Mgr. et Mgr. Eliška Jonášová
Právnická fakulta Univerzity Karlovy

Aktuální kybernetické hrozby a odpovídající právní úprava v Evropské unii a v Kanadě

Úvod

Příspěvek uvádí základní a obecný přehled vybraných kybernetických hrozeb, které jsou společné pro prostor Evropské unie a pro Kanadu, která je stejně jako členské státy EU signatářem Úmluvy o počítačové kriminalitě[1] a již disponuje pokročilou právní úpravou postihu kybernetických zločinů. Vybrané aktuální hrozby jsou doplněny o příslušné klíčové právní předpisy, které kybernetické zločiny postihují. Z důvodu specifické trestněprávní problematiky v Evropské unii je v příspěvku uvedena také odpovídající právní úprava České republiky, a to jako příklad transpozice unijních norem v kybernetické oblasti. Pro lepší přehled aktuálních kyberhrozeb jsou uváděny statistické údaje poskytnuté Policií České republiky a dále data dostupná na oficiálních stránkách odpovědných institucí a orgánů.

Přeshraniční kybernetický prostor vyžaduje účinné sdílení informací, spolupráci odpovědných složek a společný postoj k odhalování, vyšetřování a postihu kyber-zločinů napříč kontinenty. Proto tento příspěvek předkládá základní právní úpravu a zpracovaná dostupná data ve zkoumaných oblastech světa.

Právní úprava Evropské unie a Kanady

Právně politickým východiskem Evropské unie pro kybernetický prostor je Strategie kybernetické bezpečnosti z roku 2013,[2] ve které se Evropská komise zavazuje podporovat Evropské centrum pro boj proti kyberkriminalitě a ve které je zdůrazněna potřeba spolupráce mezi Agenturou Evropské unie pro bezpečnost sítí a informací (dále jen „agentura ENISA“) a Europolem z důvodu rychlého vývoje druhů kybernetických útoků a s ohledem na vyšší potřebu zajištění kybernetické bezpečnosti, zdokonalení digitálních forenzních nástrojů a technologie.

Prameny práva v dané oblasti lze nalézt především v sekundárním právu, konkrétně v podobě směrnic. Jedná se především o směrnici Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV (dále jen „směrnice o útocích

[1] Úmluva o počítačové kriminalitě. In: *Sbírka mezinárodních smluv*. Praha: Tiskárna Ministerstva vnitra, p. o., 2013, ročník 2013, částka 56.

[2] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* In: Brussels: European Commission, 2013, JOIN(2013) 1 final. Dostupné také z: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52013JC0001.

na informační systémy“) a směrnici o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací,[1] která bude nahrazena nařízením e-privacy.[2]

V českém právu je výchozím zákonem trestní zákoník,[3] podle kterého je za trestné považováno jednání spočívající mj. v neoprávněném přístupu k počítačovému systému a nosiči informací, v opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat či poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti.[4] Dále lze ovšem k postihu kyberzločinů vztáhnout například také ustanovení o podvodu, neoprávněném nakládání s osobními údaji či porušení tajemství dopravovaných zpráv.

Agentura ENISA každý rok publikuje zprávu, ve které hodnotí aktuální kybernetické hrozby. Ze zprávy pro rok 2017[5] vyplývá, že k těmto nejvýznamnějším hrozbám patří malware, útoky na webové stránky, útoky na webové aplikace, phishing, spamování, ransomware, úniky dat a informací či například krádeže identity. Sdílení informací mezi všemi zúčastněnými osobami, které je pro účinný boj proti těmto hrozbám klíčové, brání nejasné standardy struktury takových informací, motivace k jejich sdílení, související právní problematika, platformy a modely určené k takovému sdílení či kvalita a využitelnost sdílených informací.

V Kanadě je právně politickým východiskem Strategie kybernetické bezpečnosti z roku 2010,[6] která obdobně jako v případě Evropské unie zdůrazňuje potřebu vyšší ochrany fyzických a právnických osob i vlád na území celé Kanady. Z legislativní tvorby je zásadní především zákon z roku 2015 na ochranu Kanaďanů před online trestnými činy, který přidává orgánům činným v trestním řízení řadu oprávnění při jejich vyšetřování. Klíčovým je trestní zákoník vymezující trestnost neoprávněného užití počítače či držení zařízení za účelem neoprávněného užití počítačového systému či ke spáchání škody. Od roku 2014 je také účinná anti-spamová legislativa.[7]

Ze zprávy kanadského Ministerstva veřejné bezpečnosti a krizové připravenosti[8] vyplývá, že tamními nejčastějšími kybernetickými hrozbami jsou sítě botnetů, útoky na webové stránky, hacking, malware, pharming, phishing, ransomware, spamování,

---

[1] SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích) (Úř. věst. L 201, 31. 7. 2002, s. 37).

