověď u vyžádání informací policejními orgány jak pro české subjekty, tak pro zahraniční subjekty v rámci mezinárodní policejní a justiční spolupráce. Rovněž lze doporučit zavedení elektronizace celého procesu vyžádání informací, v rámci mezinárodní policejní a justiční spolupráce.

Literatura

ADLER, Freda, Gerhard O. W. MUELLER a William S. LAUFER. *Criminology*. Eight Edition. New York, NY: McGraw-Hill, [2013]. ISBN 978-0078026423.

Česká pobočka AFCEA [online]. Praha: AFCEA, 2019 [cit. 2019-04-01]. Dostupné z: https://afcea.cz/

GAU, Jacinta M. *Statistics for criminology and criminal justice*. Third edition. Los Angeles: SAGE, [2019]. ISBN 978-1506391786.

GŘIVNA, Tomáš; SCHEINOST, Miroslav; ZOUBKOVÁ, Ivana a kol. *Kriminologie*. 4. vyd. Praha: Wolters Kluwer, a. s., 2014. ISBN 978-80-7478-614-3

HAGAN, Frank E. *Introduction to criminology: theories, methods, and criminal behavior*. Ninth edition. Los Angeles: SAGE, [2017]. ISBN 978-1483389172.

JIRÁSEK, Petr; Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

Kyberkriminalita. Policie České republiky [online]. Praha [cit. 2019-03-02]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx.

Seznam se bezpečně. Stream.cz [online]. Praha: Seznam.cz, 2019 [cit. 2019-04-01]. Dostupné z: https://www.stream.cz/porady/seznam-se-bezpecne

Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě. In: Sbírka zákonu. Praha: Tiskárna Ministerstva vnitra, p. o., 2013, ročník 2013, částka 56, číslo 104.

Statistické přehledy kriminality. Policie České republiky [online]. Praha, 2018 [cit. 2019-01-19]. Dostupné z: https://www.policie.cz/clanek/statisticke-prehledy-kriminality-za-rok-2018.aspx

Středoškolská soutěž v kybernetické bezpečnosti. Kybernetická soutěž [online]. Praha: AFCEA, 2019 [cit. 2019-04-01]. Dostupné z: https://www.kybersoutez.cz/

VÁLKOVÁ, Helena a Josef KUCHTA. *Základy kriminologie a trestní politiky*. 2. vyd. Praha: C. H. Beck, 2012. Beckovy mezioborové učebnice. ISBN 978-80-7400-429-2.

Zákon o elektronických komunikacích. In: *Sbírka zákonů*. Praha: Tiskárna Ministerstva vnitra, p. o., 2005, ročník 2005, částka 43, číslo 127.

Zákon trestní zákoník. In: *Sbírka zákonů*. Praha: Tiskárna Ministerstva vnitra, p. o., 2009, ročník 2009, částka 11, číslo 40.

ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer ČR, 2017. ISBN 978-80-7552-759-2.

R E S U M É

Příspěvek pojednává o statistické analýze vývoje registrované trestné činnosti související s neoprávněnými přístupy do počítačových systémů v období 2010-2018 v České republice. Ve stanoveném období byl zaznamenán signifikantní nárůst registrovaných skutků, souvisejících s hodnocenou trestnou činností o více než 800 %. Cílem příspěvku je rovněž stanovení návrhů opatření pro prevenci a efektivnější vyšetřování kyberkriminality.

Klíčová slova: kyberkriminalita, neoprávněné přístupy, kyberútoky, vyšetřování.

S U M M A R Y

BERNÁTEK, Josef: ANALYSIS OF THE DEVELOPMENT OF CRIME RELATED TO UNAUTHORIZED ACCESS TO COMPUTER SYSTEMS IN THE CZECH REPUBLIC IN 2010-2018

The paper deals with the crime development statistical data analysis in the period 2010-2018 related to unauthorized accesses to computer systems in the Czech Republic. Significant increases in the recorded offenses associated with the assessed type of crime went up by more than 800 % in the given period. The paper also aims to set down proposals for prevention measures and more effective investigation of cybercrime.

Keywords: cybercrime, unauthorized access, cyberattacks, investigation.