[2] Nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích.

[3] Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

[4] § 230, 231, 232 zákona č. 40/2009 Sb., trestního zákoníku.

[5] *ENISA Threat Landscape Report 2017: 15 Top Cyber-Threats and Trends* [online]. Heraklion, Greece: European Union Agency For Network and Information Security, 2018 [cit. 2018-04-04]. ISBN 978-92-9204-250-9. Dostupné z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017.

[6] Canada's Cyber Security Strategy. Dostupné např. z: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-en.aspx.

[7] Canada’s Anti-Spam Legislation Requirements for Installing Computer Programs. *Government of Canada* [online]. 2015 [cit. 2018-04-11]. Dostupné z: https://crtc.gc.ca/eng/internet/install.htm.

[8] Common threats to be aware of. *Government of Canada* [online]. 2017 [cit. 2018-04-11]. Dostupné z: https://www.getcybersafe.gc.ca/cnt/rsks/cmmn-thrts-en.aspx.

spoofing, spyware a počítačové viry. Kybernetickou bezpečností se zabývá také například příručka kanadské Obchodní komory z roku 2017,[1] podle které se ve velké míře rozrůstá a bude rozrůstat pojištění kybernetických rizik, neboť hodnoty uniklých údajů jsou často zcela mimořádné a zohledňují nejen odpovědnost zasažených podniků, ale také povahu útoku či výši majetkových ztrát. Nejvíce uplatňovaných nároků na náhradu škody způsobené v kybernetickém prostoru je v Kanadě ve zdravotnickém sektoru, který je následován neziskovou, dopravní a technologickou oblastí.

Vybrané kybernetické hrozby

Na základě výše uvedených kybenetických hrozeb, které jsou pro srovnávané oblasti klíčové, jsou vybrány ty nejvýznamnější, přičemž ke každé z nich je uvedena základní definice a právní rámec jak Evropské unie, s doplněním relevantních ustanovení českého trestního zákoníku, tak odpovídající právní úprava Kanady. Rovněž jsou rozebrána základní dostupná statistická data tak, aby bylo zřejmé, nakolik jsou uvedené hrozby závažné a aktuální v obou zeměpisných oblastech. Jsou-li údaje dostupné, je uveden přehled trestního vyšetřování či vybraných kauz, které s danými hrozbami souvisí. Smyslem uvedeného dělení a statistických přehledů je souhrnně představit aktuální kybernetické hrozby, vymezit jejich právní úpravu a uvedené přístupy porovnat. Společnými hlavními kybernetickými hrozbami vybranými jako nejvíce aktuální pro účely tohoto příspěvku jsou malware, útoky na webové stránky, phishing, spamování a ransomware. Uvedených pět kybernetických hrozeb bude postupně hodnoceno z pohledu, zda právní úprava pokrývá aktuální potřeby ke zvýšení kybernetického bezpečí.

První zkoumanou hrozbou je malware, tedy počítačový program, který je určený pro vniknutí do počítačového systému nebo jeho poškození, případně jeho sledování. Pod toto označení se řadí například počítačové viry, trojské koně, spyware či adware.[2] Evropská směrnice o útocích na informační systémy stanoví, že úmyslná výroba, prodej, opatření si k užití, dovoz, distribuce nebo jiné formy zpřístupnění počítačového programu, který byl vytvořen nebo přizpůsoben prvotně pro účely spáchání některého z trestných činů uvedených ve směrnici, je trestné minimálně tehdy, pokud se nejedná o méně závažný případ. V českém právním řádu se jedná v případě útoku prostřednictvím malware o ust. § 230 trestního zákoníku,[3] které stanovuje za trestné, neoprávněný přístup k počítačovému systému a nosiči informací. Samotné opatření

[1] Cyber Security in Canada: Practical Solutions to a Growing Problem. *The Canadian Chamber of Commerce* [online]. 2017 [cit. 2018-04-11]. Dostupné z: http://www.chamber.ca/media/blog/170403-cyber-security-in-canada-practical-solutions-to-a-growing-problem/.

[2] ŠTĚDROŇ, Bohumír. *Open Source software ve veřejné správě a soukromém sektoru*. Praha: Grada, 2009. Průvodce (Grada). ISBN 9788024730479.

[3] Podle § 230 trestního zákoníku se o neoprávněný přístup k počítačovému systému a nosiči informací jedná, pokud je neoprávněně překonáno bezpečnostní opatření, a tím neoprávněně získán přístup k počítačovému systému nebo jeho části. Dále je podle uvedeného paragrafu postihováno neoprávněné užití dat uložených na v počítačovém systému nebo na nosiči informací, neoprávněné vymazání nebo různé formy poškození takových dat, padělání nebo pozměnění dat či neoprávněné vložení dat do počítačového systému nebo na nosič informací.

a přechovávání malware je trestné podle ust. § 231 trestního zákoníku, pokud je tak činěno s úmyslem spáchat trestný čin podle ust. § 182 odst. 1 písm. b), c)[1] nebo trestný čin podle ust. § 230 odst. 1, 2 trestního zákoníku.

Z dat poskytnutých Policií České republiky vyplývá, že za rok 2015 bylo spácháno celkem 578 skutků, které byly přiřazeny k ust. § 230, 231 a 232 trestního zákoníku. Z toho jich bylo spácháno 554 internetem, 24 prostřednictvím jiné počítačové sítě. Z hlediska místní působnosti se jednalo nejvíce o oblast Hl. m. Prahy, kde bylo registrováno 108 skutků. Za rok 2016 bylo ke stejným ustanovením trestního zákoníku zaznamenáno celkem 513 registrovaných skutků, z toho 475 spáchaných internetem a 38 prostřednictvím ostatní počítačové sítě. Podíl na území Hl. m. Prahy byl opět nejvyšší, v daném roce se jednalo o 129 trestných činů. V roce 2017 bylo registrováno celkem 608 skutků podle uvedených paragrafů trestního zákoníku. Na území hl. m. Prahy se jednalo o 130 trestných činů, opět nejvíce v poměru s ostatními kraji.[2] Na území Evropské unie se konkrétně s malware během roku 2017 nejvíce setkávaly státy Bulharsko, Rumunsko, Maďarsko a Irsko.[3]

Kanadské právo upravuje zákaz útoku prostřednictvím malware v zákoně,[4] který je součástí tamní anti-spamové legislativy, účinné od 1. července 2014. Významná ustanovení týkající se malware, účinná konkrétně od 15. ledna 2015, stanovují, že je zakázáno instalovat počítačový program do zařízení jiné osoby (ať se již jedná o počítač, chytrý telefon, herní konzoli či jiné připojené zařízení) v průběhu obchodní aktivity bez výslovného souhlasu majitele zařízení nebo oprávněného uživatele (např. rodinný příslušník či zaměstnanec).[5]

V počtu vyskytovaných malware se Kanada pohybuje pod světovým průměrem, neboť zatímco poměr počtu malware hlášených v rámci kybernetických zločinů je 15 - 20 %, v případě Kanady se jedná o 13-18 %. Z výskytu malware v Kanadě byla infikována v průměru tři zařízení z jednoho tisíce, zatímco ve světovém měřítku je to

[1] § 182 trestního zákoníku upravuje porušení tajemství dopravovaných zpráv, přičemž úmyslné porušení tajemství se může týkat uzavřeného listu nebo jiné písemnosti, datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací, neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci. Trestné je rovněž prozrazení tajemství, které se daná osoba dozvěděla z písemnosti, telegramu, telefonního hovoru nebo přenosu prostřednictvím sítě elektronických komunikací, které nebylo určené jí.

[2] Statistiky Policie České republiky, poskytnuté na vyžádání autorky.

[3] Ranking of the ten European Union countries with the highest malware encounter rates as of January 2017. *The Statistics Portal* [online]. Hamburg, Germany, 2018 [cit. 2018-06-25]. Dostupné z: https://www.statista.com/statistics/463460/ten-european-countries-highest-encounter-rates-spain/.

[4] An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act (S.C. 2010, c. 23).

[5] Canada's Anti-Spam Legislation Requirements for Installing Computer Programs. *Government of Canada* [online]. 2015 [cit. 2018-04-11]. Dostupné z: https://crtc.gc.ca/eng/internet/install.htm.

ze stejného počtu sedm zařízení.[1] Ze statistik týkajících se výskytu malware na území Kanady vyplývá, že v roce 2015 bylo zaregistrováno 2723 případů, přičemž například banka Toronto Dominion Bank byla malwarem atakována v uvedeném roce 359krát. Stejně jako v případě českého práva není ani v Kanadě nezákonné malware vytvořit, ovšem je trestné jej šířit do dalších zařízení. Významnou byla aplikace anti-spamové legislativy v Kanadě v roce 2015, kdy byl v Torontu zrušen server kontrolující server Win32/Dorkbot, a to za pomoci Interpolu, americké FBI a společnosti Microsoft.[2]

Útoky na webové stránky již řadu let zůstávají další významnou kybernetickou hrozbou, a to z evropského i kanadského pohledu. Jako příklady útoků lze uvést exploity pro webové prohlížeče, exploity webových služeb, drive-by útoky či útoky typu water-hole,[3] ale také tzv. DDoS útok,[4] který je variantou obyčejného útoku DoS, kde se pro generování vykonstruované zátěže používá velké množství zdrojů.[5] V evropském právu je zásadní opět směrnice o útocích proti informačním systémům, která stanoví za jednu z přitěžujících okolností případ, kdy došlo k útoku s dopadem na velký počet informačních systémů za použití nástroje, který je pro tento účel vytvořený či přizpůsobený. V České republice je postih možný podle § 182 odst. 1 písm. c) trestního zákoníku, podle kterého je chráněn neveřejný přenos počítačových dat do počítačového systému, z něj nebo v jeho rámci, a dále rovněž dle § 230 trestního zákoníku, který vymezuje neoprávněný přístup k počítačovému systému a nosiči dat. Ze statistik Policie ČR vyplývá, že za rok 2015 bylo podle ustanovení § 182 trestního zákoníku oznámeno 10 skutků, v roce 2016 dokonce pouze 5 a v loňském roce se jednalo o 8 oznámených skutků.

Trestní postih v kanadském právu vychází z ustanovení neoprávněného použití počítače. Příkladem DDoS útoku je jednání pachatele v roce 2012, kdy byla znepřístupněna po dobu dvou dnů webová stránka www.gouv.qc.ca a pachatel, vládní administrátor sítě, byl odsouzen k domácímu vězení.[6]

Jako phishing se označuje metoda, pomocí které útočníci získávají citlivé informace. Uživatelů se dotazují na hesla, čísla platebních karet a jiné osobní údaje a současně se vydávají za legitimní subjekt, například banku či firemní oddělení IT.[7]

---

[1] RAINS, Tim. The Threat Landscape in Canada – 2015 Update. *Microsoft* [online]. 2015 [cit. 2018-04-11]. Dostupné z: https://cloudblogs.microsoft.com/microsoftsecure/2015/11/30/the-threat-landscape-in-canada-2015-update/.

[2] 1st ever anti-spam warrant takes down Toronto botnet server. *CBC* [online]. Toronto, 2015 [cit. 2018-04-11]. Dostupné z: http://www.cbc.ca/news/technology/botnet-anti-spam-1.3350517.

[3] *ENISA Threat Landscape Report 2017: 15 Top Cyber-Threats and Trends* [online]. Heraklion, Greece: European Union Agency For Network and Information Security, 2018 [cit. 2018-04-04]. ISBN 978-92-9204-250-9. Dostupné z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017.

[4] *Distributed Denial of Service*

[5] HONTAÑÓN, Ramón J. *Linux: praktická bezpečnost*. Praha: Grada, 2003. ISBN 9788024706528.

[6] Cybercrime: an overview of incidents and issues in Canada. *Royal Canadian Mounted Police*[online]. 2014 [cit. 2018-04-11]. Dostupné z: http://www.rcmp-grc.gc.ca/en/cybercrime-an-overview-incidents-and-issues-canada#sec4.1.

[7] BROOKSHEAR, J. Glenn., David T. SMITH a Dennis. BRYLOW. *Computer science: an overview*. 11th ed. Boston: Addison-Wesley, c2012. ISBN 9780132569033.

V dnešní době je phishing mnohem sofistikovanější a lze se proti němu bránit pouze obtížně, protože využívá sociální inženýrství a je především povinností uživatelů zkoumat, komu svá citlivá data předávají. Dříve bylo běžné rozesílání chybného linku či stahování nežádoucí přílohy, dnes jsou ovšem využívány individualizované e-maily, ve kterých jsou uváděny detaily opravdových společností, jejich loga a podpisy.

Evropské právo výslovně pamatuje na problematiku phishingu například v ust. čl. 13 směrnice o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací. Tato směrnice ovšem bude nahrazena nařízením e-privacy. Za účelem efektivnějšího boje s phishingem by organizace měly vzdělávat své zaměstnance, jakým způsobem lze rozpoznat falešné a podvodné e-maily, a měly by provést různé simulace phishing útoků, aby zjistily, zda je vlastní infrastruktura dostatečně odolná a zda jsou zaměstnanci na takový útok schopni reagovat. Neméně důležité je zavedení funkčního filtrování spamů, nestahování příloh, u kterých není zřejmý důvěryhodný zdroj a nerozklikávání náhodných linků, které se objevují například na sociálních sítích.

V českém právu lze phishing postihnout jako podvod podle § 209 trestního zákoníku a dále jej lze postihnout jako neoprávněné nakládání s osobními údaji podle § 180 trestního zákoníku,[1] to ovšem pouze za specifických podmínek, jakou je například souvislost s výkonem veřejné moci nebo porušení státem uložené či uznané povinnosti mlčenlivosti. Jedná se o značně frekventovanou trestnou činnost a Policii České republiky více ohlašovaný skutek. V roce 2015 totiž bylo oznámeno 1851 skutků podle § 209 trestního zákoníku, ať již spácháno internetem či prostřednictvím jiných sítí, v roce 2016 se jednalo o 1841 skutků a v roce 2017 rovných 1900 skutků. V kraji hl. m. Praha se jednalo opět o nejvyšší čísla, konkrétně to bylo v uvedených letech 498, 492 a 428 oznámených skutků.

Kanadské právo phishing postihuje ust. § 380 trestního zákoníku, kde je upravena trestnost podvodu.[2] Pokud občané a obyvatelé Kanady poskytli útočníkovi své osobní údaje, mají to ohlásit nejen své finanční a další dotčené instituci, ale také místní policii a vždy Kanadskému centru proti podvodům.

Za spamování se obvykle označují automaticky zasílané zprávy mnoha adresátům, kteří si tyto zprávy neobjednali a nemají možnost odběr těchto zpráv zrušit. Zprávy obvykle přicházejí ze zahraničí, bývají v anglickém jazyce a nabízejí nejrůznější zboží.[3] Spamy dlouhodobě přetrvávají jako významná kybernetická hrozba, neboť v sobě obsahují řadu škodlivých příloh či URL a postupně zlepšují techniky tak, aby se vyhnuly spamovým filtrům.

I na problematiku spamování dopadá především směrnice o soukromí a elektronických komunikacích z roku 2002 a chystané nové nařízení přináší další právní úpravu v oblasti spamu a poskytuje větší ochranu osobním údajům. Český právní řád trestnost spamu nezakotvuje, ovšem může být spáchán trestný čin podle

[1] § 180 trestního zákoníku stanovuje za trestné i nedbalostní neoprávněné zveřejnění, sdělení, zpřístupnění, jiné zpracování či přisvojení si osobních údajů, které byly o jiném shromážděné v souvislosti s výkonem veřejné moci, a které tím způsobí vážnou újmu na právech nebo oprávněných zájmech dotčené osoby.

[2] *Canadian Anti-Fraud Centre.*

[3] ADÁMEK, Martin. *Spam: jak nepřivolávat, nepřijímat a nerozesílat nevyžádanou poštu*. Praha: Grada, 2009. Průvodce (Grada). ISBN 9788024726380.

§ 180 trestního zákoníku, který upravuje neoprávněné nakládání s osobními údaji, byť je tato aplikace omezena pouze na souvislost s výkonem veřejné moci nebo porušení státem uznané či uložené povinnosti mlčenlivosti, dále by pak trestnost byla posuzována dle obsahu samotného spamu. Počet oznámených skutků je téměř zanedbatelný, neboť v roce 2015 byl oznámen 1 skutek podle ust. § 180 trestního zákoníku, o rok později 2 a v loňském roce 5. Může ovšem být spáchán přestupek, a to podle zákona č. 480/2004 Sb., o některých službách informační společnosti. Skutková podstata přestupku je tak mj. naplněna, pokud je opakovaně či hromadně šířeno elektronickými prostředky obchodní sdělení bez souhlasu adresáta, jedná se o zřetelně a jasně neoznačené obchodní sdělení nebo sdělení neobsahující možnost jasně, zřetelně, jednoduchým způsobem, zdarma nebo na svůj účet udělit či odmítnout souhlas s využitím elektronického kontaktu při zaslání každé jednotlivé zprávy.

Kanadské právo spam upravuje v již výše zmíněné anti-spamové legislativě, která obecně zakazuje posílání obchodních elektronických zpráv bez souhlasu adresáta, což se vztahuje jak na e-maily, tak na sociální sítě a textové zprávy. Kanadská právní úprava patří v tomto směru k jedné z nejpřísnějších na světě, neboť pokud organizace nesplňují stanovené podmínky, podléhají trestnímu obvinění nebo civilní žalobě. Ředitelé či odpovědní funkcionáři mohou nést osobní odpovědnost a podnikům mohou být uloženy sankce až do deseti milionů dolarů.

Poslední kybernetická hrozba, uvedená v tomto příspěvku, je ransomware, tedy druh malware, který ovšem vykazuje určitá specifika a protože je velmi častou kybernetickou hrozbou, je řazen samostatně. Ransomware je škodlivý kód, který znepřístupní počítač nebo šifruje data uživatelů. Je evidován postupný nárůst počtu útoků ransomware a přibývají jeho nové podoby. Průměrná částka, kterou útočníci vyžadují jako formu výpalného, se pohybuje kolem tisíce dolarů, celková škoda na globální úrovni se v roce 2017 odhadovala na pět miliard dolarů.[1] Právní přístup k ransomware je v podstatě shodný jako k malware, a to ve všech právních oblastech. V evropském právu byla zaznamenána největší aktivita ransomware v případě kybernetického útoku WannaCry, kdy si členské státy velice úzce vyměňovaly informace týkající se bezpečnostních incidentů podle ustanovení směrnice o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.[2] Tento ransomware se šířil e-mailem se ZIP přílohou, která v případě otevření předala počítači virus. V kanadském právním prostředí se při postihu ransomware opět uplatní nová anti-spamová legislativa.[3] V českém právním řádu nelze uplatnit ust. § 175 trestního zákoníku definujícího vydírání, neboť uvedený paragraf stanoví podmínku násilí, pohrůžky násilí nebo jiné těžké újmy. Lze sice uvažovat o aplikaci pojmu jiná těžká újma, kdy je ovšem nutné přihlížet k závažnosti

[1] *ENISA Threat Landscape Report 2017: 15 Top Cyber-Threats and Trends* [online]. Heraklion, Greece: European Union Agency For Network and Information Security, 2018 [cit. 2018-04-04]. ISBN 978-92-9204-250-9. Dostupné z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017.

[2] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

[3] Canada's Anti-Spam Legislation Requirements for Installing Computer Programs. *Government of Canada* [online]. 2015 [cit. 2018-04-11]. Dostupné z: https://crtc.gc.ca/eng/internet/install.htm.

narušení osobních, rodinných, pracovních nebo podnikatelských poměrů oběti a jak jej útok ovlivnil na jeho psychickém stavu. Judikatura do současnosti definovala jinou těžkou újmu primárně v reálném světě, nikoli v tom kybernetickém, zůstává proto otázkou, do jaké míry budou soudy ochotny rozšířit pojem jiné těžké újmy i ve vztahu k ztrátě dat, zejména s ohledem na skutečnost, že bude muset být dále hodnocena povaha napadených dat. Proto se v dané věci uplatní ust. § 230 trestního zákoníku, vztahující se k neoprávněnému přístupu k počítačovému systému a nosiči informací.

Závěr

Cílem příspěvku bylo pouze v obecném měřítku definovat základní kybernetické hrozby, které jsou nejen v prostoru Evropské unie aktuální, a tyto hrozby blíže specifikovat z pohledu práva a dostupných statistických dat. Za hlavní kybernetické hrozby, relevantní pro Evropskou unii a pro Kanadu, byly pro účely této práce označeny malware, útoky na webové stránky, phishing, spamování a ransomware. Z hlediska právní úpravy je východiskem pro oba celky strategie týkající se kybernetické bezpečnosti, ovšem v obou případech již řadu let v nezměněné podobě. Další právní předpisy, které jsou více aktuální, byly přijaty spíše v Kanadě, neboť zde je v účinnosti široká legislativa zaměřující se jak na anti-spamovou ochranu, tak na ochranu Kanaďanů před kybernetickými trestnými činy. Institucionálně je v dané oblasti odpovědným orgánem Rádio-televizní a telekomunikační komise v Kanadě, v Evropské unii se jedná o agenturu ENISA a EUROPOL, v českém prostředí pak o Národní úřad pro kybernetickou a informační bezpečnost. Ve všech případech tyto orgány spolupracují s orgány činnými v trestním řízení.

V případě malware je postih v evropském právu upraven ve směrnici o útocích na informační systémy, která stanovuje za trestné výrobu či jiné nakládání s počítačovým programem s úmyslem spáchat některý z uvedených trestných činů. Český právní řád malware postihuje podle ust. § 231 trestního zákoníku, je-li jednání spojeno s úmyslem spáchat některý z uvedených trestných činů. Nejpřísnější je v tomto směru kanadská legislativa, podle které je zakázáno instalovat počítačový program do zařízení jiné osoby bez jejího výslovného souhlasu. Ze statistických údajů vyplývá, že Kanada se pohybuje pod světovým průměrem výskytu malware a obdobně Česká republika je ve výskytu malware v evropském měřítku pod průměrem registrovaných malware, přičemž počet skutků registrovaných Policií České republiky se v posledních letech pohybuje mezi pěti sty až šesti sty za rok.

Útoky na webové stránky jsou v evropském právu také obsaženy ve směrnici o útocích proti informačním systémům, české právo stanovuje za trestné úmyslné porušení tajemství veřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci. Kanadský právní řád spojuje tento skutek s neoprávněným použitím počítače. Z hlediska statistických dat je, na rozdíl od malware, Kanada často cílem útoků, obdobně jako více členských států Evropské unie.

Phishing je v obou právních oblastech hodnocen jako podvod, přičemž tento počítačový trestný čin má vzestupnou tendenci a na globální úrovni je považován za závažnou kybernetickou hrozbu. Je proto nezbytné neustále informovat uživatele technologických zařízení o rizicích spojených s phishingem. Kanada navíc vyžaduje ohlašování takových útoků, a to bez ohledu na jejich úspěšnost.

Úprava spamu bude v evropském právu regulována nařízením e-privacy, které nahradí stávající směrnici o soukromí a elektronických komunikacích. Toto nařízení je reakcí na platnou a účinnou kanadskou anti-spamovou legislativu, obecně považovanou za přísnou formu regulace, která je úspěšná. V českém trestním právu je odpovídající ustanovení upravující postih neoprávněného nakládání s osobními údaji, ovšem z hlediska ohlašování uvedeného trestného činu je tato evidence zatím bez většího významu.

Poslední analyzovanou kybernetickou hrozbou je specifický malware nazývaný ransomware, který právní úpravou v daných oblastech koresponduje s úpravou malware. V českém trestním právu nelze hovořit o aplikaci ustanovení upravujícím vydírání, protože zde absentuje násilí či pohrůžka násilí.

Z uvedeného vyplynula řada shodných znaků z hlediska právních ustanovení, ať se již jedná o ochranu před spamováním, regulaci phishingu z hlediska práva jako podvod, či v případě malware podmínka úmyslného jednání spáchat některý z uvedených trestných činů. Naopak odchylky spatřuji v četnosti některých kybernetických hrozeb v Evropské unii a v Kanadě, mj. v případě phishingu či ransomware. Dále jsou odchylky v konkrétních ustanoveních, například v oblasti anti-spamové právní úpravy v problematice poskytování souhlasu, vyžadování ohlašování útoků formou phishing bez ohledu na úspěšnost těchto útoků či v přísnosti některých ustanovení, například v případě postihu malware. Ačkoli je právní úprava v obou zeměpisných oblastech podrobována dalšímu hodnocení a je postupně novelizována, uvedené rozdíly mohou naznačit směr, kterým se má právo dále vyvíjet.

Různorodost kybernetických hrozeb a s tím spojené rostoucí nebezpečí vyžaduje vynaložení větších prostředků i úsilí nejen ze strany státních institucí, ale i soukromoprávních subjektů včetně nás, jednotlivců. Primárním cílem musí být odkrývání této trestné činnosti a její trestání, při zlepšování právních nástrojů tak, aby se dařilo také brzdit náskok kybernetických pachatelů.

Literatura

1st ever anti-spam warrant takes down Toronto botnet server. *CBC* [online]. Toronto, 2015. Dostupné z: http://www.cbc.ca/news/technology/botnet-anti-spam-1.3350517

ADÁMEK, Martin. *Spam: jak nepřivolávat, nepřijímat a nerozesílat nevyžádanou poštu*. Praha: Grada, 2009. Průvodce (Grada). ISBN 9788024726380.

An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act (S.C. 2010, c. 23)

BROOKSHEAR, J. Glenn., David T. SMITH a Dennis. BRYLOW. *Computer science: an overview*. 11th ed. Boston: Addison-Wesley, c2012. ISBN 9780132569033.

Canada's Anti-Spam Legislation Requirements for Installing Computer Programs. *Government of Canada* [online]. 2015. Dostupné z: https://crtc.gc.ca/eng/internet/install.htm

Canada's Cyber Security Strategy. Dostupné např. z: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-en.aspx

Common threats to be aware of. *Government of Canada* [online]. 2017. Dostupné z: https://www.getcybersafe.gc.ca/cnt/rsks/cmmn-thrts-en.aspx

Cybercrime: an overview of incidents and issues in Canada. *Royal Canadian Mounted Police*[online]. 2014. Dostupné z: http://www.rcmp-grc.gc.ca/en/cybercrime-an-overview-incidents-and-issues-canada#sec4.1

Cyber Security in Canada: Practical Solutions to a Growing Problem. *The Canadian Chamber of Commerce* [online]. 2017. Dostupné z: http://www.chamber.ca/media/blog/170403-cyber-security-in-canada-practical-solutions-to-a-growing-problem/

ENISA Threat Landscape Report 2017: 15 Top Cyber-Threats and Trends [online]. Heraklion, Greece: European Union Agency For Network and Information Security, 2018. ISBN 978-92-9204-250-9. Dostupné z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

HONTAŇÓN, Ramón J. *Linux: praktická bezpečnost*. Praha: Grada, 2003. ISBN 9788024706528.

RAINS, Tim. The Threat Landscape in Canada – 2015 Update. *Microsoft* [online]. 2015. Dostupné z: https://cloudblogs.microsoft.com/microsoftsecure/2015/11/30/the-threat-landscape-in-canada-2015-update/

Ranking of the ten European Union countries with the highest malware encounter rates as of January 2017. *The Statistics Portal* [online]. Hamburg, Germany, 2018. Dostupné z: https://www.statista.com/statistics/463460/ten-european-countries-highest-encounter-rates-spain/

ŠTĚDROŇ, Bohumír. *Open Source software ve veřejné správě a soukromém sektoru*. Praha: Grada, 2009. Průvodce (Grada). ISBN 9788024730479.

Použité právní předpisy

Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* In: Brussels: European Commission, 2013, JOIN(2013) 1 final. Dostupné také z: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52013JC0001

Nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích.

Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích) (Úř. věst. L 201, 31. 7. 2002, s. 37).

Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

Úmluva o počítačové kriminalitě. In: *Sbírka mezinárodních smluv*. Praha: Tiskárna Ministerstva vnitra, p. o., 2013, ročník 2013, částka 56.

Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

R E S U M É

Článek se zaměřuje na aktuální kybernetické hrozby v Evropské unii a v Kanadě s uvedením relevantních právních předpisů. V kontextu specifik trestního práva v EU je rovněž uvedena právní úprava v České republice, která je doplněna o zjištěné statistické údaje. Srovnání kanadského a evropského právního přístupu v závěru naznačuje možné další kroky v postihu kybernetických zločinů.

Klíčová slova: kybernetické hrozby; Evropská unie; Kanada; trestní právo.

S U M M A R Y

JONÁŠOVÁ, Eliška: CURRENT CYBERTHREATS AND CORRESPONDING LEGAL FRAMEWORK IN EUROPEAN UNION AND CANADA

The article deals with current cyberthreats in the European Union and Canada and it is complemented with the legal framework. In the context of criminal law specifics in the EU the legal framework in the Czech Republic is also mentioned presenting ascertained statistical data. The comparison of the Canadian and European legal approach in the conclusion indicates possible future steps for cybercrime punishment.

Keywords: cyberthreats, European Union, Canada, criminal law.